ANEXO 04

FUNCIONES Y OBLIGACIONES DEL PERSONAL EN MATERIA DE PROTECCIÓN DE DATOS

Contenido

1. INTRODUCCIÓN

1.1. ¿QUÉ ES LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES?

Es la normativa que regula la recogida y el tratamiento de los datos personales (dichos datos pueden ser de clientes, trabajadores, solicitantes de empleo, usuarios, etc.).

1.2. ¿QUÉ OBJETO TIENE?

Establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

Es decir, limitar el grado de intrusión en nuestra intimidad que pueden generar las nuevas tecnologías, así como el tráfico indiscriminado de datos personales.

1.3. ¿A QUIÉN INCUMBE LA LEY?

La ley obliga a su cumplimiento a todos los profesionales, empresas, organismos públicos y privados que traten con datos personales registrados en soporte informático o físico.

1.4. PRINCIPIOS QUE RIGEN LOS TRATAMIENTOS DE DATOS PERSONALES.

La normativa de protección de datos recoge los principios de actuación que deben regir el tratamiento de datos personales, tanto del responsable del tratamiento y sus empleados, como de los posibles encargados de tratamiento con los que se establezca una relación contractual.

En concreto estos principios se encuentran enumerados en el artículo 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (en adelante RGPD)

Literalmente se recoge:

1. Los datos personales serán:

   a) Tratados de manera lícita, leal y transparente en relación con el interesado **(licitud, lealtad y transparencia)**

      Es decir, para que el tratamiento sea lícito, conforme al Considerando 40 del RGPD, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho. Conforme al Considerando 39 del RGPD, cuando se dice que el tratamiento debe ser leal, significa que para las personas físicas, debe quedar totalmente claro que se están recogiendo, utilizando, consultado o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. En cuanto al principio de transparencia se exige que toda la información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.

   b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales **(limitación de la finalidad)**

   c) Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados **(minimización de datos)**

      Es decir, los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.

   d) Exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan **(exactitud)**.

      Es decir, conforme al considerando 39 del RGPD deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos.

   e) Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o

fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación delas medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado **(limitación del plazo de conservación)**

Conforme al considerando 39 del RGPD para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

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

Conforme al considerando 39 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 uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo **(responsabilidad proactiva)**.

Conforme al considerando 74 el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las persona físicas.

1.5. ¿QUÉ SON LOS DATOS PERSONALES?

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

Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- Son datos de carácter personal:
- El nombre y apellidos de una persona.
- Teléfono fijo o móvil.
- Dirección postal.
- Correo electrónico.
- DNI / NIF.
- Dirección IP.
- Una fotografía.
- Una grabación de vídeo.
- Cualquier otra información de la que se desprendan datos personales.

1.6. CLASIFICACIÓN DE LOS DATOS PERSONALES

Los datos de carácter personal se pueden clasificar en:

- **Datos identificativos:** nombre y apellidos, dirección postal, dirección electrónica, teléfono, DNI/NIF, SS/mutualidad, imagen, voz, firma o huella digitalizada, firma electrónica, etc.
- **Datos de características personales:** estado civil, familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.
- **Datos de circunstancias sociales:** características de alojamiento, vivienda, situación militar, propiedades y posesiones, aficiones y estilo de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.
- **Datos académicos y profesionales:** formación y titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o a asociaciones profesionales.
- **Datos de empleo:** profesión, puestos de trabajo, datos no económicos de nómina, historial del trabajador.

- **Datos de información comercial:** actividades y negocios, licencias comerciales, suscripciones a publicaciones y medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.
- **Datos económicos, financieros y de seguros:** ingresos y rentas, inversiones y bienes patrimoniales, créditos, préstamos y avales, datos bancarios, planes de pensiones, jubilación, datos económicos de nómina, deducciones impositivas, impuestos, seguros, hipotecas, subsidios y beneficios, historial de créditos, tarjetas de crédito.
- **Datos de transacciones de bienes y servicios:** bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones financieras, compensaciones, indemnizaciones.
- **Categorías especiales de datos personales:** son aquellos datos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como los datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

1.7. MEDIDAS DE SEGURIDAD

No es lo mismo tratar datos meramente identificativos para, por ejemplo, realizar la facturación de un servicio, que tratar el historial médico, o la vida sexual de una persona.

Hay datos mucho más sensibles que otros, y que necesitan de una mayor protección para garantizar la confidencialidad e integridad de los mismos.

En particular, los datos más sensibles (y que deben ser objeto de una mayor protección) son los detallados como categorías especiales de datos personales del apartado anterior.

Deben implantarse medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

1.8. ¿QUÉ ES UN TRATAMIENTO DE DATOS PERSONALES?

Es 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.

1.9. ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO?

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

1.10. ¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Por ejemplo, la asesoría laboral del responsable, que realiza las nóminas de sus trabajadores, es un encargado del tratamiento.

1.11. OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO DEL TRATAMIENTO

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos. Dichas medidas se revisarán y actualizarán cuando sea necesario.

La normativa también establece los requisitos documentales necesarios para poder cumplir con la citada normativa y poder ser capaz de demostrar dicho cumplimiento

Entre la documentación mínima que debe dispone la entidad se encuentra:

- El Registro de Actividades de Tratamiento, tanto como responsable del tratamiento, como encargado del tratamiento, en su caso.
- Documentación del análisis de riesgos realizado.

- La/s Evaluación/es de Impacto relativa/s a la Protección de Datos, en su caso.
- Las medidas de seguridad implantadas.
- Las funciones y obligaciones del personal con acceso a datos personales.
- El registro de incidencias y el registro de las notificaciones de las violaciones de la seguridad a la Autoridad de Control, en su caso.
- Los protocolos de atención a los derechos de los interesados.
- Los compromisos de confidencialidad con los trabajadores.
- Los contratos de acceso a datos por cuenta de terceros.
- La documentación relativa a las transferencias internacionales de datos, así como las garantías apropiadas obtenidas o las excepciones utilizadas como base jurídica para su realización.
- Toda la documentación adicional que sea necesaria para demostrar el cumplimiento de la normativa de protección de datos en la entidad (cláusulas legales, consentimientos otorgados por los interesados, autorizaciones para la contratación de subencargados del tratamiento, ponderaciones del interés legítimo, etc.).

Esta documentación debe mantenerse en todo momento actualizada y debe ser revisada siempre que se produzcan cambios que puedan repercutir en el cumplimiento de la normativa de protección de datos o en las medidas de seguridad implantadas, como son cambios relevantes en:

- la organización
- el contenido de la información incluida en los tratamientos
- los tratamientos de datos personales realizados
- los sistemas de tratamiento empleados

Debe mantenerse adecuada, en todo momento, a las disposiciones vigentes en materia de protección de los datos de carácter personal.

1.12. LOS DERECHOS DE LOS INTERESADOS

Los derechos que los interesados pueden solicitar al responsable del tratamiento son los siguientes:

- Derecho de acceso.
- Derecho de rectificación.
- Derecho de supresión («el derecho al olvido»).
- Derecho a la limitación del tratamiento.
- Derecho a la portabilidad de los datos.
- Derecho de oposición.
- Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.

El protocolo, los plazos y la forma de actuación está detallada en el ANEXO X, "Protocolos de atención a los derechos". El personal podrá solicitar una copia del mismo en cualquier momento.

Cualquier usuario que reciba una solicitud por parte de un interesado, deberá rellenar el formulario "GESTIÓN DE SOLICITUDES DE DERECHOS DE LOS INTERESADOS", que se encuentra en el APÉNDICE II, y remitirlo cuanto antes al Delegado de Protección de Datos o al responsable de gestionar los derechos de los interesados.

2. FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Usuario es todo el personal autorizado que accede a los datos de carácter personal para el desempeño de las funciones propias de su puesto de trabajo.

Todos los usuarios tienen la obligación de colaborar con el responsable del tratamiento para velar por el cumplimiento de la legislación vigente sobre protección de datos personales.

Los usuarios deben respetar los procedimientos definidos para gestionar la seguridad de la información personal que se detallan a continuación.

2.1. OBLIGACIONES GENERALES

- Guardar secreto y confidencialidad de la información tratada. Quienes intervienen en cualquier fase del tratamiento de los datos personales, están obligado al secreto profesional respecto a los datos y al deber de guardarlos, obligaciones que continúan incluso después de finalizar las relaciones con el responsable del tratamiento.
- La vulneración del deber de secreto respecto a los datos personales tratados, será considerado una falta grave, lo cual dará lugar al inicio de acciones disciplinarias, si proceden.
- No podrá enviarse información confidencial de la empresa al exterior, ni mediante soportes materiales ni a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso, salvo que se encuentre expresamente autorizado. De esta forma el envío del ANEXO 14 con los datos de adecuación de la empresa en materia de protección de datos personales, ha de estar autorizada expresamente.
- La información de EL RESPONSABLE DE TRATAMIENTO es propiedad de éste. Se considera información confidencial, a título enunciativo y sin carácter limitativo: bases de datos de personal, bases de datos de proveedores, colaboradores, voluntarios, y cualquier otro material que forme parte de las actividades propias de EL RESPONSABLE DE TRATAMIENTO.
- Los usuarios deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar, directamente ni a través de terceras personas o

empresas, la información a la que tengan acceso durante su relación laboral/profesional con EL RESPONSABLE DE TRATAMIENTO, registrada en cualquier tipo de soporte. Esta obligación continuará vigente tras la extinción del contrato laboral/mercantil.

- Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.
- Los sistemas de información, recursos, y la información personal a la que se accede, sólo se debe utilizar para las labores estrictamente profesionales que el usuario tiene asignadas.
- Facilitar a los interesados el ejercicio de sus derechos. Para ello, recogerá la solicitud escrita y la trasladará al responsable correspondiente para su atención según el protocolo establecido.

2.2. PUESTOS DE TRABAJO

- Los usuarios tienen acceso únicamente a aquellos recursos que precisan para el desarrollo de sus funciones.
- El identificador de usuario o clave de acceso son individuales y no deben ser comunicados a otras personas. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del responsable del sistema con el fin de que le asigne una nueva clave.
- Cada usuario es responsable de la confidencialidad de la contraseña que tiene para acceder a los sistemas de información. En caso que de forma accidental o intencionada esta contraseña sea conocida por personas no autorizadas, deberá registrarlo como incidencia y proceder al cambio de la misma.
- El usuario deberá cambiar la contraseña inicial asignada en el primer acceso que realice al sistema, o tras el desbloqueo de su contraseña cuando haya sido necesaria la intervención de una tercera persona para realizar el proceso. Las contraseñas deberán ser lo suficientemente complejas para no ser adivinadas de forma sencilla por un tercero. Para ello, se deberán seguir las siguientes normas para elegir la contraseña:

- Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
- No deberán coincidir, ni siquiera en parte, con el código de usuario.
- No deberán estar basados en cadenas de caracteres que sean fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).

- El usuario deberá aplicar las reglas nemotécnicas para poder construir una contraseña lo suficientemente compleja como para que no pueda ser adivinada por terceros y a la vez sean muy fáciles de recordar por él.
- Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible a personas no autorizadas.
- Los puestos de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad, así como las pantallas, impresoras y cualquier otro dispositivo conectado al puesto de trabajo y desde el que sea posible tener acceso a datos de carácter personal.
- Cuando el responsable del puesto de trabajo lo abandone, bien temporalmente, o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. Para reanudar el trabajo será necesaria la introducción de una contraseña que desactive el protector de pantalla. Deberá retirar también cualquier soporte, como documentos, fichas, discos, u otros que contengan datos del fichero, y proceder a guardarlos en su ubicación protegida habitual.
- En el caso de las impresoras, deberá asegurarse que no quedan documentos con datos personales en la bandeja de salida. Si las impresoras son compartidas, el usuario que ha mandado la impresión deberá retirar los documentos conforme vayan siendo impresos.
- Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a sistemas o redes exteriores, que no esté autorizada previamente por el responsable del tratamiento.

- Se deberá evitar el guardar copias de los datos personales en ficheros temporales. En caso de que el tratamiento haga imprescindible realizar dichas copias, se deberán adoptar las siguientes precauciones: realizar siempre las copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por el disco duro, y siempre sea posible conocer dónde están los datos temporales. Tras realizar el tratamiento que ha requerido estos datos temporales, proceder a su inmediata eliminación.

- Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir las medidas de seguridad que les corresponda en función de los datos que contienen.

- El trabajo fuera de los locales del responsable del tratamiento, solo se podrá realizar cuando exista una autorización previa del responsable del tratamiento o del encargado del tratamiento, en todo caso, deberá garantizarse la seguridad de esos datos.

- No deberá copiarse, ni transportar información en portátiles, o equipos que se encuentren fuera de las oficinas sin la correspondiente autorización del responsable del tratamiento. Especial consideración deberán tener los puestos de trabajo portátiles, como ordenadores portátiles o PDA. Estos dispositivos portátiles, cuando puedan almacenar datos personales, deberán contar con una autorización especial por parte del responsable del tratamiento.

2.3. ACTIVIDADES PROHIBIDAS

- Intentar distorsionar o falsear los registros LOG del sistema o del programa de gestión.

- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de EL RESPONSABLE DE TRATAMIENTO.

- Destruir, alterar, inutilizar o de cualquier otra forma dañar voluntariamente los datos, programas o documentos electrónicos de EL RESPONSABLE DE TRATAMIENTO o de terceros.

- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de EL RESPONSABLE DE TRATAMIENTO, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de EL RESPONSABLE DE TRATAMIENTO o de terceros.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema, sin autorización para ello.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por EL RESPONSABLE DE TRATAMIENTO, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- Borrar voluntariamente cualquiera de los programas instalados legalmente.
- Utilizar los recursos telemáticos de EL RESPONSABLE DE TRATAMIENTO, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de EL RESPONSABLE DE TRATAMIENTO, en la red corporativa del mismo.
- Utilizar ordenadores personales que no estén expresamente autorizados.

2.4. GESTIÓN DE SOPORTES

Se entiende por soporte todo objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Ejemplos de soportes: disquetes, cd-rom, dvd-rom, memoria usb, disco duro, etc.

Los usuarios deben observar las siguientes medidas de seguridad en relación con los soportes que contengan datos de carácter personal:

- Sólo están autorizados como soportes de almacenamiento de datos los homologados por EL RESPONSABLE DE TRATAMIENTO.
- Los usuarios que traten los soportes o documentos con datos de carácter personal, son los encargados de custodiarlos y vigilar para que personas no autorizadas no accedan al soporte físico o documentos a su cargo.
- Queda prohibida la utilización de ordenadores u otros dispositivos portátiles personales por parte del personal de EL RESPONSABLE DE TRATAMIENTO que no estén expresamente autorizados por el Responsable de Seguridad.
- Cuando un usuario gestione o produzca soportes que contengan datos de carácter personal, estos deberán estar claramente identificados con una etiqueta externa y, en su caso, inventariados según el protocolo establecido.
- Los soportes que contengan datos personales, deberán ser almacenados en lugares a los que no tenga acceso el personal no autorizado.
- La salida de soportes que contengan datos de carácter personal de las instalaciones bajo control del responsable del tratamiento, deberá ser autorizada previamente.
- La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o añejos a un correo electrónico, fuera de los locales bajo el control del responsable fichero o tratamiento, deberá ser autorizada previamente.
- El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación. En cualquier caso, se adoptarán las medidas necesarias dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. En todo momento el maletín o

contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

- Cuando deban ser enviados datos personales sensibles fuera de las ubicaciones del responsable del tratamiento, ya sea mediante soporte físico de grabación de datos o bien a través de correo electrónico o FTP, deberán ir cifrados o utilizar cualquier otro mecanismo que asegure que la información no es accesible ni manipulada durante su transporte.

2.4.1. DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

- Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

- Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al responsable del tratamiento.

- Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al responsable del tratamiento para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su

destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

2.5. FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir las medidas de seguridad que les corresponda.

Todo fichero temporal o copia de trabajo así creado es borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Si en el desarrollo del trabajo se necesita almacenar datos de carácter personal en ordenadores o en cualquier soporte informático, el usuario se responsabiliza de adoptar las medidas de seguridad oportunas mientras dichos datos se mantengan.

2.6. DOCUMENTACIÓN EN PAPEL (NO AUTOMATIZADA)

- **Custodia de documentación**

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

- **Traslado de documentación**

Siempre que se proceda al traslado físico de documentación que contenga datos personales (especialmente si son sensibles), deberán adoptarse las medidas que impidan el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma. Para ello, el traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación y en todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

- **Criterios de archivo**

Archivar los soportes o documentos en papel garantizando su correcta

conservación, localización y consulta de la información, de modo que posibilite el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

- **Dispositivos de almacenamiento**

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal disponen de mecanismos que obstaculizan su apertura.

En el caso de categorías especiales de datos: Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal se encuentran en áreas en las que el acceso está protegido.

- **Entrega documentación en soporte papel**

Queda estrictamente prohibido la entrega o envío de información en soporte papel relativa a personas físicas en sobres, cajas, o cualquier otro recipiente que no esté herméticamente cerrado, y cuya apertura no suponga la rotura del precinto. La entrega se realizará únicamente al titular de los datos o, a la persona que haya autorizado por escrito.

Queda estrictamente prohibido el envío de información relativa a personas físicas, o confidencial a través de medios que no aseguren el cumplimiento de las normas de seguridad exigidas por EL RESPONSABLE DE TRATAMIENTO.

- **Copia o reproducción**

Deben destruirse las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

En el caso de categorías especiales de datos: La generación de copias o la reproducción de los documentos únicamente se realiza por el personal autorizado.

- **Acceso a la documentación**

En el caso de categorías especiales de datos: El acceso a la documentación se

limita exclusivamente a los usuarios autorizados.

El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado.

Se han establecido mecanismos que permiten identificar los accesos realizados en el caso de documentos, que puedan ser utilizados por múltiples usuarios.

- **Destrucción de la documentación**

Uno de los mayores peligros para la confidencialidad de los datos son los documentos desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.

Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.

En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.

Queda prohibido deshacerse de la documentación impresa mediante su depósito en papeleras, contenedores o bolsas de basura.

El responsable del tratamiento deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

2.7. GESTIÓN DE INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa de protección de datos personales, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos personales en sus tres vertientes de confidencialidad, integridad y disponibilidad, como pueden ser la detección de un posible ciberataque o la pérdida o robo de dispositivos donde se almacene o desde donde se acceda a la información de la empresa.

Se deberán tener en cuenta, entre otras, las siguientes incidencias:

I. Incidencias que afecten a la confidencialidad:

- Lectura no autorizada de la información contenida en los ficheros o sistemas de información.
- Copia no autorizada de la información.
- Error en la distribución: que se entreguen informes, soportes, correspondencia, etc. a personas distintas de sus destinatarios.
- Manipulación no autorizada de la información.
- Obtención de información desde soportes desechados.
- Obtención de información desde equipos o soportes destinados a su reutilización.
- Descifrado de la información o de las claves.

II. Incidencias que afectan a la integridad:

- Modificación no autorizada de la información directamente de los ficheros o sistemas de información.
- Borrado no autorizado de la información.
- Destrucción parcial o total de la información por fallos en equipos, incendios,
- Inundaciones, tormentas, etc.
  Imposibilidad de reconstruir los datos partiendo de sus copias de respaldo.
- Alteración o borrado de la información durante su explotación ocasionado por fallos en el programa.

III. Incidencias que afectan a la disponibilidad:

- Modificaciones no autorizadas de permisos de acceso lógico a los ficheros.
- Imposibilidad o limitación del uso de las instalaciones por fenómenos meteorológicos, huelgas, manifestaciones, etc.
- Indisponibilidad de los sistemas por fallos informáticos.

IV. Incidencias que afectan a la autenticación:

- Suplantación del usuario autorizado:
  - Por cesión de la clave.
  - Por conocimiento de la clave de acceso.
  - Por violación de los controles de acceso.
- Fallos en los programas o dispositivos de control de acceso lógico.
- Fallos en su gestión por bajas de personas no comunicadas o autorizaciones de acceso improcedentes.

Todos los usuarios, administradores, responsables, así como cualquier persona que tenga acceso a datos de carácter personal, deben tener conocimiento de este procedimiento para actuar en caso de incidencia que se detalla a continuación:

Cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad, disponibilidad o integridad de los datos contenidos en los ficheros de la organización, deberá comunicarla inmediatamente al responsable del registro de incidencias a través del **formulario GESTIÓN DE INCIDENCIAS** anexado al final de este documento, del que se le ha hecho entrega a cada trabajador. Deberá especificar el tipo de incidencia producida y su descripción detallada, indicando las intervenciones de las personas que hayan podido tener relación con la producción de la incidencia, así como la fecha y hora en que se ha producido o detectado, la persona que realiza la notificación, a quién se comunica y los efectos que se pueden haber derivado de la incidencia.

Una vez rellena la plantilla, se obtendrán 2 copias y se entregarán

inmediatamente al responsable del tratamiento, Delegado de Protección de Datos, o a la persona en quien haya delegado la gestión de las incidencias, solicitándole el acuse de recibo en una de las copias. Esta copia se guardará como resguardo de la notificación.

El responsable del tratamiento, Delegado de Protección de Datos, o a la persona en quien haya delegado la gestión de las incidencias, quedará a cargo de la gestión, coordinación y resolución de la misma, así como al registro de la incidencia en el registro habilitado para ello.

El conocimiento y no notificación de una incidencia por parte de un usuario, será considerado como una falta de seguridad por parte de ese usuario.

2.8. PRUEBAS CON DATOS REALES

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal deberán comunicarse al Responsable de Seguridad o Personal de Informática.

2.9. TELECOMUNICACIONES

En el caso de las categorías especiales de datos: La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realiza cifrando los datos o bien utilizando mecanismos que garantizan que la información no es inteligible ni manipulada por terceros.

2.10. USO DEL CORREO ELECTRÓNICO

El sistema informático, la red corporativa y los terminales utilizados por cada usuario son propiedad de EL RESPONSABLE DE TRATAMIENTO.

Queda expresamente prohibida la utilización de cuentas de correo electrónico para uso personal.

EL RESPONSABLE DE TRATAMIENTO se reserva el derecho a revisar, sin previo aviso, los ficheros LOG de los servidores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a EL RESPONSABLE DE TRATAMIENTO como responsable civil subsidiario.

No se deberán abrir correos procedentes de direcciones desconocidas o que

no estén relacionadas con motivos de trabajo y ofrezcan las suficientes garantías, con el fin de evitar la entrada de virus.

Queda estrictamente prohibido el envío de mensajes de correo electrónico de forma masiva o con fines publicitarios o comerciales no solicitados o expresamente autorizados por el destinatario (spam).

Los mensajes de correo electrónico de la red corporativa que se envíen a múltiples destinatarios deben realizarse haciendo uso del campo de copia oculta (CCO).

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

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

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

- Realizar tareas de mantenimiento del correo electrónico.
- Garantizar la continuidad de la actividad en ausencia o cese de la persona trabajadora.

- Comprobar el uso del correo, en el seno de una información reservada o de un procedimiento disciplinario, cuando haya indicios de un posible mal uso.

1. Acceso para realizar tareas de mantenimiento del correo electrónico

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

2. Acceso para garantizar la continuidad de la actividad laboral

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

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

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

Sobre el acceso al correo electrónico cuando se produce el cese de la relación laboral:

- Cuando una persona trabajadora deje de prestar servicios en la empresa, el órgano competente, en materia de gestión de personal lo comunicará inmediatamente al responsable de seguridad para

que se inutilicen los códigos de usuario y las contraseñas del trabajador.

- La empresa procederá a incluir un mensaje de respuesta automático programado por un tiempo prudencial para dicha cuenta de correo electrónico. Así, cuando se produzca el envío de emails a la dirección de correo electrónico del extrabajador se indicará con un correo automático de respuesta, que la dirección de correo electrónico ha causado baja en la empresa y que la nueva dirección de correo electrónico con la que se deben de poner en contacto es aquella identificada como la persona o departamento que le sustituye.

- Respecto de los mensajes privados en el correo corporativo, la empresa tiene que facilitar a la persona trabajadora la obtención de los mensajes privados de la cuenta de correo, siempre que no superen el periodo máximo de conservación establecido en las normas de uso del correo para los mensajes de esta naturaleza. Se accederá a los mensajes privados en presencia de la persona trabajadora con el fin de identificar los mensajes de carácter exclusivamente personal. La persona trabajadora tiene derecho a obtener los mensajes personales que en ese momento se puedan identificar como tales. Los mensajes se pueden **borrar o transferir a otra cuenta de correo**, una vez haya transcurrido el plazo otorgado (es discrecional) a la persona trabajadora sin que haya manifestado la intención de llevarse o destruir los mensajes privados que en ella se contenían. El resto de los mensajes, se pueden analizar para determinar si resultan necesarios para la continuidad de la actividad o bien, si se pueden suprimir.
- En caso de defunción de la persona trabajadora, los mensajes personales se pueden borrar, sin perjuicio de que se mantengan, debidamente bloqueados, si las circunstancias lo aconsejan.
- En supuestos excepcionales (puestos de relevancia estratégica para la empresa o despidos conflictivos), en los que la empresa necesite saber por cuestiones de negocio o empresariales si ha existido dicha comunicación de clientes o terceros con el extrabajador, y por tanto

lo que se hará en esos casos, será lo indicado en el apartado anterior y, además, la empresa podrá, redirigir el correo electrónico que recibía el extrabajador a otra cuenta de correo o bien, autorizar el acceso a alguien que se designe internamente. Así pues, en casos justificados (puestos de responsabilidad, para garantizar la continuidad de la actividad, para comprobar notificaciones relevantes dirigidas a la organización por parte de organismos públicos, etc.), la eliminación de la cuenta se puede demorar 1 mes o como máximo 3 meses en casos excepcionales, pudiendo acceder a las notificaciones que se reciban la persona responsable que designe la empresa. En esos casos también puede estar justificada la redirección del email a otra cuenta, durante dicho plazo máximo (1 mes prorrogable hasta 3).

3. Acceso cuando haya indicios de un posible mal uso

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

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

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

Si hay indicios de un mal uso del correo por parte de la persona trabajadora, por incumplir las normas que ha aprobado la empresa, se tiene que poner en

conocimiento de la persona trabajadora, a menos que esto pueda obstaculizar las investigaciones que procedan. Cuando este mal uso pueda ser constitutivo de delito o falta, se ha de comunicar a la autoridad policial o judicial competente.

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

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

2.11 ACCESO A INTERNET

EL RESPONSABLE DE TRATAMIENTO provee de sistemas de conexión a Internet a sus empleados para mejorar los sistemas de trabajo y búsqueda de información. Este sistema es propiedad de EL RESPONSABLE DE TRATAMIENTO y se reserva el derecho de conceder o anular dichos accesos conforme a los criterios que crea convenientes.

El acceso a páginas web (www), grupos de noticias (newsgroups) y otras fuentes de información como FTP, etc. se limita a aquellas que contengan información relacionada con la actividad de EL RESPONSABLE DE TRATAMIENTO o con los cometidos del puesto de trabajo del usuario.

Queda prohibido el acceso a debates en tiempo real (chat/IRC) por ser peligroso al facilitar la instalación de utilidades que permiten accesos no autorizados al sistema.

EL RESPONSABLE DE TRATAMIENTO se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a

Internet iniciada por un usuario de la red corporativa, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la empresa como responsable civil subsidiario.

2.12 PROPIEDAD INTELECTUAL

Queda estrictamente prohibido el uso de programas informáticos que no estén homologados por EL RESPONSABLE DE TRATAMIENTO.

EL RESPONSABLE DE TRATAMIENTO se reserva el derecho de revisar, sin previo aviso, los programas instalados en todos los ordenadores de la empresa, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a ésta como responsable civil subsidiario.

Antes de instalar cualquier programa se ha de contactar con el Departamento de sistemas.

2.13 USO DEL FAX

Se deberá comprobar con carácter previo que el interesado ha autorizado el envío de información mediante este medio.

Para gestionar las autorizaciones de los usuarios en el APENDICE III se encuentra el formulario "GESTION DE AUTORIZACIONES".

3. FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Deberá:

- Elaborar el Registro de Actividades de Tratamiento.
- Realizar el análisis de los riesgos y guardar la documentación del mismo, así como, en su caso, la evaluación de impacto relativa a la protección de datos.

- Implantar y hacer cumplir las medidas de seguridad establecidas.
- Garantizar la difusión y formación al personal que trate con datos personales de las medidas de seguridad y requisitos que deben cumplir para realizar el tratamiento de datos personales.
- Mantener actualizada la documentación siempre que se produzcan cambios relevantes en:
    - El sistema de información.
    - Es sistema de tratamiento.
    - La organización.
    - El contenido de la información incluida en los tratamientos.
    - Como consecuencia de los controles periódicos realizados.
        - Se considera que un cambio es relevante cuando pueda afectar al cumplimiento de las medidas de seguridad implantadas.
- Nombrar uno o varios responsables delegados para el correcto cumplimiento de la normativa de protección de datos.
- Verificar periódicamente la eficacia de las medidas de seguridad establecidas.
- Analizar las incidencias registradas e implantará las medidas correctivas necesarias para evitar ese tipo de incidencias en el futuro.

4. FUNCIONES Y OBLIGACIONES DEL DELEGADO DE PROTECCIÓN DE DATOS O FIGURA EQUIVALENTE

El Delegado de Protección de Datos tiene las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben;

b) supervisar el cumplimiento de lo dispuesto en la normativa de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier asunto relacionado con el cumplimiento de la normativa de protección de datos. Para ello:

   1. Coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del tratamiento en su difusión y cooperará con el responsable del tratamiento controlando el cumplimiento de las mismas.

   2. Analizará las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del tratamiento.

   3. Comprobará, periódicamente, la existencia de copias de respaldo que permitan la recuperación de los datos, realizando una prueba de restaurado que verifique la correcta definición de los procedimientos y procesos de recuperación, y enviando evidencias de esta comprobación al responsable del tratamiento.

4. A su vez, también periódicamente, comunicará el responsable del fichero cualquier cambio que se haya realizado en los sistemas de información, como cambios en el hardware o software, bases de datos, aplicaciones de acceso al fichero, etc., procediendo a la actualización de la documentación pertinente.

5. Verificará, periódicamente, la veracidad del inventario de soportes.

6. Tendrá el control directo de los mecanismos que permiten el registro de accesos, sin que se deba permitir, en ningún caso, la desactivación de los mismos.

7. Se encargará de revisar, en su caso y de forma periódica, la información de control registrada en el registro de accesos y elaborará un informe que entregará al responsable del tratamiento para su revisión y archivo.

8. Periódicamente realizará una auditoría de la eficacia de las medidas de seguridad implantadas.

9. Los resultados de los controles periódicos, así como de las auditorías, serán adjuntados a la documentación acreditativa del cumplimiento de la normativa de protección de datos.

5. NORMAS DE USO DE LOS DISPOSITIVOS DIGITALES

1. Equipamiento informático y recursos

Con carácter general, en la empresa está prohibido utilizar para fines privados los recursos informáticos y telemáticos de la empresa, incluido Internet y el correo electrónico, pues su cometido es que se utilicen exclusivamente para actividades directamente relacionadas con el puesto de trabajo del usuario y con la cuenta de correo electrónico facilitada por la organización.

2. Actividades prohibidas

Está totalmente prohibida la instalación del cualquier software o aplicación que no haya sido previamente autorizada por la organización, así como la utilización de la cuenta de correo electrónico corporativa para fines ajenos a la actividad de la organización.

No se deben dejar en ningún caso los **dispositivos móviles desatendidos** en lugares públicos, **coche,** etc.

3. Dispositivos portátiles y móviles

Los dispositivos portátiles y móviles (como ordenadores, tabletas, teléfonos, etc.) que la organización pone a disposición de sus empleados y que, eventualmente, pueden utilizarse fuera de sus instalaciones, podrán ser utilizados por los usuarios para uso privado exclusivamente fuera de horas laborales, con las limitaciones establecidas en el punto anterior.

En caso de que el usuario utilice los dispositivos digitales para uso privado, se recomienda que no almacene información personal propia en dicho dispositivo (como documentos privados, fotografías, etc.), pues puede ser objeto de las revisiones establecidas en el punto siguiente.

4. Acceso al contenido de los dispositivos digitales

Tal y como establece el artículo 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la organización podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la

integridad de dichos dispositivos.

En este sentido, la organización se reserva la posibilidad de adoptar las medidas que estime más oportunas de vigilancia y control, como son las revisiones de los dispositivos proporcionados o del servidor de correo electrónico, los recursos utilizados o las conexiones a Internet realizadas, entre otras, para verificar el cumplimiento, por parte del trabajador, de sus obligaciones y deberes laborales, con los límites establecidos por la Ley y la jurisprudencia.

Finalmente, los dispositivos y soportes personales con los cuales trabaja el personal deben ser inventariados para tenerlos controlados y que no se produzcan tratamientos de datos en soportes no inventariados.

Como modelo de inventario le facilitamos un ejemplo:

Dispositivo	Especificación	Cantidad
USB	8 gigas	2
Teléfono Movil	Motorolla	1
Smarthphone	Samsung Galaxy SV	1

Un ejemplar de un modelo de esta tabla debe ser entregado por cada empleado a la Dirección de LA EMPRESA.

El empleado que utilice sus propios dispositivos con fines laborales contemplará las siguientes medidas de seguridad:

Almacenamiento de la información. No almacenar información corporativa que no sea estrictamente necesaria para el desarrollo del trabajo.
Tratamiento de información confidencial Cifrar la información confidencial y eliminarla de forma segura (o solicitar la eliminación al técnico responsable).
Conexión a redes. Conectar el portátil a redes conocidas y privadas. Optar por una conexión 3G/4G cuando el resto de las redes disponibles no sean confiables.
Notificación en caso de infección Notificar al personal técnico responsable la sospecha de infección por virus u otro software malicioso del equipo.
Transporte y custodia. No exponer el equipo a altas temperaturas. No descuidar el portátil si viajas en transporte público, no guardarlo en el coche ni dejarlo visible o fácilmente accesible. Si se trabaja en lugares donde no se garantiza su custodia, ha de anclarse con un candado de seguridad o guardarlo en un armario de seguridad. En caso de robo o pérdida del equipo, se notifica al responsable.
Uso del puesto de trabajo. Aplicar las normas recogidas en la Política de uso del puesto de trabajo relativas al uso de un equipo informático (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, etc.).
Responsabilidades. Conocer las responsabilidades que conlleva el uso de dispositivos corporativos y aplicar las normas de seguridad correspondientes.

Firma de circular para empleados sobre normas de uso de los dispositivos digitales.

Nombre y apellidos del empleado_____

NIF_____

Fdo._____

6. POLÍTICA DE DESCONEXIÓN DIGITAL EN EL ÁMBITO LABORAL

1. Derecho a la desconexión digital en el ámbito laboral

Tal y como establece el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, los empleados de la empresa tienen derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Periodos de desconexión

Se respetarán y garantizarán los tiempos de descanso de los trabajadores, sus permisos y vacaciones. En dichos periodos, con carácter general, no se contactará con los trabajadores.

3. Excepciones

En su caso, se podrá contactar con el personal fuera de su horario laboral en un supuesto excepcional y con carácter de urgente necesidad, que pueda resolverse mediante una llamada o mensaje corto y que, si no se resuelve de forma inmediata, podría implicar un perjuicio para la entidad. En estos supuestos, podrá suscribirse, si es necesario, un acuerdo en el que se fije una hora u horquilla horaria para revisar los dispositivos digitales.

4. Teletrabajo y desconexión

En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

A dichos empleados les será a aplicación los criterios de desconexión digital indicados anteriormente, pudiendo concretarse, en cada caso particular, cuál es la franja horaria de "desconexión", en la que no se podrá contactar con el trabajador en cuestión, salvo las excepciones contempladas en el punto 3.

5. Acciones de sensibilización y formación

Todos los trabajadores deben conocer esta política de desconexión digital en

el ámbito laboral.

Para ello, la organización informará y concienciará, tanto a los trabajadores existentes, como a los nuevos trabajadores que se incorporen a la organización acerca de este derecho y, en su caso, del uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En especial, a los que ocupen puestos directivos o de mando.

7. POLÍTICA DE RETENCION DE DATOS

1. Objeto del procedimiento

El Reglamento 2016/679, 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 (en adelante, el "RGPD") pretende garantizar y proteger todo lo concerniente al tratamiento de los datos personales, es decir, el uso de cualquier información de personas físicas.

Mediante la presente Política de conservación de datos personales, se pretende establecer unas directrices de actuación relativas a determinar cuándo debe procederse a la conservación o a la destrucción de los datos, a los efectos de dar cumplimiento a las exigencias derivadas del deber de calidad.

2. Ámbito

La presente Política deberá ser observada por el RESPONSABLE DE TRATAMIENTO así como por las empresas que traten datos de carácter personal en calidad de Encargados del Tratamiento, siendo de aplicación respecto de datos que sean objeto tanto de tratamiento automatizado como de tratamiento no automatizado (soporte papel).

La presente Política deberá ser observada por todo el personal que maneje datos de carácter personal en el desarrollo de su actividad diaria.

3. Obligaciones de supresión de datos personales

3.1. Consideraciones previas

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el Responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

A tal efecto, la presente Política debe guiarse por Principio de limitación del plazo de conservación del apartado e) del artículo 5.1 del RGPD, en virtud del cual los datos personales deben ser "*mantenidos de forma que se permita la*

identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales".

Esta obligación resulta de aplicación para cuando la empresa actúe como responsable del tratamiento, pero a su vez, cuando actúe como encargado del tratamiento.

En particular, cuando la entidad tenga la consideración de Encargado del Tratamiento, de conformidad con el apartado g) del art. 28.3 del RGPD, una vez cumplida la prestación contractual que dio lugar al encargo del tratamiento, los datos personales deberán, a elección del responsable, ser suprimidos o devueltos al Responsable del tratamiento, debiendo suprimir asimismo las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.

3.2 Causas habilitantes de la supresión de los datos personales

3.2.1 Terminación de la condición legitimadora del tratamiento.

Cuando los mismos ya no sean útiles ni necesarios para la finalidad que justificó su recogida y tratamiento, o una vez cumplida y agotada dicha finalidad deberá procederse a la supresión de los datos personales, siempre y cuando no sea necesario proceder al bloqueo de los mismos para responder ante posibles responsabilidades derivadas del tratamiento de datos personales y por el plazo de prescripción de las mismas previstas en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, conforme se recoge en el apartado 4.

3.2.2 Ejercicio del derecho de supresión

Cuando el interesado ejerza el derecho de supresión de los datos personales, siempre que concurran alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21.1 del RGPD (derecho de oposición), y no prevalezcan otros motivos legítimos

para el tratamiento, o el interesado se oponga al tratamiento cuando éste tenga por objeto la mercadotécnica directa (artículo 21.2 del RGPD);

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a niños, mencionados en el artículo 8.1 del RGPD.

En estos casos, deberá procederse a la eliminación de los datos personales, siempre y cuando no sea necesario proceder al bloqueo de los mismos para responder ante posibles responsabilidades derivadas del tratamiento de datos personales y por el plazo de prescripción de las mismas previstas en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, conforme se recoge en el apartado 4.

No obstante lo anterior, no se aplicará el derecho de supresión, y por tanto los datos podrán continuar siendo tratados por el responsable del tratamiento cuando el tratamiento sea necesario:

i. para ejercer el derecho a la libertad de expresión e información;
ii. para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
iii. por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
iv. con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la

medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

v. para la formulación, el ejercicio o la defensa de reclamaciones.

4. Mecanismos de supresión de los datos personales

En los supuestos en que, en atención a los criterios anteriores, se concluya el deber de suprimir los datos personales, se deberá proceder a la eliminación física de los mismos ya se encuentren éstos en soporte automatizado o no automatizados:

- Si los datos están contenidos en soporte no automatizado, se deberá proceder a la destrucción física de los documentos. A tal efecto se recomienda:
    - La utilización de proveedores de servicio de destrucción documental.
    - La utilización de herramientas de destrucción física de papel, tal y como, destructoras de papel.
    - Opcionalmente, y en el caso en que la supresión tenga como origen el ejercicio de derecho de supresión, la supresión podrá tener lugar mediante la entrega de dicha información a la persona o personas que sean titulares de la misma.

- Si los datos están contenidos en soporte informático, se procederá de igual forma a su eliminación física de la aplicación, sin que sea suficiente el empleo de una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren los derechos de supresión.

Sin perjuicio de cualquier otro método de destrucción que pudiera valorarse, a continuación, se recogen los principales métodos de borrado identificados[1], clasificados en función de la capacidad efectiva para la eliminación lógica de los datos personales así como sus ventajas e inconvenientes.

Métodos que no destruyen la información de forma segura. Comandos de borrado. Destrucción de la información mediante la utilización de comandos de borrado del sistema operativo	Formateo	Formateo de un dispositivo
	Anonimización[2]	Su eficacia dependerá de la técnica de anonimización empleada en cada caso, que deberá garantizar de forma irreversible su identificación[3]
Métodos de destrucción de la información de forma segura	Desmagnetización	Exposición de los soportes de almacenamiento a un potente campo magnético.
	Destrucción	Podrá realizarse a través de diversos procedimientos mecánicos, en función de la naturaleza del soporte, en particular: • Desintegración, pulverización, fusión e incineración. • Trituración.
	Sobre-escritura	Escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Deberá asegurarse la sobre-escritura de la totalidad de la superficie de almacenamiento para asegurar la completa destrucción de los datos.

[1] Fuente. Guía sobre borrado seguro de la información. Instituto Nacional de Ciberseguridad (INCIBE), 2016.

[2] El Considerando 26 del RGPD concluye que "Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

[3] Véase "Dictamen 05/2014 sobre técnicas de anonimización" del Grupo de Trabajo del artículo 29.

5. Plazos legales de conservación de datos

En los casos en los que exista obligación legal de conservar los datos durante un periodo de tiempo determinado y/o durante los plazos de prescripción de las acciones que pudieran derivarse de la actividad o servicio prestado, la empresa procederá al bloqueo de los datos durante los referidos plazos.

Los datos bloqueados quedarán, únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas y/o durante los plazos legales establecidos al efecto. Cumplidos los indicados plazos, deberá procederse a la supresión de los datos bloqueados de acuerdo con lo descrito en el apartado 4.

Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica, en cada caso, para cada actividad de tratamiento.

Para ello, y sin perjuicio de cualesquiera otros plazos que puedan estar previstos en otras normas o circulares que resulten igualmente de aplicación, se recogen a continuación los plazos durante los cuales será necesario conservar los datos personales que hubiesen sido objeto de tratamiento en función de la actividad que tenga causa en el tratamiento de datos personales.

PLAZOS DE CONSERVACIÓN DE LA DOCUMENTACIÓN

PROTECCIÓN DE DATOS		
PLAZO	DESCRIPCIÓN	REF. LEGAL
3 AÑOS	Prescribirán las infracciones: - Muy graves, a los 3 años. - Graves, a los 2 años. - Leves, al año.	Artículos 72.1, 73.1 y 74.1 de la Ley Orgánica 3/2018 de 58 de diciembre, de Protección de datos y Garantía de Derechos Digitales (LOPD-GDD).

ACCIONES CIVILES PERSONALES		
PLAZO	DESCRIPCIÓN	REF. LEGAL
5 AÑOS	Acciones personales de todo tipo que no tengan plazo especial de prescripción fijado desde que pudiera exigirse la obligación, teniendo en cuenta que en las obligaciones continuadas de hacer o no hacer, el plazo comenzará cada vez que se incumplan. Régimen transitorio: – Acciones derivadas de relaciones jurídicas nacidas entre el 7/10/2000 y el 7/10/2005: plazo de prescripción de 15 años. – Acciones derivadas de relaciones jurídicas nacidas entre el 7/10/2005 y el 7/10/2015: 5 años después de la entrada en vigor de la ley, es decir, 7/10/2020. – Acciones derivadas de relaciones jurídicas nacidas a partir de 7/10/2015: plazo de prescripción de cinco (5) años.	Artículo 1962 del Código Civil Artículo 1939 del Código Civil en lo que se refiere al régimen transitorio.

DOCUMENTACIÓN DE CARÁCTER LABORAL O RELACIONADA CON SEGURIDAD SOCIAL		
PLAZO	DESCRIPCIÓN	REF. LEGAL
4 AÑOS	Documentación o los registros o soportes informáticos en que se hayan transmitido los correspondientes datos que acrediten el cumplimiento de las obligaciones en materia de colocación y empleo, afiliación, altas, bajas o variaciones que, en su caso, se produjeran en relación con dichas materias, así como los documentos de	Artículo 21.1 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

	cotización y los recibos justificativos del pago de salarios y del pago delegado de prestaciones. Añadir toda la documentación contractual: el RD 1424/2002, de 27 de diciembre, por el que se regula la comunicación del contenido de los contratos y de sus copias básicas, nada establece a este respecto, por lo que analógicamente aplicaremos el precepto anterior.	

DOCUMENTACIÓN CONTABLE Y FISCAL		
PLAZO	DESCRIPCIÓN	REF. LEGAL
6 AÑOS	A efectos mercantiles: Libros, correspondencia, documentación y justificantes concernientes a su negocio, debidamente ordenados, a partir del último asiento realizado en los libros, salvo lo que se establezca por disposiciones generales o especiales. Esta obligación mercantil se extiende tanto a los libros obligatorios (ingresos, gastos, bienes de inversión y provisiones, además de la documentación y justificantes en que se soporten las anotaciones registradas en los libros (facturas emitidas y recibidas, tickets, facturas rectificativas, documentos bancarios, etc.).	Art. 30 del Real Decreto de 22 de agosto de 1885, por el que se publica el Código de Comercio.
4 AÑOS	A efectos fiscales: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc.), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tenga trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y en consecuencia, a liquidar deuda tributaria.	Sección 3ª (La prescripción), Arts. 66 a 70 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

AUDITORÍA DE CUENTAS		
PLAZO	DESCRIPCIÓN	REF. LEGAL
5 AÑOS	Los auditores de cuentas y las sociedades de auditoría de cuentas conservarán y custodiarán durante el plazo de cinco años, a contar desde la fecha del informe de auditoría, la documentación referente a cada auditoría de cuentas por ellos realizada, incluidos los papeles de trabajo del auditor que constituyan las pruebas y el soporte de las conclusiones que consten en el informe.	Artículo 30 de 22/2015, de 20 de julio, de Auditoría de Cuentas.

VIDEOVIGILANCIA		
PLAZO	DESCRIPCIÓN	REF. LEGAL
1 MES	Las imágenes/sonidos captados por los sistemas de video vigilancia serán canceladas en el plazo máximo de un mes desde su captación.	Art. 22 LOPD-GDD. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
1 MES	Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.	Artículo 8 de la Ley Orgánica 4/1997, de 4 de agosto, de utilización de videocámaras por fuerzas y cuerpos de seguridad en lugares públicos. Ver también artículos 18 y 19 del RD 596/1999 de 16 de abril.
10 DÍAS	Colocación en zonas comunes centro escolar para protección de los menores: "También contribuiría a la ponderación que estamos realizando la implantación de unos periodos de conservación muy reducidos para la	Informe Jurídico AEPD 475/2014

	conservación de las imágenes guardadas. La Instrucción 1/2006 establece en su artículo 6 un plazo de un mes desde su captación. Pero podría incluso reducirse ese plazo, teniendo en cuenta que si hubiera acaecido un suceso que afectara a los menores debería ser apreciado en un lapso de tiempo mucho más breve. Así, entendemos que podría establecerse un plazo de diez días, que por un lado es inferior a un mes, pero suficientemente extenso para que el centro docente haya podido percatarse de la existencia de un perjuicio concreto y específico para el menor que pudiera tener consecuencias jurídicas, coincidiendo así con el plazo para el ejercicio del derecho de cancelación de los datos, y conciliado con la protección de los datos personales. Transcurrido dicho plazo de diez días sólo podría conservarse las imágenes que revelaran algún tipo de hecho trascendente en relación con el interés superior del menor"	

CONTROL ACCESOS A EDIFICIOS		
PLAZO	DESCRIPCIÓN	REF. LEGAL
1 MES	Los datos incluidos en ficheros automatizados creados para controlar el acceso a edificios, deben cancelarse transcurrido 1 mes a partir de su obtención.	Norma quinta de la Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.

CONSUMIDORES Y USUARIOS		
PLAZO	DESCRIPCIÓN	REF. LEGAL
3 AÑOS	La acción para reclamar el cumplimiento de la reparación y sustitución del producto por cualquier disconformidad con el	Artículo 123.4 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se

	contrato, prescribe a los tres años desde la entrega del producto.	aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
6 MESES	La acción para reclamar el cumplimiento de lo dispuesto en la garantía comercial adicional prescribe a los seis meses desde la finalización del plazo de garantía.	Artículo 125.3 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
3 AÑOS	La acción o derecho de recuperación de los productos entregados por el consumidor y usuario al empresario para su reparación prescribe a los tres años a partir del momento de la entrega.	Artículo 127 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
3 AÑOS	La acción de reparación de los daños y perjuicios causados por productos fabricados o importados prescribirá a los tres años, a contar desde la fecha en que el perjudicado sufrió el perjuicio, ya sea por defecto del producto o por el daño que dicho defecto le ocasionó, siempre que se conozca al responsable de dicho perjuicio.	Artículo 143 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

SERVICIOS DE SOCIEDAD DE LA INFORMACIÓN Y COMERCIO ELECTRÓNICO

PLAZO	DESCRIPCIÓN	REF. LEGAL
3 AÑOS	Prescribirán las infracciones: - Muy graves, a los 3 años. - Graves, a los 2 años. - Leves, a los 6 meses.	Artículo 45 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

APÉNDICE I GESTION DE INCIDENCIAS

GESTIÓN DE INCIDENCIAS			
FECHA		HORA	
TIPO DE INCIDENCIA			
DESCRIPCIÓN:			
EFECTOS DERIVADOS:			
PERSONA QUE COMUNICA LA INCIDENCIA			
PERSONA QUE RECIBE LA NOTIFICACIÓN			
ACUSE DE RECIBO			
FECHA		HORA	
FIRMA:			

APÉNDICE II GESTION DE SOLICITUDES DE DERECHOS

GESTIÓN DE SOLICITUDES DE DERECHOS DE LOS INTERESADOS			
FECHA		HORA	
NOMBRE DEL SOLICITANTE			
APELLIDOS DEL SOLICITANTE			
NIF DEL SOLICITANTE			
DOMICILIO DEL SOLICITANTE			
DERECHO QUE DESEA EJERCER	[ ] ACCESO [ ] RECTIFICACIÓN [ ] SUPRESIÓN [ ] LIMITACIÓN DEL TTO [ ] OPOSICIÓN [ ] PORTABILIDAD [ ] DECISIONES INDIVIDUALES AUTOMATIZADAS		
OBSERVACIONES:			
[ ] FOTOCOPIA DEL NIF INCLUIDA			
[ ] OTROS DOCUMENTOS APORTADOS:			
PERSONA QUE RECIBE LA SOLICITUD			

APÉNDICE III GESTION DE AUTORIZACIONES TEMPORALES

GESTIÓN DE AUTORIZACIONES TEMPORALES			
FECHA		HORA	
AUTORIZANTE (Responsable Seguridad o DPD)			
AUTORIZADO			
PERFIL			
AUTORIZACIONES	[ ] **Permiso para acceder al lugar donde se almacenan soportes y/o documentos** [ ] **Permiso para sacar de la empresa soportes y/o documentos (incluidos los anejos a un email, por FTP o similar)** [ ] **Permiso para entregar soportes y/o documentos con datos de nivel medio y alto** [ ] **Permiso para recepcionar soportes y/o documentos** [ ] **Permiso para tratar datos de la empresa fuera de las instalaciones** [ ] **Permiso para tratar datos de la empresa en dispositivos portátiles (Tablet, teléfono móvil, ordenador portátil)** [ ] **Permiso para recuperar datos de nivel medio y alto** [ ] **Permiso para acceder a los lugares donde se encuentra el sistema de información (servidor, CPD)** [ ] **Permiso para realizar copias o reproducciones de documentos que contengan datos de nivel alto** [ ] **Permiso para acceder como administrador a la cuenta de hosting(web y email)** [ ] **Permiso para acceder como administrador a la infraestructura de comunicaciones (router, etc.)**		
FECHA INICIO DE AUTORIZACION:			
FECHA FIN DE AUTORIZACIÓN:			
FIRMA AUTORIZANTE	FIRMA AUTORIZADO		