PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

BEKA ASSET MANAGEMENT, SGIIC, S.A.

REGISTRO DOCUMENTAL

Responsable Proceso:	Responsable de seguridad

	FECHA	NOMBRE	UNIDAD ORGANIZATIVA	FIRMA
Elaborado			Delegado de Protección de Datos	
Revisado	22/12/2020		Responsable de Seguridad, Administrador del sistema y Administración	
Revisado				
Aprobado	29/12/2020		Consejo de Administración	

1.- CONTROL DE EDICIONES

FECHA	EDICIÓN	CONCEPTO	MODIFICACIÓN REALIZADA	APARTADOS / PAG. O CONTROL REVISIÓN
29/12/2020	1			

2.- NIVEL DE DIFUSIÓN

FECHA	CÓDIGOS DEPARTAMENTOS					
29/12/2020	General					

ÍNDICE

1. OBJETIVO DEL REGLAMENTO 5
2. ÁMBITO DE APLICACIÓN 6
   2.1 Ámbito jurídico 6
   2.2 Ámbito de la información 6
   2.3 Ámbito material 6
   2.4 Ámbito territorial 6
3. CONCEPTOS BÁSICOS 7
   3.1 Datos de carácter personal 7
   3.2 Tratamiento de datos de carácter personal. 8
   3.3 Responsable del tratamiento. 8
   3.4 Encargado del tratamiento. 9
   3.5 Tratamiento 10
   3.6 Principios relativos al tratamiento. 11
4. PRINCIPIO DE RESPONSABILIDAD PROACTIVA 12
5. DERECHOS DE LOS INTERESADOS 14
   5.1 Condiciones generales aplicables 15
   5.2 Procedimiento de ejercicio de los derechos de la persona afectada. 16
6. DEBER DE INFORMACIÓN 21
7. IDENTIFICACIÓN DE LA LEGITIMACIÓN EN EL TRATAMIENTO DE DATOS 24
   7.1 Cumplimiento de la obligación legal. 24
   7.2 Consentimiento. 24
   7.3 Tratamiento de categorías especiales de datos. 25
8. REGISTRO DE ACTIVIDADES DEL TRATAMIENTO 26
   8.1 Detalle de las actividades de tratamiento 27
9. SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS 29
   9.1 Análisis de riesgos 29
   9.2 Implantación de medidas de seguridad. 30
   9.3 Gestión de la violación o quiebras de la seguridad de los datos. 38
   9.4 Excepción de comunicación de las violaciones de seguridad a la AEPD 38
   9.5 Comunicación de violaciones de seguridad a la AEPD 39
   9.6 Comunicación de violaciones de seguridad a los interesados. 40
   9.7 Excepción de comunicación a los interesados. 41
   9.8 Forma de llevar a cabo las comunicaciones. 41
   9.9 Notificación, gestión y respuesta de violaciones de seguridad de los datos. 41
10. EVALUACIÓN DE IMPACTO (EIPD) 44
   10.1 Necesidad de evaluación del impacto. 45
   10.2 Contenido de la EIPD 45
   10.3 Consulta previa a la AEPD 46
11. ORGANIZACIÓN INTERNA 46

11.1 Consejo de Administración 47
11.2 Empleados y agentes 47
11.3 Funciones y Obligaciones del Responsable de Seguridad. 51
11.4 Funciones y Obligaciones del Administrador de Sistemas. 52
12. TRANSFERENCIA INTERNACIONAL DE DATOS. 55
13. INFRACCIONES Y SANCIONES 55
14. PROCEDIMIENTOS DE DESARROLLO DE LAS OBLIGACIONES DEL PERSONAL 57
14.1 Procedimiento de realización de copias de respaldo y de recuperación de datos 57
14.2 Procedimiento de identificación y autenticación de usuarios 58
14.3 Procedimiento de asignación, distribución y almacenamiento de contraseñas 59
14.4 Procedimiento de Gestión de Soportes y Documentos. 61
15. INFORMACIÓN DE DENUNCIAS INTERNAS EN MATERIA DE PROTECCIÓN DE DATOS 63
15.1 Preservación de la identidad y confidencialidad de los datos. 63
15.2 Conservación de los datos 64
16. NORMATIVA APLICABLE 65
17. ANEXOS 66
1. DOCUMENTOS CONTRACTUALES 66
2. INVENTARIO DE SOPORTES 67
3. AUTORIZACIÓN Y REGISTRO DE SALIDA DE SOPORTES 68
4. AUTORIZACIÓN Y REGISTRO DE ENTRADA DE SOPORTES 70
5. CONTROLES PERIÓDICOS Y AUDITORÍAS 72
6. DECLARACIÓN DE RECEPCIÓN DEL PROCEDIMIENTO DE LOPDGDD 73
7. COMUNICACIÓN Y REGISTRO DE VIOLACIÓN DE SEGURIDAD DE DATOS PERSONALES 74
8. RELACIÓN DE ENCARGADOS DEL TRATAMIENTO DE LA SOCIEDAD 76
9. RELACIÓN DE INFRACCIONES Y SANCIONES EN EL RGPD Y EN LA LOPDGDD 77
11. Ficha, características y análisis de riesgos y medidas (excel adjunto) 82

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. OBJETIVO DEL REGLAMENTO

En el año 2016, la Unión Europea aprobó el Reglamento General de Protección de Datos (en adelante RGPD) que, si bien entró en vigor en mayo de ese año, es de aplicación a partir del 25 de mayo de 2018. Al tratarse de un Reglamento no necesita transposición al ordenamiento jurídico español, por lo que su contenido es directamente aplicable.

El nuevo *RGPD* europeo se aplica en España de manera simultánea al resto de normas en materia de protección de datos. Así, en tanto en cuanto no contravengan lo establecido en el *RGPD*, se debe aplicar también la legislación estatal y autonómica sobre protección de datos. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), el RD 1720/2007, la estatal conexa; y todo lo derivado de las interpretaciones sobre las que se apoyan las resoluciones, los informes y las recomendaciones de la AEPD y las sentencias emanadas de la vía judicial.

El *RGPD* recoge los tratamientos de datos personales que realicen los responsables, así como los encargados.

Así, se introducen, entre otros, el principio de responsabilidad activa, el principio de minimización de datos personales, la figura del Delegado de Protección de Datos (en adelante el DPO), la Privacidad desde el Diseño, la Privacidad por Defecto, las notificaciones de quiebras de seguridad que puedan afectar a los datos personales y las Evaluaciones de Impacto en la Protección de Datos (en adelante la EIPD).

Los responsables y encargados deben configurar el denominado Registro de Actividades de Tratamiento, así como el contenido del derecho de información en la recogida de datos que debe facilitarse a los interesados.

En lo referente a seguridad, el *RGPD* parte de un análisis de riesgo inicial de los tratamientos y a partir de los resultados obtenidos del mismo, se implementan las medidas de seguridad.

La Ley Orgánica 3/2018 del 5 de diciembre, sobre Protección de Datos y Garantía de los Derechos Digitales contempla los cambios introducidos por el RGPD y, en determinados casos de su competencia los desarrolla convenientemente.

En consecuencia, en este documento se analizan los aspectos más relevantes del RGPD en relación con los tratamientos de datos de carácter personal que se debe mantener actualizado y revisado siempre que se produzcan cambios relevantes en los sistemas de información, en la organización del mismo o con el cambio de disposiciones en materia de los datos de carácter personal.

2. ÁMBITO DE APLICACIÓN

2.1 Ámbito Jurídico

Se aplica a BEKA ASSET MANAGEMENT SGIIC, S.A. (en adelante la Sociedad) en todo el ámbito en el que sea de aplicación del RGPD, siendo de obligado conocimiento y cumplimiento por todo el personal de la Sociedad y por aquellas personas que directa o indirectamente utilicen o den soporte a la información de la Sociedad.

Se entiende como personal de BEKA ASSET MANAGEMENT SGIIC, S.A. a los efectos de cumplimiento del presente documento, tanto el órgano de administración, el personal con dependencia laboral como el personal cuyos servicios se ha concertado o contratado mediante empresas de trabajo temporal o proveedores que accedan a información de carácter personal de la que sea responsable la Sociedad.

2.2 Ámbito de la información

Alcanza a toda la información de carácter personal registrada en un soporte físico ya sea automatizado o en papel, que la haga susceptible de tratamiento, y a toda modalidad de uso posterior de estos datos.

Las actividades de tratamiento de los datos de carácter personal identificados en la Sociedad se relacionan y describen en el punto 8.1 de este procedimiento.

2.3 Ámbito material

Son de aplicación a los recursos informáticos de la Sociedad que se describen:

- Red Corporativa.
- Entorno informático (red de servidores, internos o distribuidos, equipos informáticos de trabajo o cualquier otro dispositivo electrónico con acceso a la red), donde se encuentran ubicados los ficheros o desde los cuales se tenga acceso a los mismos.
- Entorno y aplicaciones web con capacidad de recopilar y almacenar datos de carácter personal ya sea de forma permanente o temporal.

2.4 Ámbito territorial

Se aplica al tratamiento de datos personales:

- En el contexto de las actividades de un establecimiento de la Sociedad o del encargado en la Unión Europea, independientemente de que el tratamiento tenga lugar en la Unión o no.

- De interesados que residan en la Unión Europea por parte de la Sociedad o encargado no establecido en la Unión Europea, cuando las actividades de tratamiento estén relacionadas con:

  a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

  b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión Europea.

La Sociedad cuenta con una oficina donde desarrolla su actividad y donde se encuentran ubicadas las distintas áreas de las sociedades que conforman el Grupo.

3. CONCEPTOS BÁSICOS

3.1 Datos de carácter personal

Podemos definir dato de carácter personal como: "toda información sobre una persona física identificada o identificable («el interesado»);

Se considera 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".

Para facilitar la comprensión de esta definición, el *RPGD* especifica que las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de "cookies" u otros identificadores, como etiquetas de radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser usados para elaborar perfiles de las personas físicas e identificarlas.

Se define la seudonimización como 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.

Asimismo, el *RGPD* define también qué se considera como "datos biométricos", que pueden ser utilizados por la Sociedad, de la siguiente forma:

- Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una

persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Respecto a esta definición hay que señalar que los datos biométricos tendrán la condición de datos sensibles sólo cuando sean utilizados para identificar unívocamente a una persona. También hay que indicar que la noción de dato biométrico es muy amplia e incluye aspectos cada vez más innovadores.

En ningún caso, y dadas las necesidades de la Sociedad para la realización de sus actividades, se deben recoger datos genéticos, que son datos personales relativos a las características genéticas heredadas o adquiridas de una persona física, que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

3.2 Tratamiento de datos de carácter personal.

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente, 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.

La Sociedad presta una serie de servicios de inversión autorizados por la Comisión Nacional del Mercado de Valores.

Para prestar los mismos, recaban y tratan datos de carácter personal de los clientes, que son tratados total o parcialmente de forma automatizada o no. Estos tratamientos se detallan en el punto 5 de este procedimiento.

Adicionalmente, el *RGPD* establece unos conceptos relativos a tratamientos específicos:

- Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
- Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

3.3 Responsable del tratamiento.

El responsable del tratamiento o responsable 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 relacionados con el tratamiento de los datos personales.

Está obligado a demostrar que sus actividades de tratamiento cumplen con los principios recogidos en el RGPD y en la LOPDGDD.

Si vulnera la legislación sobre protección de datos, se le puede imputar la comisión de alguna de las infracciones tipificadas en la LOPDGDD que pueden implicar altas sanciones.

Los empleados que realizan el tratamiento de los datos personales en la Sociedad lo hacen en cumplimiento de las funciones que la Sociedad determina como responsable del tratamiento.

3.4 Encargado del tratamiento.

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

Cuando se vaya a realizar un tratamiento la Sociedad como responsable del tratamiento debe elegir únicamente un encargado, en caso de ser necesario, que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD y la LOPDGDD y garantice la protección de los derechos del interesado.

La relación entre la Sociedad como responsable y el encargado del tratamiento debe estar regulada en un contrato o instrumento jurídico. El contrato tiene que constar por escrito y detallar las instrucciones del responsable al encargado en relación con las medidas de seguridad, el régimen de subcontratación, la confidencialidad y el destino de los datos tras finalizar la prestación del servicio.

Existe, por tanto, un deber de diligencia en la elección del responsable. El Considerando 81 del *RGPD* prevé 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, así como del cumplimiento de la normativa de protección de datos.

Además, para demostrar que el encargado ofrece garantías suficientes, el *RGPD* prevé que la adhesión a códigos de conducta o a un mecanismo de certificación sirva como mecanismos de prueba.

Al igual que el responsable del tratamiento, el encargo está obligado a demostrar que sus actividades de tratamiento cumplen con los principios relativos al tratamiento recogidos en el RGPD y en la LOPDGDD.

Respecto al contenido mínimo, estará formado por el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

En particular, el contrato o acto de encargo de tratamiento deberá contener:

- Objeto.
- La duración.
- La naturaleza y finalidad del tratamiento.
- El tipo de datos personales y categorías de los interesados.
- Las obligaciones y derechos del responsable.

En particular desarrollar:

- Las instrucciones del responsable del tratamiento.
- El deber de confidencialidad.
- Las medidas de seguridad.
- El régimen de la subcontratación.
- La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los interesados.
- La colaboración en el cumplimiento de las obligaciones del responsable.
- El destino de los datos al finalizar la prestación.

En el Anexo 8, se recoge el modelo de *"Relación de encargados del tratamiento de datos de carácter personal por cuenta de la Sociedad".*

3.5 Tratamiento

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos. De manera manual o automatizada, total o parcialmente,

Así es 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.

La elaboración de perfiles es toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física,

En particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses*, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.*

3.6 Principios relativos al tratamiento.

El *RGPD* regula los principios que deben cumplirse y respetarse cuando se realiza el tratamiento de datos personales.

<table>
<tr>
<td>1
LICITUD, LEALTAD Y TRANSPARENCIA
Los datos personales recogidos deben ser adecuados y veraces, obtenidos de forma lícita, leal y tratados de forma transparente.</td>
<td>4
EXACTITUD
Los datos personales serán exactos y si fuera necesario actualizados, adaptándose medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos a los fines para los que se tratan.</td>
</tr>
<tr>
<td>2
LIMITACIÓN DE LA FINALIDAD
Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con dichos fines.</td>
<td>5
LIMITACIÓN DEL PLAZO DE CONSERVACIÓN
Los datos personales serán mantenidos de forma que se permita la identificación de los interesados no más tiempo del necesario para los fines del tratamiento. Pueden conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos, sin perjuicio de la aplicación de las correspondientes medidas técnicas y organizativas apropiadas que impone el *RGPD*.</td>
</tr>
<tr>
<td>3
MINIMIZACIÓN DE DATOS
Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.</td>
<td>6
INTEGRIDAD Y SEGURIDAD
Los datos personales serán tratados de manera que se garantice su adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, aplicando las medidas técnicas y de organización apropiadas.</td>
</tr>
<tr>
<td colspan="2">RESPONSABILIDAD PROACTIVA
El responsable del tratamiento es responsable de cumplir estos principios y capaz de demostrar dicho cumplimiento.</td>
</tr>
</table>

4. PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Consiste en la aplicación de medidas técnicas y organizativas para, en atención al riesgo que implica el tratamiento de los datos personales, cumplir y ser capaz de demostrar evidencias del cumplimiento.

Es una de las obligaciones que se establece en el *RGPD* para asegurar el cumplimiento de los principios relativos al tratamiento indicados en el punto 3.6.

Además, el *RGPD* establece un catálogo de medidas que la Sociedad y, en ocasiones sus encargados del tratamiento, deben aplicar para garantizar que los tratamientos son conformes a la norma europea. Son aquellas que tengan en cuenta:

- La naturaleza
- El ámbito
- El contexto
- Los fines del tratamiento
- Los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas
- Estados de la técnica
- Coste de aplicación de las medidas.

Cuando sea necesario, es un requerimiento la revisión de las medidas adoptadas, lo que implica que debe la Sociedad atender en todo momento al riesgo que implique el tratamiento de datos personales para el interesado.

El *RGPD* contiene dos principios para la implementación efectiva de la responsabilidad proactiva, como son:

a) El principio de protección de datos desde el diseño que supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo.

   Estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

   Un ejemplo de dichas medidas, que se establece de forma expresa en el *RGPD*, es que el propio tratamiento incorpore medidas para la seudonimización de los datos personales o la minimización de datos.

b) La protección de datos por defecto estriba en que solo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento.

Es decir, independientemente del conjunto de datos recogidos por el responsable con el objeto de implementar los distintos servicios que se proporcionan al sujeto de los datos, el responsable ha de compartimentar el uso del conjunto de datos entre los distintos tratamientos, de tal forma que no todos los tratamientos accedan a todos los datos, sino que actúen sólo sobre aquellos que sean necesarios y en los momentos en que sea estrictamente necesario. Si fuera posible por la naturaleza del proceso, llegar incluso a que no se traten datos de carácter personal.

Además, debe tenerse en cuenta lo siguiente respecto a la protección de datos por defecto:

- Recogida de datos: analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario.

- Tratamiento de los datos: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos.

- Conservación: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios; Accesibilidad: limitar el acceso por parte de terceros a dichos datos personales.

5. DERECHOS DE LOS INTERESADOS

Los interesados, como titulares de sus datos, pueden ejercitar ante la Sociedad, los derechos de acceso, rectificación, supresión, limitación al tratamiento y oposición de acuerdo con lo recogido a continuación:

DERECHOS DEL *RGPD*	CONSISTEN EN
Derecho de acceso	A que el interesado sea informado de cómo se están tratando los datos, y de su origen:
	• Los fines del tratamiento; categorías de datos personales que se traten y de las posibles comunicaciones de datos y sus destinatarios
	• Los destinatarios a los que se comunican los datos personales.
	• De ser posible, el plazo de conservación de sus datos. De no serlo, los criterios para determinar este plazo.
	• A solicitar la rectificación o supresión de los datos, la limitación al tratamiento, u oponerse al mismo.
	• Del derecho a presentar una reclamación ante la Agencia Española de Protección de Datos.
	• Obtener una copia de los datos objeto del tratamiento.
	• Si se produce una transferencia internacional de datos, recibir información de las garantías adecuadas
	• De la existencia de decisiones automatizadas (incluyendo perfiles), la lógica aplicada y consecuencias de este tratamiento
	• Debe distinguirse del derecho de acceso de los interesados a los expedientes administrativos que regula la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como del derecho de acceso regulado en la Ley 19/2013 de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
Derecho de rectificación	• Rectificar los datos inexactos, y a que se completen los datos personales incompletos, inclusive mediante una declaración adicional.
Derecho de supresión (Derecho al olvido)	Con su ejercicio el interesado puede solicitar:
	• La supresión de los datos personales sin dilación debida cuando concurra alguno de los supuestos contemplados. Por ejemplo, tratamiento ilícito de datos, o cuando haya desaparecido la finalidad que motivó el tratamiento o recogida o el interesado retire el consentimiento, o deban suprimirse por obligación legal.
	• No obstante, se regulan una serie de excepciones en las que no procederá este derecho. Por ejemplo, cuando deba prevalecer el derecho a la libertad de expresión e información.
Derecho a la limitación del tratamiento	Permite al interesado:
	1. Solicitar al responsable que suspenda el tratamiento de datos cuando:
	• Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el responsable.

	• El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos y solicite en su lugar la limitación de su uso.
	• El responsable no necesite los datos, pero en interesado los necesite para formular reclamaciones.
	• El interesado ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre el interesado.
	2. Solicitar al responsable que conserve tus datos personales cuando:
	• El tratamiento de datos sea ilícito y el interesado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso.
	• El responsable ya no necesita los datos para los fines del tratamiento, pero el interesado si los necesita para la formulación, ejercicio o defensa de reclamaciones.
Derecho a la portabilidad de los datos	El interesado tendrá derecho a mover, copiar, recibir los datos o solicitar que sean transmitidos a otro responsable cuando:
	• El interesado dio su consentimiento para el tratamiento de sus datos personales.
	• El tratamiento se efectúe por medios automatizados.
Derecho de oposición	El interesado puede oponerse al tratamiento:
	• Cuando por motivos relacionados con su situación personal, debe cesar el tratamiento de sus datos salvo que se acredite un interés legítimo, o sea necesario para el ejercicio o defensa de reclamaciones.
	• Cuando el tratamiento tenga por objeto la mercadotecnia directa.

5.1 Condiciones generales aplicables

- Los derechos:
  - Son ejercidos únicamente por el interesado, por su representante legal o un representante voluntario expresamente designado al efecto.
  - Cada uno de los derechos es independiente en el sentido de que pueden ejercitarse de forma separada cada uno de ellos.
  - No se puede exigir contraprestación alguna por el ejercicio de los derechos.
  - La Sociedad debe responder en el plazo máximo de un mes a contar de la recepción de la solicitud.

    Este plazo puede prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes, si bien se debe informar al interesado de la citada prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

- Si el interesado presentase la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

- La Sociedad podrá denegar el acceso, la rectificación o supresión de datos en el caso de su tratamiento para fines policiales o por las Fuerzas y Cuerpos de Seguridad, en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública.
- Sin perjuicio de los derechos de rectificación y supresión los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en las relaciones contractuales establecidas entre la persona y la Sociedad.

  En todo caso, deben conservarse durante el plazo marcado en las normas de archivo de la Sociedad siempre y cuando no se exceda lo legalmente permitido.

5.2 Procedimiento de ejercicio de los derechos de la persona afectada.

5.2.1 Derecho de acceso a la información.

Solicitud del interesado de acceso a la información

La persona afectada puede utilizar para su solicitud cualquier medio que permita acreditar el envío y la recepción de la solicitud, debiendo, en todo caso, elaborar y dirigir una:

- Comunicación que contenga, al menos:
  - Nombre y apellidos del interesado y fotocopia del DNI, pasaporte u otro documento válido que lo identifique incluido aquél que permita su identificación electrónica e igual documentación en los casos de la persona que actúa en su representación junto con el documento acreditativo de tal representación.
  - Petición en que se concreta la solicitud.
  - Domicilio a efectos de notificaciones, fecha y firma del solicitante.
  - Documentos acreditativos de la petición que formula, en su caso.

En el caso de que el interesado se dirija a un encargado del tratamiento, éste debe dar traslado de la comunicación de forma inmediata a la Sociedad, como responsable del tratamiento, en la persona del Responsable de Seguridad.

Análisis de la Solicitud

El Responsable de Seguridad, debe:

- Contestar a la solicitud siempre, con independencia de que figuren o no datos personales del interesado en sus tratamientos.
- Solicitar al interesado, si la solicitud no reúne los requisitos especificados, la subsanación de los mismos.
- Conservar copia documental de las comunicaciones dirigidas al interesado.
- Asegurarse de que las personas que tratan con datos de carácter personal, pueden informar de este procedimiento a los interesados.

Resolución.

El Responsable de Seguridad, o la persona que él determine para esta función, deben:

- Verificar de forma fehaciente la identidad deL solicitante aplicando las medidas descritas en este procedimiento.
- Resolver sobre la solicitud de acceso en los plazos establecidos.
- Definir el sistema de consulta de sus datos (puede ser de forma remota, segura y directa) de entre los siguientes:
    - Visualización en pantalla.
    - Escrito, copia o fotocopia remitida por correo certificado o no.
    - Correo electrónico u otros sistemas de comunicación electrónicos.
    - Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del mismo, ofrecido por la Sociedad.
- Cuidar que al facilitar el acceso a un interesado a sus datos personales se cumplan todas las medidas de seguridad implantadas en este procedimiento y no se facilite de ninguna manera información de otros usuarios.
- La información resultante del ejercicio de acceso contendrá todos los datos de tratamiento del interesado reflejados en el cuadro resumen recogido al principio de este punto 5, los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades de almacenamiento.
- Denegar el acceso a los datos de carácter personal cuando:
    - El derecho se haya ejercitado en un intervalo inferior a seis meses y no se acredite un interés legítimo al efecto, de acuerdo al artículo 12.3 de la LOPDGDD.
    - Cuando así lo prevea una norma de derecho comunitario de aplicación directa o española o cuando estas impidan revelar a los interesados el tratamiento de los datos a los que se refiera el acceso.

- Cuando la solicitud sea formulada por persona distinta del interesado o persona que lo represente conforme a lo indicado.

En estos casos debe informar al interesado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos.

5.2.2 Derecho de rectificación o supresión de la información.

Solicitud de rectificación o supresión

La persona afectada puede utilizar para su solicitud cualquier medio que permita acreditar el envío y la recepción de la solicitud, debiendo, en todo caso, elaborar y dirigir una:

- Comunicación que contenga, al menos:
  - Nombre y apellidos del interesado y fotocopia del DNI, pasaporte u otro documento válido que lo identifique incluido aquél que permita su identificación electrónica e igual documentación en los casos de la persona que actúa en su representación junto con el documento acreditativo de tal representación.
  - Petición en que se concreta la solicitud.
  - Domicilio a efectos de notificaciones, fecha y firma del solicitante.
  - Documentos acreditativos de la petición que formula, en su caso.

La persona afectada debe:

- Indicar a qué datos se refiere y la corrección o supresión que haya que realizarse.
- Adjuntar la documentación justificativa de lo solicitado.

Análisis de la solicitud

El Responsable de Seguridad, debe:

- Asegurarse de que la solicitud de rectificación indica el dato que es erróneo y la corrección que debe realizarse.
- Contestar a la solicitud siempre, con independencia de que figuren o no datos personales del interesado en la Sociedad.

Resolución.

El Responsable de Seguridad, o la persona que él determine para esta función, deben:

- Verificar de forma fehaciente la identidad del solicitante aplicando las medidas descritas en este procedimiento.

- No realizar la supresión cuando no proceda en virtud de las disposiciones aplicables o, en su caso, en virtud de las relaciones contractuales establecidas anteriormente para su tratamiento y su cancelación pudiese causar un perjuicio a intereses legítimos del interesado o de terceros o cuando existiese una obligación de conservar los datos.
- Asegurarse que se rectifican o suprimen únicamente los datos solicitados. En caso de imposibilidad técnica se debe informar al interesado y buscar una solución. Si por motivos técnicos la supresión de un dato implica la supresión de otro que no se ha solicitado se debe informar al interesado y solicitar de nuevo los que no debieron ser suprimidos.
- Asegurar que la supresión de los datos dé lugar al bloqueo de los mismos, conservándose únicamente a disposición de las Administraciones Públicas, jueces y tribunales durante el plazo de prescripción de éstos. Cumplido el citado plazo deberá procederse a la supresión (el plazo máximo es de 3 años).
- Comunicar motivadamente si solicitada la rectificación o supresión, considera que no procede atender la solicitud del interesado.
- Denegar los derechos de rectificación o supresión cuando:
    - Así lo prevea una norma de derecho comunitario de aplicación directa o norma española o cuando éstas impidan revelar a los interesados el tratamiento de los datos a los que se refiera el acceso.
    - No se pueda identificar al solicitante o su identificación no coincida con el propietario de los datos que solicita rectificar o suprimir.
    - Cuando la solicitud sea formulada por persona distinta del interesado o persona que lo represente conforme a lo indicado.
- Comunicar al interesado la resolución asegurando que se han tomado medidas para suprimir o rectificar sus datos personales.

En estos casos debe informar al interesado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos, o en su caso, de las autoridades de control de las Comunidades Autónomas.

5.2.3 Derecho a la limitación del tratamiento.

Solicitud del derecho de limitación del tratamiento.

La persona afectada puede utilizar para su solicitud cualquier medio que permita acreditar el envío y la recepción de la solicitud, debiendo, en todo caso, elaborar y dirigir una:

- Comunicación que contenga, al menos:

- Nombre y apellidos del interesado y fotocopia del DNI, pasaporte u otro documento válido que lo identifique incluido aquél que permita su identificación electrónica e igual documentación en los casos de la persona que actúa en su representación junto con el documento acreditativo de tal representación.
- Petición en que se concreta la solicitud.
- Domicilio a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso.

La persona afectada debe:

- Solicitar que se suspenda el tratamiento de datos o que se conserven sus datos personales.

Análisis de la solicitud.

El Responsable de Seguridad, debe:

- Contestar a la solicitud siempre, con independencia de que figuren o no datos personales del interesado en la Sociedad
- Conservar copia documental de las comunicaciones dirigidas al interesado.

Resolución.

El Responsable de Seguridad, o la persona que él determine para esta función, deben:

- Verificar de forma fehaciente la identidad de solicitante aplicando las medidas descritas en este procedimiento
- No realizar la limitación cuando no proceda en virtud de las disposiciones aplicables o, en su caso, en virtud de las relaciones contractuales establecidas anteriormente para su tratamiento y su limitación pudiese causar un perjuicio a intereses legítimos del interesado o de terceros.
- Comunicar al interesado la resolución asegurando que se han tomado medidas para limitar el uso de sus datos personales.

La Sociedad cesará en el tratamiento de los datos, haciéndolo constar claramente en sus sistemas, conservándolos exclusivamente para formular, ejercer o defender reclamaciones, o con miras a la protección de los derechos de un tercero cuando se trate de los casos indicados de solicitud por el interesado de suspensión del tratamiento de datos reflejados en el cuadro resumen recogido al principio de este punto 5.

5.2.4 Derecho de oposición.

Solicitud del derecho de oposición.

La persona afectada puede utilizar para su solicitud cualquier medio que permita acreditar el envío y la recepción de la solicitud, debiendo, en todo caso, elaborar y dirigir una:

- Comunicación que contenga, al menos:
  - Nombre y apellidos del interesado y fotocopia del DNI, pasaporte u otro documento válido que lo identifique incluido aquél que permita su identificación electrónica e igual documentación en los casos de la persona que actúa en su representación junto con el documento acreditativo de tal representación.
  - Petición en que se concreta la solicitud.
  - Domicilio a efectos de notificaciones, fecha y firma del solicitante.
  - Documentos acreditativos de la petición que formula, en su caso.

La persona afectada debe:

- Indicar los motivos fundados y legítimos relativos a una concreta situación personal del interesado, que justifica el ejercicio de este derecho.

Análisis de la solicitud.

El Responsable de Seguridad, debe:

- Analizar la solicitud siempre, con independencia de que figuren o no datos personales del interesado en la sociedad del Grupo de que se trate.
- Conservar copia documental de las comunicaciones dirigidas al interesado.

Resolución.

El Responsable de Seguridad, o la persona que él determine para esta función debe:

- Verificar de forma fehaciente la identidad de solicitante aplicando las medidas descritas en este procedimiento
- Contestar a la solicitud del interesado, de acuerdo los casos recogidos en el cuadro resumen reflejado al principio de este punto 5.

6. DEBER DE INFORMACIÓN

El *RGPD* regula el derecho de información en sus Arts. 13 y 14, distinguiendo entre la información que se debe facilitar al titular de los datos dependiendo si los datos personales se han obtenido del mismo o no.

La información que debe ser comunicada al interesado en el momento de recabar datos personales es la siguiente:

- La identidad y datos de contacto de la Sociedad como responsable y en su caso de su representante.
- Los datos de contacto del Responsable de Seguridad, en su caso.
- Finalidad del tratamiento. Categorías de datos personales a tratar.
- Intereses legítimos del responsable o del tercero.
- Destinatarios o categorías de destinatarios de los datos.
- En su caso, intención de transferir datos personales a un tercer país u organización internacional y de informar de las garantías que deben ser adecuadas.
- Los derechos del interesado de acceso, rectificación, supresión o cancelación, oposición y portabilidad.
- La base jurídica del tratamiento, identificando los intereses legítimos en su caso.
- Cuando el tratamiento esté basado en el consentimiento, derecho de retirarlo.
- El plazo o criterios de conservación de la información. De no ser posible, los criterios para determinar este plazo.
- El derecho a presentar una reclamación ante la Agencia Española de Protección de Datos.
- La existencia o no de decisiones automatizadas o elaboración de perfiles.

La información se debe proporcionar de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Esta obligación de informar se debe cumplir sin necesidad de requerimiento alguno, y el responsable debe poder acreditar con posterioridad que ha sido satisfecha.

Hay una serie de supuestos en los que no es necesario cumplir con este derecho de información:

- Cuando el interesado ya disponga de la información.
- Si los datos no proceden del interesado, cuando la comunicación resulte imposible o suponga un esfuerzo desproporcionado, el registro o la comunicación esté expresamente establecido por el Derecho de la UE o de los Estados miembros, o cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

Las formas de recogida de información pueden ser muy variadas y, por tanto, los modos de informar a los interesados deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos.

En el caso de que los datos no se obtengan del propio interesado se debe informar, además de los datos anteriores, de:

- El origen de los datos.
- Las categorías de los datos.
- Dentro de un plazo razonable, pero, en cualquier caso:
    - Antes de un mes desde que se obtuvieron los datos personales.
    - Antes o en la primera comunicación con el interesado.
    - Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Por otra parte, las comunicaciones al interesado sobre datos ya disponibles, o tratamientos adicionales, pueden hacerse llegar, entre otros medios, por correo postal, mensajería electrónica, así como notificaciones emergentes en servicios y aplicaciones.

Las características de cada uno de los medios varían en cuanto a extensión, disponibilidad de espacio, legibilidad, posibilidad de vincular informaciones, etc. Se ha diseñado un modelo de información por capas o niveles, que consiste en lo siguiente:

- Primer nivel, presentación de una información básica, de forma resumida, en el mismo momento y medio en que se recojan los datos.
- Segundo nivel, la información adicional, presentando de forma detallada el resto de informaciones (podría incluirse la política de privacidad).

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 ampliada.
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	Como ejercer los derechos de acceso, rectificaciones, 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 fuentes de acceso público.
		Categorías de datos que se traten.

7. IDENTIFICACIÓN DE LA LEGITIMACIÓN EN EL TRATAMIENTO DE DATOS

7.1 Cumplimiento de la obligación legal.

El tratamiento sólo es lícito si se cumple al menos una de las siguientes condiciones:

a) El interesado da su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

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.

c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

d) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.

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.

f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En particular, y para el ámbito de la Sociedad, son relevantes las siguientes:

- El interesado da su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.
- 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.

7.2 Consentimiento.

Es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Así, en los casos en que la base jurídica de los tratamientos sea el consentimiento, éste debe ser: informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

Además, el consentimiento en el marco del *RGPD* se caracteriza por lo siguiente:

- El consentimiento puede ser para uno o varios fines. En este caso:
  - *a) Sería posible agruparlos en virtud de su vinculación (por ejemplo, consentimiento para la recepción de publicidad propia o de terceros).*
  - *b) Deben desagregarse cuando los tratamientos impliquen conductas distintas (por ejemplo, tratamiento por quien recaba los datos y cesión a terceros).*
- Debe ser prestado de forma libre.
- Revocable en cualquier momento Debe ser tan sencillo darlo como retirarlo.
- La Sociedad debe poder probar en todo momento que ha obtenido el consentimiento.
- Utilizar un lenguaje claro y sencillo.

Por otra parte, también debe tenerse en cuenta lo siguiente:

- Si se usa para obtenerlo una declaración escrita, debe quedar claramente diferenciada la parte referente a protección de datos del resto de declaraciones.

7.3 Tratamiento de categorías especiales de datos.

El *RGPD* incluye en el concepto de categorías especiales de datos los denominados datos especialmente protegidos en la LOPDGDD como son las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los que revelen el origen racial o étnico, y los relativos a la salud o a la vida u orientación sexual de una persona.

También incorpora nuevas categorías de datos como son los datos biométricos.

La regla general contemplada en el *RGPD* es la prohibición del tratamiento de categorías especiales de datos.

No obstante, se recoge un amplio abanico de excepciones a esta regla general, destacando las siguientes en relación con los tratamientos de este tipo de datos que realice la Sociedad:

- El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales.

- El tratamiento es 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 en que así lo autorice el Derecho de la UE de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.
- El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.
- El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.
- El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
- El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

8. REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

El *RGPD* establece la obligación de implementar un Registro de Actividades de Tratamiento cuando las sociedades del Grupo empleen a más de 250 personas o el tratamiento no sea ocasional. Esta obligación alcanza también a los encargados del tratamiento.

La Sociedad ha decidido mantener este registro de actividades de tratamiento que es elaborado por escrito, incluso en formato electrónico y que estará a disposición de la Agencia Española de Protección de Datos, en el que se incluya una descripción de los tratamientos de datos que realicen con la siguiente información:

CONTENIDO DE CADA ACTIVIDAD DEL TRATAMIENTO	
LA SOCIEDAD	ENCARGADOS DEL TRATAMIENTO
1. Base Jurídica.	Base Jurídica.
2. Nombre y datos de contacto del responsable (o representante).	Nombre y datos de contacto del encargado (o representante)

3. Fines del tratamiento.	Categorías de tratamientos efectuados por cuenta de cada responsable.
4. Nombre y datos de contacto del Responsable de Seguridad.	Nombre y datos de contacto del Responsable de Seguridad.
5. Descripción de las Categorías de datos personales.	---------
6. Colectivos.	---------
7. Descripción de las medidas técnicas y organizativas de seguridad cuando sea posible.	Descripción de las medidas técnicas y organizativas de seguridad, cuando sea posible.
8. Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.	Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.
9. Transferencias internacionales. Documentación de garantías adecuadas en caso del Art. del RGPD 49.1.	Transferencias internacionales. Documentación de garantías adecuadas en caso del Art. del RGPD 49.1.
10. Cuando sea posible, plazos previstos para la supresión de las diferentes categorías de datos.	----------

De acuerdo con las características de la actividad que desarrolla la Sociedad, centrada en servicios de inversión, cabe diferenciar los siguientes tipos de tratamiento de Datos y se considera necesario la adopción de las siguientes medidas mitigadoras del riesgo de infracción del derecho de privacidad asociado a las mismas.

8.1 Detalle de las actividades de tratamiento

Las actividades de tratamiento identificadas realizadas por la Sociedad están detalladas en el Anexo 11 de este procedimiento.

Otras medidas de seguridad:

- Crear y mantener una concienciación de la necesidad de seguridad de información como parte integral de la actividad diaria de la Sociedad. Con esto se consigue que todos los empleados entiendan la importancia de la seguridad de la información y la influencia de la seguridad en el éxito de las funciones desempeñadas.
- Se realizan cursos de formación para los empleados
- Este procedimiento se pone a disponibilidad de los empleados
- Asegurar que los empleados son conscientes y cumplen con la legislación relativa al tratamiento de los datos de carácter personal.

Además, es conveniente tener en cuenta la seguridad física establecida por un proveedor o por el centro en el que desarrolla sus actividades. Para este caso particular se elabora una ficha simple sin establecer un ciclo de vida o medidas de seguridad específicas.

- SEGURIDAD

1. *Base Jurídica*

   a. *El tratamiento es necesario para el cumplimiento de una misión realizada en interés público.*

   b. *En aplicación del Reglamento General de Protección de Datos y LOPDGDD.*

2. *Nombre y datos de contacto del responsable:*

   Beka Asset Management, SGIIC, S.A.
   Teléfono: 914261900

3. *Fines del tratamiento:*
   - *Garantizar la seguridad de personas, bienes e instalaciones*
   - *Registro de control en caso de salto de alarma.*

4. *Nombre y datos del Responsable de Seguridad:*

   Tania Maravillas Sanchez Vaquerizo
   Teléfono: 914261900
   Correo electrónico de contacto: t.sanchez@bekafinance.com

5. *Descripción de las categorías de datos personales:*

   Datos biométricos: huellas dactilares, imágenes y grabaciones de vídeo, reconocimiento facial, etc.

6. *Colectivos:*

   Personal de la Sociedad y personas externas que acuden a visitas, reuniones o diversas gestiones a las oficinas.

7. *Descripción de las medidas técnicas y organizativas de seguridad:*

   a. *Cámaras de seguridad y alarma conectada al centro de alarmas.*

8. *Categorías de destinatarios de comunicaciones:*

   a. *Cesión o comunicación de datos:*
      - *Empresa encargada de la seguridad de la oficina.*

   b. *Encargados del tratamiento:*
      - *Entidad que presta este servicio para la Sociedad.*

9. *Transferencias internacionales:*

   No están previstas transferencias internacionales de los datos.

10. Plazos previstos para la supresión de las diferentes categorías de datos:

Se conservarán durante el tiempo que es necesario para cumplir con la finalidad para la que se autorizó su salida.

9. SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS

El *RGDP* introduce el análisis de riesgo con la finalidad de evaluar el riesgo que puede producir el tratamiento de datos personales. Si la Sociedad no garantiza la confidencialidad del tratamiento de datos de personas físicas derivados de un procedimiento sancionador, y se produce una vulneración del deber de secreto, esta circunstancia podría suponer consecuencias negativas tanto para el responsable como para las personas físicas cuyos datos personales hayan sido revelados.

El *RGPD* regula las comunicaciones de brechas de seguridad, tanto respecto a los interesados como a la AEPD.

9.1 Análisis de riesgos

El *RGPD* obliga a que la Sociedad como responsable del tratamiento lleve a cabo una valoración del riesgo de los tratamientos que realice, con el fin de establecer las medidas a aplicar.

Este análisis del riesgo variará en función de:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de interesados.
- La cantidad y variedad de tratamientos que realice la Sociedad.

A través de este análisis de riesgo se determinan las medidas a aplicar para que los tratamientos de datos sean respetuosos con lo dispuesto en el *RGPD*, además de adoptar las correspondientes medidas de seguridad.

Deben analizarse las vulnerabilidades informáticas y potenciales brechas de seguridad lógica con el fin de seleccionar e implementar las mejores soluciones técnicas para impedir, bloquear o neutralizar los ataques.

Este análisis, así como la selección de las soluciones, debe realizarse teniendo en cuenta el estado de la técnica, es decir, deben implementarse las medidas de seguridad avanzadas, nunca obsoletas, que sean capaces de impedir o bloquear los ataques cibernéticos actuales.

El análisis de riesgo es una actividad viva en la Sociedad debido a que la norma exige la actualización constante de las medidas de seguridad y al aumento de los delitos cibernéticos, la Sociedad debe establecer un sistema de vigilancia que haga

revisiones periódicas y siempre que cambien circunstancias tecnológicas tanto en la empresa como en el sector informático.

Los Arts. 25 y 32 del *RGPD* indican que las medidas de seguridad tienen que ser adecuadas al riesgo que exista sobre los distintos ficheros, por lo que se hace necesario que la Sociedad realice obligatoriamente un análisis de riesgo.

9.2 Implantación de medidas de seguridad.

El *RGPD* no establece medidas de seguridad estáticas, por lo que corresponde a la Sociedad como responsable del tratamiento determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

Las medidas de seguridad establecidas en este procedimiento complementan cualquier política de seguridad para proteger la información crítica de negocio. Estas medidas tienden a asegurar que la información:

- Está protegida frente a accesos no autorizados, ya sean realizados por miembros de la Sociedad, personal subcontratado, visitantes u otros ajenos a la empresa.
- Está adecuadamente protegida frente a degradación o pérdida durante su entrada, procesamiento, transmisión o almacenamiento.
- Los sistemas que soportan la actividad de la Sociedad están adecuadamente protegidos frente a accesos no autorizados y ataques externos o internos que puedan comprometer la integridad, confidencialidad o disponibilidad de los datos, todo ello de acuerdo al nivel de servicio requerido.
- Crear y mantener una concienciación de la necesidad de seguridad de información como parte integral de la actividad diaria de la Sociedad.
- Asegurar que los empleados cumplen con la legislación relativa al tratamiento de los datos de carácter personal y con el cumplimiento de este procedimiento.

La información es un activo fundamental para el desarrollo de la actividad de la Sociedad. Sin la información correcta, la Sociedad es incapaz de cumplir sus responsabilidades con los clientes, su personal y organismos supervisores.

Adicionalmente, la Sociedad no solo depende de la información, sino también de los controles implantados en sus sistemas informáticos para garantizar la seguridad de la información que albergan, entendiendo por seguridad de la información la protección de la información frente a la pérdida de confidencialidad, integridad y disponibilidad:

- Confidencialidad:

La información debe permanecer confidencial. Los accesos no autorizados por parte de atacantes externos son los que más captan la atención pública, si bien hay otras formas de divulgación de información confidencial, como ataques internos, robo de documentos por parte de visitantes o por el propio personal de la Sociedad, la permanencia de la información en los monitores no protegidos, etc. La divulgación de información de la Sociedad o de sus clientes puede dar lugar a penalizaciones graves de carácter legal y penal y en gran medida en la reputación de la Sociedad de cara al exterior...

- Integridad:

  La información debe ser precisa, exacta y completa. Pese a que el fraude y los ataques externos son la causa más conocida para la alteración de la información, las causas más comunes son la inadecuada definición y cumplimiento con los procedimientos para el control de la información en su entrada o el defectuoso diseño del software empleado para su procesamiento. La pérdida de integridad de la información podría resultar en decisiones de gestión incorrectas, transacciones económicas erróneas o elaboración de información de gestión imprecisa, que podría desembocar en penalizaciones graves y denuncias.

- Disponibilidad:

  La información debe estar disponible cuando se requiera. Las principales causas de la pérdida de información suelen ser interrupciones del fluido eléctrico, incendios, inundaciones y otros desastres mayores. Sin embargo, la disponibilidad puede perderse también debido a otros muchos motivos menos obvios, como a infecciones de virus, falta de conocimiento, olvido de claves de acceso o destrucción de datos intencionada o accidentalmente, mala gestión de los servicios contratados o el incumplimiento del acuerdo legal de servicio mínimo acordado con el proveedor

9.2.1 Niveles de Seguridad aplicables a las medidas de seguridad.

Cada nivel se corresponde con el siguiente tipo de información.

- Nivel básico: Información sobre la identificación de las personas físicas.
- Nivel medio: Información sobre:
  - Comisión de infracciones administrativas o penales.
  - Solvencia patrimonial y crédito.
  - Datos responsabilidad de las Administraciones tributarias en relación con el ejercicio de sus potestades.
  - Datos en relación con la prestación de servicios de inversión por parte de las entidades financieras.

- Datos responsabilidad de las Entidades Gestoras y Servicios comunes de la Seguridad Social en relación con sus competencias, así como los de las Mutuas de Trabajo y enfermedades profesionales de la Seguridad Social.
- Conjunto de datos que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o comportamiento de los mismos.

- Nivel alto: Información sobre:
  - Datos de carácter especial: de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual (excepto cuando los mismos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los interesados sean asociados o miembros o se trate de tratamientos no automatizados en los que de forma incidental o accesoria se contengan datos sin guardar relación con su finalidad).
  - Datos recabados para fines policiales sin consentimiento de las personas afectadas.
  - Datos derivados de actos de violencia de género.

9.2.2 Ficheros Temporales o Copias de trabajo de documentos.

Son aquellos que se crean para la realización de trabajos temporales o auxiliares y deben:

- Cumplir con el nivel de seguridad que les corresponda.
- Debe ser autorizados por el Responsable de Seguridad.
- Suprimirse una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

El responsable de los sistemas informáticos debe contar con medidas de prevención para asegurar el control y supresión de dichos ficheros.

9.2.3 Medidas de Seguridad aplicables a tratamientos automatizados

De las Funciones y Obligaciones del Personal

- Todo el personal recibe un ejemplar de este procedimiento y de sus futuras actualizaciones al objeto de que conozca las normas de seguridad que le afectan en el desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento, que deben ser establecidas por la Sociedad.

Del Registro de violaciones de la seguridad.

- El procedimiento de notificación y gestión de violaciones de la seguridad que afecten a los datos de carácter personal está desarrollado en el punto 9.3.

Control de acceso y confidencialidad de la información.

- El sistema utilizado para limitar el acceso de acuerdo a los privilegios de cada usuario se describe en los procedimientos 14.2 "*Identificación y autenticación de usuarios*" y 14.3 "*Asignación, distribución y almacenamiento de contraseñas"*
- El Responsable de Seguridad, mantiene una relación actualizada de usuarios que tienen acceso autorizado a los sistemas de información y los medios o canales a través de los cuales se puede acceder
- Las medidas adoptadas deben permitir la identificación de forma inequívoca y personalizada de cualquier usuario que intente acceder al sistema de información.
- Toda la información albergada en la red corporativa de la Sociedad, de forma estática o circulando en forma de mensajes de correo electrónico, es propiedad de la Sociedad y se considera auditable en todos los casos, incluso en el de los correos electrónicos.
- Los usuarios tienen acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

Gestión de soportes y documentos

- El procedimiento para la gestión de soportes y documentos se encuentra detallado en el procedimiento 14.4 "Gestión de soportes"
- Los soportes y documentos que contengan datos de carácter personal deben permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado por el Responsable de Seguridad.
- En el caso de datos de carácter personal básicos únicamente la Sociedad, a través del Responsable de Seguridad, puede autorizar la salida de soportes (documentación física, ordenadores portátiles, USBs, discos duros extraíbles, etc.), salvo si se han identificado como tales en el procedimiento que lo desarrolla.
- Adicionalmente y, en su caso, deben cumplirse también las medidas de nivel medio consistente en la cumplimentación del registro de entrada y de salida de soportes.
- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la

información almacenada en él, previamente a que se proceda a su baja en el inventario.

- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Copias de respaldo y recuperación

- Son medidas que garantizan la reconstrucción de los datos, en el estado en que se encontraban, antes del momento de producirse la pérdida o destrucción.
- El procedimiento de realización de copias de respaldo y recuperación de datos se encuentra detallado en el procedimiento 14.4. "Gestión de Soportes"

Pruebas con datos reales.

- Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de tratamiento y exista una copia respaldo de los datos.

Controles periódicos de verificación del Cumplimiento.

- El Responsable de Seguridad, cuida de que la veracidad de los datos contenidos en los Anexos de este Documento de Seguridad, así como el cumplimiento de las normas que contiene, son periódicamente comprobadas, de forma que puedan detectarse y subsanarse anomalías.
- Los resultados de todos estos controles periódicos, así como de las auditorías son registrados en el Anexo 5 "*Controles periódicos y Auditorías"*, al que se adjuntará la documentación justificativa necesaria.
- El Responsable de Seguridad, analiza con periodicidad, al menos, semestral:
    - Las incidencias registradas en el Registro de Violaciones de seguridad correspondiente, para, independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, acometer las actuaciones correctivas que limiten esas incidencias en el futuro.
    - El cumplimiento en relación con las entradas y salidas de datos, sean por Red o en soporte magnético o físico.
- El Administrador de Sistemas, con periodicidad, al menos, semestral:

- Comunica al Responsable de Seguridad cualquier cambio que se haya realizado en los datos técnicos detallados en los Anexos, como, por ejemplo, cambios en el software o hardware, bases de datos o aplicaciones de acceso a datos personales, procediendo igualmente a la actualización de dichos anexos.
- Comprueba la existencia de copias de respaldo que permitan la recuperación de los datos y la programación de las mismas de acuerdo con lo establecido.

- El Responsable de Seguridad, cuida de que este procedimiento esté en todo momento actualizado y lo revisa siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entiende que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Auditorías.

- Los sistemas de información e instalaciones de tratamiento son auditados internamente cada 2 años para determinar que el correcto cumplimiento y la adecuación de las medidas organizativas técnicas y de seguridad de los datos.
- El informe de auditoría identifica las deficiencias y propone las medidas correctivas o complementarias necesarias. Debe incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
- Con carácter extraordinario también debe realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.
- La información no automatizada también es sometida a auditoría y deberá facilitarse cuando se solicite.
- Los informes de auditoría son analizados por el Responsable de Seguridad, o quien propone al Órgano de Administración las medidas correctivas correspondientes, y que quedarán a disposición de la AEPD.

Entorno de Sistema Operativo y de Comunicaciones.

Al estar los datos ubicados en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que lo comunican con otros ordenadores, es

posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que puedan contar las aplicaciones.

- Se regula, por tanto, también el acceso y uso de los elementos del sistema operativo, herramientas o programas de utilidad, y del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos.
- El sistema operativo y de comunicaciones tiene como responsable al Administrador de Sistemas.
- En el caso más simple de que los datos se encuentren ubicados en un ordenador personal y el único acceso sea mediante una aplicación local mono puesto, el Administrador de sistemas operativo será el mismo usuario que accede habitualmente a los datos.
- Ninguna herramienta o programa de utilidad que permita el acceso es accesible a ningún usuario no autorizado.
- El Administrador de Sistemas es responsable de guardar en lugar protegido las copias de seguridad y respaldo de los datos, de forma que ninguna persona no autorizada tenga acceso a las mismas. Si estas se hacen de forma remota o mediante un proveedor contratado el Administrador es el responsable de asegurar que se cumple lo establecido en el contrato y solamente el Administrador tiene acceso a las mismas.
- Si el ordenador en el que están ubicados los datos está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso a los datos, el Administrador de Sistemas se asegura de que este acceso no se permite a personas no autorizadas. Lo mismo sucede si los datos están guardados en la nube, éstos solamente son accesibles por los usuarios autorizados.

Entrada y Salida de Datos por Red

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello, merecen un tratamiento especial.

- Todas las entradas y salidas de datos que se efectúen mediante correo electrónico o vías de comunicaciones alternativas, se realizarán desde recursos del sistema y cuentas o direcciones de correo controladas por usuarios especialmente autorizados para este fin por la Sociedad a través del Responsable de Seguridad.

9.2.4 Medidas de seguridad aplicables a los tratamientos no automatizados.

A estos datos le son de aplicación las medidas establecidas en lo relativo a:

- Funciones y obligaciones del personal.
- Registro de Incidencias.
- Control de acceso.
- Gestión de soportes.

Criterios de archivo.

- Se realiza de acuerdo con las normas existentes en la Sociedad sobre Archivo y Salvaguarda de la Información.

Dispositivos de almacenamiento.

- Estos dispositivos cuentan con mecanismos que obstaculizan su apertura, o en su defecto, impiden el acceso a los mismos de personas no autorizadas.
- En el caso de información de nivel alto, los archivadores o elementos en los que se almacenan los datos no automatizados deben encontrarse en áreas en las que el acceso está protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Cuando no es preciso su uso estas áreas deben estar cerradas.

Custodia de los soportes.

- Es responsable de los archivos mientras dure su tratamiento la persona encargada de los mismos.

Auditoría

- La información no automatizada es sometida a auditoría, con el mismo carácter que la automatizada.

Copia o reproducción

- En el caso de información de nivel alto, las copias o reproducciones únicamente pueden ser realizadas por el personal autorizado y procederse a su destrucción inmediata de la información desechada.

Acceso a la información

- En el caso de información de nivel alto, únicamente es posible el acceso por el personal autorizado, debiendo quedar identificados los accesos realizados, en el caso de documentos que puedan ser utilizados por varios usuarios.

Traslado de la información

- En el caso de información de nivel alto, se establecen medidas que aseguren impedir el acceso o manipulación de la información objeto de traslado.

9.3 Gestión de la violación o quiebras de la seguridad de los datos.

Una violación o brecha de seguridad se produce en las siguientes situaciones:

- La destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma.
- Los supuestos de comunicación o acceso no autorizado a dichos datos.
- Incluye cualquier supuesto de pérdida o de acceso, incluso involuntario, que no se adecúen a lo que establece el RGPD
- Uso indebido de los datos de carácter personal, para el cual no se ha recogido el consentimiento explícito e inequívoco.
- Incumplimiento de los derechos ejercidos por los interesados.

Todas las situaciones se aplican al Responsable del tratamiento o al Encargado del tratamiento que debe informar y colaborar con el primero.

La Sociedad siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo:

- A la AEPD, en un plazo máximo de 72 horas. Si se incumple el plazo indicado, la notificación tardía debe acompañarse de una indicación de los motivos de la dilación.
- A las personas físicas cuyos datos personales se hayan visto interesados por la quiebra de seguridad, cuanto antes.

9.4 Excepción de comunicación de las violaciones de seguridad a la AEPD

No es necesario notificar las violaciones de seguridad que no constituyan un riesgo para los derechos y las libertades de las personas físicas.

En cuanto a qué debe entenderse que constituye riesgo para los derechos y libertades de las personas físicas, el *RGPD* incluye los tratamientos de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales. En particular, constituyen riesgo para los derechos y libertades de las personas físicas los casos en los que los datos objeto de la violación puedan dar lugar a problemas de:

a) Discriminación.
b) Usurpación de identidad o fraude.

c) Pérdidas financieras.
d) Daño para la reputación.
e) Pérdida de confidencialidad de datos sujetos al secreto profesional.
f) Reversión no autorizada de la seudonimación.
g) Cualquier otro perjuicio económico o social significativo.
h) Privación a los interesados de sus derechos y libertades o del control sobre sus datos personales,
i) Cuando se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales.
j) Cuando se traten datos personales de personas vulnerables, en particular niños,
k) Cuando el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado que se deriva de la violación de seguridad debe valorarse en atención a la naturaleza, el alcance, el contexto y los fines relacionados con la violación de seguridad que conozca la entidad.

El riesgo debe ponderarse sobre la base de una evaluación objetiva. Cabe también tener en cuenta, como elementos que minoran el riesgo derivado de la violación de seguridad:

a) La seudonimización y el cifrado de datos objeto de la violación.
b) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de pérdida, destrucción o alteración de los datos.

9.5 Comunicación de violaciones de seguridad a la AEPD

CONTENIDO MÍNIMO DE LA COMUNICACIÓN DE LA QUIEBRA DE SEGURIDAD A LA *AEPD*
• Naturaleza de la quiebra de seguridad.
• Categorías de interesados (por ejemplo: menores, discapacitados, empleados, ciudadanos).
○ N.º aproximado de interesados.

○ Categorías de datos comprometidos (por ejemplo: Identificativos, salud, laborales).
○ N.º registros de datos personales interesados.
• Nombre y datos de contacto del Delegado de Protección de Datos.
• Posibles consecuencias de la quiebra de seguridad sufrida.
• Medidas adoptadas o propuestas para remediar esta quiebra.

Por otra parte, si el encargado del tratamiento sufre una quiebra de seguridad, éste debe notificar sin dilación al responsable la existencia de la misma.

El *RGPD* no indica ni el formato de dicha notificación ni el plazo máximo para que se realice dicha notificación, ya que el plazo establecido para el responsable se fija a partir del conocimiento de la quiebra de seguridad. Por lo tanto, el responsable debe fijar por tanto las obligaciones de notificación del encargado, de tal forma que le permitan cumplir con los requisitos que a dicho responsable sí obliga el *RGPD*, en particular, en relación a los datos que es necesario notificar a terceros.

9.6 Comunicación de violaciones de seguridad a los interesados.

Si la violación de la seguridad entraña un alto riesgo para los derechos y libertades de los interesados la Sociedad lo comunicará a los interesados sin dilación indebida.

El *RGPD* no establece plazo mínimo para la comunicación. Pero, si es necesario notificarlo a la AEPD, es recomendable realizar la comunicación dentro del plazo de notificación.

La comunicación debe utilizar un lenguaje claro y sencillo, explicando:

CONTENIDO MÍNIMO DE LA COMUNICACIÓN DE LAS VIOLACIONES DE SEGURIDAD A LOS INTERESADOS
• Naturaleza de la violación de seguridad.
• Categorías de interesados (por ejemplo: menores, discapacitados, empleados, ciudadanos).
○ N.º aproximado de interesados.
○ Categorías de datos comprometidos (por ejemplo: Identificativos, salud, laborales).
○ N.º registros de datos personales interesados.
• Nombre y datos de contacto del Responsable de Seguridad o, en caso de que no esté designado un punto de contacto donde pueda obtenerse información.

• Posibles consecuencias de la quiebra de seguridad sufrida.
• Medidas adoptadas o propuestas para remediar esta quiebra y, si procede, para mitigar los posibles efectos negativos.

9.7 Excepción de comunicación a los interesados.

No es obligatoria la comunicación al interesado si se cumple alguna de las condiciones siguientes:

a) Cuando los datos personales objeto de la violación son ininteligibles para cualquier persona que no esté autorizada a acceder a ellos, como en el caso de cifrado.

b) Cuando se han adoptado medidas ulteriores que garantizan que no existe

c) probabilidad de que se concretice el alto riesgo para los derechos y

d) libertades del interesado.

9.8 Forma de llevar a cabo las comunicaciones.

Comunicación personal o pública.

- Cuando la comunicación personal de la violación de seguridad suponga un esfuerzo desproporcionado, podrá, en su lugar, realizarse una comunicación pública o alguna otra medida igualmente efectiva.

Requerimiento de la AEPD si no hay comunicación

- Si la AEPD considera que existe la probabilidad de que la violación entrañe un alto riesgo y la entidad no la hubiera comunicado al interesado, podrá exigir a la entidad que lo haga o que adopte medidas ulteriores que anulen la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.

9.9 Notificación, gestión y respuesta de violaciones de seguridad de los datos.

Definición y tipo de violaciones de seguridad de los datos.

Incidencia es cualquier anomalía que afecte o pueda afectar a la seguridad de los datos. Ante cualquier clase de duda se debe proceder a su notificación. No obstante, se detallan de forma más o menos precisa aquellas incidencias de seguridad que deben notificarse siempre:

- Control de Acceso:
    - Pérdida de información o imposibilidad de acceder a los datos.

- Pérdida o robo de credenciales que permitan el acceso a datos personales
- Acceso, modificación o borrado no autorizado de los datos contenidos en la red o en los equipos informáticos.

- Seguridad en la red:
  - Conexiones a redes de terceros que no estén debidamente autorizadas por el Responsable de Seguridad.
  - Instalar software que esté en fase de prueba en la red de producción.
  - Instalar software no autorizado por el Administrador de Sistemas y por el Responsable de Seguridad.
  - Enviar información a través de un canal inseguro que no cumpla con las medidas de seguridad.
  - Disponer de un sistema o software no actualizado y/o sin licencia
  - Antivirus desactualizado o no instalado
  - Firewall desactiva o no operativo.
- Seguridad medioambiental:
  - Fuego o fugas de agua que puedan afectar al equipo informático.
  - Vandalismo, cuando afecte a equipos informáticos.
  - Acceso de personas no autorizadas a oficinas o edificios de la Sociedad.
- Seguridad de los equipos informáticos:
  - Robo o pérdida de cualquier elemento informático (ordenadores, impresoras, etc.).
  - Daño físico o mal funcionamiento de equipos informáticos.
  - Sospecha de contener un virus, malware o similar en el dispositivo.
- Seguridad en las comunicaciones:
  - Chain letter (ej: "Si no envías este e-mail a 20 personas en 24 horas algo horrible te ocurrirá...").
  - Recepción de mails no solicitados o con remitente desconocido.
  - Acceso a sitios web de dudosa reputación y/o que no tengan conexiones seguras
- Documentos:
  - Desaparición de documentación
  - Pérdida o hurto de la llave o clave de acceso al cuarto o mueble que contiene la información.
  - Información sensible sin restricción de acceso.

Tipo de gravedad de las violaciones de seguridad de los datos

Leves: No afectan a la integridad de los datos y no necesitan una recuperación de las copias de seguridad.

Graves: Afectan a la integridad de los datos pero no requieren una recuperación mediante copias de seguridad.

Muy Graves: Afectan a la integridad de los datos y requiere la recuperación de los mismos a través de las copias de seguridad.

Descripción del procedimiento

Cualquier usuario que se halle prestando sus servicios debe:

- Notificar inmediatamente, y en cualquier caso en un plazo de tiempo no superior a una hora, al Responsable de Seguridad cualquier anomalía que detecte y que pueda afectar a la seguridad de los datos.
- Para el registro de las violaciones de seguridad de los datos, se utiliza el Anexo 7 por correo electrónico.

El Responsable de Seguridad

- Da acuse de recibo de la comunicación recibida de la notificación de incidencias.
- Procede a su registro y hace llegar la comunicación al administrador del sistema.
- Asegura que los técnicos dan respuesta inmediata a la incidencia detectada y supervisará el trabajo de subsanación de la anomalía detectada.

El Administrador del Sistema

- Remite por el mismo mecanismo las medidas adoptadas, una vez hecho el Registro correspondiente.
- Lo comunica al Responsable de Seguridad, quien, una vez finalizada la corrección, envía un informe al órgano de administración y al interesado.
- Procede al registro de la violación de seguridad de los datos.

El Responsable de Seguridad

- Cuida de que exista un registro de violaciones de seguridad actualizado, manteniendo, al menos, las de los últimos 12 meses, donde se haga constar la siguiente información relativa a las mismas:
    - Número de violación, tipo de violación, momento en el cual se ha producido la incidencia, persona que realiza la notificación, persona a quien se comunica, efectos derivados de dicha notificación, descripción detallada de la mismo.

- Procedimiento de recuperación de los datos por la persona que ejecutó el proceso, los datos restaurados, qué datos se han grabado manualmente.
- La autorización por escrito del Responsable de Seguridad para la ejecución de los procedimientos de recuperación.
- Lleva a cabo un ejercicio de concienciación con las personas con acceso a los datos de carácter personal para evitar repetir las incidencias.

10. EVALUACIÓN DE IMPACTO (EIPD)

Es una herramienta de carácter preventivo. Debe realizarse por la Sociedad, como responsable del tratamiento, en particular si se utilizan las nuevas tecnologías, cuando un nuevo tipo de tratamiento pueda entrañar un alto riesgo para las libertades y derechos de los interesados. Su objetivo es identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el fin de garantizar los derechos y libertades fundamentales de las personas físicas.

Debe determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

Diferencia entre a) la evaluación de impacto y b) el análisis de riesgo.

La primera se centra en medir el riesgo para los derechos y libertades de las personas físicas, en relación con la protección de datos;

La segunda analiza las vulnerabilidades informáticas y potenciales brechas de seguridad con el fin de seleccionar e implementar las mejores soluciones técnicas para impedir, bloquear o neutralizar los ataques.

En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

Sobre las operaciones que requieran una evaluación de impacto de acuerdo a lo dispuesto en el párrafo anterior, la AEPD establece y publica una lista al respecto.

La Sociedad puede elaborar un Plan de Contingencias con la finalidad de mitigar los daños cuando se produzca una quiebra de seguridad. También deben mantener un registro de los incidentes de seguridad.

10.1 Necesidad de evaluación del impacto.

El *RGPD* determina los siguientes supuestos en que debe realizarse una evaluación de impacto:

- Empresas que realicen una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Empresas que realicen un tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales.
- Empresas que realicen una observación sistemática a gran escala de una zona de acceso público.

Esta evaluación de impacto también podrán realizarla aquellos responsables que vayan a realizar un tratamiento a gran escala u operaciones de tratamiento que entrañen un alto riesgo para las personas.

Una de las cuestiones básicas a tener en cuenta en la realización de una evaluación de impacto es la participación del Responsable de Seguridad. Así, cuando sea probable que un tipo de tratamiento, sobre todo si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas la Sociedad realizará, antes del tratamiento, una evaluación de impacto.

Si se trata de operaciones similares que supongan riesgos similares, se podrá realizar una única evaluación.

10.2 Contenido de la EIPD

La evaluación deberá incluir como mínimo:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por la Sociedad.

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

c) Una evaluación de los riesgos para los derechos y libertades de los interesados, considerando el cumplimiento de los códigos de conducta aprobados.

d) Las medidas previstas para afrontar los riesgos, incluyendo las garantías, medidas de seguridad y mecanismos que garanticen la protección de datos

personales, y su regularidad, teniendo en cuenta los derechos intereses de los interesados.

Cuando proceda, deberá recabarse la opinión de los interesados en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento. Debe revisarse el informe cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

10.3 Consulta previa a la AEPD

Si la EIPD desvela alto riesgo para la privacidad y la Sociedad no toma medidas suficientes para mitigarlo, la Sociedad deberá someter el tratamiento a consulta a la AEPD antes de iniciarlo.

Si la AEPD considera que el tratamiento previsto podría infringir la normativa de protección, especialmente cuando no se hayan identificado o mitigado suficientemente los riesgos, deberá asesorar por escrito a la Sociedad y, para ello, podrá requerir más información, inspeccionar el tratamiento, requerir que se regularice, suspender su inicio o paralizarlo e, incluso, abrir un expediente sancionador.

La respuesta a la consulta debe tramitarse en un plazo de ocho semanas, prorrogable por seis semanas más en función de la complejidad del tratamiento.

10.3.1 Contenido de la consulta

Para presentar la consulta, debe facilitarse la siguiente información:

a) Identificación del responsable dentro del Grupo y encargados implicados en el tratamiento,
b) Los fines y medios del tratamiento previsto,
c) Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados,
d) Los datos de contacto del Responsable de Seguridad,
e) La EIPD.
f) Cualquier otra información que solicite la AEPD.

11. ORGANIZACIÓN INTERNA

La Sociedad cuenta con una estructura y medios de control interno y de comunicación adecuados para garantizar la regularidad de los tratamientos de datos personales.

Se incluyen las funciones que asume el Consejo de Administración, la descripción detallada del funcionamiento de los órganos de control interno que incluye su composición, competencias y periodicidad de sus reuniones, así como las obligaciones en materia de Protección de Datos de los empleados que componen el resto de áreas funcionales.

11.1 Consejo de Administración

El Consejo de Administración es el órgano responsable de decidir la política de la Sociedad en materia de Protección de Datos.

Entre sus funciones estarán:

- Aprobar el presente procedimiento.
- Aprobar las Políticas de tratamiento de datos de carácter personal.
- Designar al Responsable de Seguridad
- Aprobar las órdenes y directrices en materia de Protección de Datos aplicables.
- Recibir de los expertos externos los informes sobre el estado de tratamiento de datos y medidas de regularización recomendables y necesarias, adoptar, sin dilación, las medidas necesarias para solventar las deficiencias detectadas y dar seguimiento a las mismas.
- Acordar las medidas necesarias en caso de incumplimiento de obligaciones de Protección de Datos, especialmente la notificación a la Agencia Española de Protección de Datos y la información a los interesados sobre de brechas de seguridad.

El Consejo de Administración llevará un registro de la documentación e informes sometidos al mismo, así como de las decisiones que adopte en el ámbito de la Protección de Datos.

11.2 Empleados y agentes

11.2.1 Funciones y obligaciones generales del personal.

Los empleados cumplirán las obligaciones establecidas por la normativa vigente e interna, y en particular, tendrán las siguientes funciones:

- Conocer y cumplir las políticas y procedimientos de la Sociedad en materia de Protección de Datos.
- Asistir a los cursos de formación a los que sean convocados.

- Mantener confidencial y protegida toda la información personal a que accedan en el ejercicio de sus funciones, impidiendo que otras personas puedan acceder a ella.
- Advertir al Responsable de Seguridad de cualquier situación que conozcan que pueda resultar contraria o derivar en una infracción de las normas y políticas de protección de datos.

11.2.2 Funciones y obligaciones del personal en materia de seguridad de los datos.

El personal interesado se clasifica en:

1. *Usuarios de la información*, o personal que tiene acceso a la información.
2. *Administrador de Sistemas*, o persona encargada de administrar y/o mantener el entorno operativo de la información.
3. *Responsable de Seguridad*, cuyas funciones son las de coordinar y controlar las medidas definidas en el procedimiento.

Obligaciones del personal

- Para garantizar su conocimiento, los empleados firman la "*Declaración de recepción y aceptación del procedimiento de LOPDGDD"* incluida como Anexo 6 de este procedimiento.
- El puesto de trabajo, y todo el entorno conectado al mismo (sistemas en la nube, impresoras, dispositivos extraíbles, etc), está bajo la responsabilidad del usuario autorizado que garantiza que la información que muestra no pueda ser visible por personas no autorizadas.
- Las pantallas, las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deben garantizar esa confidencialidad, de acuerdo a lo siguiente:

Pantallas:

Cuando el usuario abandone su puesto de trabajo, bien temporalmente o bien al finalizar su turno de trabajo, debe dejarlo en un estado que impida la visualización de los datos protegidos.

Cuando se abandone el equipo el usuario debe bloquear la pantalla de tal forma que se solicite una contraseña, u otra medida similar establecida, para acceder de nuevo a los datos. En el caso de que el propio usuario no bloquee la pantalla, ésta deberá bloquearse automáticamente transcurridos 5 min sin actividad.

Impresoras:

Debe asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros

usuarios no autorizados para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Conexión a Redes:

Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso a los datos, salvo en los casos que resulta necesario para el desarrollo del trabajo, de los que existirá un registro de usuarios y la autorización correspondiente por parte del Responsable de Seguridad.

La revocación de esta prohibición será autorizada por el Responsable de Seguridad, quedando la oportuna constancia.

Configuración preestablecida:

Los puestos de trabajo desde los que se tiene acceso a los datos tienen una configuración preestablecida en sus aplicaciones y sistema operativo, que sólo podrá cambiarse bajo la autorización del Responsable de Seguridad o por los administradores autorizados.

Los usuarios no podrán actualizar el sistema manualmente, instalar aplicaciones o programas, importar nuevas cuentas de email, etc. No podrán realizar ninguna acción que ponga en peligro la seguridad previamente establecida, esto debe ser definido por el Responsable de Seguridad y aplicado por el administrador de sistemas.

Salvaguarda y protección de las contraseñas personales

- Cada usuario es responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicarlo como violación, según el procedimiento de notificación, gestión y respuesta ante la violación y proceder a su cambio. Lo mismo aplica para las contraseñas del correo electrónico, de acceso a sistemas en la nube, etc, en definitiva, toda contraseña que permita el acceso a datos de carácter personal.

Gestión de las violaciones de seguridad de los datos.

El personal de la Sociedad debe:

- Comunicar al Responsable de Seguridad cualquier incidencia que se produzca en los sistemas de información a los que tengan acceso, de conformidad con el procedimiento de notificación, gestión y respuesta ante las incidencias.
- Dicha comunicación debe realizarse inmediatamente y, en cualquier caso, en un plazo de tiempo no superior a 1 hora desde el momento en que se conozca dicha incidencia.

- Por los graves perjuicios que se pueden ocasionar, la Sociedad tomará medidas disciplinarias en el supuesto de que no se actúe con la máxima diligencia, ante una irregularidad en el funcionamiento del sistema informático.

Gestión de soportes y entrada o salida de datos por Red.

De forma muy especial se hace hincapié en los siguientes aspectos:

- Los soportes que contengan datos, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados conociendo de qué datos se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.
- Aquellos medios que sean reutilizables, y que hayan contenido copias de datos, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.
- Los soportes que contengan datos deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para su uso.
- Cuando la salida de datos se realice por medio de correo electrónico los envíos se realizarán, siempre y únicamente, desde una dirección de correo controlada por el administrador del sistema, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de registro de salidas que permita conocer en cualquier momento los envíos realizados, su origen, a quién iban dirigidos y la información enviada, es decir tipo de datos, formato, fecha y hora del envío.

Actos Prohibidos

- Crear ficheros de datos de carácter personal sin la autorización del Responsable de Seguridad. En cualquier caso, el procedimiento a seguir, si un usuario necesita crear un fichero es ponerlo en conocimiento del Responsable de Seguridad mediante un e-mail donde figure la autorización de su responsable.
- Almacenar información de carácter personal en un pen drive o cualquier otro soporte magnético, distintos de los autorizados por el Responsable de Seguridad, debiendo devolverlo al finalizar su uso y borrada del soporte de forma inmediata la información una vez ha sido guardada en el fichero de destino. El traslado al exterior de los locales de información de carácter personal por este tipo de soportes queda prohibido, salvo que sea autorizada por el Responsable de Seguridad, que lo autorizará, en casos excepcionales, incorporando una clave de seguridad.

- Cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa del Responsable de Seguridad.
- Cualquier otra actividad expresamente prohibida en este documento o en las normas sobre protección de datos e Instrucciones de la AEPD.

11.3 Funciones y Obligaciones del Responsable de Seguridad.

Identificación: Tania Maravillas Sánchez Vaquerizo

Teléfono Fijo: 914261900

e-mail: t.sanchezekafinance.com

Ámbito de actuación: Tanto para tratamientos automatizados como no automatizados.

Funciones:

- Coordinación y control de las medidas definidas en el presente Documento.
- Aquellas que por delegación le asigne el órgano de administración de la Sociedad.

Obligaciones:

- Coordinar la puesta en marcha de las medidas de seguridad.
- Difusión de este procedimiento
- Controlando el cumplimiento de las medidas de seguridad.
- Gestionar la resolución de las incidencias producidas en los sistemas de información.
- Habilitar un Registro de violaciones de seguridad a disposición de todos los usuarios y administradores de los datos donde se registre cualquier violación que pueda suponer un peligro para la seguridad del mismo.
- Analizar las incidencias registradas, tomando las medidas correctivas.
- Analizar los informes de auditorías, identificando las deficiencias y proponiendo al Órgano de Administración las medidas correctivas correspondientes.
- Autorizar la creación de ficheros de datos de carácter personal.
- Verificar, al menos, semestralmente, el cumplimiento de entrada y salida de datos, sea por red, por soporte magnético o físicamente.

- Comprobar la existencia de copias de respaldo que permitan la recuperación de los datos.
- Autorizar entradas y salidas de datos por correo electrónico o vías de comunicación alternativas.
- Autorizar la instalación de software y de conexiones a redes externas.
- Atender y contestar a las solicitudes de los interesados en relación con sus derechos, o designar persona para ello.
- Analizar en profundidad todas las herramientas/sistemas que se contraten a terceras partes con el fin de asegurar que cumplen los requisitos mínimos de seguridad e incorporar las cláusulas necesarias en los contratos. En el caso que estas cláusulas no puedan ser contempladas, se debe establecer un plan de contingencia y realizar una revisión periódica para asegurar, en todo momento, la seguridad de los datos.
- Asegurarse periódicamente que se cumplen las cláusulas de los contratos mencionadas en el punto anterior.
- Debe establecer un canal de comunicación rápido y eficaz con los proveedores contratados para que, en caso de incidencia, se comunique inmediatamente y se tomen las medidas oportunas. Además, se debe establecer el nivel de confianza que se tiene el proveedor y qué tipo de incidencias se deben reportar y cuáles no.
- Cualesquiera otras que se mencionen en este procedimiento.

11.4 Funciones y Obligaciones del Administrador de Sistemas.

Identificación: Lise Davenport – César Huerta

Teléfono 617 02 13 88 – 654 01 23 68

e-mail: lise@investgala.com – cesarhuerta@ithealth.es

Ámbito de actuación: El administrador de sistemas tiene como responsabilidad implementar, configurar, mantener, documentar y asegurar el correcto funcionamiento y acceso de todos los sistemas informáticos.

Su objetivo principal es garantizar el tiempo de actividad, rendimiento y acceso a recursos de manera segura y continuada en el tiempo.

En cuanto al mantenimiento de aplicaciones y bases de datos este servicio es externo a la compañía, y está bajo acuerdos con las compañías que lo implementan. Algunas de ellas son estas:

- Finametrix
- Almis

    - OpenBravo
    - Fitore
- Sage
    - Sage 50c
- Bloomberg
    - Aplicación de mercados

Funciones:

- Administrador de Seguridad, de la Red, de los Sistemas Operativos, de las bases de Datos y de las Aplicaciones. Tiene los máximos privilegios y, por tanto, el riesgo de que una actuación errónea suya pueda afectar al sistema es alto.
- Mantenimiento de los sistemas y aplicaciones. Responsable de la resolución de incidencias que puedan surgir en el entorno hardware / software de los sistemas informáticos o de las propias aplicaciones de acceso a los datos.
- Tiene acceso al software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan; todo ello, bajo estricto control de la Sociedad a través del Responsable de Seguridad.
- Actividad de Operador de Red, de los Sistemas Operativos, de las Bases de Datos y de las Aplicaciones. Su actuación está limitada a la operación de los sistemas y redes utilizando las herramientas de gestión disponibles.
- Tiene como objetivo salvaguardar la privacidad de los recursos a los que tenga acceso, así como los nominales cedidos por los usuarios con el objetivo de configurar sus entornos personales.

Obligaciones:

Del Entorno de Sistema Operativo y de Comunicaciones

- Asegurar que ninguna herramienta o programa de utilidad que permita el acceso a los datos sea accesible a ningún usuario no autorizado.
- Guardar en lugar protegido las copias de seguridad y respaldo de los datos de forma que ninguna persona no autorizada tenga acceso a las mismas o asegurar que se cumple lo reflejado en contrato, en caso de haber externalizado este servicio.
- Asegurar que no se permita a personas no autorizadas el acceso, en el caso de que el ordenador en el que está ubicados los datos esté integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso a los datos.

Del Sistema Informático o Aplicaciones de Acceso a los datos

- Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, debe ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.
- Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, debe aplicar a esos ficheros de prueba un tratamiento de seguridad similar al que aplica a los ficheros correspondientes de datos reales.

De la Salvaguarda y Protección de las Contraseñas Personales

- Asignación y cambio de contraseñas mediante el mecanismo y con la periodicidad determinada por el Responsable de Seguridad, en el procedimiento desarrollado en el punto 7.4 de este documento.
- Protección del archivo donde se almacenen las contraseñas.

De los Procedimientos de Respaldo y Recuperación

- Obtener periódicamente una copia de seguridad a efectos de respaldo y posible recuperación en caso de fallo. Estas copias deben realizarse de acuerdo al esquema de obtención de copias de respaldo descrito en el procedimiento de "*Realización de copias de respaldo y de recuperación de datos*", descrito en el punto 14.1.
- En caso de fallo del sistema con pérdida total o parcial de los datos, aplica un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos al estado en que se encontraban en el momento del fallo. En el caso de que ese servicio sea contratado a un proveedor externo, se debe asegura que se cumple lo contemplado en el contrato.
- Es necesaria la autorización del Responsable de Seguridad para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan sido realizadas para hacer posible dicha recuperación.

De los Controles Periódicos de verificación del cumplimiento

- Con periodicidad, al menos, semestral, comunica al Responsable de Seguridad cualquier cambio que se haya realizado en los datos técnicos de los anexos, como, por ejemplo, cambios en el software o hardware, bases de datos o aplicaciones de acceso a los datos, procediendo igualmente a la actualización de dichos anexos.
- Informe sobre las obligaciones indicadas en el punto anterior.

12. TRANSFERENCIA INTERNACIONAL DE DATOS.

Cuando los datos personales se envían fuera del ámbito del Espacio Económico Europeo (EEE), que comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein, se produce una transferencia internacional de datos.

Aunque podría parecer que las transferencias internacionales son poco habituales en el ámbito de la Sociedad el uso cada vez más frecuente de tecnologías de la información y la comunicación o la generalización de servicios "en nube" ("cloud computing"), supone que aumenten las posibilidades de que se transfieran estos datos fuera del EEE.

En este sentido, el *RGPD* contiene una serie de supuestos (arts. 45 y 46), que permiten realizar dichas transferencias internacionales sin necesidad de solicitar una autorización previa por parte de las autoridades de protección de datos.

Si no existe decisión de adecuación, sólo pueden transferirse datos en circunstancias limitadas:

- Sobre la base del consentimiento.
- El uso de cláusulas contractuales tipo publicadas por la Comisión Europea.
- Caso de transferencias interempresariales, el uso de normas corporativas vinculantes.
-

13. INFRACCIONES Y SANCIONES

El *RGPD* distingue dos niveles de sanciones en atención a la gravedad de los hechos:

- Infracciones menos graves: Para las que establece una sanción máxima de 10.000.000 € o el 2% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
  - Infracción de las garantías en la obtención del consentimiento de menores de edad por Internet;
  - Tratamiento sin disociación previa de datos cuando no es precisa la identificación del interesado;
  - El establecimiento de sistemas de tratamiento sin documentar la consideración previa de las implicaciones de protección de datos o tratando información excesiva;
  - Contratación de encargados del tratamiento sin cumplir las obligaciones normativas;

- Omisión de la llevanza del Registro de Actividades de Tratamiento.
- Omisión del deber de cooperación con la Autoridad de control.
- Omisión del deber de aplicación de medidas de seguridad adecuadas a las circunstancias del tratamiento.
- Omisión del deber de notificación y comunicación de violaciones de seguridad.
- Omisión del deber de realizar la evaluación previa del impacto en la privacidad en determinados tratamientos de datos (en casos de analítica para la obtención de perfiles y adopción de decisiones).
- Omisión del deber de consultar previamente a la Autoridad de Control cuando la evaluación de impacto evidencia posibles riesgos altos para la privacidad.
- Omisión del deber de designar al DPO o de garantizar el ejercicio de sus funciones.
- Infracción de las obligaciones relativas a los procesos de certificación y uso de los certificados.

- Infracciones más graves: Para las que establece una sanción máxima de 20.000.000 € o, tratándose de una empresa, el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía por las infracciones de:
  - Omisión del deber de tratar los datos de forma leal y transparente manteniendo la calidad de la información; Tratamiento sin concurrir alguna de las causas que lo legitiman; Infracción de los requisitos de calidad del consentimiento y de respeto a las obligaciones normativas relativas a los datos especialmente protegidos;
  - Omisión del deber de transparencia e información a los interesados o de atención de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad.
  - La transferencia internacional de datos personales sin cumplir las exigencias normativas.
  - Infracción de las normas que se aprueben en España respecto del tratamiento para RRHH.
  - Incumplimiento de las resoluciones de la Agencia de limitación temporal o definitiva del tratamiento o de suspensión de flujos de datos, o el impedimento a la función inspectora o a la tramitación de expedientes;
  - Incumplimiento de las resoluciones correctivas de la Agencia Española de Protección de Datos.

Dado que el *RGPD* no define suficientemente las infracciones y sanciones, la LOPDGDD desarrolla este apartado, clasificando las infracciones en leves, graves y muy graves atendiendo a los hechos y circunstancias.

Se incluye en el Anexo 9 un resumen de las infracciones y sanciones establecidas por la LOPDGDD y el *RGPD*.

14. PROCEDIMIENTOS DE DESARROLLO DE LAS OBLIGACIONES DEL PERSONAL

14.1 Procedimiento de realización de copias de respaldo y de recuperación de datos

Emisión de copias de respaldo y su archivo y salvaguarda

El Administrador de Sistemas:

- Copias de seguridad en red:

La empresa ha implantado el servicio de Sharepoint 365. Almacena una copia de seguridad de toda la configuración de Sharepoint en las instalaciones de Ithealth, bajo el software veeam backup for office 365. Este proceso se realiza de forma totalmente automática.

Recuperación de datos y su Autorización previa

En caso de fallo del sistema con pérdida total o parcial de los datos:

El Administrador de Sistemas partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia:

- Obtiene la autorización del Responsable de Seguridad para la ejecución de los procedimientos de recuperación de los datos,
- Reconstruye los datos al estado en que se encontraban en el momento del fallo.
- En el caso de producirse una incidencia que genere destrucción de información procede a la recuperación de la información destruida.
- Si dicha recuperación fuese imposible, procede a la obtención de la copia de respaldo más reciente y a restaurar la información destruida.
- Registra la incidencia, con las medidas adoptadas, y deja constancia de las manipulaciones que hayan sido realizadas para hacer posible dicha recuperación y lo notifica al Responsable de Seguridad.

14.2 Procedimiento de identificación y autenticación de usuarios

Relación de usuarios

- Entorno de red y sistemas operativos

Por cuestiones de seguridad y facilidad de uso no se transcribe la lista a papel. Dicha lista se encuentra disponible en poder del Administrador de Sistemas y del Responsable de Seguridad.

- Resto de aplicaciones principales:

Por cuestiones de seguridad y facilidad de uso no se transcribe la lista a papel. Dicha lista se encuentra disponible en poder del Administrador de Sistemas y del Responsable de Seguridad.

Procedimiento

Las contraseñas de los usuarios autorizados tendrán en general, si bien dependiendo de cada entorno puede variar en algún aspecto:

- Una longitud mínima, de 8 caracteres alfanuméricos.
- Contendrá al menos dos caracteres numéricos y una mayúscula. El uso de caracteres especiales puede estar restringido por el sistema, pero es aconsejable. Se deben evitar nombre propios o palabras con sentido que se puedan identificar con el usuario.
- Obligará a teclearla de nuevo después de 5 minutos sin estar operativa.

Adicionalmente y, en su caso, deben cumplirse también las medidas de nivel medio:

El Responsable de Seguridad establece un mecanismo que permite la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

El Responsable de Seguridad es responsable de la actualización de la lista de usuarios y de la verificación de la existencia de los códigos de identificación y autenticación. Revisa cada trimestre la lista de usuarios.

Cada usuario de la Red corporativa es responsable de los identificativos y contraseñas de acceso asignadas a él, así como de las demás aplicaciones de la Sociedad que son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pueden derivarse del mal uso, divulgación o pérdida de los mismos.

Entorno de Red	Ithealth ha implementado los equipos informáticos de Beka Finance dentro de un Azure AD (directorio activo de Azure) y ha creado una cuenta office 365 para cada trabajador.

	Comparte rack y electrónica de red con Gala Capital. No dispone de servidores físicos, tan solo usa el switch, patch panel, firewall y router para la salida a internet. Cuenta con la tecnología de Sonicwall (marca más que puntera, robusta y consolidada en el mundo IT con certificaciones contrastadas) para implementar un sistema de firewall que dota a la red de seguridad lógica. Ithealth puede acceder a los sistemas de la Sociedad de forma remota mediante el software Teamviewer
Gestión de los usuarios con acceso Sharepoint y Office 365 de Microsoft	La cuenta administradora es admin@galacapital.com, con los permisos delegados en sharepoint@bekafinance.com En sharepoint@bekafinance.com se han creado diferentes sitios añadiendo a los miembros pertenecientes. Los sitios creados son: 1. Información general Fondos alternativos 2. Eq. Fondos alternativos 3. Eq. Legal 4. Eq. Legal otros 5. Eq. Fondos tradicionales 5.2 Operaciones y finanzas 6. Eq. Fondos sociales 7. Eq. Administración 8. Cumplimiento normativo 9. Marketing- BekaAM 10. Anuska y Karen
Acceso a la información	Cada usuario tiene acceso al sitio al que pertenece a través del panel web de office 365 de su equipo o dispositivo móvil.

14.3 Procedimiento de asignación, distribución y almacenamiento de contraseñas

El Responsable de Seguridad debe establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos/perfiles distintos a los autorizados mediante las siguientes medidas:

Control de acceso al sistema:

- Al iniciar el proceso de arranque de cada ordenador conectado a la red corporativa de la Sociedad, se solicita el identificativo y clave de acceso del usuario a dicha red corporativa.
- Cada identificador tiene unos privilegios asociados, en función del cargo y las funciones del usuario que solicita el acceso.
- La introducción de una clave distinta a la autorizada impide el acceso a la red, ofreciendo la posibilidad de introducir de nuevo la clave, con el fin de subsanar errores de teclado.

Control de acceso a los datos personales:

- El acceso de los usuarios está restringido en función de los perfiles de usuario asignados.

- El sistema operativo mantiene una lista de usuarios del sistema indicando su perfil y los menús y comandos a los que tienen acceso.

Descripción del procedimiento

El Responsable de Seguridad, en función del cargo y de las funciones que vaya a desarrollar cada una de las personas de la Sociedad:

- Asigna un perfil de usuario en las distintas aplicaciones utilizadas por la Sociedad a cada una de las personas actualmente en plantilla o las de nueva incorporación.
- Hace llegar la petición al Administrador de Sistemas.

El Administrador de sistemas:

- Da de alta los perfiles generales o particulares necesarios, con la contraseña caducada para que el sistema obligue al usuario a cambiarla la primera vez que haga uso de ella.
- Informa de modo confidencial al usuario del identificador / contraseña asignada al usuario para el acceso a la aplicación, vía mail. Los identificativos y contraseñas de acceso asignadas a cada usuario de la red corporativa de la Sociedad son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de los mismos.
- Cuida, durante el tiempo que estén vigentes, que las contraseñas se almacenen de forma ininteligible.
- Elabora la relación de los usuarios de la red con acceso autorizado.
- El Responsable de Seguridad modifica los permisos concedidos y las contraseñas asignadas cuando se estime conveniente o se detecte algún uso indebido.
- Deshabilita o bloquea el usuario del identificador/contraseña asignada a algún usuario que haya dejado de formar parte de la Sociedad.
- Informa al Responsable de Seguridad en todo momento de los usuarios que tengan acceso autorizado a los sistemas informáticos, incluyendo el nivel de acceso para cada uno de ellos.

El Responsable de Seguridad:

- Custodia y actualiza la relación de todos los usuarios de la red que tienen acceso autorizado al sistema de información conjuntamente con el Administrador de Sistemas.

14.4 Procedimiento de Gestión de Soportes y Documentos.

Objeto

Descripción del procedimiento para la identificación, inventario, almacenamiento y custodia de los soportes informáticos con datos personales existentes en la Sociedad y del registro y autorización de entrada y salida de los mismos.

Alcance

Este procedimiento es aplicable a todas las sociedades enunciadas en el punto 1 y alcanza a todo el personal interesado.

Responsabilidades

Las indicadas sobre "*Funciones y obligaciones del personal*" de este documento y las que se fijan de forma específica en el desarrollo de este procedimiento.

Definición de soporte

Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Por sistema de información se entiende conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Descripción del procedimiento

Identificación de soportes

Los usuarios deben asegurar que cualquier soporte que albergue copias de respaldo de los sistemas de información de la Sociedad, esté debidamente etiquetado para su custodia con la fecha de ejecución de la copia, si es una copia diaria o mensual.

El Responsable del Área: cuida de la identificación de los soportes de su área operativa.

El Administrador de Sistemas, adicionalmente cuida de que el sistema de copias de respaldo disponga de la capacidad de identificar los datos contenidos en las mismas a nivel de detalle de archivo.

Inventario de soportes

Responsable de Área de la unidad organizativa correspondiente debe:

- Elaborar un inventario de soportes, utilizando el modelo Anexo 2 denominado "*Inventario de Soportes*".
- Contar con el Vº Bº del Responsable de Seguridad y estar a su disposición

Almacenamiento de soportes

Los soportes se deben almacenar en un lugar con acceso restringido al Administrador de Sistemas o al Responsable del Área, con las debidas medidas de seguridad que garanticen su integridad, debiendo aplicarse al menos, las medidas definidas en el procedimiento 14.4 "*Gestión de Soportes*".

Reutilización o eliminación de soportes

En el caso de reutilización o eliminación de soportes grabados con datos del Fichero se indica el método utilizado para el borrado físico de estos datos.

Se deben seguir las siguientes pautas:

- Los soportes grabados con datos personales serán borrados para su reutilización mediante una triple acción de dar formato (caso de discos duros).
- No se recomienda la reutilización para salvar otro tipo de información del resto de soportes (cintas, diskettes, discos magneto-ópticos, etc.).
- La destrucción de cualquier soporte con datos, se hará de forma que los materiales sensibles a la grabación de datos queden totalmente inservibles, o bien, borrados mediante varias pasadas por el dispositivo desmagnetizador existente.

Entrada y Salida de soportes informáticos

El Responsable de Seguridad debe autorizar cualquier entrada en los locales de la Sociedad o salida fuera de los mismos, de soportes donde estén ubicados los ficheros.

El responsable de la recepción o entrega del soporte debe:

- Estar autorizada por el Responsable de Seguridad y será como mínimo el Responsable del área.
- Para cada entrada o salida puntual debe cumplimentar el impreso denominado "Autorización y registro de entrada y salida de soportes" Anexo 3 y 4 de forma previa a su ejecución y tener los documentos de solicitud, autorización y registro y de recepción o envío debidamente cumplimentados.

Pueden identificarse dos tipos de registros de soportes de entrada y salida:

- Registros de entradas y salidas puntuales: corresponden a peticiones concretas en un momento dado (Anexos 3 y 4).
- Registros de entradas y salidas periódicos: corresponden a los que manejan diariamente los departamentos operativos (Anexo 4).

Cada entrada o salida conformará un registro independiente, y contendrá los datos necesarios identificativos relativos a: Tipo de soporte/Fecha y hora/Emisor/Finalidad y destino/Forma de envío/El número de soportes/El tipo de

información que contienen/Persona responsable de la recepción o entrega/Autorización/Documentación de la entrada o salida.

- La salida de soportes por Red o correo electrónico o vías de comunicación alternativas, se realizarán desde recursos del sistema y cuentas o direcciones de correo controladas por usuarios especialmente autorizados para este fin por el Responsable de Seguridad.

EL Responsable de Seguridad debe:

- Mantener el "Registro y autorización de salida de soportes" general de la sociedad, formado por todas las hojas de registro elaboradas por los Responsables de Área.
- Asegurar que en carpeta distinta se custodia la documentación relativa a los demás documentos que soportan la entrada o salida, existiendo una relación con el registro mediante el código de cada registro.

15. INFORMACIÓN DE DENUNCIAS INTERNAS EN MATERIA DE PROTECCIÓN DE DATOS

La Sociedad en cumplimiento del Art. 24 de la LOPDGDD establece un canal interno específico de denuncias para que los empleados y directivos puedan comunicar, incluso anónimamente, información sobre posibles incumplimientos cometidos en el seno de la Sociedad o en la actuación de terceros que contraten con la Sociedad, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que es aplicable.

15.1 Preservación de la identidad y confidencialidad de los datos

Se refiere a la preservación de la identidad y confidencialidad de los datos de las personas afectadas y especialmente de la persona denunciante.

El Responsable de Seguridad:

- Puede recibir de cualquier empleado y directivo las comunicaciones sobre posibles incumplimientos mediante el envío del modelo denominado "Formulario para la Comunicación de Infracciones del RGPD o de la LOPDGDD", (anexo 10), que no identifica a la persona que lo emite, y que introducido en un sobre cerrado dirigido a él puede remitírselo por correo postal, garantizando así su confidencialidad, sin perjuicio de que pueda utilizar el mismo modelo de comunicación y dirigirlo por correo electrónico al Responsable de Seguridad si así lo desea a la dirección:
- El acceso a estas comunicaciones de denuncias internas de posibles

incumplimientos de la normativa de protección de datos de carácter personal únicamente será accesible por el Responsable de Seguridad, por la función de Cumplimiento Normativo y por el órgano de administración de la Sociedad, debiendo cumplir en todo momento la normativa sobre protección de datos de carácter personal de los sistemas de información de denuncias internas utilizados por estos motivos.

- Los datos de quien formule la comunicación y de los empleados y terceros se conservan por el Responsable de Seguridad en el sistema de denuncias, que se constituye como un registro de las mismas y de un expediente digitalizado o en soporte papel únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

De esta forma se asegura la identidad y se garantiza la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la Sociedad, en caso de que se hubiera identificado.

15.2 Conservación de los datos

El Responsable de Seguridad:

- Transcurridos tres meses desde la introducción de los datos, debe proceder a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica.
- Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la LOPDGDD.

La función de Cumplimiento Normativo:

- Transcurrido el plazo mencionado en el apartado anterior los datos podrán seguir siendo tratados, por el órgano al que corresponda, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención sobre la investigación de los hechos denunciados, registrando de forma anónima las denuncias que no se hayan dado curso. También suprimir del sistema de denuncias sin obligación de bloqueo cuando dichas denuncias no hayan sido cursadas.

El Órgano de Administración de la Sociedad:

- Además, el órgano de administración de la Sociedad garantiza la protección frente a posibles represalias, discriminaciones y cualquier otro tipo de trato

injusto por el hecho de que el empleado o directivo comunique las posibles infracciones.

16. NORMATIVA APLICABLE

La normativa básica en materia de protección de datos aplicable en España está compuesta fundamentalmente por los siguientes textos:

- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
- Reglamento (UE) 2016/679 del PE y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre. (vigente en aquellos artículos que no contradigan al RGPD).
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

17. ANEXOS

1. DOCUMENTOS CONTRACTUALES

- Contrato con encargados del tratamiento.
- Alta de clientes.
- Contratos con clientes.
- Órdenes de operación.

2. INVENTARIO DE SOPORTES

NOMBRE DEL FICHERO:	N.º INSCRIPCIÓN

ALTAS	FECHA	BAJAS		
		Reutilización	Destrucción	Método

ENTIDAD	ÁREA	FECHA
RESPONSABLE DEL ÁREA Nombre: Firma:		

3. AUTORIZACIÓN Y REGISTRO DE SALIDA DE SOPORTES

Carácter • PUNTUAL

Núm.: 20 /---

AUTORIZACIÓN DEL RESPONSABLE DEL FICHERO	
Nombre:	
Cargo:	
Sociedad:	
Fecha:	Firma:

SOPORTE	
Tipo de soporte y número	
Contenido	
Fichero de donde proceden los datos	
Fecha de Creación:	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona responsable de la entrega	
Persona que autoriza	

Cargo / puesto	
Observaciones	
Firma:	

Fecha y hora de envío

Documentación Soporte:

- Petición de soporte
- Documento de Salida
- Documentos de Interés
- Correo Electrónico

4. AUTORIZACIÓN Y REGISTRO DE ENTRADA DE SOPORTES

Carácter • PUNTUAL Núm.: 20 /---

AUTORIZACIÓN DEL RESPONSABLE DE SEGURIDAD	
Nombre:	
Cargo:	
Sociedad:	
Fecha:	Firma:

SOPORTE	
Tipo de soporte y número	
Contenido	
Fichero de donde proceden los datos	
Fecha de Creación:	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona responsable de la entrega	

Persona que autoriza	
Cargo / puesto	
Observaciones	
Firma:	

Fecha y hora de entrada

Documentación Soporte:

- Petición de soporte
- Documento de Entrada
- Documentos de Interés
- Correo Electrónico

5. CONTROLES PERIÓDICOS Y AUDITORÍAS

Referencia de los informes relativos a los controles periódicos descritos y de las auditorías realizadas, tanto externas como internas.

FECHA DEL INFORME	EMPRESA QUE REALIZA EL INFORME	UNIDAD ORGANIZATIVA	NOMBRE DEL INFORME	PERIODICIDAD

Fecha	Firma del Responsable de Seguridad

(*) A este documento se le anexiona la documentación soporte necesario

6. DECLARACIÓN DE RECEPCIÓN DEL PROCEDIMIENTO DE LOPDGDD

COMPROMISO SOBRE CONFIDENCIALIDAD DE LA INFORMACIÓN OBTENIDA DE CLIENTES Y DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LOS CLIENTES

XXXXXXXXXXXXXXXXX, como empleado de BEKA ASSET MANAGEMENT SGIIC, S.A. (en adelante la Sociedad), con la firma en este documento acepto el cumplimiento del compromiso de confidencialidad a que está obligada la Sociedad en su relación con los clientes recogidas en los contratos firmados de prestación de servicios, asumiendo las consecuencias que, en caso contrario, pudieran derivarse por ley y, así mismo me doy por enterado de que el incumplimiento de las normas indicadas en este documento o en cualquier otro elaborado por la Sociedad sobre esta materia puede dar lugar a la adopción de las medidas disciplinarias oportunas.

En especial, en materia de confidencialidad declaro haber comprendido y cumplir las normas siguientes:

- Considerar como información confidencial, toda aquella que tenga origen en el contrato firmado y en la prestación de servicios dados al cliente y que sea susceptible de ser revelada de palabra, por escrito o por cualquier otro medio o a través de cualquier soporte, actualmente conocido o que se invente en el futuro.
- Mantener estricta confidencialidad sobre la información confidencial a la que tenga acceso, tanto durante la relación contractual mantenida con el cliente como una vez extinguida la misma por cualquier causa y referida al cliente y a los clientes de éste.
- Mantener la información confidencial fuera del alcance de las personas que no tengan autorizado su acceso, debiendo tomar todas las medidas necesarias para mantener en confidencialidad dicha información, cumpliendo con los protocolos de seguridad relativos al almacenamiento, transmisión y custodia de la misma.
- Compromiso de no divulgar información confidencial a ninguna persona ni entidad ajena a la Sociedad.

Asimismo, declaro haber recibido y leído el procedimiento denominado "Protección de datos de carácter personal".

En especial, declaro haber comprendido las normas siguientes:

- Como usuario de sistemas de información de carácter personal tengo activado un protector de pantalla con clave de acceso.
- Soy responsable de las consecuencias que pueda tener el que otras personas tengan acceso a mis contraseñas, o a cualquier otro método de autenticación.
- Sin la autorización correspondiente no realizaré la instalación de software adicional (incluso legal) ni conexión a cualquier red externa.
- Cualquier software o información que reciba de una fuente externa, vía internet, disquete o CD, la trataré como sospechosa de contener virus y, por tanto, no la utilizaré, instalaré o ejecutaré en tanto no haya sido escaneada con el antivirus.
- Como empleado, asumo que estoy obligado al secreto profesional y a no revelar información sin el previo consentimiento por escrito del interesado. Estas obligaciones subsistirán aún después de finalizar mi relación laboral con la Sociedad.
- Soy responsable de los equipos que me sean asignados y tomo las medidas necesarias para la conservación, custodia y el buen funcionamiento de los mismos.
- Realizaré copias de seguridad de toda aquella información del disco duro que considere crítica o que así haya sido determinada en el Documento de Seguridad y los procedimientos relacionados.
- Haré un buen uso del correo electrónico, los mensajes no serán ilegales, difamatorios, obscenos, pornográficos, ofensivos o dañinos, o que puedan ser considerados por otras causas de ofensa sexual, racial o cualquier otro tipo de discriminación.

Área: XXXXXXXXXXXXXX Fecha y Lugar: Madrid, xx de XXXXX de 20XX

Firma:

7. COMUNICACIÓN Y REGISTRO DE VIOLACIÓN DE SEGURIDAD DE DATOS PERSONALES

SOCIEDAD	N.° DE REGISTRO

COMUNICACIÓN PARA	CORREO ELECTRÓNICO	TELÉFONO

1. IDENTIFICACIÓN DE LA VIOLACIÓN

COMUNICADA POR (Nombre)	ÁREA	FUNCION

TIPO DE VIOLACIÓN DE LA SEGURIDAD	FECHA	HORA

CATEGORÍA DE LOS INTERESADOS	NUM. APROXIMADO DE INTERESADOS
CATEGORÍA DE LOS REGISTROS DE DATOS INTERESADOS	NUM. APROXIMADO DE REGISTROS INTERESADOS
DETALLE DE LA VIOLACIÓN DE SEGURIDAD	

2. CONSECUENCIA QUE PUEDE PRODUCIR LA VIOLACIÓN DE SEGURIDAD

3. MEDIDAS ADOPTADAS PARA MITIGAR LOS POSIBLES EFECTOS NEGATIVOS

4. RECUPERACIÓN DE DATOS (Rellenar sólo si la violación es de este tipo)

Procedimiento realizado:	
Datos restaurados:	
Datos grabados manualmente:	

Persona que ejecutó el proceso:	

FECHA Y HORA DE LA SOLUCIÓN

FIRMA DEL RESPONSABLE

A rellenar por el receptor de la VIOLACIÓN de SEGURIDAD

8. RELACIÓN DE ENCARGADOS DEL TRATAMIENTO DE LA SOCIEDAD

IDENTIFICACIÓN					FECHA:	
FICHERO	TRATAMIENTO	NOMBRE DEL ENCARGADO	NOMBRE DEL RESPONSABLE DEL FICHERO	PERIODO DE VIGENCIA DEL ENCARGO	FECHA DEL CONTRATO	TRAT. EXCLUSIVO

9. RELACIÓN DE INFRACCIONES Y SANCIONES EN EL RGPD Y EN LA LOPDGDD

1. Clases de infracciones

El *RGPD* y la LOPDGDD describen las conductas constitutivas de infracciones en protección de datos, clasificándolas en muy graves, graves y leves en el caso de la LOPDGDD, mientras que el RGPD distingue las infracciones en atención al importe de la sanción que les corresponde. En todo caso, la distinción de niveles que realiza la LOPDGDD puede aplicarse también a la distinción que hace el RGPD.

1.1. Infracciones consideradas muy graves (Artículo 72 LOPDGDD y 82.5 RGPD).

Se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en el RGPD, y en particular:

a) El tratamiento de datos personales infringiendo los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento:

- Vulnerando los principios de licitud, lealtad y transparencia en relación con el interesado,
- De manera incompatible con los fines determinados, explícitos y legítimos informados al interesado, iniciales.
- Excesivos o inadecuados en relación con los fines para los que son tratados.
- Inexactos o desactualizados.
- Innecesarios para los fines del tratamiento por haberse culminado el mismo («limitación del plazo de conservación»),
- Sin garantizar la seguridad técnica y organizativa apropiada que impida el tratamiento no autorizado o ilícito, así como su pérdida, destrucción o daño accidental.

La Sociedad tiene que demostrar que cumple todos estos principios, invirtiéndose la carga de la prueba.

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del RGPD *(Consentimiento, necesidad para la ejecución de un contrato o para cumplir una obligación legal o interés legítimo de la entidad).*

c) El tratamiento en base a un consentimiento inválido, que ocurre cuando la sociedad no sea capaz de acreditarlo, o el consentimiento no sea libre, específico o revocable.

d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del interesado o con una base legal para ello.

e) El tratamiento de datos personales especialmente protegidos, salvo bajo los requisitos establecidos en la norma.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad, salvo bajo los requisitos establecidos en la norma.

g) El tratamiento de datos de carácter personal relacionados con infracciones y sanciones administrativas, salvo bajo los requisitos establecidos en la norma.

h) La omisión del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal.

i) La vulneración del deber de confidencialidad.

j) La exigencia de pago de un canon para facilitar la información legalmente obligatoria o para atender las solicitudes de ejercicio de derechos de los interesados, salvo los casos previstos en la norma.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos de los interesados.

l) La transferencia internacional de datos de carácter personal sin cumplir las garantías, requisitos o excepciones de la norma.

m) El incumplimiento de las resoluciones dictadas por la AEPD en el ejercicio de sus funciones.

n) El incumplimiento de la obligación de bloqueo de los datos inexactos, innecesarios o cuyo tratamiento infrinja una ley o la ley haya ordenado que se interrumpa.

o) Impedir el acceso a los datos personales, a la información, locales, equipos y medios de tratamiento requeridos por la AEPD para el ejercicio de sus poderes de investigación.

p) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

q) No atender debidamente las resoluciones de la AEPD de atención de los derechos de los interesados, de regularización del tratamiento, de comunicación a los interesados de las brechas de seguridad, de limitación temporal o definitiva del tratamiento, de eliminación de datos personales o de suspensión de flujos internacionales de datos.

Además, el *RGPD* califica como muy graves las infracciones de las normas nacionales que se dicten en relación con los tratamientos de datos en relación con las libertades de expresión e información, tratamientos en el ámbito laboral y en materia de deber de secreto.

1.2 Infracciones consideradas graves (Artículo 73 LOPDGDD y 82.4 RGPD).

Se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en el RGPD, y en particular las siguientes:

a) El tratamiento de datos de carácter personal de un menor de trece años sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de la patria potestad o tutela.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de trece años o por el titular de su patria potestad o tutela.

c) El impedimento, obstaculización o la no atención reiterada de los derechos de los interesados en los tratamientos de datos seudonimizados cuando el interesado haya facilitado información adicional que permita su identificación.

d) La no aplicación de los principios de protección de datos desde el diseño y por defecto.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar la minimización de datos.

f) La contratación de un encargado de tratamiento que no ofrezca las garantías suficientes para cumplir el RGPD.

g) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato conforme a los requisitos del RGPD.

h) No disponer del registro de actividades de tratamiento.

i) No facilitar a la AEPD el registro de actividades de tratamiento.

j) No cooperar con la AEPD en el desempeño de sus funciones salvo cuando constituye una infracción muy grave.

k) El tratamiento de datos sin la previa valoración de riesgos en los derechos de los interesados.

l) El incumplimiento del deber de notificación a la Agencia Española de Protección de Datos de una violación de seguridad de los datos personales.

m) El incumplimiento del deber de comunicación al interesado de una violación de la seguridad de los datos salvo cuando constituya una infracción muy grave.

n) El tratamiento de datos de carácter personal sin haber llevado a cabo la evaluación del impacto en la protección de datos personales en los supuestos en que la misma sea exigible

o) El tratamiento de datos de carácter personal sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva.

p) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento.

q) Impedir al DPO el desempeño de sus funciones.

r) La utilización indebida de un sello o certificación en materia de protección de datos.

NOTA: Se han suprimido, para facilitar la claridad y eficiencia de la información, aquellas infracciones que no se adecuan a la actividad y perfil de la Sociedad.

1.3 Infracciones consideradas leves (Artículo 74 LOPDGDD).

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal del RGPD y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del interesado por no facilitar toda la información exigida por el RGPD.

b) La exigencia del pago de un canon excesivo para facilitar al interesado la información sobre el tratamiento o para atender las solicitudes de ejercicio de derechos de los interesados, cuando está permitido requerirlo.

c) No atender las solicitudes de ejercicio de los derechos de los interesados, salvo cuando constituya infracción muy grave.

d) No atender los derechos de los interesados en los tratamientos de datos seudonimizados cuando el interesado haya facilitado información adicional que permita su identificación.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.

f) El incumplimiento de la obligación de informar al interesado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los interesados o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los interesados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento.

j) Disponer de un Registro de actividades de tratamiento incompleto o inexacto.

k) La notificación incompleta o defectuosa a la Agencia Española de Protección de Datos de la información relacionada con una violación de seguridad de los datos.

l) El incumplimiento de la obligación de documentación de cualquier violación de seguridad.

m) El incumplimiento del deber de comunicación al interesado de una violación de la seguridad de los datos, cuando sea aplicable.

n) Facilitar información inexacta a la Agencia Española de Protección de Datos en los supuestos en que sea preceptiva.

o) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea obligatorio.

NOTA: Se han suprimido, para facilitar la claridad y eficiencia de la información, aquellas infracciones que no se adecuan a la actividad y perfil de la Sociedad.

2. Sanciones por infracciones muy graves

Conforme al artículo 58.2 del RGPD, las infracciones de las garantías y obligaciones y mandatos que establece el RGPD pueden sancionarse, en función de las circunstancias de cada caso individual, con las siguientes sanciones:

a) Una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento.

b) Apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento,

c) Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento,

d) Ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado,

e) Ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales,

f) Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición,

g) Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19,

h) Retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación,

i) Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

Además, este mismo apartado prevé que, en función de las circunstancias de cada caso individual, puedan imponerse multas administrativas a título adicional o sustitutivo de las medidas anteriores, que, en todo caso, deben ser efectivas, proporcionadas y disuasorias en cada caso individual y con un importe de:

– Para las infracciones muy graves, 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

– Para las infracciones graves, 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Ninguna de las dos normas, ni el RGPD ni la LOPDGDD prevén multas en el caso de infracciones leves.

Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados interesados y el nivel de los daños y perjuicios que hayan sufrido.

b) La intencionalidad o negligencia en la infracción;

c) Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados,

d) El grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado,

e) Toda infracción anterior cometida por el responsable o el encargado del tratamiento,

f) El grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción,

g) Las categorías de los datos de carácter personal interesados por la infracción,

h) La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida,

i) Cuando las medidas indicadas en el artículo 58, apartado 2, del RGPD hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas,

j) La adhesión a códigos de conducta en virtud del artículo 40 RGPD o a mecanismos de certificación aprobados con arreglo al artículo 42 RGPD, y

k) Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Además, el artículo 76.2 de la LOPDGDD dispone que para graduar la sanción se tengan también en consideración:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del interesado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del RGPD, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

10. FORMULARIO PARA LA COMUNICACIÓN DE INFRACCIONES DEL RGPD O DE LA LOPDGDD

Fecha de comunicación:

Descripción de la denuncia

Normativa infringida del RGPD o de la LOPDGDD

Normativa infringida del manual de PD u otra normativa interna de la Sociedad

Documentación remitida

Comunicación que se realiza en cumplimiento del Art. 24 de la Ley Orgánica 3/2018 y de acuerdo con lo recogido en el punto 15 de este manual de PD de la Sociedad.

11. Ficha, características y análisis de riesgos y medidas (excel adjunto)

Este procedimiento debe llevar adjunto un Excel en el que se detalla la siguiente información:

- Una ficha para cada una de las actividades del tratamiento tal y como están descritas en el punto 8 de este procedimiento.
- Las características de cada tratamiento en el que se detalla el ciclo de vida y los elementos intervinientes
- Los riesgos asociados y las medidas a adoptar para cada una de las actividades del tratamiento.