Anexos I

ANEXO. 1

REGISTRO DE ACTIVIDADES DE TRATAMIENTO DEL INSS

Tratamientos RGPD

Instituto Nacional de la Seguridad Social

Delegada de Protección de Datos

2020 / 11 / 20

Versión: 1.6

Tabla de contenido

- ATENCIÓN E INFORMACIÓN MULTICANAL. RELACIONES EXTERNAS. MEJORA DE LOS SERVICIOS. 4
- AUXILIO POR DEFUNCIÓN 5
- AYUDA CUIDADO DE MENORES A CARGO (CÁNCER Y OT.ENF) 6
- CONTROL DE LA INCAPACIDAD TEMPORAL Y OTRAS PRESTACIONES DE CORTA DURACIÓN 7
- CONTROL DE PENSIONES 8
- EJERCICIO CORRESPONSABLE DEL CUIDADO DEL LACTANTE 9
- ELIMINACIÓN DE SERIES DOCUMENTALES 10
- FAVOR DE FAMILIARES INTERNACIONAL 11
- FAVOR DE FAMILIARES NACIONAL 12
- FORMACIÓN 13
- GESTIÓN DE CONSULTAS, RECURSOS, INDEMNIZACIONES A TANTO ALZADO Y OTROS SUPUESTOS DE RESPONSABILIDAD. 14
- GESTIÓN DE LOS RECURSOS HUMANOS 15
- GESTIÓN DEL DERECHO A LA ASISTENCIA SANITARIA NACIONAL 16
- GESTIÓN DEL DERECHO ASISTENCIA SANITARIA INTERNACIONAL 17
- GESTIÓN Y PROCESOS DE UNIDADES MÉDICAS 18
- INCAPACIDAD PERMANENTE INTERNACIONAL 19
- INCAPACIDAD PERMANENTE NACIONAL 20
- INCAPACIDAD TEMPORAL 21
- INGRESO MÍNIMO VITAL 22
- JUBILACIÓN INTERNACIONAL 23
- JUBILACIÓN NACIONAL 24
- NACIMIENTO Y CUIDADO DE MENOR 25
- ORFANDAD INTERNACIONAL 26
- ORFANDAD NACIONAL 27
- PARTICIPACIÓN DE LOS INTERESADOS EN LA GESTIÓN 28

- PENSIONES EXTRAORDINARIAS DERIVADAS DE ACTOS DE TERRORISMO 29
- PLATAFORMA "TU SEGURIDAD SOCIAL" 30
- PRESTACIONES FAMILIARES 31
- PROCESOS AUTOMATIZADOS DE GESTIÓN DOCUMENTAL 32
- PROCESOS DE GESTIÓN ECONÓMICA-PRESUPUESTARIA Y ESTUDIOS ECONÓMICOS 33
- PROCESOS DE LUCHA CONTRA EL FRAUDE 34
- PROCESOS DE REGISTRO Y ARCHIVO 35
- PROCESOS INTERNOS DE INSPECCIÓN 36
- PROCESOS NO AUTOMATIZADOS DE GESTIÓN DOCUMENTAL 37
- PROCESOS RELATIVOS AL FONDO ESPECIAL 38
- RIESGO DURANTE EL EMBARAZO/LACTANCIA NATURAL 39
- SALUD LABORAL Y PREVENCIÓN DE RIESGOS LABORALES 40
- SEGURO ESCOLAR 41
- SÍNDROME TÓXICO 42
- TARJETA SOCIAL DIGITAL (TSD) 43
- VIDEOVIGILANCIA Y SEGURIDAD 44
- VIUDEDAD INTERNACIONAL 45
- VIUDEDAD NACIONAL 46

- ATENCIÓN E INFORMACIÓN MULTICANAL. RELACIONES EXTERNAS. MEJORA DE LOS SERVICIOS.

FINES	ATENCIÓN E INFORMACIÓN MULTICANAL Y MEJORA DE LOS SERVICIOS. GESTIÓN DEL SERVICIO DE CITA PREVIA. GESTIÓN DE LA INFORMACIÓN PRESENCIAL, TELEFÓNICA, TELEMÁTICA Y POR OTROS MEDIOS (INCLUIDA LA GRABACIÓN DE LAS LLAMADAS DEL CENTRO TELEFÓNICO Y TELEMÁTICO DE LA SEGURIDAD SOCIAL Y EL TRATAMIENTO DE LOS DATOS DE LOS USUARIOS DEL SERVICIO). COMUNICACION INSTITUCIONAL. RELACIONES EXTERNAS. ENCUESTAS Y OTRAS ACTIVIDADES DE MEJORA DE LOS SERVICIOS (QUEJAS Y SUGERENCIAS, BUZÓN DE OPINIÓN...).
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento 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.
CATEGORÍA INTERESADOS	Ciudadanos, trabajadores y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, rúbrica, voz.
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	Secretaria General
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- AUXILIO POR DEFUNCIÓN

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) del auxilio por defunción.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos bancarios, datos personales de familiares, rúbrica.
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- AYUDA CUIDADO DE MENORES A CARGO (CÁNCER Y OT.ENF)

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la ayuda por cuidado de menores a cargo afectados por cáncer u otra enfermedad grave. Control del
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos fiscales, datos bancarios, datos profesionales, porcentaje de discapacidad del titular, datos
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT) y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- CONTROL DE LA INCAPACIDAD TEMPORAL Y OTRAS PRESTACIONES DE CORTA DURACIÓN

FINES	Control del mantenimiento del derecho a la prestación de la incapacidad temporal y otras prestaciones de corta duración. Gestión de las actividades relacionadas con los derechos económicos de los perceptores de la prestación de la incapacidad temporal y otras prestaciones de corta duración Gestión de infracciones y sanciones relacionadas con la incapacidad temporal y otras prestaciones de corta duración.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos fiscales, datos bancarios, porcentaje de discapacidad del titular, datos de salud, datos
CATEGORIAS DESTINATARIOS	Mutuas colaboradoras con la Seguridad Social, Inspección de Trabajo y Seguridad Social.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- CONTROL DE PENSIONES

FINES	Verificación del mantenimiento del derecho al percibo de las prestaciones del Sistema de la Seguridad Social. Gestión de las actividades relacionadas con los derechos económicos de los perceptores de las prestaciones. Coordinación de entidades y organismos que gestionan prestaciones públicas y colaboración administrativa. Control de concurrencias entre pensiones ajenas y de Seguridad Social.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos. trabajadores, pensionistas y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, rúbrica.
CATEGORIAS DESTINATARIOS	Organismos extranjeros competentes en el supuesto de prestaciones reconocidas al amparo de normativa internacional, Agencia Estatal de la Administración Tributaria (AEAT), Ministerio de Justicia, entidades financieras pagadoras, organismos autonómicos responsables de la gestión de las pensiones no contributivas. Ministerio de Trabajo, Migraciones y Seguridad Social. Empresas y organismos que gestionan pensiones públicas incluidas en el banco de datos de pensiones públicas. Otras AAPP.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- EJERCICIO CORRESPONSABLE DEL CUIDADO DEL LACTANTE

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la prestación por ejercicio corresponsable del cuidado del lactante.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos fiscales, datos bancarios, porcentaje de discapacidad del titular, datos personales de familiares,
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT) y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- ELIMINACIÓN DE SERIES DOCUMENTALES

FINES	Gestión de las actividades de eliminación de series documentales en papel.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Cualquier dato personal que haya sido objeto de tratamiento en la Entidad que se encuentre en soporte papel.
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Recursos Humanos y Materiales
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- FAVOR DE FAMILIARES INTERNACIONAL

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la pensión y subsidio de favor de familiares, por legislación internacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, convivencia, rúbrica.
CATEGORIAS DESTINATARIOS	Organismos extranjeros competentes para el trámite de la solicitud.
TRANSFERENCIAS INTERNACIONALES	Organismos extranjeros competentes para el trámite de la solicitud.
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- FAVOR DE FAMILIARES NACIONAL

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la pensión y subsidio de favor de familiares, por legislación nacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, datos de convivencia,
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- FORMACIÓN

FINES	Gestión integral de la formación.
BASE JURÍDICA	RGPD.- Artículo 6. 1. b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Empleados y sus representantes legales.
DATOS PERSONALES	Datos de identificación del empleado (nombre, apellidos, número de documento de identidad, número de registro de personal) domicilio, teléfono, correo electrónico, datos bancarios, rúbrica.
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Recursos Humanos y Materiales
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- GESTIÓN DE CONSULTAS, RECURSOS, INDEMNIZACIONES A TANTO ALZADO Y OTROS SUPUESTOS DE RESPONSABILIDAD

FINES	Gestión de consultas, expedientes de responsabilidad patrimonial, recursos de alzada de empresarios individuales y empresas, y solicitudes de sustitución de la pensión de incapacidad permanente total por una indemnización a
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, pensionistas y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos de salud, rúbrica.
CATEGORIAS DESTINATARIOS	Inspección de Trabajo y Seguridad Social. Otras Administraciones Públicas.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Ordenación y Asistencia Jurídica
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- GESTIÓN DE LOS RECURSOS HUMANOS

FINES	Gestión integral de los recursos humanos de la Entidad, de las ayudas de acción social y del Fondo Especial. Gestión de expedientes disciplinarios, denuncias y recursos de empleados. Gestión de los seguros para los empleados.
BASE JURÍDICA	RGPD.- Artículo 6. 1. b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Empleados y sus representantes legales.
DATOS PERSONALES	Datos de identificación del empleado (nombre, apellidos, número de documento de identidad, número de afiliación SS o mutualidad, número de registro de personal) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, datos de salud (del empleado y/o sus familiares), fotografía, rúbrica.
CATEGORIAS DESTINATARIOS	Agencia Tributaria (AEAT), entidades financieras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Recursos Humanos y Materiales
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- GESTIÓN DEL DERECHO A LA ASISTENCIA SANITARIA NACIONAL

FINES	Atención e información, trámite, resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) y mantenimiento del derecho a la asistencia sanitaria nacional así como la gestión de la aportación a la prestación farmacéutica. Facturación.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, número de la tarjeta sanitaria, fecha de nacimiento) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos, datos personales de familiares, rúbrica, datos de salud, datos de
CATEGORIAS DESTINATARIOS	Servicios públicos de salud.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- GESTIÓN DEL DERECHO ASISTENCIA SANITARIA INTERNACIONAL

FINES	Atención e información, trámite, resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) y mantenimiento del derecho a la asistencia sanitaria internacional. Reembolso de gastos de asistencia sanitaria en el extranjero. Facturación.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, número de la tarjeta sanitaria, fecha de nacimiento) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos bancarios, datos personales de familiares, rúbrica, datos de salud.
CATEGORIAS DESTINATARIOS	Organismos internacionales competentes.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- GESTIÓN Y PROCESOS DE UNIDADES MÉDICAS

FINES	Gestión y procesos de unidades médicas / ICAM en la Comunidad Autónoma de Cataluña.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos bancarios, rúbrica, datos de salud, grado de incapacidad, datos profesionales.
CATEGORIAS DESTINATARIOS	Mutuas colaboradoras con la Seguridad Social, Agencia Estatal de la Administración Tributaria (AEAT), Servicios Públicos de Salud.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Coordinación de Unidades Medicas
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- INCAPACIDAD PERMANENTE INTERNACIONAL

FINES	Trámite y resolución de las prestaciones de incapacidad permanente por legislación internacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, rúbrica, datos de salud, grado de incapacidad, datos profesionales.
CATEGORIAS DESTINATARIOS	Mutuas colaboradoras con la Seguridad Social, Agencia Estatal de la Administración Tributaria (AEAT), organismos extranjeros competentes para el trámite de la solicitud.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- INCAPACIDAD PERMANENTE NACIONAL

FINES	Trámite y resolución de las prestaciones de incapacidad permanente por legislación nacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, rúbrica, datos de salud, grado de incapacidad, datos profesionales.
CATEGORIAS DESTINATARIOS	Mutuas colaboradoras con la Seguridad Social, Agencia Estatal de la Administración Tributaria (AEAT), entidades financieras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- INCAPACIDAD TEMPORAL

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la prestación de incapacidad temporal.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos fiscales, datos bancarios, porcentaje de discapacidad del titular, datos de salud, datos
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT), Mutuas colaboradoras con la Seguridad Social y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- INGRESO MÍNIMO VITAL

FINES	Actuaciones administrativas necesarias para el reconocimiento, mantenimiento, extinción, control y supervisión del derecho a la prestación del Ingreso Mínimo Vital.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos Real Decreto-ley 20/2020, de 29 de mayo, por el que se establece el ingreso mínimo vital, y el 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado y, en su caso, de su representante legal; Datos relativos al estado civil, nacionalidad y vecindad: Domicilio; Datos de contacto; Datos relativos a la unidad de convivencia/unidad familiar; Datos relativos a la situación laboral; Datos económicos, patrimoniales y fiscales; Datos de prestaciones económicas de carácter social; Datos relativos a la salud (incapacidad y discapacidad); Datos relativos a la condición de víctima (violencia de género, trata de seres humanos o explotación sexual).
CATEGORIAS DESTINATARIOS	Organismos Tributarios de la AGE, CC.AA, y EE.LL; Organismos y/o Unidades de la AGE, CC.AA, o EE.LL. con competencias en materia de asistencia social; Entidades financieras; Otras administraciones públicas con habilitación legal para acceder a los datos. pagadoras y organismos internacionales competentes.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- JUBILACIÓN INTERNACIONAL

FINES	Trámite y resolución de la pensión de jubilación, por legislación internacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, rúbrica.
CATEGORIAS DESTINATARIOS	Organismos extranjeros competentes para el trámite de la solicitud.
TRANSFERENCIAS INTERNACIONALES	Organismos extranjeros competentes para el trámite de la solicitud.
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- JUBILACIÓN NACIONAL

FINES	Trámite y resolución de la pensión de jubilación, en sus distintas modalidades, por legislación nacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, rúbrica.
CATEGORIAS DESTINATARIOS	Organismos extranjeros competentes para el trámite de la solicitud.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- NACIMIENTO Y CUIDADO DE MENOR

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias, de la prestación por nacimiento y cuidado de menor y del subsidio no contributivo por nacimiento.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos fiscales, datos bancarios, porcentaje de discapacidad del titular, datos personales de familiares,
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT) y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- ORFANDAD INTERNACIONAL

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la pensión y prestación de orfandad, por legislación internacional
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, concurrencia de violencia de género, datos personales de
CATEGORIAS DESTINATARIOS	Organismos extranjeros competentes para el trámite de la solicitud.
TRANSFERENCIAS INTERNACIONALES	Organismos extranjeros competentes para el trámite de la solicitud.
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- ORFANDAD NACIONAL

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la pensión o prestación de orfandad, por legislación nacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, concurrencia de violencia de género, datos personales de
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PARTICIPACIÓN DE LOS INTERESADOS EN LA GESTIÓN

FINES	Dar participación a los interesados en la gestión y funcionamiento de la Entidad
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, rúbrica, voz, imagen y, puntualmente, datos de salud, laborales, económicos y familiares.
CATEGORIAS DESTINATARIOS	Agentes sociales con representación en los órganos de participación de los interesados en la gestión de la Seguridad Social.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	Secretaria General
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PENSIONES EXTRAORDINARIAS DERIVADAS DE ACTOS DE TERRORISMO

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de las pensiones extraordinarias derivadas de actos de terrorismo.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, actos de terrorismo,
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PLATAFORMA "TU SEGURIDAD SOCIAL"

FINES	Poner a disposición de los ciudadanos un espacio privado donde obtener información personalizada y actualizada de su situación con la Seguridad Social, así como efectuar gestiones en ese ámbito. Ayudar al ciudadano, a través de nuestros servicios de información presencial, en sus gestiones de Seguridad Social a través la plataforma "Tu
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos. trabajadores, pensionistas y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación), domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos de salud.
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PRESTACIONES FAMILIARES

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de las prestaciones familiares en sus distintas modalidades incluida, en su caso, la gestión internacional. Control del mantenimiento del derecho a las prestaciones.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad del titular y/o beneficiarios, datos de familiares, datos profesionales, datos de otras prestaciones reconocidas, rúbrica.
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT), organismos autonómicos competentes para la gestión de las pensiones no contributivas, entidades financieras pagadoras y organismos internacionales competentes.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PROCESOS AUTOMATIZADOS DE GESTIÓN DOCUMENTAL

FINES	Gestión de las bases de datos documentales automatizadas de la Entidad.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, pensionistas y trabajadores y, en su caso, sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, rúbrica. imagen, datos económicos, de salud, laborales, concurrencia de violencia de género, datos relativos a actos derivados de
CATEGORIAS DESTINATARIOS	Ministerio de Justicia, interesados en el procedimiento y otras Administraciones Públicas.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	Secretaria General
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PROCESOS DE GESTIÓN ECONÓMICA-PRESUPUESTARIA Y ESTUDIOS ECONÓMICOS

FINES	Trámite de pagos y contratos administrativos.
BASE JURÍDICA	RGPD.- Artículo 6. 1. b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, empleados y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, rúbrica, datos profesionales.
CATEGORIAS DESTINATARIOS	Tribunal de Cuentas y otros organismos dedicados a la intervención y control. Otras Administraciones Públicas.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión Económico - Presupuestaria y Estudios Económicos
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PROCESOS DE LUCHA CONTRA EL FRAUDE

FINES	Actuaciones en el marco de la lucha contra el fraude en el ámbito de la Secretaría de Estado de la Seguridad Social. Control y prevención del fraude en materia de prestaciones de la Seguridad Social. Gestión del Convenio de colaboración con la Inspección de Trabajo y Seguridad Social (ITSS) y otros organismos con competencias en la
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, pensionistas y trabajadores y, en su caso, sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, datos de salud, datos
CATEGORIAS DESTINATARIOS	Sección de Investigación de la Seguridad Social (Ministerio del Interior), Gerencia de Informática de la Seguridad Social (GISS), Inspección de Trabajo y Seguridad Social, Tesorería General de la Seguridad Social (TGSS) y otras
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	Secretaria General
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PROCESOS DE REGISTRO Y ARCHIVO

FINES	Gestión del registro y los archivos documentales de la Entidad.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, trabajadores, pensionistas y empleados y, en su caso, sus representantes legales.
DATOS PERSONALES	Datos de identificación del empleado (nombre, apellidos, número de documento de identidad, número de afiliación SS o mutualidad, número de registro de personal) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos personales de familiares, datos de salud, imagen, voz, rúbrica.
CATEGORIAS DESTINATARIOS	Otras Administraciones Públicas.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Recursos Humanos y Materiales
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PROCESOS INTERNOS DE INSPECCIÓN

FINES	Gestión de las denuncias a nivel interno y externo dentro del ámbito de competencias del Instituto Nacional de la Seguridad Social (INSS).
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, pensionistas y trabajadores y, en su caso, sus representantes legales.
DATOS PERSONALES	Datos de identificación del denunciante y del denunciado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de sus representantes legales, domicilio, teléfono, correo electrónico, rúbrica, imagen, voz, dirección IP, datos económicos, de salud, laborales y familiares.
CATEGORIAS DESTINATARIOS	Sección de Investigación de la Seguridad Social (Ministerio del Interior), Gerencia de Informática de la Seguridad Social (GISS), Inspección de Trabajo y Seguridad Social, Tesorería General de la Seguridad Social (TGSS) y otras
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	Secretaria General
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PROCESOS NO AUTOMATIZADOS DE GESTIÓN DOCUMENTAL

FINES	Gestión de las bases de datos documentales no automatizadas de la Entidad.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, pensionistas y trabajadores y, en su caso, sus representantes legales.
DATOS PERSONALES	Datos de identificación del denunciante y del denunciado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de sus representantes legales, domicilio, teléfono, correo electrónico, rúbrica, imagen, voz, dirección IP, datos económicos, de salud, laborales y familiares.
CATEGORIAS DESTINATARIOS	Sección de Investigación de la Seguridad Social (Ministerio del Interior), Gerencia de Informática de la Seguridad Social (GISS), Inspección de Trabajo y Seguridad Social, Tesorería General de la Seguridad Social (TGSS) y otras
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	Secretaria General
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- PROCESOS RELATIVOS AL FONDO ESPECIAL

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de las prestaciones de la Mutualidad de funcionarios del Fondo Especial.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos, trabajadores y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos fiscales, datos bancarios, porcentaje de discapacidad del titular, datos personales de familiares,
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT) y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- RIESGO DURANTE EL EMBARAZO/LACTANCIA NATURAL

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de la prestación de riesgo durante el embarazo o la lactancia natural.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos de salud, datos laborales, datos fiscales, datos bancarios, rúbrica.
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT) y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- SALUD LABORAL Y PREVENCIÓN DE RIESGOS LABORALES

FINES	Gestión de las actividades relacionadas con la salud laboral y de los servicios de prevención.
BASE JURÍDICA	RGPD.- Artículo 6. 1. b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. 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.
CATEGORÍA INTERESADOS	Empleados y sus representantes legales.
DATOS PERSONALES	Datos de identificación del empleado (nombre, apellidos, número de documento de identidad, número de afiliación SS o mutualidad, número de registro de personal) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos de salud, rúbrica.
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Recursos Humanos y Materiales
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- SEGURO ESCOLAR

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de las prestaciones de seguro escolar. Control y mantenimiento del derecho.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, datos de matriculación o escolarización, datos de salud (prestación por accidente escolar, prestaciones sanitarias), datos profesionales, datos de identificación de testigos
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT) y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- SÍNDROME TÓXICO

FINES	Atención e información, trámite y resolución (incluida la fase administrativa y, en su caso, la ejecución de sentencias) de las prestaciones del síndrome tóxico.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación, fecha de nacimiento) y, en su caso, de su representante legal o tutor, domicilio, teléfono, correo electrónico, datos fiscales, datos bancarios, porcentaje de discapacidad del titular, datos de salud, datos
CATEGORIAS DESTINATARIOS	Agencia Estatal de la Administración Tributaria (AEAT), Mutuas colaboradoras con la Seguridad Social y entidades financieras pagadoras.
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S. G. de Gestión de Incapacidad Temporal, Prestaciones Económicas del Sistema de la Seguridad Social en Su Modalidad No Contributiva y Otras Prestaciones a Corto Plazo
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- TARJETA SOCIAL DIGITAL (TSD)

FINES	La Tarjeta Social Digital se destinará a la gestión de los datos identificativos de las prestaciones sociales públicas de contenido económico y situaciones subjetivas incluidas en su ámbito de aplicación y de sus beneficiarios, mediante la formación de un banco de datos automatizado; al conocimiento coordinado y la cesión de datos entre las entidades y organismos afectados, con el fin de facilitar el reconocimiento y supervisión de las prestaciones sociales públicas por ellos gestionadas; al acceso y la consulta de las administraciones públicas y otras entidades del sector público integradas en el sistema que gestionen prestaciones sociales públicas de contenido económico así como para la explotación estadística con la finalidad de elaborar estudios y formular análisis encaminados a la
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto-ley 20/2020, de 29 de mayo, por el que se establece el ingreso mínimo vital. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos. trabajadores, pensionistas y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación), domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos de salud.
CATEGORIAS DESTINATARIOS	Administraciones públicas.
TRANSFERENCIAS INTERNACIONALES	NO APLICA
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- VIDEOVIGILANCIA Y SEGURIDAD

FINES	Velar por la seguridad de las personas, instalaciones y edificios en los que desempeñan las actividades que derivan de las competencias de la Entidad
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento 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.
CATEGORÍA INTERESADOS	Ciudadanos, trabajadores, pensionistas, trabajadores y empleados y, en su caso, sus representantes legales.
DATOS PERSONALES	Datos de identificación del empleado (nombre, apellidos, número de documento de identidad, número de registro de personal) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, imagen, voz, rúbrica.
CATEGORIAS DESTINATARIOS	Fuerzas y cuerpos de seguridad del Estado. Empresas encargadas de tratamiento
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Recursos Humanos y Materiales
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- VIUDEDAD INTERNACIONAL

FINES	Trámite y resolución de la pensión y prestación temporal de viudedad, por legislación internacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos de pensión compensatoria, concurrencia de violencia de género, datos personales de familiares, rúbrica.
CATEGORIAS DESTINATARIOS	Organismos extranjeros competentes para el trámite de la solicitud.
TRANSFERENCIAS INTERNACIONALES	Organismos extranjeros competentes para el trámite de la solicitud.
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad.
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

- VIUDEDAD NACIONAL

FINES	Trámite y resolución de las pensiones y prestaciones temporales de viudedad, por legislación nacional.
BASE JURÍDICA	RGPD.- Artículo 6. 1. c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD.- Artículo 6. 1. e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. RGPD.- Artículo 89. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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. Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso
CATEGORÍA INTERESADOS	Ciudadanos y sus representantes legales.
DATOS PERSONALES	Datos de identificación del interesado (nombre, apellidos, número de documento de identidad, número de afiliación) y, en su caso, de su representante legal, domicilio, teléfono, correo electrónico, datos económicos y fiscales, datos bancarios, porcentaje de discapacidad, datos de pensión compensatoria, concurrencia de violencia de género, datos personales de familiares, rúbrica.
CATEGORIAS DESTINATARIOS	
TRANSFERENCIAS INTERNACIONALES	
PLAZOS DE CONSERVACIÓN	Todas las categorías. - Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad
MEDIDAS DE SEGURIDAD	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RESPONSABLE TRATAMIENTO	S.G. de Gestión de Prestaciones
EMAIL RESPONSABLE	consultas.inss-sscc.proteccion-de-datos@seg-social.es
DELEGADO PROTECCIÓN DE DATOS	delegado.protecciondatos@seg-social.es

ANEXO. 2

CUESTIONARIO DE AUDITORÍAS LOPD

CUESTIONARIO GENERAL DE AUDITORÍA LOPD A CUMPLIMENTAR POR EL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS

Dirección Provincial:

Nombre del fichero protegido:

Fecha/BOE de inscripción

Finalidad del fichero protegido:

Documento de Seguridad **(arts. 88 del Reglamento de desarrollo de LOPD)**	
¿Existe un documento de seguridad del fichero?	

Registro de incidencias **(art. 90 del Reglamento de desarrollo de LOPDP)**	
¿Se cuenta con un registro de incidencias?	
¿Se realiza un seguimiento de las incidencias y se tipifican?	

Control de acceso **(art. 91 del Reglamento de desarrollo de LOPDP)**	
¿Quién cursa las autorizaciones para acceder al fichero? ¿Cuál es el procedimiento?	
El personal externo con acceso a los recursos está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio (ej. firma de compromiso confidencialidad…)	

Gestión de soportes informatizados y no informatizados **(art. 92 del Reglamento de desarrollo de LOPD)**	
¿Hay algún tipo de registro/ inventario de la documentación/los soportes?	
¿Hay criterios para el archivo/inventario de la documentación/los soportes? ¿Permiten identificar la información que contienen?	
¿Se traslada esta documentación/soportes (incluso mediante correo electrónico)?	
En caso afirmativo ¿están autorizadas las personas que realizan el traslado? ¿Por quién? ¿Se ha establecido un procedimiento para el traslado de documentación para evitar la pérdida, sustracción o acceso indebido a la información durante el transporte. ?	
¿Se destruye la documentación/soportes?	
En caso afirmativo ¿Cómo se destruye? ¿Con que periodicidad se destruye?	

Tratamiento No Automatizado Art. 105 - 108 del Reglamento de la LOPD	
¿Está previsto que el documento de seguridad se aplique a la documentación en papel	
¿Dónde está ubicada la documentación?	
¿Existen dispositivos de seguridad para el almacenamiento de la documentación?	
En caso afirmativo ¿cuántas personas cuentan con llave de acceso? Indicar nombres o procedimiento para conocer esta información.	

Tratamiento no automatizado (art. 111-114 del Reglamento de desarrollo de LOPD)	
¿Existen fotocopiadoras? ¿Quiénes las usan? ¿Está autorizada la copia de documentos a determinadas personas?	
¿Hay destructoras de papel? ¿Se usan?	
¿Se han establecido mecanismos que permiten identificar los accesos realizados a la documentación?	
Si se traslada la documentación ¿existe un procedimiento con medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado?	

Gestión de soportes (art. 97 del Reglamento de desarrollo de LOPD)	
¿Se envían/reciben datos personales del fichero en soporte informático no controlado por la UPI (CD, pendrive, cinta)?	
En caso afirmativo, ¿Hay registro de entrada/salida de soportes informáticos?	
La personas que realizan la recepción de soportes, ¿están debidamente autorizadas, y se mantiene una lista actualizada de estas personas autorizadas?	
¿Se actualiza el inventario cuando se ha desechado o reutilizado un soporte?	

Control de acceso físico (art. 99 del Reglamento de desarrollo de LOPD)	
¿Existe una lista del personal (o procedimiento para obtener dicha información) con acceso a los locales donde están los sistemas de información con datos de carácter personal?	

Registro de accesos (art. 103 del Reglamento de desarrollo de LOPD)	
¿Se revisa periódicamente la información guardada en el registro de accesos? Si es así, indicar con qué periodicidad se hace esta revisión.	
¿Se hace un informe de cada revisión realizada al registro de accesos? ¿Cada cuanto tiempo se realiza dicho informe?	

EL/LA RESPONSABLE DE PROTECCIÓN DE DATOS PROVINCIAL	EL/LA SUBDIRECTOR/A PROVINCIAL RESPONSABLE DEL FICHERO/TRATAMIENTO DE LOS DATOS
Fdo.	Fdo.

ANEXO. 3

MODELO DE INFORME DE AUDITORÍA

INFORME RESUMEN DE AUDITORÍA PROVINCIAL SIN INCIDENCIA

Dirección Provincial:

Mes / Año:

Nombre del fichero auditado y finalidad	Nivel de Seguridad	Tratamiento (automatizado- mixto- no automatizado)	Incidencias detectadas	Acciones de mejora	Unidades responsables de su implantación	Plazo de implantación
			SIN INCIDENCIAS			

EL/ LA DIRECTOR/A PROVINCIAL

Documento a enviar al buzón de correo 99IU263 (INSS SSCC SG, AUDITORIAS LOPD)

INFORME RESUMEN DE AUDITORÍA PROVINCIAL CON INCIDENCIA

Dirección Provincial:

Mes / Año:

Nombre del fichero auditado y finalidad	Nivel de Seguridad	Tratamiento (automatizado- mixto-no automatizado)	Incidencias detectadas	Acciones de mejora	Unidades responsables de su implantación	Plazo de implantación

EL/ LA DIRECTOR/A PROVINCIAL

ANEXO. 4

INFORME DE ANÁLISIS DE IMPACTO DEL RGPD

PRINCIPALES ASPECTOS A TENER EN CUENTA EN LA ADAPTACIÓN DE ESTE INSTITUTO AL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

RESUMEN EJECUTIVO

El nuevo Reglamento General de Protección de Datos (RGPD, en adelante) representa un **cambio de orientación y mentalidad** en materia de protección de los datos, no sólo a nivel técnico-jurídico al tratarse de un Reglamento (directamente aplicable y que desplaza la normativa interna en caso de contradicción) sino también respecto del enfoque, pasando de un modelo focalizado en el control del cumplimiento de medidas altamente especificadas a otro muy amplio y de menor grado de especificación, si bien, de **mayor exigencia** para los responsables del tratamiento, que descansa sobre el denominado principio de **«responsabilidad activa»** (o *accountability en inglés)*. Esta evolución podría simbolizarse como el paso a un enfoque «*de mayoría de edad»* en el que se establece una amplia responsabilidad en cuanto al resultado pero no se fijan más que unas pautas generales y directrices guía que no se detallan en exceso. Lo anterior se combina con otra innovación respecto a lo que conocíamos hasta ahora, **el enfoque del riesgo** desde la perspectiva de los **derechos y libertades de las personas**.

Este cambio de filosofía tiene múltiples consecuencias, que son objeto de análisis de este informe, y que **obligan a la adaptación de nuestros procesos**, con especial incidencia en:

- nuestra **relación con los interesados** *(deber de información, consentimiento, derechos, transparencia),*
- el **análisis de los riesgos** *(no respecto de la seguridad de los datos sino de los riesgos para los derechos y libertades de los interesados) para determinar las medidas de seguridad aplicables),* y
- la **contratación administrativa** *(regulación de las relaciones con los adjudicatarios de contratos públicos con acceso a datos personales, clausulado y garantías, deber de diligencia en su elección).*

Además, esta adaptación deberá ser **ágil y realizarse en un breve período de tiempo**, dado que el RGPD será plenamente aplicable el 25 de mayo de 2018, es decir, en aproximadamente **tres meses**. En este sentido, habrán de tenerse en cuenta las **dificultades añadidas** que entraña la amplia descentralización de nuestra gestión.

Las **principales consecuencias** que se derivan de este cambio normativo son:

- Necesidad de **identificar con precisión las finalidades y la base jurídica** de los tratamientos que se llevan a cabo. Ambas habrán de hacerse públicas.
- **Modificación del régimen en que se puede prestar consentimiento** eliminándose la posibilidad de que éste sea tácito o basado en la inacción (afectando incluso a los consentimientos prestados con anterioridad al RGPD).

- Necesidad de **adecuar la información que se ofrece a los interesados** cuando se recogen sus datos (formularios en papel y electrónicos, locuciones telefónicas, aplicaciones y entorno web…). Esto conllevará una **considerable labor de revisión, actualización y rediseño de los soportes actuales**.

- Inclusión de **nuevos derechos adicionales** a los denominados ARCO (que a efectos de este informe denominaremos ARCO+) y novedades en su forma de **ejercicio**.

- **Garantías adicionales en materia de encargos de tratamiento** (tratamientos por cuenta de terceros), su formalización y participación en las labores relativas a la protección de datos. Otros efectos en materia de contratación administrativa (confidencialidad, clausulado[1], protección de datos desde el diseño y por defecto).

- Necesidad de establecer un **Registro de Actividades de Tratamiento** que, de confirmarse la redacción actual del proyecto de Ley Orgánica de Protección de Datos (PLOPD, en adelante), deberá ser **público y accesible** por medios electrónicos. Ello requerirá una **ardua labor** de revisión de los tratamientos llevados a cabo en la Entidad y el establecimiento de criterios homogéneos para su determinación.

- Necesidad de **realizar análisis de riesgo para los derechos y libertades de los ciudadanos** de todos los tratamientos de datos que se desarrollen y, en su caso, la realización de **Evaluaciones de Impacto sobre la Protección de Datos** (EIPD, en adelante) porque supongan un alto riesgo para los derechos y libertades de los interesados, así como disponer de una **metodología** para llevarla a cabo.

- Necesidad de **revisar las medidas de seguridad** que se aplican a los tratamientos a la luz de los resultados del análisis de riesgo de los mismos.

- Designación del **Delegado de protección de datos** (DPD, en adelante) y coordinación de su labor en nuestro contexto específico (subdelegado de protección de datos, Comisión de protección de datos, instrucciones que regulen su funcionamiento, equipos de apoyo, articulación dentro de la Entidad, etc.).

El informe se **estructura y** trata el siguiente **contenido**:

Por una parte, se realiza un **estudio jurídico-práctico** que se centra en el nuevo régimen normativo y lo **compara** con la situación actual, aprovechando la **experiencia acumulada** en las actuaciones de esta Inspección.

Respecto de cada cuestión analizada se recogen las **principales consecuencias** que se derivan de los cambios introducidos y las **adaptaciones** que deberían realizarse. Además, se añade el **análisis del proyecto de Ley Orgánica de Protección de Datos** (PLOPD, en adelante) en los términos en los que está redactado en el momento de elaborar este informe.

[1] En este sentido, dada la inminencia de la aplicación de la nueva legislación en materia de contratación pública que conlleva la revisión de los contratos y pliegos tipo, podría ser conveniente que se **sincronicen** dichos trabajos con la adecuación al nuevo marco normativo de protección de datos o que se **tenga en cuenta** éste a la hora de su elaboración.

Además de lo anterior, se añaden una serie de **anexos** que dan información complementaria al contenido del presente informe y que versan sobre:

- Anexo I. Tabla ejemplo del sistema propuesto de doble capa para cumplir con el **deber de informar**.
- Anexo II. **Nueva ley de contratos**, confidencialidad, encargo de tratamiento y protección de datos *(articulado que hace referencia a dichas materias)*.
- Anexo III. **Modelo** de cláusulas contractuales para el **contrato de encargo de tratamiento** adaptado al nuevo Reglamento.
- Anexo IV. **Lista de verificación de tareas a realizar y cronograma genérico** por etapas para la **adaptación** al nuevo Reglamento.
- Anexo V. Informe propuesta sobre la articulación de la **figura del DPD**.
- Anexo VI. **Bibliografía consultada.**

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 realizadas 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 DDPP 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 establecido en el nuevo RGPD.

Responsable del tratamiento

Se define en el artículo 4 del RGPD y las responsabilidades que le corresponden vienen recogidas en el artículo 24. Además, se introduce el concepto de **corresponsables del tratamiento** en el artículo 25 del Reglamento donde se establecen las normas para el reparto transparente de responsabilidades entre ellos. Este podría ser el caso de tratamientos de ficheros que se utilizan por distintas unidades de gestión. Recordemos que la nota distintiva que supone la consideración de responsable del tratamiento es **tener la potestad de decidir sobre la finalidad y medios del tratamiento**.

Concepto de datos de salud

Dada la **relevancia** que tienen los tratamientos de datos relacionados con la salud en nuestra Entidad, merece la pena detenerse en el concepto que da el RGPD en su Considerando 35 incluyendo lo siguiente:

- Datos relativos al estado de salud del interesado que den información sobre su estado de **salud física o mental pasado, presente o futuro**.
- La información sobre la persona física recogida con ocasión de su inscripción a efectos de **asistencia sanitaria o con ocasión de tal prestación**.
- Todo **número, símbolo o dato asignado** a una persona física que la **identifique de manera unívoca** a efectos sanitarios.
- La información obtenida de **pruebas o exámenes** de una parte del cuerpo o de una sustancia corporal (también datos genéticos y muestras biológicas).
- Cualquier información relativa, por ejemplo, a una enfermedad, discapacidad, riesgo de padecer enfermedades, **historial médico**, tratamiento clínico o el estado fisiológico o biomédico del interesado con independencia de su fuente.

Categorías especiales de datos personales

Quedan **prohibidos** los tratamientos de datos personales que, entre otros, revelen la **afiliación sindical** y los datos relativos a la **salud**. No obstante, no será de aplicación esta prohibición cuando concurra alguna de las circunstancias siguientes –se mencionan las que expresamente pueden afectarnos- (Artículo 9, RGPD):

- **Consentimiento explícito** (salvo que la normativa aplicable impida levantar la prohibición por el interesado).
- Cuando sea **necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento** o del interesado en el ámbito del Derecho laboral y de la seguridad y **protección social** en la medida que así lo autorice el Derecho de la UE, de los EEMM o un convenio colectivo.
- Cuando sea necesario para fines de medicina preventiva o laboral, **evaluación de la capacidad laboral del trabajador** (…) sobre la base del Derecho de la UE o de los EEMM.

En los Considerandos[2] 52 y 53 se **exceptúa la prohibición del tratamiento de datos de salud** si se dan determinadas circunstancias tales como el interés público, en particular, a efectos de **legislación laboral y de protección social**, haciendo mención expresa a las **pensiones**. En el 53 se aborda el tratamiento con **fines de salud** de datos personales que merecen **mayor protección**. En este caso, sólo se permite en determinados contextos entre los que se alude expresamente al de la **protección social** y otros relacionados con la gestión de la **asistencia sanitaria**.

[2] Un **«considerando»** razona el contenido de la parte dispositiva (articulado) del acto. Según se establece en el punto 10 de la ***«Guía práctica común para la redacción de textos legislativos de la UE»***, *"la **finalidad** de los considerandos será **motivar** de modo conciso las disposiciones esenciales de la parte dispositiva sin reproducir ni parafrasear su texto. Los considerandos no deben incluir disposiciones de carácter normativo o desiderata de carácter político"*.

1.0. Consecuencias para la gestión

- El tratamiento de datos de salud está permitido en el ámbito en que nuestra Entidad realiza el mismo. No obstante, hay que tener presente que dichos tratamientos deben encontrar su base en la normativa legal aplicable o en el consentimiento explícito del interesado. A estos efectos, a la hora de **detectar** tratamientos de este tipo de datos **es fundamental** que las unidades **conozcan el alcance del concepto de «datos de salud» en el ámbito de la protección de datos** ya que en las visitas de inspección realizadas se ha constatado que éste se desconoce, lo que conlleva, entre otras consecuencias, el que no se apliquen las garantías oportunas a este tipo de tratamientos. Para ello es necesario que **se emitan instrucciones y se imparta formación** que alcance al máximo de plantilla posible.

2. Bases de legitimación para el tratamiento de datos

Si bien se mantienen las **mismas bases jurídicas** que en la Directiva anterior y que se recogen en nuestra aún vigente LOPD, a saber:

- Consentimiento
- Relación contractual
- Intereses vitales del interesado o de otras personas
- Obligación legal para el responsable **("el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento")**
- Interés público o ejercicio de poderes públicos *(establecido en norma legal)*
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos *(limitado para las autoridades públicas, véase último párrafo de este apartado)*

El **principio de responsabilidad activa** introduce algunos matices respecto de lo que se venía aplicando hasta ahora:

- Deberá documentarse e identificarse claramente la **base legal** sobre la que se desarrollan los tratamientos.
- Además, la base legal **deberá incluirse en la información obligatoria que se pone a disposición de los interesados** a la hora de la recogida de los datos.
- El consentimiento debe ser **"inequívoco"**, por lo que la figura del consentimiento tácito o basado en la inacción desaparece ya que sólo se entenderá por inequívoco aquel que sea prestado mediante una **manifestación del interesado o mediante una clara acción afirmativa**, por ejemplo, continuar con la navegación en una página web una vez se ha informado de las implicaciones que tiene a nivel de protección de datos (siendo el ejemplo típico para ilustrarlo, el uso de cookies en una web y continuar con la navegación).
- Cuando el **consentimiento** se preste en declaración escrita que también se refiera a otros asuntos, el consentimiento se solicitará de tal forma que **se distinga claramente del resto** de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo (Artículo 7.2 RGPD).

- Debe poder **demostrarse** que se ha prestado el consentimiento y que haya **garantías** de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. (Considerando 42)
- Para que el consentimiento se considere **informado** el interesado debe conocer al menos la identidad del responsable del tratamiento y los fines del mismo a los que serán destinados los datos personales recabados. No se considerará libremente prestado cuando el interesado no goce de verdadera libertad o no pueda denegar (o retirar) su consentimiento sin sufrir perjuicio alguno. (Considerando 42)
- El interesado tendrá derecho a **retirar su consentimiento** en cualquier momento. La retirada del consentimiento afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será **informado** de ello. Será **tan fácil retirar el consentimiento como darlo** (Artículo 7.3. RGPD).

Cuando el consentimiento afecte a una **pluralidad de finalidades** será necesario que conste de manera específica e inequívoca que dicho consentimiento se otorga para cada una de ellas (artículo 6 del PLOPD). En este sentido el Considerando 43 establece que **no se considerará que el consentimiento ha sido prestado libremente** cuando no se permita **autorizar por separado** las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto o cuando se haga depender la prestación de un servicio o cumplimiento de un contrato consentimiento, aunque éste no sea necesario para tal prestación. El Considerando 50 añade que el tratamiento de datos personales con **fines distintos para los que fueron recogidos inicialmente** sólo será permitido cuando sea **compatible** con los fines de su recogida inicial.

El Considerando 43 merece especial atención puesto que en él se aclara que el consentimiento **no se entiende otorgado libremente** cuando hay un **desequilibro claro** entre el interesado y el responsable del tratamiento, motivo éste por el que no puede considerarse una base jurídica válida para el tratamiento. Esta aclaración no tendría una relevancia especial si no fuera porque se hace **mención expresa a que ese desequilibrio se presume en el caso de responsables que son autoridad pública** lo que puede tener **importantes consecuencias** en el régimen jurídico de la figura del consentimiento en nuestro caso particular.

En los casos en que el tratamiento de datos se fundamente en una **obligación legal** exigible al responsable, ésta **deberá constar en una norma de derecho de la UE o en una ley**. **La finalidad del tratamiento deberá quedar determinada en dicha base jurídica**. De igual modo si se fundamentase en **una misión realizada en interés público o en el ejercicio de poderes públicos** deberá derivarse de una competencia atribuida por la **ley**, en los términos establecidos en el artículo 8 del PLOPD. En este sentido el RGPD (Considerando 40) no exigía que la base jurídica o medida legislativa derivara de un acto legislativo adoptado por un **Parlamento**, tan sólo establecía que esa base jurídica o medida legislativa fuera **clara y precisa y su aplicación previsible para sus destinatarios** (Considerando 45).

El **interés legítimo**, como establece el Considerando 47 y artículo 6.1.f del RGPD **no deberá utilizarse en el caso de las autoridades públicas** en el ejercicio de sus funciones dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos

personales por parte de las mismas. El tratamiento de datos estrictamente necesario para la **prevención del fraude** constituye un interés legítimo del responsable del tratamiento de que se trate.

Tratamiento de datos relativos a infracciones y sanciones administrativas (Art. 27 PLOPD)

En este caso se establece que el tratamiento de datos de infracciones y sanciones administrativas (incluidos el mantenimiento de registros relacionados con las mismas) **exige**:

- que los responsables de los tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, la declaración de las infracciones o la imposición de las sanciones.
- que el tratamiento se **limite** a los datos **estrictamente** necesarios para la finalidad perseguida.

En caso de **no cumplirse alguna de las condiciones anteriores** será necesario que el tratamiento esté autorizado por una **ley** en la que además se regularán, en su caso, las garantías adicionales para los derechos y libertades de los afectados.

Tratamiento de los registros de personal del sector público (DA 15ª, PLOPD)

A estos efectos habrá de tenerse en cuenta lo establecido en la Disposición adicional decimoquinta del PLOPD que se refiere a los **tratamientos de los registros de personal del sector público** que considera que dichos tratamientos se hacen en virtud del **ejercicio de poderes públicos** conferidos a sus responsables. Además permite expresamente el tratamiento de datos personales referidos a **infracciones y condenas** penales e infracciones y sanciones administrativas para el **estricto cumplimiento de sus fines**. Asimismo permite el tratamiento de datos que hayan sido **limitados** en virtud del derecho a la limitación del tratamiento reconocido en el artículo 18 del RGPD por considerarlo de "interés público importante" cuando ello sea **necesario** para el desarrollo de los procedimientos de personal.

2.0. Consecuencias en nuestra gestión

- Deberá analizarse cada uno de los tratamientos que se realizan tanto a nivel centralizado como descentralizado y **documentar cuál es la base legal que los soporta**. Y constatar que, de confirmarse la redacción actual del PLOPD, en caso de que la legitimación para el tratamiento **parta de una obligación legal exigible al responsable**, ésta derive de la **norma de derecho de la UE o de una ley**. Esta información deberá **incorporarse a las fuentes de recogida de datos** (en formato papel o electrónico e incluso en las locuciones y/o entrevistas telefónicas, en su caso) para que los interesados la conozcan en el momento en que proporcionen los datos. Este aspecto será desarrollado en otro punto de este informe *(véase: el deber de informar).*
- A estos efectos será necesario que se fije un **criterio común** para determinar **qué constituye un tratamiento** a los efectos de esta norma y su nivel de agregación o

desagregación (incluida la geográfica[3]) para una aplicación homogénea en toda la organización. Así como dar **pautas** respecto de cómo identificar la base jurídica que justifique el tratamiento.

- Cuando la base jurídica sea el **consentimiento**, habrá de verificarse que este se obtuvo en una forma compatible con el actual RGPD[4] ya que, en otro caso, deberá estudiarse si puede sustituirse por otra base legal y, si esto no fuera posible, obteniendo el consentimiento de los interesados nuevamente conforme a los requerimientos del Reglamento. Una de las obligaciones que se derivan del principio de responsabilidad activa es estar en disposición de **demostrar su cumplimiento**, por lo que este consentimiento deberá quedar debidamente documentado.
- Sería conveniente, asimismo, **comprobar** que no se están realizando tratamientos obteniendo el **consentimiento por omisión** y, en su caso, **cesar** en su obtención sustituyéndola por una forma compatible con la nueva normativa. De igual forma habrá de revisarse que en caso de consentimiento que afecte a **más de una finalidad**, cumple con las previsiones del PLOPD en cuanto a que debe quedar claro que se presta para cada una de ellas.
- Deberá articularse el modo en que el **consentimiento puede retirarse**, que deberá ser igual de sencillo que prestarlo, las **instrucciones** para ello así como la forma en que esto queda **documentado**.
- **El consentimiento en el caso de datos de especial protección**, como es el caso de la salud (el que se da con mayor frecuencia en nuestro actividad), deberá ser expreso, como ya establecía la norma anterior.
- En el caso del tratamiento de **datos relativos a infracciones y sanciones**, cuando no seamos el órgano competente para la instrucción, declaración o imposición se deberá analizar si existe una norma que autorice a dicho tratamiento o bien cesar en el mismo, en caso de no encontrar base legal para su tratamiento.

---

[3] En este sentido ha de tenerse en cuenta la definición del término **fichero** que según el RGPD es "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica" y el **ámbito de aplicación material** establecido en su artículo 2.1 cuando dice que "El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales **contenidos o destinados a ser incluidos en un fichero**", lo que abre la puerta a un nivel de agregación mayor a la hora de definir los tratamientos siempre que estos tengan un nivel de homogeneidad suficiente.

[4] Esto incluye que:

- el consentimiento esté basado en una clara acción afirmativa o manifestación del interesado;
- en caso de categorías especiales de datos (como son los de salud), es expreso;
- debe quedar claro respecto a qué tratamiento se otorga;
- en caso de pluralidad de finalidades, se otorga para cada una de ellas;
- sea informado y libremente prestado;
- el interesado sea consciente de que lo ha prestado;
- queda documentado y el responsable del tratamiento pueda demostrar que se han cumplido con estas garantías;
- el sistema para darlo y retirarlo es igual de sencillo y se ha informado de tal posibilidad al interesado sin que su retirada le cause perjuicios;
- en caso de utilizarse para fines distintos a los inicialmente previstos, estos sean compatibles con los de su recogida inicial.

- Deberá analizarse el **alcance jurídico** del Considerando 43 a efectos de nuestra consideración como **«autoridad pública[5]»** y los efectos que de ésta se deriven 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

3.0. Consecuencias para nuestra gestión

Lo anterior implica que:

- La **información** deberá facilitarse **por escrito o medios electrónicos**, en su caso.
- **Se evitará la remisión a textos legales**. No se usarán fórmulas complejas optándose 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 continuación.

Por tanto **habrán de revisarse todas las comunicaciones y formatos que faciliten esta información** para que cumplan con dichos requerimientos y estén, en todo caso, **disponibles por escrito o formato electrónico**, en su caso.

4. El deber de informar

En los artículos 13 y 14 del RGPD se aborda **el deber de información en sus dos vertientes**, cuando los datos personales se obtienen directamente del interesado y cuando se obtienen de otras fuentes. Sus **notas características** son:

- La obligación de informar a los interesados **recae sobre el responsable del tratamiento**.
- La información debe ponerse a disposición de los interesados **en el mismo momento** en que se soliciten los datos **y con carácter previo a su recogida o registro** cuando

[5] A efectos de ese análisis conviene tener en cuenta las definiciones del artículo 4 del RGPD en los puntos 7 a 10 y 21 de los que parece deducirse que a efectos de este Reglamento el término **«autoridad pública»** se refiere en **sentido amplio** a cualquier organismo con potestades administrativas. Lo que parece confirmarse en el punto 21 cuando define el término «autoridad de control» como *"la **autoridad pública** independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51".*

éstos se obtengan directamente del interesado (artículo 13 RGPD). En otro caso, cuando se trate de datos procedentes de una **cesión legítima o fuente de acceso público**, deberá informarse en un plazo razonable: antes de un mes o en la primera comunicación con el interesado (artículo 14 RGPD).

- El deber de informar opera sin necesidad de requerimiento previo y el responsable deberá estar en condiciones de **acreditar** que ha cumplido con él.

Cómo se concreta este deber:

- Debe adaptarse al **procedimiento de recogida** correspondiente y mantener siempre un lenguaje claro y sencillo y proporcionarse la información de forma concisa, transparente, inteligible y de fácil acceso.
- Para facilitar que esta mayor exigencia de informar sea compatible con que ésta se haga llegar al interesado de forma concisa, transparente y de fácil acceso la AEPD ha propuesto un sistema de **información por capas**. (Para más información véase el **Anexo *I. Tabla resumen de la información por capas para cumplimiento del deber de informar)***.
- La información deberá quedar **claramente identificada bajo el título «Información básica sobre protección de datos»** y se propone como mejor forma de presentación la **tabla** (de forma análoga a la información nutricional alimentaria).
- La **primera capa** contiene la información básica y resumida mientras que en la **segunda** se incorpora la información adicional y un mayor detalle de la que se contenía en la primera.
- Deberá quedar dentro del **campo de visión del interesado**, por tanto deberá tener una **ubicación privilegiada** en los formularios en papel y en pantalla, cuando se utilicen medios electrónicos o entornos web.
- Cuando por motivos de diseño sea necesario podrá **sustituirse por una llamada** que indique dónde puede consultarse esta información, por ejemplo: “antes de firmar la solicitud, debe leer la información básica sobre protección de datos que se presenta al pie o reverso de esta página”.
- Del mismo modo, en las **locuciones telefónicas** o atención por este medio, deberá comunicarse en el **momento más propicio** y que asegure que la información llega al destinatario. Además se da una vuelta más de tuerca en esta exigencia ya que deberá **garantizarse que el interlocutor ha comprendido la información suministrada**.
- Deberá ponerse a disposición de los interesados la **información adicional** a la proporcionada en la locución por otros medios (p.ej. en un apartado de la página web).
- Además, en caso de que el interesado solicite alguna aclaración se deberá ofertar una **locución complementaria** con la información adicional del apartado por el que se haya interesado.
- La **segunda capa** deberá contener toda la información adicional más la que ya se había incorporado en la primera capa. La forma de poner a disposición esta información es más **flexible** pero siempre deberá mantenerse el fácil acceso y la conservación de esta información por parte del interesado.

- El estilo **deberá evitar citas legales o términos ambiguos**. Lo que se busca es claridad y transparencia así como generar confianza. Por ello **se puede mejorar lo propuesto por el propio Reglamento ampliando la información proporcionada** (buenas prácticas, garantías, medidas adicionales aplicadas y usos y prácticas que expresamente se van a evitar).

El Considerando 62 y artículo 14.5.c. del RGPD establecen varias **excepciones** al deber de informar **en los casos en que los datos no se hayan obtenido directamente del interesado**, si bien, una de ellas merece destacarse pese a no ser novedosa: no será necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información o cuando **el registro o la comunicación de los datos personales estén expresamente establecidos por el Derecho de la UE o de los Estados miembros** o cuando sea imposible o suponga un esfuerzo desproporcionado, entre otros supuestos.

Videovigilancia y el deber de informar (Art. 22 PLOPD)

Su régimen se **mantiene** en líneas generales tal y como estaba regulado hasta ahora teniendo en cuenta que se establece en la propia norma:

- cómo **deberá identificarse la zona vigilada** *(lugar suficientemente visible)*
- el **contenido de este dispositivo informativo** *(existencia del tratamiento, identidad del responsable y posibilidad de ejercitar los derechos ARCO+ -establecidos en los artículos 15 a 22 del RGPD-)*
- además, deberá mantenerse a **disposición** de los afectados esa información *(parece que en el mismo sentido que se regulaba anteriormente respecto a la cláusula informativa)*

4.0. Consecuencias para la gestión

- Deberán **revisarse** todas las **cláusulas informativas** de protección de datos para su clarificación y desarrollo en los términos establecidos en el RGPD.

- También deberá **revisarse la redacción de las fórmulas para la obtención del consentimiento** y su **ubicación** en los formularios en papel o electrónicos para mejorar su visibilidad.

- En el momento de aplicación de la normativa **deberán haberse adaptado todos los soportes a través de los cuales se recojan o registren datos personales** (formularios en papel y electrónicos, aplicaciones, páginas web, locuciones telefónicas, etc.) incluyendo la información necesaria en el formato de doble capa propuesto. Esto supone que sería conveniente iniciarse esta revisión lo antes posible, tal y **como recomienda la AEPD**, ya que el día 25 de mayo de este año debemos estar en condiciones de cumplir con las exigencias del deber de informar.

- Deberá **identificarse** los casos en que esté previsto **recabar datos por cesión legítima** de datos y, en caso de que esta cesión no esté expresamente prevista en una norma, cumplir con las obligaciones respecto al deber de informar.

- Todo lo anterior también deberá **analizarse** desde el punto de vista del **cliente interno**, por ejemplo, solicitudes y tratamientos de datos de la plantilla, cuando sea aplicable.

- En los casos en que exista servicio de **videovigilancia**, deberá **revisarse** que se cumple con las obligaciones establecidas en la norma.

5. Derechos

A los derechos ARCO que ya asistían a los interesados con la normativa anterior se añaden el **derecho al olvido, a la portabilidad y a la limitación de tratamiento** (Artículo 15 a 22 RGPD). En principio, estos dos primeros derechos tienen menor incidencia en nuestro ámbito de gestión pero deberá estudiarse su aplicabilidad y, en su caso, el procedimiento para su hipotético ejercicio, pudiendo tener el tercero mayor impacto.

Por su parte se mantiene el **plazo de un mes** para atender la petición o explicar los motivos de no hacerlo, en su caso (Considerando 59). Este plazo se podrá **ampliar** por otros **dos meses** si fuera necesario debido a la complejidad y al número de solicitudes. El responsable deberá informar dentro del plazo del mes siguiente a la solicitud de la prórroga y los motivos de la dilación.

Además la norma incorpora otras **novedades en el ejercicio de los derechos ARCO**:

- **Verificación de identidad** de los solicitantes de ejercicio de los derechos ARCO (esta cuestión no nos afecta puesto que ya se procedía a dicha verificación con carácter general).

- Se podrá pedir **especificación de la información** a la que se solicita acceso en los casos en los que el responsable trate gran cantidad de información, como ocurre en nuestro caso.

- Se podrá contar con la **colaboración de los encargados de tratamiento** en el ejercicio de estos derechos, cuestión que podría hacerse constar en el propio contrato de encargo de tratamiento (esta cuestión tiene poca incidencia en nuestra gestión –videovigilancia, letrados, traslado y desecho de documentación-).

- En el caso del derecho de acceso se ha reconocido expresamente al **derecho a obtener copia de los datos personales** que son objeto de tratamiento. Este acceso podría ser remoto si se pone a disposición del interesado un sistema seguro que así lo permita.

El **PLOPD** establece como **novedad** en su artículo 3 los derechos de acceso, rectificación o supresión de los **herederos** debidamente acreditados salvo que mediara prohibición legal o expresa del causante. También se establece esta posibilidad para el caso de **albaceas**

testamentarios, representantes legales de menores, Ministerio Fiscal y, en caso de personas discapacitadas, por aquellas **personas designadas para el ejercicio de funciones de apoyo**.

En dicho proyecto también se establece en su artículo 12 que el responsable del tratamiento estará **obligado a informar** al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. No obstante, **no especifica** si esta información es de carácter rogado o si debe entenderse proactivo implicando el que se deba disponer de cartelería o trípticos informativos a disposición de los interesados.

En cuanto al **derecho de acceso** se permite pedir **aclaración** al solicitante de datos cuando no especifique qué datos desea conocer y tratemos un gran volumen de ellos. Se considerará asimismo como **novedad** que es **repetitivo** el ejercicio del derecho de acceso si se ejerce en más de una ocasión durante el plazo de **seis meses** (antes un año). En estos casos podrá:

- **Negarse** a actuar respecto a la solicitud
- Cobrar un **canon** razonable en función de los costes administrativos de atender esta solicitud

La **prueba** del carácter repetitivo recae sobre el responsable del tratamiento.

En el considerando 63 del RGPD establece que el derecho de acceso incluye expresamente al acceso de los interesados a los **datos relativos a la salud**, por ejemplo, los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas.

5.0. Consecuencias para la gestión

Sería conveniente:

- confeccionar un **protocolo centralizado**
- elaboración de **modelos** para el ejercicio de derechos y puesta a disposición de las DDPP
- que el mencionado protocolo aborde, al menos, el **contenido** siguiente:
  - derechos ARCO+
  - pautas a seguir en cada caso
  - instrucciones de cómo actuar en caso de ejercicio de derechos por parte de herederos y otros autorizados a ejercer estos derechos de personas fallecidas
  - actuaciones en caso de ejercicio repetitivo del derecho de acceso
  - forma de acceso de los interesados a los datos relativos a la salud
  - participación de las DDPP y plazos en caso de ejercicio descentralizado de estos derechos
- En cuanto al deber de informar respecto al ejercicio de derechos (verificar el alcance del artículo 12 del PLOPD), la edición de un **tríptico u hoja informativa** que esté disponible en los distintos puntos de contacto con el ciudadano (CAISS -incluido también en CAISSgestiona-, web, locución telefónica, aplicaciones…).

ⓘ **Realidad práctica**: Hasta ahora cada DP había elaborado su propio **protocolo** bien a iniciativa propia o bien derivado de una instrucción de la Inspección dentro del programa de Protección de datos que ésta lleva a cabo. Eso ha supuesto distintos enfoques a la hora de protocolizar las actuaciones necesarias en caso de recibir una petición de ejercicio de derechos y la confección de formularios que no se ciñen a las normas de modelaje y de identidad corporativa de la organización. Los protocolos no suponían un valor añadido ya que, por lo general, se han remitido a citas textuales de la norma, resultando poco clarificadores en la práctica. Tampoco especifican medidas y responsables concretos a los que remitir las peticiones en caso de recibir una solicitud.

6. Relaciones entre responsable y encargado del tratamiento

El RGPD ha avanzado en esta materia incluyendo **obligaciones** expresamente dirigidas a los **encargados de tratamiento**, si bien, **la responsabilidad última sigue correspondiendo al responsable del tratamiento** (Artículos 24 a 31 RGPD).

Otro de los cambios introducidos, de gran relevancia, es que **el responsable del tratamiento debe adoptar medidas dirigidas a garantizar que el tratamiento se adecúa al RGPD y estar en condiciones de demostrarlo**. Esto significa que en virtud del principio de responsabilidad activa esa responsabilidad abarca **la elección del encargado** de tratamiento y obliga a una especial **diligencia** en la misma. Para ello se prevé la posibilidad de adherirse a **códigos de conducta o certificarse** dentro de alguno de los esquemas establecidos para ello.

Habrá de tenerse especial cuidado en la **contratación administrativa** que deberá incluir estos aspectos a la hora de establecer los criterios para la adjudicación y el clausulado que regule la relación entre la Entidad y el adjudicatario.

En cuanto a la **formalización del encargo** de tratamiento se admite no sólo el **contrato**, como hasta ahora, sino que también se incluye un **acto jurídico**, por ejemplo, en nuestro caso, una resolución administrativa debidamente notificada al encargado.

El **contenido mínimo** de los contratos de encargo se especifica de forma detallada en el RGPD (art. 28):

- Objeto
- Duración
- Naturaleza y finalidad del tratamiento
- Tipo de datos personales
- Categorías de interesados
- Obligaciones y derechos del responsable

Las instrucciones del responsable del tratamiento al encargado deberán quedar **documentadas** de forma precisa identificando de forma clara y concreta cuáles son los tratamientos de datos a realizar.

Importante: aquellos contratos de encargo concluidos con anterioridad a la aplicación del RGPD **deben modificarse y adaptarse para respetar este contenido**. No serán válidas remisiones genéricas al artículo del RGPD que los regula. No obstante, la Disposición transitoria quinta del PLOPD ha establecido que:

> "Los contratos de encargado del tratamiento **suscritos con anterioridad al 25 de mayo de 2018** al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal **mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos** y, en caso de haberse pactado de forma **indefinida**, hasta transcurridos **cuatro años** desde la citada fecha.
>
> En caso de que los contratos previesen su **prórroga** al término de su vencimiento, ya fuera por mutuo acuerdo entre las partes o en ausencia de denuncia por cualquiera de ellas, **deberá producirse su adaptación con anterioridad al momento en que estuviera prevista dicha prórroga**."

Esta previsión sólo afectaría en caso de que la LO **haya sido publicada y sea plenamente aplicable** en la fecha que lo será el RGPD, ya que si, como algunas fuentes apuntan, la tramitación no finaliza a tiempo, esta modificación **no podría aplicarse** y eso supondría que los contratos suscritos con anterioridad **deberían de haber sido adaptados** al nuevo marco normativo con anterioridad al 25 de mayo.

> ⓘ **Realidad práctica**: en las visitas de inspección realizadas se ha constatado que en muchos de los casos se han **omitido** las garantías establecidas para la figura del encargado del tratamiento porque no se ha detectado la existencia de la misma. Esta omisión se tipificaba en la normativa anterior como una **infracción grave** así como también lo hace el actual proyecto de LOPD en su artículo 73.k.

Por tanto, **se hace necesario clarificar e impartir instrucciones** en este sentido para que las DDPP conozcan **en qué casos deberán formalizar esta relación**, el modo en que habrán de hacerlo y otras obligaciones que puedan derivarse del **encargo de tratamiento** de que se trate.

La elección del encargado de tratamiento

Existe un **deber de diligencia** en la elección del encargado por parte del responsable. Esto se concreta en términos del considerando 81 del RGPD en que el encargado del tratamiento **debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos**, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento. Es **muy importante** tener en cuenta que **el responsable es quien ostenta la responsabilidad del tratamiento** y de la garantía de los derechos de las personas afectadas aunque el tratamiento lo esté realizando el encargado.

El contrato o acto jurídico que vincula al responsable y el encargado del tratamiento

Además de lo ya mencionado antes se podrán establecer **cláusulas tipo** por parte de la Comisión Europea o autoridad de control competente, no obstante, mientras tanto la AEPD ha propuesto unas cláusulas orientativas para que puedan servir de base en la regulación de las relaciones entre responsable y encargado.

No existe obligación de comunicar a los interesados la existencia de un encargo de tratamiento pero puede ser **aconsejable**, según manifiesta la AEPD, hacer pública esta información en aras de una mayor transparencia.

El deber de confidencialidad

En el contrato o acto jurídico deberá quedar establecida la forma en que el encargado del tratamiento **garantizará** que las personas autorizadas para tratar los datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o si esta obligación es de naturaleza estatutaria. **Muy importante**: el cumplimiento de esta obligación debe quedar **documentado** y a disposición del responsable del tratamiento.

El artículo 5 del PLOPD puntualiza algunos aspectos de este deber como el que la **obligación de confidencialidad** se mantendrá (se entiende, indefinidamente) después de haber finalizado la relación del obligado con el responsable o encargado del tratamiento.

Las medidas de seguridad

En el acuerdo debe figurar la **obligación del encargado de adoptar todas las medidas de seguridad necesarias** (art. 32 RGPD).

El responsable deberá realizar la **evaluación de riesgos** para determinar las medidas de seguridad apropiadas, pero también el encargado debe evaluar los posibles riesgos derivados del propio tratamiento y otras circunstancias que pudieran incidir en la seguridad como sería que ese encargado realice otros tratamientos. En base al resultado de esas evaluaciones se establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo existente. Entre ellas se pueden incluir la seudonimización, cifrado y un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas establecidas para garantizar la seguridad del tratamiento. Se prevé que la adhesión a códigos de conducta o la obtención de certificaciones pueden servir como forma de demostrar que se cumple con los requisitos establecidos.

Las medidas de seguridad pueden establecerse como una **lista exhaustiva o bien puede realizarse una remisión a un estándar o marco reconocido**. Sería el caso del Esquema Nacional de Seguridad o las Políticas de seguridad y uso seguro que operan en nuestra Entidad.

Régimen de subcontratación

Dentro del acuerdo debe establecerse el régimen de subcontratación exigiéndose por parte del RGPD que exista una autorización previa por escrito:

- General: el encargado deberá informar al responsable de la incorporación de un subencargado o su sustitución, dando la oportunidad al responsable de oponerse a dichos cambios. La forma y plazo para esta oposición sería aconsejable que apareciese recogida en el acuerdo.

- Específica: esto es, en favor de un subencargado concreto.

En todo caso el subencargado **queda obligado en los mismos términos** que el encargado y debe **quedar vinculado de la misma forma** (acuerdo por escrito o acto jurídico vinculante). En caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones del subencargado.

Nueva ley de contratos, confidencialidad, encargo de tratamiento y protección de datos

*Véase **Anexo II** donde se recogen los artículos y disposiciones que guardan relación con esta materia en la citada normativa.*

Derechos de los interesados

Debe establecerse la forma en la que el encargado del tratamiento **asistirá** al responsable en el cumplimiento de la obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el RGPD. En el acuerdo debe constar claramente **a quién corresponde** atender y dar respuesta a las solicitudes de ejercicio de estos derechos y en caso de optar porque sea al responsable del tratamiento, determinar la obligación del encargado de comunicar al responsable del tratamiento que se ha ejercido esta petición, la forma y el plazo para hacerlo. En caso de optar porque sea el encargado quien atienda estas solicitudes deberá regularse la forma y plazos para ello.

El **derecho de información**, al no tratarse de un derecho rogado, **no queda incluido** en las previsiones anteriores, no obstante, sería **recomendable** que, en el caso de que el encargo de tratamiento supusiera la recogida de datos, se regule la forma y momento en que ha de cumplirse con este deber dentro del contrato o acto jurídico que regule la relación entre el responsable y el encargado.

Colaboración en el cumplimiento de las obligaciones del responsable

También deberá determinarse la forma en que el encargado **ayudará** al responsable a garantizar el cumplimiento de las obligaciones relativas a:

- la aplicación de medidas de seguridad que correspondan

- la notificación de violaciones de datos a las autoridades e interesados

- realización de evaluaciones de impacto relativa a la protección de datos

- realización de consultas previas, en su caso.

Según la naturaleza del tratamiento encargado procederá o no regular estas cuestiones pudiendo incluso el responsable **delegar** en el encargado el cumplimiento de estas obligaciones.

Destino de los datos al finalizar la prestación

Deberá determinarse en el contrato o acto jurídico cuál será el **destino de los datos al finalizar** la prestación, bien sea la destrucción, bien la devolución de los datos al responsable o a otro encargado designado por el responsable, determinando la forma y plazo para ello.

Los datos deberán ser devueltos cuando se requiera que los datos personales deban ser conservados en virtud del derecho de la UE o de los Estados Miembros. No obstante, podrá conservarse una copia de los datos debidamente **bloqueados** mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Colaboración con el responsable para demostrar el cumplimiento

Es preciso también establecer la obligación de que el encargado ponga a disposición del responsable toda la información necesaria para **demostrar** el cumplimiento de las obligaciones establecidas en esta materia, así como para contribuir a la realización de auditorías.

Modelo de cláusulas contractuales

En el Anexo III se recoge un modelo de contrato de encargo de tratamiento **propuesto por la AEPD y las Agencias vasca y catalana de protección de datos** que puede servir de base para la elaboración de un modelo propio y adaptado a las especificidades de nuestro ámbito de actuación. Asimismo se incluye un **resumen** del contenido que debe tratar un contrato o acto jurídico que regule la relación entre el responsable y el encargado del tratamiento según lo recogido en la guía editada por la AEPD titulado “Directrices para la elaboración de contratos entre responsables y encargados de tratamiento”.

Véase el Anexo III. ***Modelo de cláusulas contractuales para el contrato de encargo de tratamiento adaptado al nuevo Reglamento.***

Protección de datos desde el diseño y por defecto en la contratación pública

Apuntar que el Considerando 78 en su inciso final hace mención expresa a que **los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos**.

Previsiones del proyecto de Ley orgánica de protección de datos en materia de encargo de tratamiento

En el PLOPD se establece en su artículo 33 en relación con la figura del encargado de tratamiento lo siguiente:

- **Será considerado responsable del tratamiento** y no encargado quien **actúe en su propio nombre y sin que conste que lo hace por cuenta de otro** estableciendo relaciones con los afectados aunque se haya formalizado un acto jurídico o contrato en

los términos establecidos en el RGPD. No obstante, se establece una **excepción** para esta situación en aquellos encargos de tratamiento efectuados **en el marco de la legislación de contratación del sector público**.

- Una vez finalizado el encargo, **no procederá la destrucción** de los datos cuando exista una previsión legal que obligue a la conservación de los mismos. En estos casos serán **devueltos** al responsable que será el encargado de garantizar su conservación mientras la obligación persista sin perjuicio de que el encargado pueda conservar, debidamente **bloqueados**, los datos en tanto puedan derivarse responsabilidades de la relación con el responsable del tratamiento.

- En el ámbito del **sector público** podrán atribuirse las **competencias** propias de un **encargado del tratamiento** a un determinado órgano de la AGE, de las CCAA o Admón. local u organismos vinculados o dependiente mediante la adopción de una norma reguladora de dichas competencias, **que deberá incorporar el contenido exigido por el artículo 28.3 del RGPD**.

Lo tratado en este último punto, es una **novedad** en relación con la normativa anterior que no mencionaba esta posibilidad de forma directa, si bien, el **Informe 0333/2012 del Gabinete Jurídico de la AEPD** se pronunciaba en esta sentido sobre la posición de la Gerencia de Informática de la Seguridad Social (GISS) respecto del tratamiento de los ficheros de las distintas entidades gestoras y servicios comunes de la SS. Entendiéndose en este caso que de la regulación contenida en el decreto de estructura así como de las atribuciones de competencias que se hacen en favor de este Servicio Común se desprende que existe un encargo de tratamiento formalizado por escrito y que cumplía con los requerimientos que imponía la normativa aplicable en ese momento en materia de protección de datos.

6.0. Consecuencias para la gestión

Sería aconsejable dictar **pautas** y fijar criterios comunes en cuanto a:

- Establecer instrucciones para la correcta **detección** de casos en los que nos encontramos ante un encargo de tratamiento (para evitar que no se tomen las medidas oportunas por no ser detectada esta circunstancia).

- Fijar las **garantías** mínimas en materia de protección de datos (conocimientos especializados, fiabilidad y recursos) que deben acreditar los adjudicatarios cuando exista un encargo de tratamiento. Deberá estudiarse cómo impacta este deber de diligencia en la contratación administrativa y elaborarse un **clausulado tipo o impartirse instrucciones para su correcta definición**, así como sobre las formas de acreditación válidas.

- Establecer pautas sobre la forma en que se garantizará el **compromiso de confidencialidad** de las personas autorizadas al acceso a datos, cómo habrá de documentarse tal circunstancia y ponerse a disposición de la Entidad, en su caso. Exigibilidad del registro de actividades de tratamiento (si <250 trabajadores).

- Determinar cómo ha de **formalizarse el encargo** (contrato o acto jurídico). Fijando pautas sobre la forma, contenido, delimitación del encargo, medidas de seguridad o remisión a un estándar o marco reconocido, colaboración con el responsable en distintas materias, destino de los datos al finalizar la prestación, nivel de detalle de cada uno de los apartados a tratar o modelo estandarizado, en su caso, si fuera posible.

- Configurar el régimen de **subcontratación**. Forma de autorización (general o específica). Requisitos para su formalización. Obligaciones que de él se derivan.

- **Obligaciones** para responsable y encargado durante la vigencia del contrato: evaluación de riesgos, adopción de medidas de seguridad y valoración de la eficacia de las mismas.

- Determinar la **colaboración** del encargado en el cumplimiento de las obligaciones del responsable (o delegación, en su caso), en función de la naturaleza del tratamiento objeto de encargo, incluido el ejercicio de derechos por parte de los interesados y, si procede, el derecho de información. Asimismo, deberá determinarse la exigencia de colaborar con el responsable para demostrar el cumplimiento de las obligaciones establecidas en la norma.

- **Decisión** sobre si se **comunica** a los interesados la existencia de un encargo de tratamiento.

Deberán **revisarse los contratos actuales** en los que exista un encargo de tratamiento para adaptarlos a las exigencias del nuevo RGPD. Esta revisión también podría servir para detectar posibles encargos de tratamiento que **no hayan sido formalizados debidamente** y regularizar así su situación. En este sentido, deberá decidirse si se revisan los contratos ya existentes con anterioridad al 25 de mayo, en previsión de la que el PLOPD no finalizara su tramitación antes de dicha fecha.

Tendría que **revisarse la norma reguladora de las competencias de GISS** para **comprobar** que se cumple con lo establecido en el Art. 28.3 del RGPD respecto del contenido que debe incorporar a efectos de **encargo de tratamiento** y, en caso de no hacerlo, iniciar los trámites oportunos para su **modificación y adecuación a la nueva norma**. En este sentido, sería interesante conocer la **"Propuesta para la adecuación al RGPD desde el rol de encargado de tratamiento"**, documento elaborado por la GISS y que fue premiado como ***Buena práctica en privacidad y protección de datos personales sobre iniciativas para adaptarse al RGPD*** por parte de la AEPD.

Debería considerarse **cómo se concreta el principio de protección de datos desde el diseño y por defecto en materia de contratación pública,** así como las implicaciones de la excepción contenida en el PLOPD en cuanto a que en el marco del sector público no tenga la consideración de responsable del tratamiento aquel que actúe en su propio nombre y sin que conste que lo hace por cuenta de otro aunque hayan formalizado el contrato de encargo de tratamiento.

7. Medidas de responsabilidad activa

La introducción en el RGPD de la responsabilidad activa implica que **no sólo existe responsabilidad por una infracción tipificada**, sino que la no adopción del conjunto de medidas requeridas para el perfecto cumplimiento normativo, o la falta de diligencia al hacerlo, supone también una responsabilidad punible para las organizaciones. Por tanto, **no se considera suficiente el no incumplimiento normativo**, incluyendo las obligaciones dirigidas a la prevención de los mismos, siendo sancionable la no aplicación de estas medidas preventivas. Se exige, además, que las medidas técnicas y organizativas que se adopten en la organización **se revisen y se actualicen cuando sea necesario**. Es decir, se trata de una **obligación permanente** durante todo el periodo en que el tratamiento de datos se produzca.

> ⓘ **Realidad práctica:** hasta ahora, en muchos de los casos analizados en las inspecciones de servicios realizadas, las medidas implantadas y los documentos que se habían elaborado para el cumplimiento de la norma **no se revisaban ni actualizaban** reduciendo aún más si cabe su efectividad respecto a la protección de datos que se perseguía.

Es por ello que es necesario concienciar a quienes tienen responsabilidades en esta materia para que se interiorice la filosofía de la protección de datos como una **obligación continua y que debe tenerse en cuenta desde el mismo planteamiento y planificación de cualquier proyecto que se implante** y tenga relación directa o indirecta con el tratamiento de datos personales.

7.0. Principios relativos al tratamiento

El artículo 5 del RGPD establece los **principios que han de regir los tratamientos** de datos personales que son los siguientes:

- Licitud, lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva (que se refiere a la responsabilidad del responsable del tratamiento en el cumplimiento de los principios anteriores y en su capacidad de demostrarlo).

7.1. Evaluación del riesgo

Deberá realizarse una **valoración del riesgo** de los tratamientos que se llevan a cabo en la Entidad a fin de poder determinar qué medidas de seguridad deben aplicarse. Este análisis incluirá:

- Tipo de tratamiento,
- Naturaleza de los datos,
- Número de interesados afectados,
- Cantidad y variedad de tratamientos que se lleven a cabo.

Existen **metodologías** diseñadas para llevar a cabo este análisis, por ejemplo la ISO 31000, estando prevista la publicación de una versión revisada de la guía editada por la AEPD tratando esta cuestión.

7.2. Registro de actividades de tratamiento

Tanto los responsables como los encargados de tratamiento (novedad) deberán mantener un registro de operaciones de tratamiento donde se incluirá la siguiente información (art. 30, RGPD):

- Nombre y datos de contacto del responsable (y corresponsable, en su caso), del representante y del DPD
- Fines del tratamiento
- Descripción de categorías de interesados y de datos personales
- Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales (incluidos los que se encuentren en terceros países u organizaciones internacionales)
- Transferencias de datos a terceros países u organizaciones de internacionales
- Plazos previstos para la supresión de las diferentes categorías de datos (cuando sea posible)
- Descripción general de las medidas técnicas y organizativas de seguridad (cuando sea posible)

Importante: se establece una exención de esta obligación para aquellas organizaciones que empleen menos de 250 trabajadores (siempre que no se traten de tratamientos que puedan entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales –incluye datos de salud y afiliación sindical- o datos personales relativos a condenas e infracciones penales).

Recomendaciones de la AEPD:

- Partir de los **ficheros actualmente notificados** y detallar todas las operaciones que se realizan sobre cada conjunto estructurado de datos.
- En caso de finalidades básicas comunes, **se puede organizar el registro en torno a las operaciones de tratamiento concretas** vinculadas a dichas finalidades.

Existe la posibilidad de **solicitar el listado e información en formato electrónico** de los ficheros notificados a la AEPD a través de su sede electrónica.

EL PLOPD establece en su artículo 31 lo siguiente al respecto del **registro de actividades** de tratamiento:

- Podrá **organizarse** en torno a conjuntos estructurados de datos
- Cuando exista un **DPD** deberá comunicarse cualquier adición, modificación o exclusión en el contenido del registro
- Determinadas entidades del sector público (entre las que nos encontramos, artículo 77.1 PLOPD) deberán **hacer público un inventario de sus actividades de tratamiento** accesible por **medios electrónicos** en el que constará **la información que ya incluía el Registro de actividades de tratamiento y su base legal**.

7.3. Protección de datos desde el diseño y por defecto

Esta medida de responsabilidad activa (Artículo 25 RGPD) se refiere a la necesidad de **integrar la protección de los datos desde la fase de planificación y diseño de los tratamientos** (antes de que estos se pongan en marcha) así como durante su desarrollo (obligación permanente y continua durante el tiempo que se realicen los tratamientos). Se trata de pensar en términos de "protección de datos" desde el momento mismo de la toma de decisiones y la puesta en marcha de proyectos para que tratamiento y protección vayan de la mano desde el principio.

Otro aspecto relevante que se deriva de lo anterior es la orientación de que desde el diseño se busque garantizar que **sólo se tratan los datos estrictamente necesarios** (desde el punto de vista de la cantidad, la extensión del tratamiento, conservación y accesibilidad de los datos). En este sentido el Considerando 39 del RGPD da una vuelta de tuerca más en esa **autolimitación** estableciendo que los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados lo que, según añade a continuación, requiere, en particular, garantizar que **se limite a un mínimo estricto su plazo de conservación**. Para ello establece que:

- Los datos personales solo deben tratarse si la finalidad del tratamiento **no pudiera lograrse razonablemente por otros medios**.
- El responsable del tratamiento **deberá establecer plazos para la supresión o revisión periódica de los datos personales tratados**.

- Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para **impedir el acceso** o uno no autorizados de dichos datos y del equipo utilizado en el tratamiento.

7.4. Medidas de seguridad

Otra novedad del RGPD afecta a las medidas de seguridad aplicables (Artículo 32 RGPD). No sólo desaparece la clasificación por niveles de seguridad (básico, medio y alto) sino que también dejan de incluirse pautas y medidas concretas respecto a cómo han de protegerse los datos, dejando a responsables y encargados, en su caso, **la responsabilidad de establecer qué medidas técnicas y organizativas son las apropiadas según el nivel de riesgo que se haya detectado** en el análisis previo al tratamiento. Por tanto las medidas ya no van ligadas exclusivamente al tipo de datos que se tratan sino a otros factores y variables que pueden afectar al nivel de riesgo del tratamiento lo que ha de conllevar una mejor protección de los datos personales.

Tampoco se menciona el **documento de seguridad**, por lo que debemos entender que ya no será obligatorio, sin perjuicio de otros documentos que puedan elaborarse con un contenido análogo. Del mismo modo ya no se establece una pauta regular de realización de **auditorías** en los términos que se venían realizando hasta ahora con una periodicidad de 2 años.

Las medidas técnicas y organizativas que se establezcan **deberán tener en cuenta**:

- Coste de la técnica
- Costes de aplicación
- Naturaleza, alcance, contexto y fines del tratamiento
- Riesgos para los derechos y libertades

Respecto del **esquema anterior de medidas establecidas en el Reglamento de desarrollo de la LOPD** dejará de ser válido desde el momento en que sea de aplicación el nuevo RGPD lo que no obsta para que pueda concluirse que las medidas que allí se recogían sean las adecuadas y oportunas en función del resultado del análisis de riesgos realizado o que éstas deban completarse con otras adicionales o incluso suprimirse alguna de las que ya se venían aplicando.

El Considerando 74 establece que el responsable debe estar obligado no sólo a aplicar medidas oportunas y eficaces y estar en condiciones de demostrar la conformidad de las actividades de tratamiento con el RGPD sino que también debe estar en disposición de poder **demostrar la eficacia de las medidas aplicadas**.

Se establece la obligación de responsable y encargado del tratamiento de tomar medidas para **garantizar** que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales **solo pueda tratar dichos datos siguiendo instrucciones del**

responsable, salvo que esté obligada a ello en virtud de normativa europea o nacional (Artículo 32.5 RGPD).

Una medida a la que se le da gran relevancia en el RGPD es la **seudonimización** que viene definida en el artículo 4 del RGPD en los siguientes términos:

> *"**Seudonimización:***
> ***El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional**, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".*

7.5. Notificaciones de violaciones de seguridad de los datos

La regulación de esta cuestión por parte del nuevo Reglamento (Artículos 33 y 34) es **muy amplia** e incluye los siguientes **incidentes**:

- Destrucción,
- Pérdida, o
- Alteración accidental o ilícita de datos personales ya sean transmitidos, conservados o tratados de otro forma
- Comunicación, o
- Acceso no autorizado a dichos datos

Esto **implica** que cuestiones tales como:

- La pérdida de un ordenador portátil
- El acceso no autorizado a las bases de datos de la organización (incluso por su propio personal)
- Borrado accidental de algunos registros

constituyen violaciones de seguridad en los términos del RGPD **y deben tomarse las siguientes medidas** al respecto:

- **Notificación** a la autoridad de protección de datos competente (AEPD) salvo que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.
- **Notificación** sin dilación y siempre que sea posible dentro de las 72 horas siguientes a que se tenga constancia de ella.
- **Contenido mínimo**:
  - Naturaleza de la violación

- Categoría de datos e interesados afectados
- Medidas adoptadas para solventar la quiebra
- Medidas aplicadas para paliar los efectos negativos sobre los afectados, si procede.

- Todas las violaciones deberán quedar **documentadas** por el responsable.

- Cuando las violaciones entrañen un **alto riesgo** para los derechos o libertades de los interesados la notificación deberá completarse con una **notificación dirigida a los interesados**.

- El fin último de esta notificación es que **los interesados puedan tomar medidas para protegerse** de las consecuencias negativas que pueda tener la violación por lo que aunque no se establece un plazo concreto para llevarla a cabo deberá ser lo antes posible para que puedan reaccionar en consecuencia y con la mayor eficacia. En la notificación se podrán incluir **recomendaciones** a los interesados para ayudarles a hacer frente a las consecuencias de la quiebra de seguridad.

- **No será necesaria la notificación** si se han tomado medidas, antes o después de la quiebra, que garanticen que no hay posibilidad de que el alto riesgo se materialice. Tampoco será necesaria si el esfuerzo que deba realizarse es desproporcionado y puede sustituirse por otras medidas alternativas como puede ser una comunicación pública.

- Está previsto que existan **modelos armonizados** de comunicación de quiebras de seguridad y un canal específico establecido para su comunicación a la AEPD.

¿Cómo se analiza la probabilidad de riesgo para los derechos y libertades de los afectados?

- Debe **analizarse** las características del accidente y determinar hasta qué punto éste puede causar un daño a los derechos o libertades del interesado.

- Hay que entender **daño** desde la perspectiva material e inmaterial de sus consecuencias (p.ej. perjuicios económicos o exposición pública de datos confidenciales, exclusión o discriminación derivadas de dicha exposición).

- El **alto riesgo** vendrá determinado por la probabilidad de que se ocasionen perjuicios de entidad a los interesados.

7.6. Evaluación de impacto sobre la protección de datos

Deberán llevarse a cabo **antes de iniciarse un tratamiento** cuando este suponga un **alto riesgo** para los derechos y libertades de los interesados (Artículos 35 y 36 RGPD).

En el caso de **tratamientos iniciados con anterioridad** a la aplicación del Reglamento deberá realizarse cuando del análisis de riesgos realizados se concluya que el tratamiento entraña alto riesgo para los derechos y libertades de los interesados.

En caso de que el alto riesgo se considere que no puede mitigarse por medios razonables en términos de los costes y la tecnología aplicable, el responsable deberá elevar **consulta** a la AEPD para que pueda emitir recomendaciones o ejercer cualquier otro de los poderes que el Reglamento confiera a la autoridad de protección de datos entre las que se encuentra la prohibición del tratamiento.

A estos efectos se ha elaborado una **lista indicativa** de supuestos en los que los tratamientos conllevan un alto riesgo y por tanto deberá llevarse a cabo una **EIPD**:

- Elaboración de perfiles para la toma de decisiones con efectos jurídicos o de análoga relevancia para los interesados.
- **Tratamiento a gran escala de datos sensibles**. *(Nuestro caso)*
- Observación sistemática a gran escala de una zona de acceso público.

Para considerar que estamos ante un **tratamiento a gran escala** el Grupo de Trabajo del artículo 29[6] (GT 29) ha establecido que debe tenerse en cuenta:

- Número o proporción de interesados afectados
- Volumen y variedad de datos tratados
- Duración o permanencia de la actividad de tratamiento
- Extensión geográfica de la actividad de tratamiento

Además, el PLOPD establece en su artículo 28 las **obligaciones generales del responsable y encargado del tratamiento** respecto de las medidas de responsabilidad activa estableciendo una serie de situaciones que pueden resultar en mayores riesgos para el tratamiento y pudieran hacer aconsejable una EIPD.

En el momento de aplicación del RGPD la AEPD publicará **listas adicionales** de tratamiento de datos que requieren de una EIPD y cuáles no. No obstante, eso no sustituye la obligación del responsable de efectuar el análisis de riesgo y de la responsabilidad última del responsable respecto del tratamiento realizado, por lo que podría decidir realizar una evaluación aun cuando en principio pudiera no ser obligatoria cuando del resultado del análisis se extraiga su conveniencia. En esta línea se está trabajando por parte del GA29 para **orientar y establecer parámetros homogéneos para determinar cuándo es necesaria una EIPD.**

[6] Este grupo de trabajo creado por la Directiva 95/46/CE, es un **órgano consultivo independiente** integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Las funciones del GT29 reconocidas por la Directiva incluyen estudiar toda cuestión relativa a la **aplicación de las disposiciones nacionales** tomadas para la aplicación de la Directiva, emitir dictámenes sobre el **nivel de protección existente** dentro de la Comunidad y en países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, y **formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea**.

Cuando los tratamientos sean similares y los riesgos también, podrá optarse por realizar **una única EIPD**. También podrá ser necesaria cuando haya **variaciones en el tratamiento o los riesgos asociados al mismo**.

7.7. Consecuencias en la gestión

- Deberá **valorarse** si a los tratamientos actuales se les está aplicando los **principios** contenidos en la norma, en particular aquellos que se refieren a la minimización de datos y la limitación del plazo de conservación.

- Debe realizarse una **evaluación del riesgo de los tratamientos** que se hayan identificado.

- Establecer un **registro de tratamiento** que, además de requerir que se fije un **criterio homogéneo** en la determinación de qué se entiende por tratamiento, también hace necesaria la determinación de un enfoque centralizado, descentralizado o mixto, es decir, si todos los tratamientos se registrarán en SSCC con independencia de su distribución física por el territorio o si por el contrario se establecerá un registro independiente en cada DP y otro en SSCC, o en última instancia, se combinarán ambas opciones. Las **modificaciones** que se realicen deberán comunicarse al DPD.

- Una vez realizado ese registro deberá **publicarse un inventario de las actividades de tratamiento** accesible por medios electrónicos con la información establecida en el artículo 31 del PLOPD, todo ello siempre que se confirme la redacción del citado proyecto de ley orgánica.

- En todos los **proyectos** que se elaboren en la Entidad deberá tenerse presente el impacto en materia de protección de datos, siguiendo el **enfoque de la protección desde el diseño y por defecto**, analizando si entraña un nuevo tratamiento de datos o modificación de uno existente o si afecta a alguno de los aspectos incluidos en la normativa.

- Deberá valorarse el mantenimiento del esquema anterior de **medidas de seguridad** que venían aplicándose o su modificación en función de los resultados de los análisis de riesgos realizados, las EIPD, en su caso y **cambiando el enfoque a la perspectiva del riesgo para los derechos y libertades de los interesados**, enfoque éste más amplio y que incluye también el **uso responsable** a nivel interno de los datos que tratamos y la propia **limitación** de los mismos a aquellos **exclusivamente necesarios** para los fines para los que se recabaron y por el **plazo imprescindible** para ello.

- Deberá estudiarse cómo se demostrará la **eficacia de las medidas aplicadas**, en especial aquellas que no son de carácter automatizado y que afectan a la documentación en papel. También cómo se **garantizará** que quienes acceden a los datos sólo pueden tratar esos datos según las instrucciones impartidas.

- Deberá decidirse si se mantiene la elaboración de **documentos de seguridad y el régimen de auditorías,** así como el **objetivo institucional** relacionado con ellas.

- Sería conveniente el estudio de las ventajas e inconvenientes que pueden implicar la aplicación de la medida de **seudonimización** en los tratamientos que se realizan en la Entidad.

- Tendrá que establecerse un **criterio** sobre qué constituye una **violación o quiebra de seguridad** (partiendo de lo que establece la norma para que a través de la especificación se facilite la detección de las mismas, en su caso, en las DDPP o SSCC), en especial, en cuanto a aquellas que deban considerarse de una gravedad tal que deban ser **notificadas** (AEPD, interesados…) para lo que sería positivo definir unos parámetros que sirvan de guía en esta valoración. También deberá establecerse la forma en que deberán quedar **documentadas**. Puede ser aconsejable establecer **pautas de actuación** para los casos de quiebras de seguridad más probables en aras de una mayor homogeneidad en su resolución.

- Deberán llevarse a cabo las **EIPD** pertinentes según los resultados de los análisis de riesgo realizados sobre los tratamientos actuales y los que se puedan establecer en el futuro. En este sentido, los tratamientos más afectados serán aquellos que traten **datos de salud** aunque no hay que olvidar también los que implican **violencia de género** y no entran por el circuito de ocultación de datos, aunque éstos, por su reducido volumen y según la metodología aplicable podrían obtener una valoración de riesgo inferior. Y, en su caso, elevar **consulta** a la AEPD, si bien, esta opción parece improbable.

- Se deberá estar atento a lo que **publiquen** las autoridades europeas y españolas con competencia en la materia respecto de los tratamientos que pueden considerarse de alto riesgo y que por tanto deban ser objeto de evaluación.

8. Delegado de protección de datos

En el caso de nuestra organización tiene carácter **obligatorio** (Artículos 37 a 39 RGPD) ya que somos un organismo público y además tratamos datos sensibles a gran escala (en especial relativos a la salud y capacidad laboral de los interesados).

En fecha 6 de marzo de 2017 se presentó un **informe** (anexo V) respecto de esta figura y las propuestas motivadas en cuanto a su mejor articulación en nuestra Secretaría de Estado. En él se defendía la necesidad de que nuestro Instituto tuviera **un papel líder en la adaptación a la nueva norma dado que nuestra Entidad es la que con mayor incidencia va a verse afectada por su implantación y es la que trata mayor volumen de datos sensibles**. Además, los efectos de la implantación de medidas de seguridad pueden **afectar seriamente** a la gestión de las prestaciones, motivo por el que se consideraba necesaria una **participación al más alto nivel en la toma de decisiones** sobre la forma en que se produciría la adaptación y aplicación de las nuevas obligaciones impuestas por el Reglamento.

No obstante, la decisión que se tomó a nivel de SE fue establecer **un único delegado de protección de datos**. Su perfil es eminentemente jurídico y se hace necesaria la coordinación tanto técnica (por parte de GISS) como desde la práctica de la gestión (INSS y resto de entidades y servicios comunes) para llevar a cabo de forma adecuada y menos gravosa para la

gestión la necesaria adaptación. Además, ésta deberá ser ágil ya que **las obligaciones establecidas en la norma serán exigibles desde el día 25 de mayo**.

En el **borrador de Resolución del Secretario de Estado de la SS por la que se designa DPD de la Admón. de la SS**, se crea una **Comisión de protección de datos de la Admón. de la SS** compuesta por una serie de **subdelegados** en representación de las distintas entidades y servicios comunes que componen la SS. Sus componentes apoyarán al DPD en su misión de adaptación y cumplimiento de la nueva normativa. Esta fórmula **se aproxima a las propuestas** que se realizaban en el ya citado informe sobre la figura del DPD emitido por esta Inspección de Servicios, si bien, **no recoge plenamente el espíritu de la recomendación efectuada**, en particular, respecto de la **posición de liderazgo** que se considera que debería tener nuestra Entidad en el **proceso de adaptación inicial y en el posterior seguimiento ordinario del cumplimiento** de la nueva normativa de protección de datos.

Por otra parte, según lo establecido en el punto 9 del documento "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento) editado por la AEPD y teniendo en cuenta que los servicios prestados por GISS se consideran un **encargo de tratamiento**, de forma análoga, podría entenderse que el **Servicio Jurídico de la SESS** se encuentra en la misma situación con respecto a las entidades gestoras y servicios comunes y, por tanto, si eso es así, debería f**ormalizarse un contrato de encargo o acto jurídico vinculante** que regulase esta situación.

8.0. Consecuencias en la gestión

- Sería necesario **articular el funcionamiento de la figura del Subdelegado de protección de datos** (SPD, en adelante) para que operase **como un verdadero DPD**, dejando a éste último el necesario papel de coordinador. Esto permitiría que la labor del SPD **se ajuste de mejor forma a las necesidades específicas y peculiaridades propias de la actividad encomendada a cada una de las entidades** gestoras o servicios comunes, en su caso.

- A estos efectos, e incluso aunque la primera de las recomendaciones no se llevara a efecto, se entiende fundamental la **constitución de un equipo de apoyo al SPD** en nuestro Instituto que tenga **representación** del ámbito jurídico, del de la gestión y de la visión práctica (y armonizadora, propia de la actuación de la Inspección).

- En cualquier caso será necesaria una **estrecha colaboración y una comunicación muy fluida** con la oficina del DPD para asegurar la mejor coordinación y éxito en las actuaciones y planes que se lleven a cabo.

- La primera y más importante labor para asegurar el éxito en el resultado de las actuaciones posteriores será el **fijar criterios comunes y homogéneos** en diversas cuestiones así como llevar a cabo actuaciones tales como:

- Consideración de **qué constituye un tratamiento**[7] **y su nivel de agregación** o desagregación[8].

- En caso de considerarse algunos **tratamientos responsabilidad directa de la DDPP**, establecimiento de las **pautas e instrucciones necesarias** para que la actuación de éstas se adecúe a la norma y sea homogénea en todo el territorio.

- **Adopción de un modelo de análisis de riesgos**, forma en que este análisis se realizará (centralizado, descentralizado, por parte de cada uno de los responsables…), desarrollo e impartición de instrucciones,...

- **Adopción de una metodología de EIPD** y puesta en práctica en aquellos casos en que se considere necesario.

- **Valoración de las medidas de seguridad aplicables** en cada caso.

- Impartición de **instrucciones para la determinación de la base legal** que legitima cada uno de los tratamientos.

- **Establecimiento del modelo y formato** con el que se cumplirá con el **deber de informar**.

- **Definición de las violaciones o quiebras de seguridad** y protocolo de actuación.

- **Participación como asesores en los proyectos** que se lleven a cabo para hacer efectiva la **protección de datos desde el diseño y por defecto.**

- **Articulación del ejercicio de los derechos ARCO+.**

- **Colaboración con la Inspección de Servicios** en el marco del control de la efectiva adaptación y adecuado cumplimiento de la norma.

- **Colaboración con todas las unidades de gestión en labores de asesoramiento** para el mejor cumplimiento de la legislación en materia de protección de datos.

- Deberá analizarse si el DPD designado debe tener la **consideración de encargado del tratamiento** y, de ser así, formalizarse el contrato o acto jurídico correspondiente.

---

[7] Debe tenerse en cuenta que los **ficheros declarados de las DDPP** no pueden considerarse una lista exhaustiva ya que en muchos de los casos lo declarado no responde a la realidad del conjunto de tratamientos existentes a nivel descentralizado ni a un criterio homogéneo y coherente en cuanto a qué y cómo debe declararse.

[8] En este sentido hay **varios** criterios que oscilan entre la **máxima agregación posible** (simplificando y centralizando incluso a nivel geográfico lo que dificulta un tratamiento pormenorizado y adaptado a toda la amplia y diversa casuística que puede llegar a englobar ese nivel de agrupación) **a la más detallada desagregación** (lo que se desaconseja pues añade complejidad a la gestión sin aportar mayores garantías para la protección de los datos). **La situación actual debe regularizarse** ya que hay una **gran disparidad de criterios** entre las distintas DDPP. En este particular, entendemos que **el criterio que ha de primar a la hora de tomar una decisión es adoptar aquél que se derive de las finalidades y bases jurídicas legítimas que nos habilitan para llevar a cabo cada tratamiento**. Si bien, esto supondrá un esfuerzo adicional a la hora de establecer las medidas de seguridad y pautas de actuación en el ámbito descentralizado de la gestión.

9. Transferencias internacionales

En el caso de la entidad esta cuestión tiene poca incidencia más allá de los datos que se comparten con otros organismos extranjeros de Seguridad Social dentro del ámbito de los **Reglamentos Comunitarios y los Convenios Internacionales** firmados en la materia. En cualquier caso, los principios rectores del Reglamento deberán aplicarse en cualquier movimiento de datos que pueda producirse y cumplirse con el resto de obligaciones en la materia cuando, en su caso, puedan efectuarse.

9.0. Consecuencias en la gestión

- Estudio jurídico desde las unidades afectadas.

10. Tratamiento de datos de menores

En principio este aspecto de la norma también tiene un **impacto reducido** en nuestra Entidad ya que el volumen de datos de menores que se tratan es proporcionalmente bajo y, por lo general, se fundamentan en una base legal que así lo justifica, no obstante, pueden existir tratamientos basados en el consentimiento que deban tener en cuenta las previsiones contenidas en la normativa e impliquen alguna adaptación en nuestra gestión lo que deberá ser objeto de análisis en cada uno de los casos.

10.0. Consecuencias en la gestión

- Estudio jurídico desde las unidades afectadas.

11. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos

En la DA 9ª del PLOPD se establece que cuando la **publicación de un acto administrativo** contenga **datos de carácter personal** del afectado se le identificará con su nombre y apellidos y 4 últimas cifras numéricas de su DNI o documento de identidad equivalente.

Cuando se trate de notificación por medio de **anuncios**, en particular cuando se trate de los casos del artículo 44 de la Ley 39/2015, de 1 de octubre[9], se identificará al interesado exclusivamente por el número completo del DNI o documento de identidad equivalente.

---

[9] **Artículo 44. Notificación infructuosa. Ley 39/2015.**

Cuando los interesados en un procedimiento sean desconocidos, se ignore el lugar de la notificación o bien, intentada ésta, no se hubiese podido practicar, la notificación se hará por medio de un anuncio publicado en el «Boletín Oficial del Estado».

Asimismo, previamente y con carácter facultativo, las Administraciones podrán publicar un anuncio en el boletín oficial de la Comunidad Autónoma o de la Provincia, en el tablón de edictos del Ayuntamiento del último domicilio del interesado o del Consulado o Sección Consular de la Embajada correspondiente.

Si se carece de documento de identidad se le identificará exclusivamente con su nombre y apellidos.

En ningún caso deberá publicarse el nombre y apellidos de manera conjunta con el número completo del documento de identidad.

11.0. Consecuencias en la gestión

- Deberán **dictarse instrucciones y adaptarse**, si no lo estuvieran, **los sistemas de notificación y anuncios** para cumplir con las exigencias establecidas en la norma.

12. Potestad de verificación de las Administraciones Públicas

Según establece la Disposición adicional décima del PLOPD, en caso de **solicitudes formuladas por medios electrónicos en las que se declaren datos personales que obren en poder de las AAPP**, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

12.0. Consecuencias en la gestión

- Esto opera como **habilitación legal** para acceder a esos datos como parte de la verificación de los datos declarados por los interesados en las solicitudes que estos presenten por medios electrónicos. Lo que excluye las solicitudes que se presenten en la vía presencial.

Las Administraciones Públicas podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión, que no excluirán la obligación de publicar el correspondiente anuncio en el «Boletín Oficial del Estado».

ANEXO I. **TABLA EJEMPLO DEL SISTEMA PROPUESTO DE DOBLE CAPA PARA CUMPLIR CON EL DEBER DE INFORMAR.**

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

ANEXO II. **NUEVA LEY DE CONTRATOS, CONFIDENCIALIDAD, ENCARGO DE TRATAMIENTO Y PROTECCIÓN DE DATOS**

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.

Artículo 133. Confidencialidad.

1. Sin perjuicio de lo dispuesto en la legislación vigente en materia de acceso a la información pública y de las disposiciones contenidas en la presente Ley relativas a la publicidad de la adjudicación y a la información que debe darse a los candidatos y a los licitadores, los órganos de contratación no podrán divulgar la información facilitada por los empresarios que estos hayan designado como confidencial en el momento de presentar su oferta. El carácter de confidencial afecta, entre otros, a los secretos técnicos o comerciales, a los aspectos confidenciales de las ofertas y a cualesquiera otras informaciones cuyo contenido pueda ser utilizado para falsear la competencia, ya sea en ese procedimiento de licitación o en otros posteriores.

El deber de confidencialidad del órgano de contratación así como de sus servicios dependientes no podrá extenderse a todo el contenido de la oferta del adjudicatario ni a todo el contenido de los informes y documentación que, en su caso, genere directa o indirectamente el órgano de contratación en el curso del procedimiento de licitación. Únicamente podrá extenderse a documentos que tengan una difusión restringida, y en ningún caso a documentos que sean públicamente accesibles.

El deber de confidencialidad tampoco podrá impedir la divulgación pública de partes no confidenciales de los contratos celebrados, tales como, en su caso, la liquidación, los plazos finales de ejecución de la obra, las empresas con las que se ha contratado y subcontratado, y, en todo caso, las partes esenciales de la oferta y las modificaciones posteriores del contrato, respetando en todo caso lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. El contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato a la que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal. Este deber se mantendrá durante un plazo de cinco años desde el conocimiento de esa información, salvo que los pliegos o el contrato establezcan un plazo mayor que, en todo caso, deberá ser definido y limitado en el tiempo.

Artículo 346. Registro de Contratos del Sector Público.

5. El Registro de Contratos del Sector Público facilitará de modo telemático el acceso a sus datos a los órganos de las Administraciones Públicas que los precisen para el ejercicio de sus competencias legalmente atribuidas.

Asimismo, de conformidad con lo establecido en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y con las limitaciones que

imponen las normas sobre protección de datos de carácter personal, facilitará el acceso público a los datos que no tengan el carácter de confidenciales y que no hayan sido previamente publicados de modo telemático y a través de Internet.

Disposición adicional vigésima quinta. Protección de datos de carácter personal.

1. Los contratos regulados en la presente Ley que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo.

2. Para el caso de que la contratación implique **el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquel tendrá la consideración de encargado del tratamiento.**

En este supuesto, el acceso a esos datos **no se considerará comunicación de datos**, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán de constar por escrito *(CONTRATO DE ENCARGO DE TRATAMIENTO).*

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que esta hubiese designado.

El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:

a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.

b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.

c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento.

ANEXO III. **MODELO DE CLÁUSULAS CONTRACTUALES PARA EL CONTRATO DE ENCARGO DE TRATAMIENTO ADAPTADO AL NUEVO REGLAMENTO**

Este modelo está **adaptado al Reglamento (UE) 2016/679** y se ha extraído del documento *"Directrices para la elaboración de contratos entre responsables y el encargado del tratamiento"*, de 2017 -**elaborado por la AEPD, la Autoridad Catalana de Protección de Datos, y la Agencia Vasca de Protección de Datos**- con pequeñas adaptaciones y anotaciones aplicables a nuestro contexto específico.

Ha de tenerse en cuenta que el modelo en principio está orientado **al caso en el que el tratamiento de datos se realice en los locales y con los sistemas del encargado del tratamiento**, ejemplos de esta situación en nuestro ámbito son la videovigilancia prestada de forma remota desde la central de alarmas y la destrucción de documentación en papel en las dependencias del adjudicatario. No obstante, su contenido es de fácil adaptación y no reviste importantes especialidades por lo que **también es aplicable a los casos más frecuentes en nuestro ámbito, aquellos que se prestan con nuestros sistemas y en nuestros locales** como es el caso de la videovigilancia prestada por el adjudicatario desde nuestros propios puestos de vigilancia, la destrucción de papel con maquinaria industrial propia y los letrados apoderados contratados.

En todo caso, **este modelo no tiene la consideración de cláusulas tipo a los efectos del artículo 28.8 del RGPD**.

_____, a _____ de _____ de 20___

REUNIDOS

DE UNA PARTE:

«ENTIDAD A», con domicilio social en _____ (_____), y con CIF: _____, debidamente representada en este acto por D. /Dña._____.

En calidad de RESPONSABLE DEL FICHERO, en adelante, «EL RESPONSABLE»,

DE OTRA PARTE:

«ENTIDAD B», con domicilio social en _____, C/_____ y con CIF: _____, debidamente representada en este acto por D./Dña. _____.

En calidad de ENCARGADO DEL TRATAMIENTO, en adelante, «EL ENCARGADO».

Ambas partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato de encargo de tratamiento de datos personales y para quedar obligadas en la representación en que respectivamente actúan, en los términos convenidos en él. A tal fin,

EXPONEN

I. Que «EL RESPONSABLE» es una entidad dedicada a .....
II. Que «EL ENCARGADO» es una empresa dedicada, entre otras actividades propias de su objeto social, a las de .....

III. Que entre ambas partes existe una relación contractual por la cual «EL ENCARGADO» presta servicios relacionados con la *(indicar actividad)* ..... a favor de «EL RESPONSABLE», que puede implicar un tratamiento del fichero con datos personales titularidad de este último (en adelante, LOS SERVICIOS).

IV. Que, al objeto de dar cumplimiento a lo dispuesto en el artículo 28 del 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, ambas partes acuerdan suscribir un contrato de encargo de tratamiento de datos personales, el cual formalizan de común acuerdo, sobre la base de las siguientes

ESTIPULACIONES

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la *(indicar empresa adjudicataria)* ....., encargada del tratamiento, para tratar por cuenta de ...., Responsable del Tratamiento, los datos de carácter personal necesarios para prestar el servicio de..... .

El tratamiento consistirá en: *(descripción detallada del servicio)*

Concreción de los tratamientos a realizar:

□ Recogida	□ Consulta	□ Supresión
□ Registro	□ Comunicación por transmisión	□ Destrucción
□ Estructuración	□ Difusión	□ Conservación
□ Modificación	□ Interconexión	□ Comunicación
□ Conservación	□ Cotejo	□ Otros:.....
□ Extracción	□ Limitación	

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad ....., Responsable del Tratamiento, pone a disposición de la *(indicar empresa adjudicataria)* ....., encargada del tratamiento, la información que se describe a continuación:

- .....
- .....

3. Duración

El presente acuerdo tiene una duración de .....

NOTA: En algunos casos, en particular determinados supuestos sometidos al derecho administrativo (convenios, contratos de gestión de servicios públicos, etc.), la duración del encargo puede estar limitada por la duración establecida por la legislación vigente para la prestación de servicios.

Una vez finalice el presente contrato, el Encargado del Tratamiento debe suprimir/devolver al responsable/devolver a otro encargado que designe el responsable *(indicar la opción que proceda y especificar, en su caso, el encargado correspondiente)* los datos personales y suprimir cualquier copia que esté en su poder *(NOTA: téngase en cuenta que en algunos casos procede la conservación de los datos debidamente bloqueados).*

4. Obligaciones del Encargado del Tratamiento

El Encargado del Tratamiento y todo su personal se obliga a:

1º. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

2º. Tratar los datos de acuerdo con las instrucciones del Responsable del Tratamiento. Si el Encargado del Tratamiento considera que alguna de las instrucciones infringe el Reglamento (UE) 2016/679 o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

3º. Llevar, por escrito, un registro de todas actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

NOTA: Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del Reglamento (UE) 2016/679, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del Reglamento (UE) 2016/679 , la documentación de garantías adecuadas.
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
    - La seudonimización y el cifrado de datos personales.
    - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
    - La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
    - El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

4º. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del Tratamiento, en los supuestos legalmente admisibles. El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

5º. Subcontratación.

(Escoger una de las opciones)

Opción A

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de ..... *(NOTA: Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación)*....., indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido. El subcontratista, que también tendrá la condición de Encargado del Tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el Encargado del Tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

Opción B

Se autoriza al encargado a subcontratar con la empresa ..... las prestaciones que comporten los tratamientos siguientes: .....

Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de .....

(NOTA: Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación)

El subcontratista, que también tiene la condición de Encargado del Tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el Encargado del Tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

6º. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.
7º. Garantizar que las personas autorizadas para tratar datos personales se comprometen, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

NOTA: Si existe una obligación de confidencialidad de naturaleza estatutaria o legal (por ejemplo, abogados) deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.

8º. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
9º. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
10º. Asistir al Responsable del Tratamiento en la respuesta al ejercicio de los derechos de:

- Acceso, rectificación, supresión y oposición
- Limitación del tratamiento
- Portabilidad de datos
- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

(Escoger una de las opciones)

Opción A

El Encargado del Tratamiento debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.

(NOTA: A pesar de que la delegación en el encargado es una decisión que corresponde al responsable, resulta especialmente recomendable en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado).

Opción B

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el Encargado del Tratamiento, éste debe comunicarlo por correo electrónico a la dirección ..... *(dirección que indique el responsable)*. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la misma.

(NOTA: Plazo y medio recomendados a fin de que el responsable pueda resolver la solicitud dentro del plazo establecido).

11º. Derecho de información

(Escoger una de las opciones)

Opción A

El Encargado del Tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

Opción B

Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

12º. Notificación de violaciones de la seguridad de los datos

El Encargado del Tratamiento notificará al Responsable del Tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de ..... *(NOTA: El plazo debe ser inferior a 72 horas en cualquier caso)*, y a través de..... , las violaciones de seguridad de los datos personales a su cargo de las que tenga conocimiento, junto con toda la información relevante para la documentación y comunicación de la incidencia. No será necesaria la notificación cuando sea improbable que dicha violación de seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

(Escoger alguna o las dos opciones, en su caso)

NOTA: Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al Responsable del Tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.

Opción A.- Corresponde al Encargado del Tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

La comunicación contendrá, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Opción B.- Corresponde al Encargado del Tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

- Explicar la naturaleza de la violación de datos.
- Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el Responsable del Tratamiento para poner remedio a la violación de la seguridad de los datos

personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

13º. Dar apoyo al Responsable del Tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

14º. Dar apoyo al Responsable del Tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

15º. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

16º. Implantar las medidas de seguridad siguientes:

(Escoger una o las dos opciones)

Opción A

Las medidas de seguridad siguientes, de acuerdo con la evaluación de riesgos realizada por....., en fecha ...:

- .....
- .....

(NOTA: Debe indicarse si la evaluación de riesgos ha sido realizada por el responsable o por el Encargado del Tratamiento).

Opción B

Las medidas de seguridad establecidas en .....

(NOTA: Debe indicarse el código de conducta, el sello, la certificación u otro estándar donde estén definidas las medidas aplicables).

En todo caso, deberá implantar mecanismos para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.

17º. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable *(cuando así lo determine la norma).*

(NOTA: El delegado de protección de datos debe designarse, según establece el artículo 37 del Reglamento Europeo de Protección de Datos, cuando: a) El tratamiento lo lleve a cabo una

autoridad o un organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala; c) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.)

18º. Destino de los datos:
(Escoger una de las 3 opciones siguientes)

Opción A

Devolver al Responsable del Tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos en poder del encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción B

Devolver al encargado que designe por escrito el Responsable del Tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción C

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al Responsable del Tratamiento. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones del Responsable del Tratamiento
Corresponde al Responsable del Tratamiento:

1. Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
2. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
3. Realizar las consultas previas que corresponda.
4. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento (UE) 2016/679 por parte del encargado.
5. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6. **Responsabilidad del Encargado del Tratamiento.**
    a. El Encargado del Tratamiento será considerado Responsable del Tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el Encargado del Tratamiento responderá de las infracciones en que hubiera incurrido personalmente *(NOTA: hay que tener en cuenta la excepción que introduce el PLOPD en su artículo 33).*
    b. El Encargado del Tratamiento indemnizará al Responsable del Tratamiento por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.
    c. A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El Encargado del Tratamiento, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.
    d. La responsabilidad del Encargado del Tratamiento incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el Responsable del Tratamiento, como resultado del incumplimiento del Encargado del Tratamiento de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del Responsable del Tratamiento en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

7. **Controles y auditorías.**

El Responsable del Tratamiento, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del Encargado del Tratamiento del presente contrato. Por su parte, el Encargado deberá facilitar al Responsable del Tratamiento cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

8. **Notificaciones.**
    a. Cualquier notificación que se efectúe entre las partes se hará por escrito y será entregada personalmente o de cualquier otra forma que certifique la recepción por la parte notificada.
    b. Cualquier cambio de domicilio de una de las partes deberá ser notificado a la otra de forma inmediata y por un medio que garantice la recepción del mensaje.

9. **Cláusulas generales.**
    a. La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituye una renuncia a dichos derechos en el futuro.
    b. La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.

c. Si se llegara a demostrar que alguna de las estipulaciones contenidas en este Contrato es nula, ilegal o inexigible, la validez, legalidad y exigibilidad del resto de las estipulaciones no se verán afectadas o perjudicadas por aquélla.
d. El presente Contrato y las relaciones entre el Responsable del Tratamiento y el Encargado del Tratamiento no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.
e. Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

D:/Dña. _____

En nombre de «EL RESPONSABLE»

D:/Dña. _____

En nombre de «EL ENCARGADO»

CONTENIDO QUE TIENE QUE TENER EL CONTRATO O ACTO JURÍDICO QUE REGULA LA RELACIÓN RESPONSABLE/ENCARGADO DEL TRATAMIENTO.

Contenido extraído de las: "Directrices para la elaboración de contratos entre responsables y el encargado del tratamiento", de 2017, elaborado por la AEPD, la Autoridad Catalana de Protección de Datos, y la Agencia Vasca de Protección de Datos.

INSTRUCCIONES DOCUMENTADAS RESPECTO DEL ENCARGO REALIZADO.	Se debe documentar de forma precisa las instrucciones respecto del encargo realizado. Es necesario identificar de forma clara y concreta cuáles son los tratamientos de datos a realizar por el encargado del tratamiento, atendiendo al tipo de servicio prestado y a la forma de prestarlo. Es especialmente necesario determinar de forma clara las comunicaciones a terceros que el responsable encomienda al encargado o que se derivan del servicio prestado. La sujeción a las instrucciones del responsable deberá producirse igualmente en el caso de las transferencias internacionales de datos que puedan producirse como consecuencia de la prestación del servicio. Si el encargado del tratamiento está obligado legalmente, por el Derecho de la Unión o de un Estado miembro, a transferir datos a un tercer país deberá informar al responsable antes de llevar a cabo el tratamiento, salvo que tal derecho lo prohíba por razones importantes de interés público. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado deberá informar inmediatamente al responsable.
DEBER DE CONFIDENCIALIDAD	Hay que establecer la forma en que el encargado del tratamiento garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o, en su caso, si están sujetas a una obligación de confidencialidad de naturaleza estatutaria. El cumplimiento de esta obligación debe quedar documentado y a disposición del responsable del tratamiento.
MEDIDAS DE SEGURIDAD	El acuerdo debe establecer la obligación del encargado de adoptar todas las medidas de seguridad necesarias, de conformidad con lo establecido en el artículo 32 del RGPD. Corresponde al responsable del tratamiento realizar la evaluación de riesgos para determinar las medidas de seguridad apropiadas

para garantizar la seguridad de la información tratada y los derechos de las personas afectadas. Así mismo el encargado también debe evaluar los posibles riesgos derivados del tratamiento, teniendo en cuenta los medios utilizados (tecnologías, recursos etc.) y otras circunstancias que puedan incidir en la seguridad, como por ejemplo que el encargado lleve a cabo otros tratamientos.

A partir de aquí, la determinación de las medidas de seguridad concretas puede realizarse a través de una lista exhaustiva de las mismas o de la remisión a un estándar o marco nacional o internacional reconocido.

Así, 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 los riesgos de probabilidad y gravedad variables para los derechos y las libertades de las personas físicas, el responsable y el encargado del tratamiento establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo existente que, en su caso, incluyan, entre otros:

a) La seudonimización y el cifrado de datos personales;

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y

c) resiliencia permanentes de los sistemas y servicios de tratamiento;

d) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de

e) forma rápida, en caso de incidente físico o técnico;

f) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las

g) medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

La adhesión a códigos de conducta o la posesión de una certificación son elementos que sirven para demostrar el cumplimiento de los requisitos anteriormente indicados.

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos

	siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.
EL RÉGIMEN DE LA SUBCONTRATACIÓN	El acuerdo debe establecer el régimen de subcontratación. El RGPD exige la autorización previa por escrito del responsable del tratamiento para que el encargado del tratamiento pueda recurrir a otro encargado (subencargado) para desarrollar el servicio encomendado, cuando esto conlleve el tratamiento de los datos personales por parte de un tercero. Esta autorización puede ser específica (identificación de la entidad concreta) o general (sólo autorizando la subcontratación, pero sin concretar la entidad). En el supuesto que la autorización sea de carácter general, el encargado informará al responsable de la incorporación de un subencargado o su sustitución por otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios. Puede ser de utilidad establecer en el acuerdo o acto la forma (que en todo caso deberá constar por escrito) y el plazo para que el responsable pueda manifestar su oposición. En todo caso, el subencargado del tratamiento debe estar sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y en la misma forma (acuerdo por escrito o acto jurídico vinculante) que el encargado del tratamiento en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En caso de incumplimiento por el subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones del subencargado. Cuando sea aplicable la legislación de contratos del sector público, habrá que tener en cuenta también las disposiciones específicas previstas en dicha ley.
LOS DERECHOS DE LOS INTERESADOS	Hay que establecer la forma en la que el encargado del tratamiento asistirá al responsable en el cumplimento de la obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del RGPD: – Acceso a datos personales

	– Rectificación – Supresión (derecho al olvido) – Limitación del tratamiento – Portabilidad de datos – Oposición – A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles) El acuerdo deberá establecer de forma clara si corresponde al encargado del tratamiento atender y dar respuesta a las solicitudes de estos derechos o bien establecer expresamente que su única obligación es comunicar al responsable del tratamiento que se ha ejercido un derecho. En el primer supuesto, el acuerdo debe establecer la forma y los plazos para atender o, en su caso, dar respuesta a las solicitudes de ejercicio de derechos. En el segundo supuesto, debe establecerse la forma y el plazo en que la solicitud y, en su caso, la información correspondiente al ejercicio del derecho se debe comunicar al responsable del tratamiento. En cuanto al derecho de información de las personas afectadas, se trata de un derecho no sujeto a solicitud y, por tanto, no sujeto a las previsiones del artículo 28.3.e) del RGPD. Pese a ello, en aquellos casos en que el encargado deba realizar la recogida de datos es recomendable establecer en el acuerdo o acto jurídico la forma y el momento en que debe darse el derecho de información.
LA COLABORACIÓN EN EL CUMPLIMIENTO DE LAS OBLIGACIONES DEL RESPONSABLE	Se debe establecer la forma en que el encargado ayudará al responsable a garantizar el cumplimiento de las obligaciones relativas a la aplicación de las medidas de seguridad que correspondan, la notificación de violaciones de datos a las Autoridades de Protección de Datos, la comunicación de violaciones de datos a los interesados, la realización de las evaluaciones de impacto relativa la protección de datos y, en su caso, la realización de consultas previas. El cumplimiento de esta obligación queda supeditado a la naturaleza del tratamiento realizado y a la información que esté a disposición del encargado. El responsable puede delegar en el

	encargado el cumplimiento de estas obligaciones.
EL DESTINO DE LOS DATOS AL FINALIZAR LA PRESTACIÓN	Hay que prever si, una vez finalice la prestación de los servicios de tratamiento, el encargado del tratamiento debe proceder a la supresión o a la devolución de los datos personales y de cualquier copia existente, ya sea al responsable o a otro encargado designado por el responsable. El acuerdo debe establecer de forma clara cuál de las dos opciones es la elegida por el responsable, así como la forma y el plazo en que debe cumplirse. En todo caso, los datos deberán ser devueltos al responsable cuando se requiera la conservación de los datos personales, en virtud del Derecho de la Unión o de los Estados miembros. No obstante, el encargado puede conservar una copia con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación. Sin embargo, en el artículo 28.3.g) del RGPD, a diferencia de lo que se decía en el artículo 22 del RLOPD, no se hace referencia a esta posibilidad de conservar los datos bloqueados a efectos de defensa frente a posibles responsabilidades en las que pudiera incurrir el encargado.
LA COLABORACIÓN CON EL RESPONSABLE PARA DEMOSTRAR EL CUMPLIMIENTO	Es preciso establecer la obligación del encargado de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, realizadas por el responsable o por otro auditor autorizado por el responsable.

La figura del Delegado de protección de datos

El nuevo Reglamento General de Protección de Datos (RGPD) que entró en vigor en mayo de 2016 será aplicable a partir de mayo de 2018. Este período transitorio en el que conviven ambas normativas sirve también como un período amplio de adaptación a la nueva norma.

El nuevo Reglamento no se aleja en exceso de la normativa anterior, no obstante, sí que plantea nuevas exigencias y un cambio de mentalidad en la aplicación de la norma y de la concepción de la protección de los datos personales, virando hacia una actitud proactiva que tiene su reflejo en una serie de medidas.

En esta línea se crea una nueva figura, la del Delegado de Protección de Datos (DPD). En el caso de las autoridades y organismos públicos es de creación **obligatoria**, si bien, el RGPD deja margen en cuanto a la forma en que puede configurarse.

Los aspectos más importantes a tener en cuenta son:

- **Carácter obligatorio para los organismos públicos**
- **Cualificación profesional:** que aúne el conocimiento de la legislación y la práctica de la protección de datos.
- **Requisitos principales:**
  - Total autonomía en el ejercicio de sus funciones
  - Relación con el nivel superior de la dirección
  - Obligación de que disponga de todos los recursos necesarios para desarrollar su actividad
- Dedicación a **tiempo completo o parcial**, siempre que se evite el conflicto de intereses.
- **Podrá existir un único delegado de protección de datos** para varias autoridades u organismos públicos en función de su **estructura organizativa y su tamaño** (art. 37).
- **Funciones** (art. 39):
  - Información y asesoramiento al responsable o encargado del tratamiento y empleados respecto de sus obligaciones en la materia
  - Supervisar el cumplimiento de lo dispuesto en el RGPD (incluyendo la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes).
  - Asesoramiento en la evaluación de impacto relativa a la protección de datos
  - Cooperar con la autoridad de control
  - Actuar como punto de contacto de la autoridad de control

También debe tenerse en cuenta lo expresado por el *Grupo del artículo 29,* como órgano consultivo independiente de la Unión Europea en materia de protección de datos y privacidad, en su informe “Directrices sobre los Delegados de la protección de datos” de 13 de diciembre de 2016.

En dicho documento, este órgano considera como elemento nuclear para este *nuevo marco jurídico de cumplimiento modernizado basado en la rendición de cuentas* la figura del Delegado de Protección de

Datos (DPD). De su análisis **interesa resaltar los siguientes aspectos que vienen a completar y matizar lo anteriormente expuesto**:

- **Disponibilidad y accesibilidad:** los datos de contacto del DPD serán conocidos dentro y fuera de la organización para garantizar una comunicación eficaz.
- Deberá tener **suficiente comprensión de las operaciones de tratamiento llevadas a cabo y los sistemas de información**, así como de las necesidades de seguridad y protección de los datos del responsable del tratamiento.
- Integridad y nivel elevado de **ética profesional.**
- **Implicación** del DPD **en todas las cuestiones relacionadas con la protección de datos personales.**
- La organización debe **respaldar** a su DPD proporcionando los **recursos** necesarios para llevar a cabo sus tareas y para que acceda a los datos personales y a las operaciones de tratamiento, así como para mantener su conocimiento experto (formación). Este respaldo **se concretaría en**:
  - **Apoyo** de la alta dirección.
  - **Tiempo suficiente** para cumplir con sus funciones.
  - Apoyo adecuado en cuanto a **recursos económicos, infraestructura y personal**.
  - **Formación** continua.
  - **Equipo del DPD**: en función del tamaño y la estructura de la organización puede ser necesario establecer un equipo. Cuanto más complejas o sensibles sean las operaciones de tratamiento más recursos deberán destinarse al DPD.
  - **No podrán ser destituidos ni penalizados** por el responsable o encargado por llevar a cabo sus funciones.
  - Posibilidad de **compatibilización de funciones** pero evitando siempre el conflicto de interés.
- **Funciones**:
  - Controlar el cumplimiento de la NGPD.
  - Ayudar al responsable o al encargado del tratamiento a controlar el cumplimento interno del reglamento:
    - Recabar información para determinar las actividades de tratamiento.
    - Analizar y comprobar la conformidad de las actividades de tratamiento.
    - Informar, asesorar y emitir recomendaciones al responsable o al encargado del tratamiento.
  - Asesoramiento al responsable del tratamiento:
    - Procedencia o no de una evaluación de impacto de protección de datos.
    - Metodología para efectuarla.
    - Uso de recursos propios o ajenos en la misma.
    - Deberá considerar debidamente el riesgo asociado a las operaciones de tratamiento, teniendo en cuenta la naturaleza, alcance, contexto y fines del tratamiento.
    - Podrá establecerse como una de sus funciones el mantenimiento de los registros de los tratamientos de datos que se llevan a cabo en la organización.

Escenarios analizados:

A. Un único DPD a nivel del Ministerio o Secretaría de Estado.
B. Un único DPD a nivel de Ministerio o Secretaría de Estado con un equipo multidisciplinar con representación de las entidades y servicios comunes (INSS, ISM, TGSS, GISS…).
C. Un DPD por entidad o servicio común (con o sin equipo).
D. Un DPD por entidad o servicio común con un coordinador a nivel de Ministerio o coordinación rotativa entre los distintos responsables.

Dentro de los posibles escenarios analizados podrían considerarse como **más adecuados** para favorecer la eficacia de la actuación del DPD aquellos que suponen **la existencia de un Delegado por entidad con o sin fórmulas de coordinación específicas.** Los principales argumentos en los que se apoya dicho análisis son los siguientes:

Volumen de gestión

El volumen de gestión de la entidad, y su traducción en el consiguiente tratamiento de datos necesario para llevar a cabo dicha gestión, avala la propuesta de disponer de un Delegado de Protección de Datos específico en el INSS. En el cuadro se reflejan los datos más relevantes referidos al ejercicio 2015.

Actuaciones más relevantes desarrolladas durante el ejercicio	Datos básicos
Pensiones en vigor a 31 de diciembre	9.353.988
Prestaciones gestionadas en 2015	1.762.026
Presupuesto total	120.491,40 millones de €
Gasto en prestaciones económicas	119.473,12 millones de €
Plantilla	11.425
Consultas presenciales atendidas	11.808.602
Consultas telefónicas atendidas	1.117.528
Trámites realizados a través del Registro Electrónico	84.412

Volumen de tratamiento de datos personales

A los datos arriba reflejados también hay que sumar el número de ficheros declarados ante la Agencia Española de Protección de Datos (AEPD) por parte del INSS que alcanzan los **1330 ficheros**. Para poner en valor esta cifra puede compararse con la de otras entidades dentro de la Secretaría de Estado, como es la Tesorería General de la Seguridad Social (TGSS), servicio común que tiene declarados en todo el territorio 375 ficheros.

Volumen de datos sensibles

De los ficheros declarados por nuestra entidad, la mayor parte son de **nivel de seguridad medio o alto**, lo que implica la articulación de medidas de seguridad más exigentes, en particular, cuando se trata de datos especialmente sensibles, como son los datos de salud, cuyo tratamiento es clave en una importante parte de nuestra gestión diaria y que obliga a prestar una especial atención en la estrategia para salvaguardar la seguridad de esta información.

Dispersión geográfica de los centros de tratamiento

Otro aspecto a considerar es la dispersión geográfica de los centros de gestión donde se tratan los datos. Del mismo modo que ocurre con la plantilla con acceso a datos y a su tratamiento.

Estas circunstancias añaden un plus de complejidad a la gestión de la seguridad de los datos tratados y exigen un control y supervisión más estrechos. En este sentido, también es importante señalar que el nuevo Reglamento incide en la accesibilidad del DPD, esa accesibilidad se verá mejorada en la forma en que el ámbito de actuación del DPD se limite a una única entidad.

Peculiaridades del tratamiento y nivel de sensibilidad de la gestión ante modificaciones

Asimismo, como establece la nueva normativa, el DPD debe conocer el funcionamiento de la organización y tener un perfil jurídico-técnico. En el caso de nuestra entidad, este aspecto cobra especial relevancia puesto que la seguridad de los datos, las medidas de seguridad que se establezcan para garantizarla y su influencia en la gestión diaria están estrechamente ligadas dado que la gestión que tenemos encomendada se basa en su práctica totalidad en la gestión intensiva de datos. Por tanto, el DPD **deberá ser capaz de aunar en la estrategia de protección de datos el establecimiento de los mayores estándares de seguridad con el mantenimiento, e incluso mejora, de la agilidad y eficacia de la gestión. Por ello debería tratarse de una persona que conozca de cerca la gestión del INSS,** las peculiaridades del tratamiento de datos en nuestra entidad, que lo diferencian de los tratamientos llevados a cabo por otras entidades y servicios comunes, así como la influencia en la gestión de las medidas de seguridad que puedan establecerse. Para completar su perfil, el DPD debería contar con apoyo técnico bien a través de un especialista o bien con un pequeño equipo en el que se integrara también personal con esa cualificación técnica específica.

Perfil del Delegado de Protección de Datos

Por tanto, como resultado de este análisis, se considera que **no sería recomendable**, en ningún caso, **que el DPD fuera ajeno a la entidad** o con un perfil eminentemente técnico, pues debe tener un alto grado de comprensión del tratamiento de datos que se realiza en el INSS a través de su red de DDPP y a nivel centralizado, así como de las interrelaciones con otras entidades y AAPP, **no sólo para llevar a cabo sus funciones de la forma más adecuada sino también para hacerlo en línea con una gestión ágil y eficiente de las prestaciones y los servicios que son nuestra razón de ser.**

Coordinación de actividades

En cuanto a la **coordinación de las actividades de los DPD** de las distintas entidades, si bien, el Reglamento establece que el delegado deberá gozar de autonomía en su actividad esto no obsta para que en aras al establecimiento de estándares, pautas o actuaciones coordinadas se establezca algún tipo de mecanismo de coordinación entre los distintos delegados de protección de datos de las entidades. En función de la consideración que se haga de las necesidades de coordinación que puedan existir este mecanismo podrá consistir en:

- Coordinador a nivel de Ministerio o Secretaría de Estado
- Coordinación rotativa entre los distintos responsables
- Establecimiento de un Comité Asesor o Consultivo u órgano colegiado análogo
- Reuniones de coordinación entre DPD sin el establecimiento de la figura de un coordinador como tal

CUADRO RESUMEN: PRINCIPALES VENTAJAS E INCONVENIENTES DE LOS DISTINTOS ESCENARIOS ESTUDIADOS

A. UN ÚNICO DPD A NIVEL DE MINISTERIO

VENTAJAS	INCONVENIENTES
‣ Centralización ‣ Homogeneidad	‣ Dimensión de la organización ‣ Volumen de datos tratados ‣ Diferencias entre las entidades y SSCC ‣ Dispersión geográfica ‣ Desconocimiento operativo de las entidades ‣ Menor capacidad de control y supervisión ‣ Menor accesibilidad

B. UN ÚNICO DPD A NIVEL DE MINISTERIO CON UN EQUIPO MULTIDISCIPLINAR CON REPRESENTACIÓN DE LAS ENTIDADES Y SSCC (INSS, ISM, TGSS, GISS)

VENTAJAS	INCONVENIENTES
‣ Centralización ‣ Homogeneidad ‣ Coordinación y colaboración entre entidades	‣ Dimensión de la organización ‣ Volumen de datos tratados ‣ Dispersión geográfica ‣ Menor capacidad de control y supervisión ‣ Menor accesibilidad

C. UN DPD POR ENTIDAD O SERVICIO COMÚN (CON O SIN EQUIPO) INDEPENDIENTE

VENTAJAS	INCONVENIENTES
‣ Dimensión ‣ Volumen de datos tratados ‣ Peculiaridades en el tratamiento entre las entidades y SSCC ‣ Dispersión geográfica ‣ Conocimiento operativo de cada Entidad/SC ‣ Capacidad de control y supervisión ‣ Mayor accesibilidad ‣ Grado de autonomía	‣ Coordinación ‣ Homogeneidad

D. UN DPD POR ENTIDAD O SERVICIO COMÚN CON UN COORDINADOR A NIVEL DE MINISTERIO O COORDINACIÓN ROTATIVA ENTRE LOS DISTINTOS RESPONSABLES O UN COMITÉ ASESOR

VENTAJAS	INCONVENIENTES
‣ Dimensión ‣ Volumen de datos tratados ‣ Peculiaridades en el tratamiento entre las entidades y SSCC ‣ Dispersión geográfica ‣ Conocimiento operativo de cada Entidad/SC ‣ Coordinación entre entidades ‣ Tendencia a la homogeneidad ‣ Capacidad de control y supervisión	‣ Grado de autonomía

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

Este 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 casilla (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 DPD o SPD (valorar la propuesta de este informe respecto a una unidad con tres pilares: jurídico, gestión y experiencia teórico-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 geográfica) 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 cada 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**.						

17. **Articulación de mecanismos** (debe ser igual de fácil darlo que retirarlo) **e impartición de instrucciones** respecto a la **retirada del consentimiento.** 18. Estudio especial de los casos en los que los **datos no se obtienen directamente de los interesados (cesión legítima de datos)**. 19. Identificación y cumplimiento de la **obligación de informar** a estos efectos salvo que pueda aplicarse la excepción del artículo 14.5.c del RGPD. 20. Estudio de los tratamientos relativos a **infracciones y sanciones administrativas** y si se cumplen las condiciones para dicho tratamiento (en caso de confirmarse la redacción del art. 47 PLOPD). 21. Aplicación de lo anterior a los **tratamientos de datos respecto del personal.**						
22. **Obtención y/o determinación del resto de datos necesarios para elaborar el registro de actividades de tratamiento** (nombre y datos de contacto del responsable, posibles corresponsables, del representante y del DPD; fines del tratamiento; descripción de categorías de interesados y de datos personales; categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales; transferencias de datos a terceros países u organizaciones de internacionales; plazos previstos para la supresión de las diferentes categorías de datos (cuando sea posible); descripción general de las medidas técnicas y organizativas de seguridad (cuando sea posible)) 23. Incorporación de los datos en el **registro de actividades de tratamiento**.						
24. **Comunicar las modificaciones que se produzcan en el registro de actividades de tratamiento al DPD.**						
25. Elaboración y publicación por medios electrónicos del **Inventario de actividades de tratamiento** (que resultará de añadir la base legal del tratamiento a lo ya contenido en el Registro de actividades de tratamiento) Este será centralizado o descentralizado en función de los criterios que se hayan establecido en el punto 7. Para ello deberá confirmarse la redacción del PLOPD en este particular. 26. **Difusión**, al menos, entre el personal del emplazamiento donde vaya a ubicarse.						
27. **Adaptación** (a los requerimientos del principio de transparencia e información) **y rediseño** (a efectos de ubicación y visibilidad de la información), en su caso, de los **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**. 28. Aplicación, en su caso, a los **tratamientos de datos internos** respecto de nuestro personal. 29. Articular los **mecanismos para acreditar que se ha cumplido con el deber de informar**. 30. Comprobación de que se cumple con el deber de informar en el caso de **videovigilancia** (instrucciones e informe de la DP en el que se garantice que se cumple con estas exigencias: cartelería, ubicación, contenido del dispositivo informativo, información disponible para los interesados).						

31. Análisis del **alcance jurídico** del régimen de protección de datos en caso de **transferencias internacionales** y el posible impacto de éste en nuestra gestión. 32. Efectuar las adaptaciones que sean oportunas.						
33. 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. 34. Efectuar las adaptaciones que sean necesarias.						
35. **Análisis de los tratamientos para verificar que se están realizando según los principios del nuevo Reglamento**, en especial, en cuanto a la minimización de datos y la limitación del plazo de conservación.						
36. Verificación y, en su caso, adaptación –técnica, impartición de instrucciones, introducción de modificaciones en los procesos que sea necesario- a lo establecido en el proyecto de LO –DA novena- *(de confirmarse su redacción en los términos actuales)* respecto de la identificación de los interesados en las notificaciones por medio de **anuncios y publicaciones de actos administrativos**.						
37. **Estudio** de los **nuevos derechos ARCO+** y su régimen de ejercicio. 38. **Desarrollo de mecanismos para su ejercicio.**						
39. **Elaboración de un Protocolo de derechos ARCO+.** 40. Edición de **formularios** para el ejercicio de los mismos. 41. **Publicación** en la Intranet corporativa y en el **aplicativo** CAISSGestiona. 42. **Difusión** entre el personal de la Entidad. 43. Puesta a disposición de la información y formularios por **medios electrónicos**. 44. Posible edición de un **díptico informativo** para los interesados (análisis del artículo 12 del PLOPD).						
45. Adopción de una **metodología de análisis de riesgos**.						
46. **Realizar los análisis de riesgos de los tratamientos existentes y que puedan realizarse en el futuro.**						
47. Determinación de las **medidas de seguridad aplicables** (valoración de las medidas aplicables hasta la fecha, con especial incidencia en los tratamientos mixtos y no automatizados, desde el **nuevo enfoque del riesgo para los derechos y libertades de los interesados** que incluye el uso responsable de los datos, la autolimitación de los tratamientos y sus plazos de conservación; también **deberá valorarse** el mantenimiento o supresión de los documentos de seguridad, del régimen actual de auditorías bienales, objetivo institucional que controla su cumplimiento; valoración de la **aplicabilidad de la medida de seguridad de seudonimización en nuestro ámbito** tanto para los tratamientos automatizados como no automatizados y mixtos). 48. 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.						
49. Adopción de una **metodología evaluación de impacto de protección de datos**.						
50. **Llevar a cabo las evaluaciones de impacto de protección de datos** (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.						
51. Determinación de **medidas de seguridad** aplicables **o elevación de consulta**, en su caso. En este punto es aplicable parte de lo expuesto en el punto 47.						
52. Seguimiento de las decisiones en esta materia (publicación de tratamientos que sean considerados como de alto riesgo susceptibles de EIPD) por parte de las autoridades en materia de protección de datos tanto europeas como nacionales.						
53. Implantación **de las medidas que se hayan determinado según el resultado del análisis de riesgo y, en su caso, de la EIPD.**						
54. Definición de qué constituye una **violación o quiebra de seguridad**. 55. **Protocolos de actuación** (con la posible edición de instrucciones o guías de actuación ante la casuística más frecuente) **y**, en su caso, **notificación**. 56. **Establecer la forma de documentación y registro de las violaciones o quiebras de seguridad detectadas**.						
57. **Contratación administrativa**. Adaptación de las **cláusulas de confidencialidad**. 58. **Detección** de la existencia de encargos de tratamiento no regularizados. 59. Revisión o elaboración, en su caso, de los **contratos de encargo de tratamiento** (o acto administrativo, cuando proceda). En este sentido habrá de tenerse en cuenta si la nueva LOPD ya es aplicable o no. 60. **Adaptación** a las premisas del contenido y regulación del encargo de tratamiento de la **norma reguladora de las competencias** de la GISS. 61. Dictado de **instrucciones** para la selección de **encargados de tratamiento que ofrezcan las garantías** establecidas en la norma. 62. Elaboración de un **clausulado y pliegos tipo**.						
63. Participación en proyectos como asesores a efectos de aplicar la **protección de datos desde el diseño y por defecto.**						
64. Emisión de **instrucciones** generales (ámbito centralizado y descentralizado). Acciones de **comunicación interna**. Impartición de **formación**.						
65. **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 solicitudes formuladas por medios electrónicos a la que habilita la DA 10ª del proyecto de LO.						

ANEXO VII. **BIBLIOGRAFÍA CONSULTADA**

- **Normativa**:
  - 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).
  - Proyecto de ley orgánica de protección de datos según lo publicado en el Boletín Oficial de las Cortes Generales en fecha 24 de noviembre 2017.
  - Borrador de Resolución del Secretario de Estado de la Seguridad Social por la que se designa Delegado de Protección de Datos de la Administración de la Seguridad Social.

- **Libros y manuales de referencia**:
  - Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad. José Luis Pilar Mañas.
  - Practicum de protección de datos 2018. Thomson Reuters.
  - Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo. Luis Felipe López Álvarez. Claves Prácticas Francis Lefevre.

- **Guías, informes y directrices**:
  - Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. Agencia Española de Protección de Datos en colaboración con las Agencias vasca y catalana de protección de datos.
  - Guía para el cumplimiento del deber de informar. Agencia Española de Protección de Datos en colaboración con las Agencias vasca y catalana de protección de datos.
  - Informe “El impacto del Reglamento General de Protección de Datos sobre la actividad de las administraciones públicas” publicado por la Agencia Española de Protección de Datos.
  - Guía para una Evaluación de Impacto en la protección de datos personales, publicada por la Agencia Española de Protección de Datos.
  - Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento. Agencia Española de Protección de Datos en colaboración con las Agencias vasca y catalana de protección de datos.
  - Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Grupo “Protección de datos” del artículo 29.

ANEXO. 5

NORMATIVA REGULADORA DEL DELEGADO DE PROTECCIÓN DE DATOS DE LA SEGURIDAD SOCIAL

MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

Resolución de 17 de abril de 2018, de la Secretaría de Estado de la Seguridad Social, sobre funciones del Delegado de protección de datos de la Seguridad Social y creación de la Comisión de protección de datos de la Administración de la Seguridad Social.

El artículo 37.1 del 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), prevé la existencia de un Delegado de protección de datos siempre que los tratamientos de datos de carácter personal y el resto de operaciones a los que se refiere el citado reglamento los lleve a cabo una autoridad u organismo público. Por su parte, en su artículo 37.3 se prevé la posibilidad de designar un único Delegado de protección de datos para varias autoridades u organismos cuando así parezca adecuado en atención a su estructura, circunstancia esta que concurre en el ámbito de la Administración de la Seguridad Social, cuya estructura básica se articula sobre la base de distintas entidades gestoras y servicios comunes para el cumplimiento de los fines de la Seguridad Social. A tal efecto, cabe señalar que en el Consejo General de Administración Electrónica de la Seguridad Social de fecha 31 de enero de 2017, con la asistencia de los distintos responsables y encargados de tratamiento, se tomó el acuerdo de que existiera un único Delegado de protección de datos en el ámbito de la Secretaría de Estado de la Seguridad Social.

El Delegado de protección de datos, en atención a lo previsto en el artículo 37.5 del Reglamento (UE) 2016/679, de 27 de abril de 2016, debe ser designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones previstas en el artículo 39 del citado reglamento comunitario.

Asimismo, la Agencia Española de Protección de Datos ha emitido diversas recomendaciones y criterios en relación con la designación y funciones del Delegado de protección de datos en el ámbito de las administraciones públicas, recomendaciones que se siguen en la adopción de esta resolución.

En consecuencia, en atención a las facultades atribuidas a esta Secretaría de Estado por el artículo 5 del Real Decreto 703/2017, de 7 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Empleo y Seguridad Social y se modifica el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales, y oídas las consideraciones efectuadas por la Agencia Española de Protección de Datos, vengo a dictar las siguientes instrucciones:

Primera. *Ámbito de aplicación.*

A efectos de esta resolución, las funciones del Delegado de protección de datos de la Seguridad Social se extenderán al ámbito de las entidades gestoras y servicios comunes dependientes de la Secretaría de Estado de la Seguridad Social y a aquellos otros centros directivos, órganos o unidades dependientes de la Secretaría de Estado de la Seguridad Social que lleven a cabo tratamientos de datos de carácter personal.

Segunda. *Funciones del Delegado de protección de datos de la Seguridad Social.*

Son funciones del Delegado de protección de datos las previstas en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y en el resto de normativa que resulte de aplicación, entre las que cabe reseñar, en particular, las siguientes:

a) Informar y asesorar a los responsables o encargados del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en materia de protección de datos.
b) Supervisar el cumplimiento de lo dispuesto en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes.
c) Ofrecer el asesoramiento que se le solicite acerca de las evaluaciones de impacto relativas a la protección de datos y supervisar su aplicación.
d) Cooperar con la Agencia Española de Protección de Datos.
e) Actuar como punto de contacto de la Agencia Española de Protección de Datos para cuestiones relativas al tratamiento.

Asimismo, el Delegado de protección de datos de la Seguridad Social podrá llevar a efecto aquellas otras actividades de información, coordinación, supervisión, formación o consulta que, en materia de protección de datos, considere procedentes para el debido cumplimiento de la normativa de protección de datos en el ámbito de la Administración de la Seguridad Social.

Tercera. *Dirección de contacto del Delegado de protección de datos.*

La dirección de contacto del Delegado de protección de datos se publicará en la sede electrónica de la Secretaría de Estado de la Seguridad Social.

Cuarta. *Comisión de protección de datos de la Administración de la Seguridad Social.*

Para el ejercicio de sus funciones, el Delegado de protección de datos contará con el apoyo de la Comisión de protección de datos de la Administración de la Seguridad Social que se crea en esta resolución.

Formarán parte de la Comisión de protección de datos de la Administración de la Seguridad Social los subdelegados de protección de datos de cada una de las entidades, servicios, unidades, centros directivos y órganos a los que alcance lo establecido en esta resolución. A tal fin, los responsables designarán, de acuerdo con el Delegado de protección de datos, un subdelegado de protección de datos en su respectivo ámbito.

La Comisión de protección de datos de la Administración de la Seguridad Social tendrá como función contribuir a dar cumplimiento a las obligaciones establecidas en el Reglamento (UE) 2016/679, de 27 de abril de 2016, y en el resto de normativa en materia de protección de datos de carácter personal que resulte de aplicación en el ámbito de la Administración de la Seguridad Social. Con tal finalidad adoptará los acuerdos y se pronunciará sobre aquellos aspectos que resulten precisos.

La Comisión se reunirá, previa convocatoria del presidente, al menos, dos veces al año y en todos aquellos supuestos en los que, de oficio o a instancia de cualquiera de los subdelegados de protección de datos, así esté establecido en las instrucciones de desarrollo de esta resolución o cuando lo considere necesario el Delegado de protección de datos. Su régimen jurídico de funcionamiento se ajustará a lo previsto para los órganos colegiados en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Quinta. *Composición y funcionamiento de la Comisión de protección de datos de la Administración de la Seguridad Social.*

La Comisión de protección de datos de la Administración de la Seguridad estará presidida por el Delegado de protección de datos de la Seguridad Social.

Actuará como vicepresidente el Letrado-jefe de la Unidad de asesoramiento de la Dirección del Servicio Jurídico de la Administración de la Seguridad Social, que sustituirá al presidente en caso de ausencia, vacante o enfermedad. En las instrucciones que se dicten en desarrollo de esta resolución, el Delegado de protección de datos, en atención al apoyo que precise, podrá atribuir funciones específicas a cada uno de los miembros de la Comisión.

Formarán parte de la Comisión de protección de datos de la Administración de la Seguridad Social, como vocales, los subdelegados de protección de datos de la Tesorería General de

la Seguridad Social, del Instituto Nacional de la Seguridad Social, del Instituto Social de la Marina, de la Gerencia de Informática de la Seguridad Social, de la Intervención General de la Seguridad Social y de la Dirección General de Ordenación de la Seguridad Social. Asimismo, podrá incorporarse a la Comisión un representante de la Secretaria de Estado de la Seguridad Social. En caso de ser necesario podrá acordarse la asistencia, en calidad de asesores, con voz pero sin voto, de las personas que se estime conveniente en atención de los temas a tratar.

Actuará como secretario de la Comisión, con voz pero sin voto, un Letrado de la Administración de la Seguridad Social adscrito a la Dirección del Servicio Jurídico de la Administración de la Seguridad Social.

Sexta. *Relación de miembros de la Comisión de protección de datos de la Administración de la Seguridad Social.*

En anexo a esta resolución se recogen los miembros de la Comisión de protección de datos de la Administración de la Seguridad Social, identificando al Delegado de protección de datos de la Seguridad Social, que actuará como presidente, en la persona titular de la Dirección del Servicio Jurídico de la Administración de la Seguridad Social, conforme al acuerdo adoptado en el Consejo General de Administración Electrónica de la Seguridad Social y a su designación mediante Resolución de 6 de marzo de 2018 , de la Subsecretaría del Ministerio de Empleo y Seguridad Social . Asimismo, y como vicepresidente y vocales de la Comisión, se identifican, en el anexo, a los subdelegados de protección de datos de cada una de las entidades, centros directivos, órganos y unidades que la integran, y el Letrado que actuará como secretario de la misma.

El Delegado de protección de datos mantendrá actualizada la relación de subdelegados de protección de datos que forman parte de la Comisión. Para ello, a propuesta de los respectivos responsables y encargados del tratamiento, modificará la relación que figura como anexo a esta resolución.

Séptima. *Los subdelegados de protección de datos.*

Los subdelegados de protección de datos de cada entidad, centro directivo, órgano o unidad de la Administración de la Seguridad Social actuarán bajo la dirección y coordinación del Delegado de protección de datos de la Seguridad Social, dentro del ámbito de competencias que a este último le atribuye el Reglamento (UE) 2016/679, de 27 de abril de 2016, y el resto de normativa aplicable. En el Servicio Jurídico de la Administración de la Seguridad Social, el Letrado-jefe de la Unidad de Asesoramiento actuará como subdelegado de protección de datos.

Los subdelegados de protección de datos ejercerán, en su ámbito, las funciones de información, asesoramiento y supervisión que les encomiende el Delegado de protección de datos. Los subdelegados de protección de datos darán cuenta al Delegado de protección de datos de las actuaciones que lleven a efecto en relación con el cumplimiento de sus funciones. El Delegado de protección de datos podrá establecer los criterios que considere necesarios para la actuación homogénea y coordinada de los distintos subdelegados de protección de datos.

Octava. *Peticiones, consultas o reclamaciones en materia de protección de datos.*

En el ámbito de la Administración de la Seguridad Social se establecerán los mecanismos y procedimientos necesarios para dar una respuesta rápida a los interesados que formulen peticiones, consultas o reclamaciones en materia de protección de datos. A tal fin, el Delegado de protección de datos establecerá los procedimientos a seguir para tramitar y dar respuesta a las posibles peticiones o quejas que puedan formular los interesados.

Novena. *Colaboración de la Gerencia de Informática de la Seguridad Social y otros órganos con el Delegado de* protección de datos.

En atención a sus competencias y a sus recursos materiales y humanos, la Gerencia de Informática de la Seguridad Social prestará al Delegado de protección de datos la colaboración técnica que este le requiera para el debido cumplimiento de sus funciones.

Las comisiones, comités y otros órganos que puedan existir en el ámbito de la Secretaria de Estado de la Seguridad Social podrán solicitar el asesoramiento del Delegado de protección de datos en relación con aquellas materias propias de su competencia.

Décima. *Respaldo al Delegado y a los subdelegados de protección de datos.*

De conformidad con lo previsto en el artículo 38.2 del Reglamento (UE) 2016/679, de 27 de abril de 2016, las entidades, centros directivos, órganos y unidades que puedan verse afectadas por lo dispuesto en esta resolución respaldarán al Delegado y a los subdelegados de protección de datos en el desempeño de sus funciones, facilitándoles los recursos necesarios para el desarrollo de dichas funciones, el acceso a los datos personales y a las operaciones de tratamiento y para el mantenimiento de sus conocimientos especializados. A tal fin, pondrán a su disposición los medios materiales o personales que, a juicio del Delegado de protección de datos, resulten precisos para el adecuado desarrollo de sus competencias.

Undécima. *Unidad de apoyo al Delegado de protección de datos.*

El Delegado de protección de datos contará con una unidad de apoyo para el adecuado desarrollo de su función, unidad que será dotada con los medios personales y materiales necesarios para dar debido cumplimiento a sus cometidos.

Duodécima. *Participación en reuniones y solicitud de asesoramiento.*

El Delegado de protección de datos, o el miembro o miembros de la Comisión de protección de datos de la Administración de la Seguridad Social a quien este designe, participará en aquellas reuniones en las que vayan a adoptarse decisiones que puedan afectar o tener incidencia sobre tratamientos de datos de carácter personal en el ámbito de la Seguridad Social. A tal fin se remitirá la oportuna convocatoria al Delegado de protección de datos en la que deberán constar los asuntos a examinar en la misma.

Decimotercera. *Posibilidad de dictar instrucciones, criterios o recomendaciones.*

El Delegado de protección de datos dictará aquellas instrucciones, criterios o recomendaciones que considere precisas para el desarrollo de lo previsto en esta resolución.

Asimismo, para el debido cumplimiento de las funciones que tiene encomendadas en la normativa de protección de datos, el Delegado de protección de datos podrá adoptar las recomendaciones que considere precisas; en todo caso, las someterá a la consideración de la Comisión de protección de datos de la Administración de la Seguridad Social con el fin de conseguir un alto grado de actuación homogénea.

Madrid, 17 de abril de 2018

El Secretario de Estado de la Seguridad Social

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
SECRETARÍA DE ESTADO DE SEGURIDAD SOCIAL

Tomás Burgos Gallego.

ANEXO

Miembros de la Comisión de protección de datos de la Administración de la Seguridad Social

- Presidenta: D.ª María Nieves Ciruelos Carrasco, Directora del Servicio Jurídico de la Administración de la Seguridad Social (designada Delegada de protección de datos mediante Resolución de 6 de marzo de 2018, de la Subsecretaría del Ministerio de Empleo y Seguridad Social).

- Vicepresidente primero: D. Alberto Llorente Álvarez, Letrado Jefe de la Unidad de Asesoramiento Jurídico del Servicio Jurídico de la Administración de la Seguridad Social.

- Vocales:

  a) D. José Manuel Aceituno Arenas, Secretario General de la Tesorería General de la Seguridad Social.

  b) D.ª Rosa María Fuentes Carretero, Secretaria General del Instituto Nacional de la Seguridad Social.

  c) D.ª Rosa del Carmen Montero González, Jefa de los Servicios de la Inspección del Instituto Social de la Marina.

  d) D.ª Concha Hortigüela Hortigüela, Directora del Centro- Dirección de Seguridad, Innovación y Comunicación de la Gerencia de Informática de la Seguridad Social.

  e) D. Gregorio González Valero, Jefe de Área de Administración Electrónica de la Intervención General de la Seguridad Social.

  f) D.ª María Cecilia de la Concha Renero, Subdirectora General de Ordenación Jurídica de la Seguridad Social de la Dirección General de Ordenación de la Seguridad Social.

- Secretaria: D.ª Pilar Canalda Ramos, Letrada del Servicio Jurídico de la Administración de la Seguridad Social.

ANEXO. 6

INSTRUCCIONES DE LA SUBDELEGADA DE PROTECCIÓN DE DATOS DEL INSS EN MATERIA DE PROTECCIÓN DE DATOS

PROTECCIÓN DE DATOS

INSS

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

INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL

SECRETARÍA GENERAL
SUBDELEGADA DE PROTECCIÓN DE DATOS

INTRODUCCIÓN

Los cambios legislativos que se han sucedido en los últimos años en materia de protección de datos personales han propiciado una actualización de las políticas de privacidad que este Instituto viene implementando con el fin de salvaguardar la integridad, confidencialidad, disponibilidad y resiliencia permanente de los datos personales obtenidos y custodiados por el mismo.

El Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), de obligado cumplimiento desde el 25 de mayo de 2018, así como la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), en vigor desde el 7 de diciembre de 2018, hacen recaer en el responsable del tratamiento de los datos personales la responsabilidad de diseñar las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar un uso adecuado de los datos personales de los ciudadanos, medidas que en todo caso deberán revisarse y actualizarse periódicamente.

Dentro de este nuevo marco normativo, el INSS está comprometido con el respeto a la intimidad del usuario. Para ello, cuenta con todos los medios técnicos a su alcance que permitan garantizar una seguridad adecuada de los datos personales, evitando la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados a dicho organismo.

En virtud de esta responsabilidad activa por la cual deben protegerse los datos desde el diseño y por defecto, resulta necesario actualizar nuestra política de privacidad apoyándonos en los siguientes principios:

1. Debemos ser **proactivos** y no reactivos, deben establecerse medidas preventivas antes que correctivas, anticipándonos a los eventos que puedan afectar a la privacidad de los datos personales;
2. Ha de establecerse una **configuración predeterminada de la privacidad**, limitando la recogida, uso y acceso a los datos personales a los estrictamente necesarios para poder lograr la finalidad del tratamiento en el cual se están utilizando;
3. En el diseño de los sistemas de información, aplicativos informáticos para la tramitación y demás servicios utilizados en la gestión ordinaria, deben **adoptarse desde su inicio las medidas necesarias** para salvaguardar la privacidad de los datos personales tratados por los mismos;
4. Ha de **asegurarse la privacidad en todo el ciclo de vida de los tratamientos**, desde su fase de diseño inicial, hasta la destrucción o archivo de los datos, pasando por la fase de gestión/tramitación.
5. **Visibilidad y transparencia**, para poder garantizar la privacidad debemos poder demostrarla, y así comprobar que es acorde con la información dada, demostrando la diligencia y responsabilidad proactiva requerida por cada tipo de tratamiento;
6. El **ciudadano siempre ha de ser el centro de nuestro enfoque**, tanto desde el punto de vista de la gestión como de la protección de datos, el fin último debe ser garantizar los derechos y libertades de los ciudadanos, tanto a nivel interno como externo, sin obviar los interese legítimos de la organización.

Por todo ello, se dictan las pautas de actuación que se exponen a continuación.

INSTRUCCIONES

PRIMERA. Digitalización y archivo electrónico de la documentación.

La 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), estableció como herramienta informática para la digitalización y archivo electrónico el aplicativo SARTIDO en su funcionalidad de gestor documental.

Por la Resolución de 23 de febrero de 2016, del Instituto Nacional de la Seguridad Social, por la que se regula la tramitación electrónica automatizada de diversos procedimientos de gestión de determinadas prestaciones del sistema de la Seguridad Social, se acordó que los expedientes administrativos generados se almacenaran en el mencionado gestor documental.

Simultáneamente, desde la Gerencia de Informática de la Seguridad Social (GISS), en desarrollo del aplicativo SARTIDO, se estableció la arquitectura compartimental del mismo, mediante el uso de carpetas y subcarpetas de archivo, editándose el documento técnico con las especificaciones formales de los códigos de Tipo de Gestión en la aplicación SARTIDO de Gestión Provincial. Documento técnico que recoge un total de 80 códigos tipo en los que encuadrar la documentación utilizada en la gestión ordinaria del INSS.

En atención a todo ello, deberá analizarse si la documentación utilizada en la gestión ordinaria de la Dirección provincial se está indexando adecuadamente en la carpeta o subcarpeta de SARTIDO correspondiente de conformidad con los códigos tipo de gestión disponibles, y en su caso establecer las medidas correctivas pertinentes. Así mismo, y debido al carácter especial de los datos personales contenidos en la documentación a integrar en las carpetas que se mencionan a continuación, se deberán adoptar las medidas siguientes:

1. Realizar una revisión y actualización del registro del personal funcionario con acceso a dichas carpetas, comprobando que se mantiene el motivo por el que requieren dicha habilitación, así como que el perfilado de usuario es acorde a las funcionalidades requeridas por el mismo.
2. Realizar un inventario en el que se recoja y clasifique la totalidad de la documentación que ha de indexarse en las carpetas y subcarpetas correspondientes, así como el código tipo de gestión documental asignado en su caso.
3. Dicho registro de usuarios e inventario de documentación, se revisarán y actualizarán anualmente, siendo objeto de supervisión por parte de la Inspección de Servicios del INSS.
4. Deberá prestarse una especial atención a la carpeta “Documentación sensible”, cuyo registro de personas autorizadas para acceder a la misma deberá estar constituido por un mínimo de 3 funcionarios y un máximo equivalente al doble de personas que integren el equipo directivo de la Dirección provincial más el número de directores de CAISS que existan en la D.P., debiéndose justificar los incrementos que superen dicha cifra.
5. Deberán analizarse de forma expresa e implementarse las medidas anteriormente expuestas respecto de las siguientes carpetas de gestión documental:

   - **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.

     La subcarpeta fija se utilizará para la documentación del expediente inicial, y las siguientes se irán creando para incorporar exclusivamente la documentación médica aportada en la reclamación, revisión, determinación de contingencia….

001-Subcarpeta fija, para la documentación médica del expediente inicial hasta la resolución del expediente.

002-Reclamación, se identificará con la misma denominación que la reclamación AAAA/NNNN incluida en la carpeta 04.

003-Revisión, se identificará con la misma denominación que la revisión AAAA/NNNN incluida en la carpeta 05.

004-Determinación de Contingencia.

005-Otros trámites.

En los expedientes de incapacidad permanente, especialmente por el volumen de documentación médica, con el fin de evitar repeticiones e indexaciones masivas e indiscriminadas, deberá seleccionarse la información, desechando informes repetidos, y en la medida de lo posible, ordenarse cronológicamente y por especialidades, lo que haría su localización más rápida y eficaz.

999-Incidencias inspección médica, recogerá las incidencias reseñables que estime el inspector médico en relación con la inspección médica realizada por él mismo a un expediente concreto.

- **06-Sentencias:** Documentación relacionada con demandas y sentencias para el trámite administrativo en las que el INSS sea parte o interesado. Se pueden crear tantas subcarpetas como demandas interpuestas o sentencias recibidas:
  001-NNNNN (nº autos, 1 a 5 dígitos) /AAAA (año, 4 dígitos) /JJJJJ nombre del juzgado o tribunal que ha dictado la sentencia (1 a 5).
  002-….

  En este clasificador se incluirán todas las sentencias de los distintos órganos judiciales, cada una en la subcarpeta correspondiente en la que además se incorporará toda la documentación que se genera de la aplicación de dichas sentencias.

  Muy Importante: cuando en el contenido de la sentencia se relaten hechos que revelen datos especialmente sensibles (malos tratos, abusos sexuales, lesiones, etc.), en esta carpeta tan solo se depositará una hoja informativa en la que se recojan los datos estrictamente necesarios para la gestión de las prestaciones, indicándose que la sentencia se encuentra indexada en la carpeta “Documentación sensible”.

- **08-Retenciones y embargos:** Documentación relativa a retenciones y embargos sobre el importe de la prestación.
  Se crearán por AAAA (años) las carpetas opcionales necesarias:
  001-AAAA/Nº de registro del embargo por año.
  002-AAAA/identifica a la entidad pública o privada que comunica el embargo. Se creará para aquellos embargos comunicados, pero no aplicables por la cuantía de pensión o por quedar a la espera.

- **13-Control de deudas:** Documentación generada desde la declaración de deudor hasta la cancelación de la deuda. Se crearán tantas subcarpetas como deudas.
  001-AAAA (año)/NNNN (nº de MIDAS)
  Los inicios de deuda automáticos que vayan a la carpeta 10-Control de pensiones, se quedarán allí y el resto de la documentación se escaneará en esta carpeta.
  002-AAAA/nº MIDAS.
  003-….

- **14-Servicio jurídico:** Documentación de expedientes del servicio jurídico, que no corresponde al expediente administrativo.
  Carpeta de acceso limitado, la incorporación de documentos se realiza por el personal de este servicio conforme a sus propios criterios.
  Recomendación: incluir en el nombre de la subcarpeta opcional el nº de demanda o el nº de expediente jurídico.

- **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**, 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.
  001-Documentación sensible.

- **97-Carpeta expediente electrónico judicial:** Documentos que integran el expediente electrónico remitido al Juzgado o Tribunal a través de la plataforma de interconexión con la administración de justicia, y que no se incluye en la carpeta 14-Servicio jurídico.
  001-Expediente electrónico judicial

- **99-Carpeta Puente:** Documentación pendiente de asignar a la carpeta correspondiente. La documentación se deberá incorporar diariamente a la carpeta adecuada.
  001-Carpeta puente (Subcarpeta fija)
  Subcarpetas opcionales sólo para SARTIDO 3.0

Cuestiones a tener en cuenta para facilitar la identificación, localización e incorporación de los documentos:

- Las subcarpetas opcionales, pueden tener una longitud máxima de 32 caracteres, incluidos los tres dígitos numéricos asignados automáticamente desde la aplicación, pueden incluir caracteres alfabéticos y numéricos, además de los siguientes símbolos /, -, y el espacio en blanco.
- Las subcarpetas con nº de autos deben de ceñirse al siguiente formato:
  001-NNNN (nº autos, 1 a 5 dígitos) /AAAA (año, 4 dígitos)-nombre del juzgado o tribunal que ha dictado la sentencia (1 a 5).
- En la carpeta 01-expediente inicial, las páginas de documentación aportada para Registro de salida SICRES pueden ser identificadas ya que la aplicación permite el cambio de nombre. Sin embargo, las páginas de documentación procedente de Registro de entrada no permiten el cambio de nombre.
- Se pueden mover imágenes de un expediente a otro excepto aquellas incorporadas con el código de barras procedente de alguna aplicación corporativa, salvo que hayan sido trasladadas previamente desde Registro.

SEGUNDA. Bloqueo/Marcaje de expedientes.

El protocolo por el que se aprueba 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 las personas que así lo hubieran solicitado", vigente en la actualidad, establece las pautas a seguir para poder realizar el marcaje/bloqueo en las bases de datos y sistemas de información en los que consten expedientes con datos personales de los ciudadanos solicitantes de tales medidas.

Con el bloqueo de datos se restringe el acceso a los mismos, mediante la anotación de una marca por la GISS y el bloqueo, por los propios Centros de Desarrollo de las Entidades, respecto de los datos obrantes

en sus respectivas bases de datos y gestores documentales, impidiendo el acceso de los usuarios, salvo los que especialmente estuviesen autorizados, emitiéndose un mensaje referido al bloqueo en todas las transacciones informáticas utilizadas en la gestión.

En el ámbito de nuestra Entidad, dichas actuaciones se realizan a través de las transacciones del sistema SILCON, opción 5 del menú: Aplicaciones de prestaciones (SILSSP), opción 11: Gestión de Usuarios con Acceso a Datos Protegidos, opciones: 1) Alta de usuario, 2) Baja de Usuario y 3) Consulta de usuario. Pudiéndose acceder directamente a través de la transacción PDP61.

Con la finalidad de ir un paso más allá e implementar el principio de responsabilidad proactiva en la revisión de tal procedimiento de actuación, se deberán adoptar las siguientes medidas:

1. Realizar un registro del personal funcionario habilitado para poder acceder a los expedientes marcados/bloqueados cuando así lo requieran los trámites administrativos de gestión, indicando la unidad de destino y fecha en la que se permite o restringe el acceso a los expedientes bloqueados. Dicho registro deberá estar constituido por un mínimo de 3 funcionarios y un máximo equivalente al doble de personas que integren el equipo directivo de la Dirección provincial más el número de directores de CAISS que existan en la D.P., debiéndose justificar los incrementos que superen dicha cifra.
2. El registro de personal autorizado se revisará y actualizará semestralmente.
3. Desde la Dirección provincial se deberá realizar un seguimiento en prensa y medios de comunicación de las noticias referidas a casos de violencia de género que se produzcan en su ámbito geográfico, analizando si las posibles víctimas son beneficiarias, perceptoras o causantes de alguna de las prestaciones cuya gestión tiene encomendada el INSS, procediéndose al marcaje/bloqueo de oficio de los expedientes que pudiesen resultar afectados.

¿Cómo actuar cuando un ciudadano/ una ciudadana, con sus datos bloqueados/ocultados, se persona en un CAISS para solicitar un servicio?

1. Cuando esté realizando una solicitud de un servicio que contenga datos personales, la entrega o comunicación de estos, ha de ser realizada exclusivamente por y al titular de los datos en cuestión, debiendo de estar identificado mediante DNI o documento equivalente.
2. La solicitud se ha de realizar siempre por escrito, en los formularios establecidos al efecto, debiendo estar firmada por la persona interesada. En estos supuestos solo se admitirá la representación del interesado de forma excepcional, máxime cuando la persona que aparentemente asume la representación sea la pareja o cónyuge de la persona interesada.
3. En el registro de entrada, que será remitido, en todo caso, al director/a provincial, solo deberá figurar el nombre y apellidos de la persona solicitante, indicando en observaciones “DATOS PROTEGIDOS”. (no deberá escanearse ningún documento en el registro,)
4. El director del CAISS, indexará la solicitud y documentación aportada en la carpeta “documentación sensible” de SARTIDO, o en su defecto, remitirá la documentación por valija, en sobre cerrado con indicación de “DATOS PROTEGIDOS”.
5. Una vez recibida la solicitud en la Dirección provincial y realizada la gestión correspondiente, la resolución de esta se remitirá al director del CAISS, por correo electrónico encriptado o por valija, en sobre cerrado con la indicación de “DATOS PROTEGIDOS”.
6. La entrega de la resolución o documentación correspondiente se realizará, exclusivamente, a la persona titular de los datos, debiendo firmar ésta un acuse de recibo de este, que será indexada en la mencionada carpeta de “documentación sensible” de SARTIDO por parte del director del CAISS.

MUY IMPORTANTE: El bloqueo, marcaje u ocultación de los datos personales de las personas interesadas, en ningún caso supone impedimento alguno para tramitar cualquiera de las prestaciones o realizar alguno de los

servicios competencia u ofertados por el INSS, tan solo supone restringir el acceso a los expedientes de las personas interesadas a la generalidad de los funcionarios, de tal forma que solo pueden ser accesibles a los funcionarios habilitados para consultar dichos datos/expedientes. Nunca se podrá denegar un servicio, gestión o información solicitada por una persona cuyos datos estén bloqueados por no ser visibles al funcionario que esté atendiendo la solicitud, resultando imprescindible que todos los empleados de la entidad sean conocedores de las personas habilitadas para acceder a dichos expedientes bloqueados, para que sean estos últimos quienes en todo momento puedan atender a las personas cuyos datos/expedientes estén bloqueados.

TERCERA. Traslado y trasmisión de documentación a otros organismos.

En atención a la labor prestacional realizada por este Instituto y la información de carácter personal que custodia en sus bases de datos y sistemas de información, son múltiples las peticiones y actuaciones de suministro de información recibidas y realizadas en y por nuestra organización en los supuestos en los que la ley habilita a ello.

A pesar de las prescripciones establecidas por la LOPDGDD en cuanto a la potestad de verificación de las Administraciones Públicas respecto de los datos personales de los interesados en las solicitudes presentadas ante las mismas (DA Octava) y la legitimación de los tratamientos de datos personales en cumplimiento de una obligación legal o el ejercicio de poderes públicos exigible al responsable del tratamiento (art.6.1 c) y e) del RGPD), los datos obtenidos por la Administración de la Seguridad Social tienen el carácter de reservados de conformidad con el art. 77.1 del texto refundido de la Ley General de la Seguridad Social (TRLGSS), norma de carácter especial y aplicación preferente respecto del resto del ordenamiento jurídico.

Es por ello, por lo que sólo podrán ser objeto de cesión en los supuestos contemplados en el mencionado art. 77.1 TRLGSS, a excepción de que o bien el tratamiento para el que estén siendo solicitados, se encuentre regulado por una norma con rango de ley que contemple de forma expresa la cesión o acceso a dichos datos, en cuyo caso sería de aplicación preferente al TRLGSS, o bien el interesado titular de los datos personales haya dado su consentimiento.

En consecuencia, deberán adoptarse las siguientes medidas:

1. Se realizará un **registro de las solicitudes de cesión de datos** recibidas de otros organismos y en el que consten los siguientes extremos:
   - Organismo, entidad o sujeto solicitante.
   - Datos de carácter personal solicitados.
   - Finalidad para la que se solicitan los datos y norma que atribuye la competencia administrativa al solicitante respecto de la finalidad expresada.
   - Norma que autoriza al INSS a ceder los datos o en su defecto consentimiento del titular.
   - Fecha y medio por el que se produce la trasmisión de los datos.
   - Unidad de trámite o funcionario que realiza la cesión/trasmisión.
   - Unidad de trámite o funcionario que recibe la información.
2. Las trasmisiones de datos deberán realizarse de conformidad con los principios de actuación contenidos en la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo relativo a tramitación electrónica y a relaciones electrónicas entre unidades administrativas y organismos, a través de medios electrónicos, siendo siempre preferente el uso de los canales o servicios ya establecidos en la sede electrónica de la Seguridad Social (funcionalidad Cesión de Datos e Informes) o en la Plataforma de Intermediación de Datos (PID) del INSS con el resto de las Administraciones Públicas. En su defecto, deberán realizarse a través del correo electrónico corporativo, cifrando en todo caso la información a suministrar y dirigiéndola a una dirección de

correo electrónica oficial del organismo solicitante. Siendo preferente el uso de alguno de los procedimientos de cifrado para el intercambio seguro de archivos, establecidos por el Centro de Seguridad de la Información (Área de Políticas y Auditoria de Seguridad de la Gerencia de Informática de la Seguridad Social), en su versión 1.3 de 21 de mayo de 2019. En todo caso, las contraseñas para desactivar el cifrado de la información no podrán facilitarse a la misma dirección de correo a la que se haya remitido la información solicitada.

3. Para el supuesto de que la trasmisión de la documentación no pueda realizarse por medios electrónicos, la misma se realizará a través del servicio postal universal. Cuando los datos personales objeto de transmisión tengan la consideración de categoría especial, además deberá realizarse por una modalidad de mensajería que permita acreditar la recepción efectiva de la documentación por el destinatario de la misma. Dichos extremos deberán indicarse en el registro mencionado en el punto 1.

4. Excepcionalmente podrá realizarse la trasmisión de la documentación cedida mediante personal adscrito a la Dirección provincial, en cuyo caso, deberán utilizarse medios que salvaguarden la integridad y confidencialidad de los documentos, los cuales irán seriados y numerados, obteniéndose la correspondiente diligencia de entrega por parte del destinatario cuando se produzca la misma. Dichos extremos deberán indicarse en el registro mencionado en el punto 1.

CUARTA. Comunicaciones seguras.

En el desarrollo de la gestión ordinaria de nuestra organización nos encontramos con diversas situaciones en las que se requiere contactar con otras unidades de nuestra u otra administración, o bien con los ciudadanos o interesados en los trámites administrativos de nuestra competencia.
Con el fin de establecer unas reglas que permitan incrementar los niveles de seguridad en las comunicaciones a realizar y teniendo en cuenta las pautas establecidas por la Resolución de 12 de mayo de 2011, de la Secretaría de Estado de la Seguridad Social, por la que se modifica la Resolución de 15 de febrero de 2011, por la que se dictan instrucciones sobre el uso y la gestión del sistema de correo electrónico como medio de comunicación en el ámbito de la Administración de la Seguridad Social, así como la Norma por la que se establece la Política de uso seguro de los sistemas de información de la Seguridad Social, aprobada y supervisada por el Comité de Seguridad de los Sistemas de Información de la Seguridad Social, se establecen las siguientes medidas:

1. Las comunicaciones requeridas para el desempeño de las funciones propias del puesto de trabajo se realizarán obligatoriamente por **correo electrónico**, cuando el destinatario sea una unidad o funcionario dependiente de una administración pública o mutua colaboradora de la Seguridad Social, o en su defecto, una persona jurídica o un profesional de los obligados a relacionarse electrónicamente con las Administraciones Públicas conforme la Ley 39/2015.

2. Cuando en la comunicación se contengan datos de carácter personal, la misma deberá realizarse obligatoriamente de forma **cifrada**. Siendo preferente el uso de alguno de los procedimientos de cifrado para el intercambio seguro de archivos, establecidos por el Centro de Seguridad de la Información (Área de Políticas y Auditoria de Seguridad de la Gerencia de Informática de la Seguridad Social), en su versión 1.3 de 21 de mayo de 2019. En todo caso, las contraseñas para desactivar el cifrado de la información no podrán facilitarse a la misma dirección de correo a la que se haya remitido la comunicación.

3. En el supuesto de que el **destinatario de la comunicación sea un ciudadano**, la misma se realizará preferentemente a la dirección de **correo electrónico** que nos haya facilitado el mismo, y que conste en nuestras bases de datos, salvo que se carezca de dicha dirección de correo electrónico, en cuyo caso se utilizará el servicio postal universal.

4. En el caso de que deba quedar constancia documental de haberse producido la comunicación efectiva al ciudadano, o la comunicación contenga datos personales de **categoría especial**, la misma se realizará a través de una modalidad de **mensajería postal** que permita acreditar la recepción efectiva de la documentación por el destinatario de la misma.
5. Deberá realizarse un **registro de funcionarios autorizados** a utilizar el correo hacia el exterior, indicando el motivo de dicha funcionalidad, revisándose periódicamente dichas autorizaciones.

QUINTA. Comunicaciones Telefónicas.

En las comunicaciones telefónicas a mantener con los ciudadanos deberá prestarse una especial atención a la identificación del interlocutor y la información que se le suministra, debiendo atenderse al protocolo de identificación telefónica aprobado por el INSS.

Así pues, se deberá realizar una comprobación entre los datos facilitados por el interlocutor telefónico y los datos que figuran en nuestras bases datos o sistemas de información, y en el caso de que se observe concordancia entre los mismos, se podrá suministrar la siguiente información en función del trámite concreto:

Información sobre expedientes en trámite

- Información sobre la fase del trámite, desde su apertura hasta el momento en que recaiga la resolución.

  Si el trámite sobre el que se solicita información ya está resuelto, se podrá informar de los siguientes aspectos relacionados con el mismo:

- Si la resolución es aprobatoria o denegatoria
- Fecha de la resolución
- Tiempo estimado que tarda en llegar al domicilio.

IMPORTANTE: No se facilitarán datos referidos al tipo concreto de prestación económica solicitada, cuantía reconocida, causas de denegación, ni otros datos personales que afecten de alguna forma a la intimidad o privacidad de las personas, especialmente los de contenido sanitario como informes médicos, tipo o grado de incapacidad, etc.

Si el expediente está cancelado o sin efectos económicos se podrá informar del motivo de tal situación de acuerdo con lo anteriormente expuesto.

Resolución recaída y primer pago

- Si se supera el protocolo de identificación telefónica se facilitará información sobre los datos contenidos en la resolución o notificación que previamente suministrará el propio interesado.
- Si el ingreso en la entidad financiera es anterior a la recepción de la resolución y el interlocutor aporta correctamente los datos de importe y los cuatro últimos dígitos de la cuenta bancaria, se facilitará información sobre el ingreso efectuado.
- En el caso de subsidios, si la persona nos facilita el dato del último pago y los cuatro últimos dígitos de la cuenta bancaria, se podrá facilitar información sobre el siguiente pago.

Revalorización y paga única

- Hasta el ingreso en cuenta de la pensión revalorizada o paga única: se facilitará información general.

- Desde el ingreso en cuenta o recepción de la notificación, si se supera el protocolo de identificación telefónica, se facilitará información sobre los datos contenidos en la notificación, datos que previamente suministrará el propio interesado.
- Si el ingreso en la entidad financiera es anterior a la recepción de la notificación y el interlocutor aporta correctamente los datos de importe y los cuatro últimos dígitos de la cuenta bancaria, se facilitará información sobre el ingreso efectuado.
- Si después de la explicación del informador hay disconformidad con el importe de la revalorización o paga única, el ciudadano puede presentar reclamación previa, para lo que se le direccionará a atención presencial.

Control periódico de rentas (control de mínimos de pensiones, control de PF, de favor de familiares, etc.)

- Si se supera el protocolo de identificación telefónica, se facilitará información sobre los datos contenidos en la resolución o notificación, datos que previamente suministrará el propio interesado.
- En el caso de suspensión de la prestación, se indicará al ciudadano el motivo de esta suspensión (superación de rentas, falta de documentación, etc.)

Información sobre otros datos de la prestación (complementos por mínimos, incompatibilidades, concurrencia, IRPF, etc.)

- Si se supera el protocolo de identificación telefónica, se facilitará información sobre los datos que previamente suministrará el propio interesado sobre la notificación recibida.
- Si el interlocutor aporta correctamente los datos de importe y los cuatro últimos dígitos de la cuenta bancaria, se facilitará información sobre el ingreso efectuado y el porcentaje de IRPF aplicado.

Incapacidad temporal transcurridos 365 días (El interesado solicita información sobre su situación en el proceso de IT: alta médica, prórroga de IT, propuesta de IP)

- Si se supera el protocolo de identificación telefónica, se facilitará información sobre los datos que aporte el propio interesado, contenidos en la notificación o resolución.

Asistencia sanitaria

- Si se supera el protocolo de identificación telefónica, se podrá facilitar al usuario información sobre su derecho a la asistencia sanitaria y la modalidad de aseguramiento.
- Si el usuario facilita información sobre los beneficiarios (nombre y apellidos, fecha de nacimiento y parentesco) se le podrá facilitar, además información sobre el derecho de éstos.
- Si el usuario alega una situación de aseguramiento distinta de la existente en BADAS, se le informará sobre los canales para concertar cita o, en su caso, se le facilitará cita para un CAISS, informándole de los trámites, formularios necesarios y documentación a aportar.

Seguro escolar

Se le informará sobre los canales para concertar cita o, en su caso, se le facilitará cita para un CAISS, previa información sobre los trámites, formularios necesarios y documentación a aportar.

Síndrome tóxico

Se direcciona a la unidad de gestión de prestaciones económicas y sociales del Síndrome Tóxico, ya que la gestión está centralizada.

Reclamaciones previas y revisiones (pensiones y subsidios)

- Se preguntará la fecha de presentación de la reclamación previa o revisión.
- Si el plazo es inferior a 2 meses se responderá que continúa en trámite.
- No obstante lo anterior, se informará de la posibilidad de interponer demanda ante el juzgado una vez transcurridos los 45 días que señala la Ley reguladora de la jurisdicción social para entender desestimada la reclamación.
- Si el plazo es superior a 2 meses y se supera el protocolo de identificación telefónica, se informará al usuario de que la Administración siempre emitirá una resolución y que en ella se establecerá el plazo para interponer la demanda.
- Si ya está aprobada (consultar P3D62, LBP67 o IN053) y el interesado aún no ha recibido la resolución, se le indicará si ha sido estimada o no y se facilita la fecha de la resolución y el tiempo estimado que tarda en llegar al domicilio.
- No se facilitarán datos concretos relativos a la aprobación de la prestación como: cuantía reconocida, ni otros datos personales que afecten de alguna forma a la intimidad o privacidad de las personas, especialmente los de contenido sanitario como informes médicos, tipo o grado de incapacidad, etc.
- Si el interesado ha recibido la resolución, se facilitará información sobre los datos contenidos en ésta que previamente habrá de suministrar el propio interesado.

Reclamación de deudas por cobros indebidos de prestaciones (MIDAS)

- Si se supera el protocolo de identificación telefónica, únicamente se facilitará información sobre la fase en la que se encuentra el expediente o sobre los datos contenidos en la resolución o notificación, datos que previamente habrá de suministrar el propio interesado.
- Si el ingreso en la entidad financiera tras la deducción es anterior a la recepción de la notificación y el interlocutor aporta correctamente los datos de importe y los cuatro últimos dígitos de la cuenta bancaria, se facilitará información sobre el ingreso minorado efectuado.

Retenciones judiciales, embargos y otras materias análogas

- Si se supera el protocolo de identificación telefónica, y una vez consultadas las bases de datos corporativas se observa la existencia de una retención judicial o embargo, únicamente se le informará de que tiene que recibir un escrito informándole del motivo y la cuantía de la deducción.
- Si el usuario desea más información se le informará sobre los canales para concertar cita o, en su caso, se le facilitará cita para un CAISS.

Comprobación de variaciones de datos (domicilio, entidad financiera, modalidad de cobro)

- Si se supera el protocolo de identificación telefónica, se comprobará si ya está efectuada la variación.
- Si no es así y el usuario tiene residencia en España, se le informará sobre los canales para concertar cita o, en su caso, se le facilitará cita para un CAISS, indicando los trámites necesarios, documentos a aportar y formularios necesarios.
- Si tiene residencia en el extranjero, estas variaciones deben ser solicitadas por escrito a la Dirección Provincial correspondiente.

SEXTA. Actividad contractual, cláusula de protección de datos.

El RGPD y la LOPDGDD han reforzado los requisitos respecto de la contratación de servicios con los encargados de tratamiento, como son establecer que la relación entre responsables y encargados deba formalizarse siempre mediante un contrato o un acto jurídico que vincule al encargado, y establecer una

obligación de diligencia debida en la elección de los encargados de tratamiento por parte de los responsables, contratando únicamente encargados que estén en condiciones de cumplir con las prescripciones legales impuestas por la nueva normativa en materia de protección de datos.

No obstante, aunque inicialmente los contratos suscritos con anterioridad al 25 de mayo de 2018, mantendrán su vigencia como máximo hasta el 25 de mayo de 2022, deben tenerse en cuenta las modificaciones operadas por el 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, y en concreto por su artículo 5, por el que se modifica 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.

Es por todo ello, por lo que a fin de implementar las nuevas directrices sobre protección de datos en los pliegos de cláusulas administrativas y/o técnicas de los próximos contratos a celebrar y cuya gestión corresponda a las direcciones provinciales, se deberán adoptar las medidas necesarias:

1. Se realizará un inventario en el que conste la totalidad de los contratos públicos realizados por cada Dirección provincial, en los cuales se haga un uso de datos personales y se encuentren vigentes en la actualidad. En el mismo se indicará el objeto del contrato, datos personales a los que de forma directa tendrá acceso el prestatario u obligado del contrato, fecha de finalización de este, y cláusula contractual referida a la confidencialidad o deber de sigilo que en su caso conste en el contrato y/o pliego de cláusulas administrativas o técnicas.

2. Deberá obtenerse e incorporar obligatoriamente en los pliegos una cláusula tipo sobre protección de datos personales o confidencialidad referente a la cesión de datos por parte de los futuros contratistas, en aplicación del Reglamento 2016/679 del Parlamento Europeo y del Consejo, y Ley Orgánica 3/2018, de 5 de diciembre, en aquellos contratos cuya ejecución requiera el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento. De este modo, en el pliego se hará constar y se calificarán como “Obligaciones Esenciales”, los siguientes extremos:

   a) La finalidad para la cual se cederán dichos datos.

   b) La obligación del futuro contratista de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos, sin perjuicio de lo establecido en el último párrafo del apartado 1 del artículo 202.

   c) La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.

   d) La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra c) anterior.

   e) La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas.

3. Por otro lado, también será obligatorio el establecimiento de una condición especial de ejecución, que haga referencia a la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos, advirtiéndose además al contratista de que esta obligación tiene el carácter de obligación contractual esencial.

4. En atención al carácter especial de los datos personales a tratar, deberá analizarse de forma expresa los contratos cuya finalidad sea:

- Reconocimientos médicos y seguimiento de la salud laboral de los trabajadores dependientes de la Dirección provincial.
- Traducciones de documentación presentada en lenguas cooficiales del Estado español, así como en lenguas extranjeras.
- Realización de pruebas clínicas a petición de las unidades médicas de valoración de incapacidades (UMEVI).
- Servicio de Seguridad y Videovigilancia.

En los mismos deberán constar qué datos personales van a ser utilizados, quienes podrán acceder a los mismos, destinatarios o cesionarios, forma de comunicación o trasmisión de los datos, medidas de seguridad establecidas, y encargado de custodiar los mismos.

SÉPTIMA. Bases de información y ficheros de datos.

La totalidad de las gestiones administrativas desarrolladas por el INSS se encuentra aglutinada en los 43 tratamientos que componen el Registro de Actividades de Tratamientos (RAT) de esta entidad, y que, en atención a la finalidad perseguida por el tratamiento, permite la organización y estructuración de los más de 1300 ficheros de datos personales inventariados en el conjunto de las 52 Direcciones provinciales.

Todos los datos personales utilizados en los mencionados tratamientos y ficheros se encuentran residenciados en las 5 grandes bases de datos que posee este Instituto: el Registro de Prestaciones Sociales Públicas (RPSP), el sistema de información Tarjeta Social Digital (TSD), la Base de Datos de Asistencia Sanitaria Nacional (BADAS) y los aplicativos informáticos ATRIUM e INCA.

No obstante, dentro de la búsqueda de la eficacia y mejora de los procesos de actuación, cada Dirección provincial puede diseñar y desarrollar sus propias bases de datos y sistemas de información que estimen necesarios para mejorar la eficiencia de nuestra organización, siempre cumpliendo con los requisitos técnicos y de seguridad establecidos por la normativa y bajo la supervisión de la GISS, en su caso.

Es por ello, por lo que se establecen las siguientes medidas:

1. Deberá mantenerse un inventario completo por cada Dirección provincial en el que se recojan la totalidad de bases de datos, sistemas de información, ficheros automatizados o no automatizados y aplicativos informáticos de ámbito provincial utilizados por la misma. Dicho inventario deberá contener la siguiente información:
   - finalidad perseguida
   - datos utilizados,
   - unidades de destino
   - funcionarios con acceso a las mismas
   - fecha en la que se habilita el acceso
   - medidas de seguridad establecidas para salvaguardar la confidencialidad e integridad de los datos personales.
2. Toda base de datos, sistema de información, fichero automatizado o no automatizado y aplicativo informático de ámbito provincial nuevo que se desarrolle, deberá ser comunicado a la Inspección de Servicios del INSS, indicando los extremos señalados en el punto 1.
3. Se procederá a la revisión y actualización de dicho inventario con carácter anual.

OCTAVA. Sistemas de videovigilancia.

Conforme el artículo 12 del RGPD y 22 de la LOPDGDD, se podrá llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con el fin de preservar la seguridad de las personas y bienes, así como sus instalaciones, siendo lícito el captar imágenes de la vía pública en la medida que resulte imprescindible para lograr la finalidad perseguida.

No obstante, en base al derecho de información que tienen los ciudadanos cuya imagen pueda ser captada por dichos sistemas, lo cual constituye un deber para esta administración como responsable de dichos sistemas de videovigilancia, se deberán adoptar las siguientes medidas:

1. Actualización de los dispositivos informativos (carteles zona videovigilada) en lugares de máxima visualización, identificando en los mismos los siguientes extremos:
   - Nombre del tratamiento
   - Identidad del responsable
   - Posibilidad de ejercitar los derechos previstos en los arts. 1 a 22 del Reglamento (UE) 2016/679.
   - Dirección de internet donde ampliar dicha información.
2. Hoja informativa con la información referida en el punto anterior a disposición de los ciudadanos solicitantes de la misma, tanto en soporte físico como digital.
3. Inventario del número de cámaras de videovigilancia existentes en todas las instalaciones dependientes de la Dirección provincial, indicando localización física, justificación de la misma, y número de carteles informativos existente, así como su localización. Dicho inventario deberá revisarse y actualizarse en su caso, anualmente.

NOVENA. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

En aplicación de la Disposición adicional séptima de la LOPDGDD, por la que se establece que cuando sea necesaria la publicación de un acto administrativo que contenga datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente, con el fin de lograr una homogeneidad en las actuaciones desarrolladas por el conjunto de las Direcciones provinciales así como las Subdirecciones generales que integran esta Entidad, se deberá adoptar el criterio conjunto establecido por la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía, garantizando la protección de la divulgación de los documentos identificativos de los interesados.

Así pues, la publicación del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente deberá realizarse de la siguiente forma:

- Dado un DNI con formato 12345678X, se publicarán los dígitos que en el formato dado ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo: ***4567**.
- Dado un NIE con formato L1234567X, se publicarán los dígitos que en el formato dado ocupen las posiciones cuarta, quinta, sexta y séptima, evitando el primer carácter alfabético. En el ejemplo: ****4567*.
- Dado un pasaporte con formato ABC123456, al tener sólo seis cifras, se publicarán los dígitos que en el formato ocupen las posiciones, evitando los tres caracteres alfabéticos, tercera, cuarta, quinta y sexta. En el ejemplo: *****3456.

- Dado otro tipo de identificación, siempre que esa identificación contenga al menos 7 dígitos numéricos, se numerarán dichos dígitos de izquierda a derecha, evitando todos los caracteres alfabéticos, y se seguirá el procedimiento de publicar aquellos caracteres numéricos que ocupen las posiciones cuarta, quinta, sexta y séptima. Por ejemplo, en el caso de una identificación como: XY12345678AB, la publicación sería: *****4567***
- Si ese tipo de identificación es distinto de un pasaporte y tiene menos de 7 dígitos numéricos, se numerarán todos los caracteres, alfabéticos incluidos, con el mismo procedimiento anterior y se seleccionarán aquellos que ocupen las cuatro últimas posiciones. Por ejemplo, en el caso de una identificación como: ABCD123XY, la publicación sería: *****23XY.

Los caracteres alfabéticos, y aquellos numéricos no seleccionados para su publicación, se sustituirán por un asterisco por cada posición.

DÉCIMA. Identificación de los empleados públicos.

De conformidad con el art. 53 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas por el que se recogen los derechos del interesado en el procedimiento administrativo, este tendrá derecho a identificar a las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos.

Por su parte, el art. 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno determina en su apartado 2 que "Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano". Habiendo sido interpretado dicho precepto por la Agencia Española de Protección de Datos en el sentido de considerar que los datos referidos al nombre y apellidos de la persona que ocupa un puesto en la Administración no son más que datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano, y, por tanto, subsumibles en el art. 15.2 de la Ley 19/2013.

No obstante, la resolución de 25 de noviembre de 2015 de la Secretaria de Estado para la Administración Pública por la que se establece el protocolo de prevención de violencia en el trabajo establece entre las actuaciones previas a una situación de riesgo aquellas medidas proactivas destinadas a proteger la persona del funcionario, entre las que se cita expresamente el "proteger la identidad de los empleados, utilizando tarjetas con número de seguridad".

Teniendo en cuenta los preceptos anteriormente expuestos y con el fin de adoptar medidas proactivas destinadas a proteger la persona del empleado público de previsibles riesgos, se establecen las siguientes medidas:

1. En las solicitudes presentadas por los ciudadanos en las que se pretendan conocer los datos identificativos de los funcionarios bajo cuya responsabilidad se está tramitando un procedimiento administrativo en los que consten como interesados, la identificación del funcionario concreto se realizará mediante el número de usuario silcon o cualquier otro código alfanumérico que permita individualizarlo, junto con la denominación del puesto concreto que ocupa, pero sin que en ningún caso se revelen los datos identificativos personales del funcionario (nombre y apellidos o DNI). Dicha medida no será de aplicación respecto del funcionario que resuelva el trámite administrativo que afecte a los derechos del ciudadano, quienes deberán indicar su nombre, apellidos y denominación de su puesto de trabajo.

2. En las tarjetas identificativas y demás medios establecidos por la administración con fines identificativos, se podrá adoptar la misma medida expuesta anteriormente, siempre a petición del empleado público, previa justificación/exposición del riesgo a evitar.

UNDÉCIMA. Estructura organizativa.

La entrada en vigor del RGPD y de la LOPDGDD ha supuesto instaurar una nueva estructura organizativa en las administraciones públicas con el fin de facilitar y supervisar la implementación de las medidas necesarias en materia de protección de datos. Así pues, en el ámbito concreto del INSS nos encontramos con:

1. **DELEGADO DE PROTECCIÓN DE DATOS**

   El RGPD previó 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, celebrado el 31 de enero de 2017, tomó el acuerdo de que existiera un único DPD en el ámbito de la Secretaría de Estado de la Seguridad Social, designación que recayó en el titular de la Dirección del Servicio Jurídico de la Administración de la Seguridad Social.

   Sus funciones son:

   - Informar y asesorar a responsables y encargados de los tratamientos
   - Supervisar el cumplimiento de lo dispuesto en materia de protección de datos
   - Ofrecer el asesoramiento que se le requiera en materia de evaluación de impacto
   - Cooperar con la AEPD
   - Actuar como punto de contacto con la AEPD para cuestiones relativas al tratamiento.

2. **COMISIÓN DE PROTECCIÓN DE DATOS DE LA ADMINISTRACIÓN DE LA SEGURIDAD SOCIAL:**

   La Resolución de la Secretaría de Estado de la Seguridad Social, de 17 de abril de 2018, reguló la creación de la Comisión, constituida por los Subdelegados de Protección de Datos de cada entidad y servicio común (INSS, TGSS, ISM, GISS, IGSS, DGOSS, SJSS), tiene funciones de apoyo al DPD y de contribución al cumplimiento de las previsiones en materia de protección de datos.

3. **SUBDELEGADO DE PROTECCIÓN DE DATOS DEL INSS:**

   Es el titular de la Secretaría General, en el que, además de la competencia de velar por el cumplimiento de las previsiones en materia de protección de datos, concurre la competencia de coordinación de las Subdirecciones generales de la entidad, encomendada a esta unidad orgánica en las normas sobre estructura y competencias del INSS.

   La constitución de un Grupo de trabajo de Protección de Datos del INSS, previa convocatoria de la Secretaria General responde a esas funciones de coordinación.

4. **GRUPO DE PROTECCIÓN DE DATOS DEL INSS**

   Está integrado por representantes de todas las Subdirecciones generales, así como de la Secretaría general, encargado de apoyar al SPD en el análisis, revisión y actualización de las políticas de privacidad en nuestra entidad. Se coordina por la Jefa de la Inspección y por un Jefe de Área adscrito a la citada Inspección, responsable del programa de protección de datos y de impulsar y supervisar el cumplimiento efectivo de las obligaciones derivadas de la normativa en materia de protección de datos en el INSS.

Debido a la necesidad de incardinar la estructura de protección de datos de nuestra entidad en el seno de las Direcciones provinciales, se acuerdan las siguientes medidas:

1. Se deberá designar en cada Dirección provincial un funcionario a quien se le encomendará supervisar el cumplimiento efectivo de la normativa de protección de datos, así como de asesorar sobre dicha materia en relación con las consultas que surjan en la gestión ordinaria de la Dirección provincial.
2. Las dudas o consultas que no puedan ser resueltas por el funcionario expuesto en el punto anterior, se transmitirán por parte de este, a los Servicios Centrales para su resolución, siempre a través del buzón de correo electrónico creado específicamente para dicha misión: **consultas.inss-sscc.proteccion-de-datos@seg-social.es**
3. Las solicitudes de ejercicio de derechos en materia de protección de datos que se presenten directamente en las Direcciones provinciales deberán ser resueltas por las mismas, enviando al buzón de correo mencionado en el punto anterior, una copia de la solicitud recibida y de la respuesta evacuada.

DUODÉCIMA. Ejercicio de derechos en materia de Protección de Datos Personales.

Cuando un ciudadano desee ejercitar alguno de los derechos reconocidos en la normativa de protección de datos, se le facilitará el modelo correspondiente. Una vez cumplimentado se registrará y se enviará al responsable provincial en materia de protección de datos para su tramitación quien recabará el apoyo de la unidad competente. La unidad competente se determinará por la ubicación del fichero, base de datos o sistema de información, y trámite de gestión afectado.

Además del modelo oficial, los usuarios podrán presentar su propia solicitud siempre que cumpla, como mínimo, los siguientes requisitos:

- Nombre y apellidos del interesado
- Fotocopia del DNI, pasaporte, o NIE. También la de la persona que lo representa cuando se actúe en representación. Si la solicitud se realiza por medios telemáticos, se acreditará a través de la firma electrónica
- Dirección a efectos de notificaciones
- Petición en que se concreta la solicitud
- Fecha y firma

Una vez presentada, se entregará al interesado una copia sellada de la solicitud.

Si la solicitud no reúne los requisitos especificados anteriormente, se deberá solicitar la subsanación de estos, fijándose un plazo de subsanación será de 10 días. De no presentarse en el citado plazo, se considerará como desistida su petición, de conformidad con los artículos 68 y 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Cuando la solicitud se refiere a ficheros o bases de datos personales que no son responsabilidad del INSS, deberá remitirse a la institución u organismo competente, comunicando al interesado dicha circunstancia y la fecha del traslado.

La Dirección provincial donde se haya presentado la solicitud para el ejercicio de los derechos, deberá resolver en el plazo de un mes.

En caso de que surjan dudas sobre cómo se ha tramitar la solicitud, se deberá recabar el asesoramiento de la Subdelegada de Protección de Datos del INSS a través del buzón de consultas corporativo:

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

Cuando la petición se desestime, se informará al interesado de las causas del desistimiento, y en todo caso, de su derecho a recabar la tutela de la Delgada de Protección de Datos de la Administración de la Seguridad Social, así como de la Agencia Española de Protección de Datos (AEPD).

DÉCIMOTERCERA. Comunicación de Brechas de Seguridad. Medidas de Seguridad.

Conforme el Esquema Nacional de Seguridad (ENS) y la Directiva NIS, se define un "incidente de seguridad" como aquel evento o serie de eventos, inesperados o no deseados, con consecuencias negativas para la seguridad del sistema de información, y que, con una gran probabilidad, van a comprometer las operaciones de la organización y a amenazar la seguridad de la información, teniendo efectos adversos en la seguridad de las redes y sistemas de información.

No obstante, a efectos de protección de datos, solo resultan de interés aquellos incidentes de seguridad que deban considerarse como una "brecha de seguridad".

Un incidente de seguridad constituirá una brecha de seguridad cuando cumpla todas las condiciones siguientes:

1. Afecte a la seguridad de información, es decir, ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
2. Afecte a datos personales.
3. Suponga un riesgo para los derechos y libertades de las personas físicas titulares de los datos.

Las brechas de seguridad pueden producirse tanto en sistemas informáticos (aplicativos informáticos, bases de datos, ficheros informáticos, tabletas, PCs, teléfonos móviles, cds, memorias de almacenamiento, etc.), como en tratamientos en papel (formularios o expedientes en papel, carpetas o archivadores a-z, radiografías, pruebas médicas, titulaciones académicas …).

La normativa vigente impone al responsable del tratamiento (INSS) la obligación de notificar a la autoridad de control (AEPD) toda brecha de seguridad que se haya producido en el ámbito de su competencia, en el plazo máximo de 72h desde que haya tenido conocimiento de ello.

Así pues, todo trabajador adscrito o dependiente del INSS que se encuentre ante una brecha de seguridad, deberá comunicarlo a la mayor brevedad posible, conforme el siguiente procedimiento:

1. Informará a la persona titular de la Subdirección provincial y a la persona responsable en materia de protección de datos de la Dirección provincial, de la situación producida. En el caso de haberse producido en los Servicios Centrales, deberá comunicárselo a la persona titular de la Subdirección general, así como al representante designado por la Subdirección general para participar en el Grupo de Trabajo de Protección de Datos en el INSS.
2. Una vez comunicados lo hechos o situación producida a los responsables señalados en el punto anterior, estos deberán confirmar que el incidente en cuestión se trata de una brecha de seguridad.
3. Tras la confirmación de que la situación producida constituya (o pueda constituir) una brecha de seguridad, en el caso de que la misma afecte a bases de datos, ficheros o sistemas de información de carácter informático, el responsable en materia de protección de datos de la Dirección provincial o de la Subdirección general avisará a la UPI provincial o bien al Centro de Desarrollo del INSS (CDINSS) de los hechos para que adopte las medidas oportunas para poner fin a la brecha de seguridad. y para corregir y paliar los efectos nocivos que se hayan podido producir.
4. En el caso de que la brecha de seguridad afecte a bases de datos, ficheros o sistemas de información no automatizados, o automatizados, pero no supervisados por la UPI o el CDINSS, el

responsable en materia de protección de datos de la Dirección provincial o de la Subdirección general, en coordinación con la persona responsable funcional de los mismos, adoptará las medidas necesarias para poner fin a la brecha, y para corregir y paliar los efectos nocivos que se hayan podido producir.

5. Todo lo expuesto en los puntos anteriores, se deberá comunicar a la mayor brevedad posible, y siempre antes del transcurso de 48 horas desde que se produjo o se tuvo conocimiento de la incidencia, a la Subdelegada de Protección de Datos del INSS a través del buzón de consultas de protección de datos (**consultas.inss-sscc.proteccion-de-datos@seg-social.es**) o al buzón de la Inspección de Servicios (**inspeccion.inss-sscc.sg@seg-social.es**), en ambos casos del INSS. Dicha comunicación se realizará por parte de la persona titular de la Dirección provincial o del responsable en materia de protección de datos de esta. En el caso de los SS.CC, la comunicación se realizará por parte del responsable en materia de protección de datos de la Subdirección general correspondiente.
6. La comunicación expuesta en el punto anterior deberá contener la siguiente información:
    1. Naturaleza de la brecha de seguridad:
        - Brecha de confidencialidad (acceso no autorizado)
        - Brecha de integridad (modificación no autorizada)
        - Brecha de disponibilidad (desaparición o pérdida)
    2. Categorías de afectados:
        - Menores o discapacitados.
        - Empleados públicos.
        - Ciudadanos.
    3. Medio por el que se ha materializado la brecha:
        - Dispositivo perdido o robado.
        - Documentación perdida, robada.
        - Correo perdido o abierto.
        - Datos personales mostrados al individuo incorrecto.
        - Revelación verbal no autorizada de datos personales.
        - Eliminación incorrecta de datos personales formato papel.
        - Datos personales residuales en dispositivos obsoletos.
    4. Número aproximado de afectados.
    5. Categorías de datos comprometidos:
        - Identificativos, DNI, NUSS, NIE.
        - Credenciales de acceso o identificación.
        - Datos de contacto o residencia.
        - Datos económicos o financieros.
        - Datos de salud.
    6. Número de registros de datos personales afectados.
    7. Posibles consecuencias de la brecha de seguridad sufrida.
    8. Medidas adoptadas o propuestas para remediar la brecha.
    9. Si se le ha comunicado la brecha al afectado.
    10. Fechas en las que han sucedido todos los hechos.

IMPORTANTE:

Es fundamental que las brechas de seguridad se comuniquen al buzón indicado en el **plazo máximo de 48h.**

Si no se dispone de toda la información, es posible su ampliación con posterioridad, lo urgente es la comunicación inicial.

Las notificaciones a la AEPD solo se realizarán por parte de la Subdelegada de Protección de Datos.

DÉCIMOCUARTA. Medidas de Seguridad.

La Agencia Española de Protección de Datos, al interpretar el RPGP ha establecido la figura del Responsable de Seguridad como aquella persona diferente del Delegado de Protección de Datos (DPD) que, de acuerdo con el esquema nacional de seguridad, deberá determinar las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios. Siempre de forma diferenciada y bajo las directrices del DPD en cuantos a las medidas que puedan afectar a la protección de datos personales.

Dichas figura y funciones de Responsable de Seguridad en el ámbito de la Administración de la Seguridad Social recaen en el Comité de Seguridad de los Sistemas de la Información de la Seguridad Social (CSSISS), el cual, con el apoyo de la GISS, dicta las Normas técnicas precisas para garantizar la integridad y seguridad de los sistemas de información y equipamientos electrónicos.

Así pues, dada la relación directa existente entre las medidas de seguridad de los sistemas de información y las medidas necesarias para garantizar la integridad y confidencialidad de los datos de carácter personal utilizados por este Instituto, se acuerda la siguiente medida:

1. Se deberá difundir a todo el personal de la Dirección provincial la norma por la que se establece la Política de uso seguro de los sistemas de información de la Seguridad Social, en su versión de 20 de septiembre de 2019.
2. Igualmente, deberá difundirse el procedimiento para el intercambio seguro de archivos, aprobado por el Centro de Seguridad de la Información (GISS), en su última versión de 21 de mayo de 2019.

ANEXO. 7

CLÁUSULAS DE CONTRATACIÓN ADMINISTRATIVA. EXTRACTO QUE AFECTA A LA PRIVACIDAD.

13.5.5 La empresa adjudicataria responderá ante el INSS, al que mantendrá indemne de todos los daños, gastos, costes, perjuicios y pérdidas de cualquier tipo que pudiera tener o en los que pudiera incurrir como consecuencia de las reclamaciones de cualquier tipo, que pudieran originarse por el incumplimiento de las obligaciones establecidas bien a consecuencia de la actuación de la empresa y de su personal como de las empresas y personal que haya subcontratado.

13.5.6 **Cumplimentar según ANEXO XVIII**

13.5.7 **En su caso, cumplimentar según ANEXO XIX**

13.6 Serán a cargo del adjudicatario todos los gastos, incluidos los fiscales, que se deriven de la licitación, adjudicación, formalización y ejecución de este contrato.

De acuerdo con lo previsto en el apartado g) del artículo 67.2 del Reglamento General de la Ley de Contratos de las Administraciones Públicas, atendiendo a la naturaleza del presente procedimiento de licitación, no se prevén gastos de publicidad para la licitación de este contrato.

13.7 El contratista estará obligado a guardar sigilo respecto a los datos o antecedentes que, no siendo públicos o notorios, estén relacionados con el objeto del contrato, de los que tenga conocimiento con ocasión del mismo.

Esta obligación, se hace expresamente extensiva al personal que emplee en la ejecución del contrato, y con ocasión de la documentación o información de la que aquél pueda tener conocimiento como consecuencia de la prestación de los servicios en las dependencias del Instituto Nacional de la Seguridad Social, debiendo guardar absoluto secreto en relación con dicha documentación o información.

En todo caso, el contratista se somete a la normativa nacional y de la Unión Europea en materia de protección de datos, y asume la obligación de respetarla, resultando de aplicación asimismo las previsiones contenidas en la disposición adicional vigésima quinta de la LCSP, y en lo que respecta al deber de confidencialidad, las establecidas en el artículo 133 de dicha ley.

De forma específica, el adjudicatario quedará obligado al cumplimiento de lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, conforme al contenido previsto en la cláusula decimoctava de este pliego.

DECIMOCUARTA.- PENALIDADES

Cumplimentar según ANEXO XX

18.4 Cuando la ejecución de los servicios se desarrolle en las instalaciones del INSS, la empresa adjudicataria se obliga a informar previamente a éste de la identidad del personal designado para desarrollar tales servicios, quienes se comprometerán y atendrán al cumplimiento de las normas, especificaciones y procedimientos de seguridad y acceso establecidos por el INSS.

18.5 La empresa adjudicataria responderá ante el INSS, al que mantendrá indemne de todos los daños, gastos, costes, perjuicios y pérdidas que pudiera tener o en las que pudiera incurrir como consecuencia de las reclamaciones de cualquier tipo, que pudieran originarse por el incumplimiento por parte de aquélla del deber de confidencialidad o de cualquier otro deber legal o por revelación de secreto y, muy especialmente, de cualquier reclamación o sanción administrativa de cualquier tipo, fruto del incumplimiento de las obligaciones asumidas en materia de protección de datos frente al INSS o frente a los titulares de los datos personales objeto de tratamiento por el INSS.

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.

En la consideración de que en el presente contrato se requiere el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento, y de conformidad con lo dispuesto en el artículo 122.2 de la LCSP, se hace constar:

a) La finalidad para la cual se ceden lo datos es la siguiente: …….

b) El contratista se somete en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos.

c) La empresa adjudicataria se obliga a presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.

d) El contratista está obligado a comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere el apartado anterior.

e) Si los licitadores tienen previsto subcontratar servidores o los servicios asociados a los mismos, deben indicar en la documentación a que se hace referencia en el apartado 6.4.2 de este pliego (sobre único: declaración y oferta), el nombre o perfil empresarial de los subcontratistas a los que se vaya a encomendar su realización, con indicación de las condiciones de solvencia técnica que reúnen.

Las obligaciones que se recogen en las letras a) a e) de este apartado tienen la consideración de obligaciones esenciales en el contrato a suscribir con el adjudicatario, y su incumplimiento será causa de resolución contractual

Sentado lo anterior, resultarán aplicables en materia de protección de datos las siguientes consideraciones:

18.1 La empresa adjudicataria, en su condición de encargado del tratamiento de los datos responsabilidad del Instituto Nacional de la Seguridad Social, garantiza en todo momento la confidencialidad de los datos personales y de todo tipo, recibidos del responsable del tratamiento, tanto antes como después de ser utilizados, así como que el uso de los mismos será exclusivamente para el desarrollo de las tareas precisas para poder prestar los servicios acordados.

La empresa adjudicataria, en dicha condición de encargado del tratamiento, reconoce expresamente que cualquier soporte donde se contengan datos personales, es de exclusiva titularidad del INSS, tratándose la relación de un acceso a los datos por cuenta de tercero, por lo que aquélla no utilizará los datos con fines distintos a las instrucciones del INSS, cumpliendo así con las obligaciones adquiridas en estas cláusulas.

La empresa adjudicataria no cederá en ningún caso a terceros los datos, ni tan siquiera para su conservación.

18.2 El régimen de subcontratación de los servicios objeto de este contrato se ajustará a lo dispuesto en el artículo 21 del Reglamento de desarrollo de la Ley de Protección de datos de carácter personal, aprobado por RD 1720/2007, de 21 de diciembre. En su caso, la empresa adjudicataria se obliga a celebrar con los subcontratistas un contrato con las mismas especificaciones en materia de protección de datos contenidas en este pliego; remitiendo copia del mismo al INSS.

18.3 Una vez cumplida la prestación de servicios pactada, y cuando ya no sean necesarios para continuar con el encargo realizado, los datos personales serán devueltos por la empresa adjudicataria, junto con cualquier soporte o documento en el que consten datos personales responsabilidad del INSS a los que aquélla haya tenido acceso y que hayan sido objeto del tratamiento. En ningún caso, podrá conservar copia alguna de todo o parte de estos datos.

Tampoco podrá transferir, duplicar o reproducir todo o parte de la información propiedad del INSS, y/o datos personales, para fin distinto del objeto del contrato, salvo para cumplir con lo dispuesto en el art. 94 del Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Asimismo, la empresa adjudicataria, como encargado del tratamiento, se compromete a impartir a todas las personas a su cargo las instrucciones precisas para el efectivo conocimiento y obligado cumplimiento de estas instrucciones y de las responsabilidades que asumen, en virtud de estas cláusulas, sobre confidencialidad en el tratamiento de datos personales, automatizados o no.

La empresa adjudicataria responderá frente al INSS si tales obligaciones son incumplidas por sus empleados.

18.4 Si los servicios contratados se realizasen, previa autorización del INSS, en las instalaciones de la empresa adjudicataria, ésta se compromete a adoptar las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos personales a que se refiere el art. 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y evitar su alteración, pérdida, tratamiento y acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan éstos, de la acción humana o del medio físico o natural.

En estos casos, la empresa adjudicataria se compromete a custodiar en sus instalaciones los datos personales responsabilidad del INSS, con las debidas condiciones de seguridad y protección contra el acceso de terceras personas y facilitando únicamente el acceso a la información recibida al personal autorizado por el encargado de tratamiento.

Todos los equipos que contengan o accedan a los datos de los que sea responsable el INSS, deben cumplir los requisitos mínimos de actualización tanto en sistemas operativos, como en programas antivirus, conforme a lo que establezca el INSS.

Asimismo, las aplicaciones informáticas a utilizar por parte de la empresa adjudicataria, deberán incluir en su descripción técnica el nivel de seguridad que permitan alcanzar, y que será, como mínimo, el nivel de seguridad que se requiera para el tratamiento de los datos de los que es responsable el INSS.

Si, por el contrario, la empresa adjudicataria prestase sus servicios en las instalaciones del INSS, informará previamente a éste de los datos del personal que designe para desarrollar estos servicios, quienes se atendrán a las especificaciones realizadas en el Documento de Seguridad del INSS.

A tales efectos, la empresa adjudicataria se compromete a informar al INSS de cualquier incidente o riesgo de seguridad que potencialmente pueda afectar a la seguridad de la información, a cooperar con el INSS en la investigación de incidentes o riesgos de seguridad, y a ejecutar las acciones que se acuerden para la resolución de las incidencias y la minimización de los riesgos detectados.

En ningún caso la empresa adjudicataria intentará explotar ni probar de forma independiente ninguna vulnerabilidad de seguridad que pudiera detectar.

18.5 La empresa adjudicataria responderá ante el INSS, al que mantendrá indemne de todos los daños, gastos, costes, perjuicios y pérdidas que pudiera tener o en las que pudiera incurrir como consecuencia de las reclamaciones de cualquier tipo, que pudieran originarse por el incumplimiento por parte de aquélla del deber de confidencialidad o de cualquier otro deber legal o por revelación de secreto y, muy especialmente, de cualquier reclamación o sanción administrativa de cualquier tipo, fruto del incumplimiento de las obligaciones asumidas en materia de protección de datos frente al INSS o frente a los titulares de los datos personales objeto de tratamiento por el INSS.

18.6 La empresa adjudicataria estará obligada a guardar el secreto profesional sobre los datos personales a que tenga acceso, debido a su relación contractual con el INSS. Esta obligación de secreto profesional se mantendrá durante y después de la realización del trabajo encomendado o de la finalización del contrato, por cualquier causa, tratándose por lo tanto de una obligación indefinida.

18.7 La empresa adjudicataria y los subcontratistas, en su caso, quedan sujetos y prestarán su ayuda incondicional para que el INSS pueda efectuar las auditorias que estime precisas, para asegurar el cumplimiento de las medidas técnicas y organizativas que se hayan establecido.

18.8 En los casos en que se produzca una brecha de seguridad, el encargado del tratamiento deberá inmediatamente ponerlo en conocimiento del INSS, adoptando en todo caso las medidas que sean necesarias para salvaguardar los datos.

ANEXO. 8

CLÁUSULAS DE PROTECCIÓN DE DATOS DEL ENCARGO A MEDIOS PROPIOS PARA LA ASISTENCIA TÉCNICA DE APOYO A LA TRAMITACIÓN DEL INGRESO MÍNIMO VITAL

e) El INSS designará un Director Facultativo de la actuación para la ejecución de los trabajos encargados, el cual dirigirá los mismos y revisará la actuación realizada por parte de TRAGSATEC.

El Director Facultativo se encargará de las siguientes funciones:

a) Realizar el seguimiento y control de la ejecución de las actividades.

b) Aceptar, si procede, el grado de avance de los trabajos realizados en el periodo correspondiente.

c) Validar la facturación de acuerdo al grado de avance de los trabajos.

Cuarta. Titularidad de la competencia.

Este Encargo no supone cesión de la titularidad de las competencias ni de los elementos sustantivos de su ejercicio, atribuidas al INSS. Es responsabilidad del INSS dictar los actos o resoluciones de carácter jurídico que den soporte o en los que se integre la concreta actividad material objeto del presente encargo.

Quinta. Vigilancia, control y coordinación.

El INSS velará por la adecuada realización del objeto del presente encargo, autorizando, en su caso, las alteraciones en la asignación de recursos a las actividades encargadas que mejoren el cumplimiento del mismo.

Sexta. Protección de datos personales.

a) Normativa

La prestación objeto del Encargo para la asistencia técnica «Apoyo a la atención e información telefónica relativa al Ingreso Mínimo Vital» implica el tratamiento por parte de TRAGSATEC de datos personales de los cuales es responsable el INSS.

En consecuencia, resulta de aplicación lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (en adelante, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD), teniendo

el INSS la condición de responsable del tratamiento y TRAGSATEC la de encargado del tratamiento.

Asimismo, resulta aplicable la disposición adicional vigésima quinta de 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.

b) Objeto

Mediante la presente clausula se habilita a TRAGSATEC para tratar por cuenta del INSS los datos personales necesarios para la ejecución del Encargo. Esta decisión se toma considerando lo establecido en el artículo 28.1 del RGPD, en relación a la elección de un encargado de tratamiento que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del citado Reglamento y garantice la protección de los derechos del interesado.

c) Obligaciones del responsable

El INSS, como responsable del tratamiento, se obliga a:

a) Facilitar por escrito al encargado las instrucciones necesarias para el tratamiento de los datos personales, y específicamente en lo referente a las medidas técnicas y organizativas a aplicar y destrucción o devolución de los datos.

b) Dar respuesta al interesado respecto a sus solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y portabilidad de los datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan. Dichas solicitudes se ejercitarán a través de la dirección de correo electrónico del responsable: consultas.inss-sscc.proteccion-de-datos@seg-social.es.

c) Cumplir con el deber de información, según lo establecido en el artículo 13 del RGPD.

d) En su caso, notificar las violaciones de seguridad a la Autoridad de Control y al interesado.

e) Realizar el análisis de riesgos, o en su caso, elaborar la evaluación de impacto cuando proceda.

f) Efectuar las consultas a la Autoridad de control, cuando proceda.

g) Cualquier otra recogida en la legislación en vigor y aplicable a los responsables de tratamiento de datos personales.

d) Obligaciones del encargado del tratamiento

TRAGSATEC, como encargado del tratamiento, se obliga a lo establecido en el RGPD, en este aspecto particular, cabe destacar lo establecido en su artículo 28 dedicado a las obligaciones del encargado del tratamiento. Según lo establecido en él, TRAGSATEC se obliga a:

a) Utilizar los datos personales objeto de tratamiento sólo para la finalidad prevista en el encargo, sin que en ningún caso pueda utilizarlos para sus propias finalidades.

b) Tratar los datos de acuerdo con las instrucciones escritas del responsable del tratamiento e informar de forma inmediata al responsable si considera que alguna de ellas infringe la normativa de protección de datos aplicable.

c) No comunicar, ceder o difundir los datos a los que tenga acceso con motivo de este encargo a terceros, salvo que cuenten con la autorización expresa del responsable del tratamiento.

d) Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad, necesarias o convenientes para asegurar la confidencialidad, secreto, disponibilidad, integridad de los Datos Personales a los que tenga acceso, y en particular las equivalentes o compensatorias a las del Anexo III del ENS, nivel básico.

e) Mantener la confidencialidad respecto a los datos de carácter personal a los que tenga acceso en virtud del encargo, incluso después de que finalice, y garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y cumplir con las medidas de seguridad correspondientes.

f) Garantizar la formación necesaria en materia de protección de datos personales a las personas autorizadas para tratar datos personales e informarlas previamente de las medidas de seguridad correspondientes.

Asimismo, TRAGSATEC, como encargado del tratamiento, se compromete a impartir a todas las personas a su cargo las instrucciones precisas para el efectivo conocimiento y obligado cumplimiento de las instrucciones impartidas por el INSS y de las responsabilidades que asumen, en virtud de estas

cláusulas, sobre confidencialidad, seguridad de la información y protección de datos con motivo del encargo y el tratamiento automatizado o no de datos de carácter personal, que ese encargo implica.

TRAGSATEC responderá frente al INSS si tales obligaciones son incumplidas por sus empleados.

g) Notificar al responsable del tratamiento, sin dilación indebida, las violaciones de seguridad de los datos personales a su cargo de las que tenga conocimiento, junto con toda la información relevante para la documentación y comunicación de la incidencia.

h) Cuando los afectados ejerzan los derechos establecidos en los artículos 15 a 22 del RGPD ante el encargado, este lo comunicará por correo electrónico al responsable de forma inmediata, trasladando, en su caso, la información que pueda ser relevante para resolver la solicitud.

i) Mantener a disposición del responsable del tratamiento la documentación acreditativa del cumplimiento de sus obligaciones establecidas en la norma, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

g) TRAGSATEC no recurrirá a otro encargado de tratamiento sin la autorización previa por escrito, específica o general, del INSS. En el caso de que sea autorizado para hacerlo, deberá cumplir con lo establecido en la normativa aplicable y, en particular, con lo estipulado en el artículo 28.4 del RGPD.

h) Cumplir, cuando proceda, con lo establecido en relación con el Registro de actividades del tratamiento, en el artículo 30.2 del RGPD.

i) Cualquier otra recogida en la legislación en vigor y aplicable a los encargados de tratamiento de datos personales.

e) Duración y obligaciones a la finalización del encargo

Una vez finalice el encargo, y conforme a las instrucciones que el responsable consigne por escrito al encargado de tratamiento, este devolverá al responsable los datos personales y, si procede, los soportes donde consten, o bien suprimirá los datos personales y, una vez destruidos, certificar por escrito su destrucción al responsable.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado, si bien éste puede conservar

una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación objeto del contrato o por obligaciones legales.

- **Deber de confidencialidad**

Los trabajos se realizarán por TRAGSATEC con el máximo cuidado y diligencia respecto a los intereses del INSS y el personal de TRAGSATEC estará obligado a guardar la debida confidencialidad respecto a los hechos, datos e informaciones que conozca en el curso del encargo.

Esta obligación de confidencialidad se mantendrá durante y después de la realización del trabajo encomendado o de la finalización del encargo, por cualquier causa, tratándose por lo tanto de una obligación indefinida.

Asimismo, se compromete a proteger la documentación e información generada y obtenida (en cualquier formato) a la que tenga acceso su personal autorizado con motivo de la ejecución de las actividades encargadas, con las medidas, procedimientos y medios adecuados para garantizar la confidencialidad, integridad, disponibilidad de la información manejada, así como la trazabilidad de las acciones realizadas por su personal en el desarrollo de su trabajo conforme a la normativa vigente de general aplicación. TRAGSATEC establecerá las medidas, procedimientos y medios de seguridad necesarios y adecuados para impedir que la utilización de la información en provecho de terceras personas, especialmente en el caso de tratamiento de datos personales sensibles especialmente protegidos por las normas vigentes en materia de protección de datos personales expresamente relacionadas en el presente encargo.

- **Alcance de la responsabilidad del encargado de tratamiento**

TRAGSATEC responderá ante el INSS, al que mantendrá indemne de todos los daños, gastos, costes, perjuicios y pérdidas que pudiera tener o en las que pudiera incurrir como consecuencia de las reclamaciones de cualquier tipo, que pudieran originarse por el incumplimiento por parte de TRAGSATEC del deber de confidencialidad o de cualquier otro deber legal o por revelación de secreto y, muy especialmente, de cualquier reclamación o sanción administrativa de cualquier tipo, fruto del incumplimiento de las obligaciones asumidas en materia de protección de datos frente al INSS o frente a los titulares de los datos recogidos en los ficheros responsabilidad del INSS.

- **Acceso a las instalaciones, uso de equipos y redes del responsable y obligaciones respecto a otros datos personales no sujetos al encargo de tratamiento**

Durante la prestación de sus servicios, TRAGSATEC se obliga expresamente a no acceder a otros sistemas informáticos, armarios y archivadores donde se traten, almacenen o conserven datos personales y documentos que los contengan objeto de tratamiento por el INSS, distintos a los que expresamente se les haya autorizado para ello.

En el supuesto de que para la correcta prestación de sus servicios, el personal de TRAGASATEC pueda acceder a documentación, datos, equipos, sistemas informáticos, despachos y ubicaciones donde se almacenen o conserven datos de carácter personal y/o documentación que contenga esta tipología de datos, requerirá de expresa autorización en tal sentido, obligándose a mantener la absoluta confidencialidad y secreto de toda aquella información a la que pueda acceder, no pudiendo transferir, duplicar o reproducir todo o parte de la información propiedad del INSS y / o datos personales.

Cuando la ejecución del encargo se desarrolle en las instalaciones del INSS, TRAGSATEC se obliga a informar previamente al INSS de la identidad del personal designado para desarrollar tales servicios, quienes se comprometerán y atendrán al cumplimiento de las normas, especificaciones y procedimientos de seguridad y acceso establecidos por el INSS.

Séptima. Desarrollo y seguimiento del encargo. Personal adscrito.

Corresponde exclusivamente a TRAGSATEC la selección del personal que, reuniendo los requisitos de titulación y experiencia exigidos, formará parte del equipo de trabajo adscrito a la ejecución del encargo.

El INSS podrá solicitar a TRAGSATEC información sobre la cualificación técnica de los trabajadores adscritos a la prestación del servicio.

TRAGSATEC facilitará la autorización de los trabajadores al INSS, al objeto de poder verificar su cualificación técnica.

TRAGSATEC prestará sus servicios en las dependencias o instalaciones del INSS, el personal de TRAGSATEC ocupará y accederá sólo a los espacios de trabajo que se determinen por el INSS y que serán diferenciados de los ocupados por el personal del INSS. Corresponde también a TRAGSATEC velar por el cumplimiento de esta obligación.