ACTA DE APROBACIÓN DE CONTROLES PARA LA PREVENCIÓN DE LA COMISIÓN DE DELITOS EN EL CONTEXTO DE LA PERSONA JURÍDICA

En San Sebastián de los Reyes, a 21 de febrero de 2023

En el día de hoy, el Órgano de Administración de **SEGURA E HIJOS, S.A.** ha aprobado la implantación de los siguientes controles para la prevención de la comisión de delitos en el contexto de la persona jurídica:

- Uso de medios tecnológicos
- Política de Protección de datos (ya implementada en 2018)
- Uso de vehículos (ya implementada en 2020)
- Política de Derechos Humanos
- Política de Recursos Humanos e Igualdad
- Política Medioambiental (ya implementada)
- Política de Calidad (ya implementada)
- Política de Prevención de Blanqueo de Capitales y Financiación del Terrorismo

Fdo. Demetrio Segura Martín
Administrador solidario 1

Fdo. Francisco Segura Martín
Administrador solidario 2

POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS

21 de febrero de 2023

ÍNDICE

1.- Objeto

La presente política de uso de medios tecnológicos (en adelante, la **"Política"**) tiene por finalidad garantizar que los empleados de **Segura e Hijos, S.A.** (en adelante, la ***"Empresa"*** o "**SeH**", indistintamente) como usuarios de los medios tecnológicos puesto a su disposición, hagan un uso adecuado, responsable y lícito de los mismos.

A efectos de la presente Política, tendrán la consideración de medios tecnológicos (en adelante, los **"Medios Tecnológicos")**, entre otros, los siguientes: ***(i)*** equipos, servidores de aplicaciones, terminales de acceso remoto, ordenadores de mesa o portátiles, PDAs, Tablets y dispositivos similares o equivalentes, ***(ii)*** cualquier aplicación o programa de *software*, red corporativa y sistemas, ***(iii)*** servicios de Internet, Intranet y correo electrónico, ***(iv)*** las cuentas que dan acceso al uso de *hardware*, *software* y sistemas de información, y ***(v)*** teléfonos fijos, teléfonos móviles, *smartphones*, *GPS*, etc.

Resulta preciso señalar que los Medios Tecnológicos de los que dispone la Empresa son instrumentos de producción al servicio del negocio y a través de ellos se cumple la prestación profesional. Por este motivo, la Empresa se reserva el derecho de comprobar si su uso se ajusta a las finalidades que lo justifican. Atendiendo a lo expuesto, son finalidades de la presente Política las siguientes:

- Propiciar un uso de los Medios Tecnológicos orientado a atender las necesidades productivas garantizando la correcta prestación del servicio por parte del trabajador.

- Verificar el correcto cumplimiento de las obligaciones de los empleados y permitir que, en el caso de que se detecte que se han utilizado indebidamente la Organización pueda poner fin a las conductas prohibidas y exigir responsabilidades que resulten necesarias.

- Tratar de prevenir que los Medios Tecnológicos a los que se ha hecho referencia sean utilizados para incurrir en algún tipo de conducta prohibida (por ejemplo, revelar información confidencial, violar la normativa sobre protección de datos personales, actos de competencia desleal contra la Empresa, etc.).

2.- Reglas Generales de Uso de los Medios Tecnológicos

Con carácter general, los Medios Tecnológicos deben ser considerados herramientas de producción al servicio del negocio de **SeH**, por lo que el uso de éstos debe estar destinado al cumplimiento de las prestaciones para las que fue contratado el trabajador, debiendo utilizarse de forma adecuada a su naturaleza y a sus fines profesionales, sin que exista, por tanto, ninguna expectativa de intimidad o confidencialidad en su uso. En todo caso, queda prohibido el uso de los Medios Tecnológicos que suponga la violación del contrato que rija la relación laboral.

Debido a que los Medios Tecnológicos son herramientas de uso estrictamente profesional, los empleados no deberán transmitir, distribuir, almacenar, descargar, instalar, copiar, visualizar o enviar contenidos ajenos al desarrollo de la actividad profesional que efectúan en **SeH**.

Con relación a las obligaciones, prohibiciones y/o limitaciones sobre la facultad de control de **SeH** en el uso de los Medios Tecnológicos facilitados por ésta a los empleados para el cumplimiento de las prestaciones para las que fueron contratados, la Organización respetará y observará lo dispuesto en la normativa aplicable y vigente en cada momento.

3.- Reglas Específicas de Uso de los Medios Tecnológicos

A continuación, se recogen las reglas específicas relativas al uso de ciertos Medios Tecnológicos por parte de los empleados:

3.0. General

Con carácter general, el empleado deberá cuidar todos los equipos y herramientas tecnológicas de trabajo que se le faciliten, sus accesorios, carcasas y cajas que deberá conservar en todo momento y poner a disposición de la empresa si le fueran requeridos.

3.1. Equipos y *Software*

Los equipos (o *hardware*) son el conjunto de elementos físicos o materiales que componen un sistema de información, tales como ordenadores, impresoras, monitores, *PDAs*, tablets, , etc.

Los equipos, las aplicaciones y programas de los que **SeH** es propietaria o titular del derecho de uso serán contratados según los procedimientos internos vigentes en cada momento y teniendo en cuenta los estándares establecidos por la Empresa.

Por este motivo, en relación con la instalación y mantenimiento de los equipos, el trabajador no podrá realizar ningún cambio, manipulación o modificación sin la autorización expresa del Departamento de Informática. En este sentido, queda prohibida la instalación de cualquier elemento *hardware* adicional sin su previa autorización.

Con respecto a la instalación de *software*, cada equipo contendrá las aplicaciones y programas informáticos necesarios para facilitar la correcta prestación de servicios por parte del trabajador, por ello, este deberá justificar las peticiones de instalación de nuevo *software*, que ser aprobadas por el Departamento de Informática de la Empresa.

Queda prohibida, además de las conductas prohibidas con carácter general en la presente Política, la realización de las siguientes acciones:

- Instalar, sin autorización previa del Departamento de Informática cualquier programa o aplicación informática a iniciativa propia del empleado o profesional.

- Acceder y utilizar *software* no licenciado o “pirata” (conducta ilícita que puede conllevar graves responsabilidades de tipo penal y civil además de poner en riesgo evidente tanto los equipos informáticos como la información que contienen).

- Instalar en los equipos, certificados digitales, especialmente aquéllos que puedan utilizarse para representar a la entidad, sin previa autorización del Departamento de Informática de SeH.

- Queda estrictamente prohibida la instalación de cualquier tipo de programa P2P, o cualquier otra aplicación para el intercambio de archivos que saturen el ancho de banda de la conexión a Internet, impidiendo el acceso a los demás usuarios o entorpeciendo las conexiones a la red. Todo daño causado en los equipos informáticos, así como de los sistemas de información por la intrusión de virus informáticos o programas maliciosos que deriven de la utilización de programas de intercambio de archivos, será sancionado por la legislación vigente aplicable, así como por las sanciones impuestas por incumplimiento en la relación laboral o negocial.

3.2. Portátiles

A título enunciativo, se consideran dispositivos portátiles, los ordenadores portátiles, *PDAs*, teléfonos móviles, *smartphones*, tablets, CDs, DVDs, discos duros portátiles, memorias USB, tarjetas de memoria, etc.

Con carácter general, queda prohibida la utilización de *pen drives*, discos duros externos y otros medios de almacenamiento extraíbles

El trabajador deberá utilizar los mecanismos de seguridad que le facilite la entidad para evitar el robo o pérdida de los dispositivos y/o de la información que albergan y deberá cumplir con las instrucciones del fabricante, facilitadas al empleado o profesional por el Departamento de Informática de la Empresa.

En relación con los dispositivos portátiles, conviene señalar que su uso por los trabajadores única y exclusivamente para la prestación de los servicios contratados y siguiendo lo dispuesto en la presente política.

3.3. Correo Electrónico Corporativo

En relación con el uso del correo electrónico corporativo, cada empleado o profesional accederá únicamente a la dirección o direcciones que le hayan sido facilitadas por SeH. El uso correcto del servicio de correo electrónico supone que el empleado no debe utilizarlo para la comisión de cualquier ilícito contemplado en la normativa vigente, para las acciones prohibidas con carácter general en esta Política, ni para las que se muestran a continuación:

- Vulnerar las normas internas de Seguridad de la Información.
- Acceder o utilizar la cuenta de correo de otro empleado o profesional sin autorización.
- Suplantar -o intentar suplantar- a otros empleados o profesionales utilizando este medio.
- Simular la pertenencia a una compañía ajena a SeH.
- Iniciar o participar en la propagación de cartas encadenadas o acciones análogas.
- Utilizar buzones privados de correo ofrecidos por cualquier proveedor de Internet para fines profesionales relacionados con la entidad.

- Utilizar el correo electrónico como herramienta de comunicación con fines de venta u otros de naturaleza comercial independiente a la Organización y uso de cuentas no autorizadas por la empresa como Gmail o Hotmail, etc.).

- Enviar o solicitar mensajes, archivos o materiales con contenidos de carácter explícitamente sexual, de discriminación, que puedan llegar a ser ofensivos, difamatorios, amenazantes o insultantes para cualquier persona.

- Divulgar información corporativa de uso interno, confidencial o comercial de SeH. Con carácter general, no se permite a los profesionales redireccionar automáticamente los correos electrónicos recibidos en cuentas de correo corporativas a cuentas de correo no corporativas y viceversa. En el caso de que un profesional necesite redireccionar una cuenta de correo, deberá solicitar autorización motivada y por escrito al Departamento de Informática de SeH que se ocupará de ejecutar, si finalmente se aprueba, el redireccionamiento.

3.4. Internet

SeH facilita y permite a sus trabajadores el acceso a Internet para la correcta prestación de los servicios contratados. En este sentido, el empleado es responsable del material que visualice y descargue de Internet. Por tanto, debe realizar un uso responsable y lícito de la red desde cualquier Medio Tecnológico utilizado.

El acceso a Internet o a cualquier otra red de ordenadores se deberá realizar a través de las conexiones permitidas, habilitadas y configuradas por el Departamento de Informática de SeH. Cualquier otra conexión diferente pondrá en riesgo la seguridad de los sistemas de información de la Organización y, en este sentido, está terminantemente prohibida.

Queda prohibida la utilización de la red para navegar por sitios web de Internet para otros usos que no sean los permitidos para el desempeño de su actividad. Se reconoce la posibilidad de emplear diverso software para filtrar los accesos a los sitios web que a consideración del administrador de sistemas sean inapropiados para la entidad, o innecesarios para la actividad laboral.

La navegación por sitios web, el envío de mensajes, registros, altas, relleno de formularios y cualquier otra actividad realizada vía Internet, serán completa responsabilidad del usuario emisor y en todo caso deberá asumir las consecuencias que emanen de su actuación. Está estrictamente prohibido el acceso a páginas con contenidos ilícitos, material pornográfico, de contenido racista, sexual, o cualquier material que atente contra la dignidad de las personas o la propiedad intelectual.

Todo daño causado en los equipos informáticos, así como de los sistemas de información por la intrusión de virus informáticos o programas maliciosos que deriven

de la utilización de programas de intercambio de archivos, será sancionado por la legislación vigente aplicable, así como por las sanciones impuestas por incumplimiento en la relación laboral.

3.5. Medios Sociales

SeH es consciente de que el uso de medios sociales (tales como *blogs*, redes sociales, *wikis*, etc.) se presenta como una nueva oportunidad para la comunicación, la colaboración y la participación empresarial, y por ello anima a sus empleados a la participación en los mismos. No obstante, dicha participación, que nunca podrá llevarse a cabo utilizando los Medios Tecnológicos, implica una serie de responsabilidades por parte del empleado o profesional, que debe tener en cuenta cuando haga uso de dichos medios sociales.

El empelado deberá dejar claro que los puntos de vista expresados en los medios sociales son personales y nada tienen que ver con opiniones vertidas en nombre de **SeH**. Asimismo, el empleado no podrá manifestar o comentar hechos que comprometan el nombre, reputación, imagen y prestigio de **SeH**, de sus administradores y socios, ni tampoco el de otros profesionales o personal al servicio de la Empresa.

Así, cuando un empleado emita cualquier tipo de comentario u opinión acerca de cualquier tema o mencione a **SeH** en los perfiles de las cuentas en medios sociales de las que sea usuario, éste asumirá la responsabilidad que, en su caso, se pueda derivar de tal actuación, pudiendo la Empresa ejercitar cuantas acciones legales considere oportunas.

El empleado que utilice este tipo de medios sociales deberá guardar estricta confidencialidad acerca de los datos de los que disponga por su condición de empleado acerca de la Organización u otras empresas o personas, especialmente aquellos a los que se tenga acceso gracias a los equipos o Medios Tecnológicos proporcionados **SeH** para el desarrollo de las funciones laborales. Se encuentra prohibido divulgar toda clase de información económica, financiera, o de cualquier otra índole, obtenida a través de las herramientas puestas por parte de **SeH** a disposición de los empleados.

3.6. Canales Corporativos en Plataformas y Medios Sociales

El alta o registro por cualquiera de los trabajadores de **SeH** en cualquier medio social o plataforma titularidad de terceros (por ejemplo, canal en Youtube, Vimeo, cuenta en Twitter, Facebook, etc.) que implique el uso de la marca Segura e Hijos requerirá de la autorización previa y por escrito la Empresa.

En caso de incumplimiento de lo anterior, **SeH** se reserva el derecho a ejercitar cuantas acciones legales considere oportunas al efecto.

3.7. Acceso a través de la red

La utilización de las redes de datos corporativas deberá regirse por el uso correcto de los recursos que las componen, quedando expresamente prohibidas las siguientes actividades, además de las recogidas con carácter general en la presente Política:

- Destruir, alterar, inutilizar o dañar los datos, programas o documentos electrónicos de la entidad, sus empleados, o de terceros.

- Intentar acceder, leer, borrar, copiar o modificar los archivos de otros trabajadores sin el conocimiento y consentimiento de su autor, o en su caso, de la Empresa.

- Intentar acceder a áreas restringidas de los sistemas informáticos de la entidad, empleados o de terceros.

- Intentar acceder a páginas web o áreas cifradas, pertenecientes a la porción de Internet no indexada, que puedan poner en riesgo la seguridad de los sistemas y/o equipos informáticos de la Empresa.

- Introducir programas, virus, macros, controles o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los recursos informáticos.

- Causar daños de cualquier clase, a raíz de un uso negligente de los equipos informáticos, aplicaciones, herramientas informáticas y todo dispositivo o medio tecnológico.

- Obstaculizar voluntariamente el acceso de otros empleados o profesionales a los equipos y sistemas de la entidad por el consumo masivo de los recursos informáticos y telemáticos, así como realizar acciones que dañen, interrumpan o generen errores en dichos equipos y sistemas.

- Intentar aumentar el nivel de privilegios en el sistema.

- Introducir, reproducir o distribuir programas informáticos no autorizados expresamente por la Empresa, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros.

- Poner a disposición de terceros no autorizados los equipos y el software suministrados por la entidad. El empleado o profesional deberá usar los programas antivirus corporativos y sus actualizaciones, para prevenir que el material

descargado desde Internet o facilitado por un tercero pueda destruir o corromper los datos informáticos.

En relación con las conexiones remotas a la red de la entidad, solamente se realizarán a través de los medios destinados a tal fin, siendo éstos la única vía permitida de acceso, y siempre previa autorización del Departamento de Informático de **SeH**. Todos los equipos que pretendan conectarse de forma remota a la red de **SeH**, deberán tener implantados y correctamente actualizados los controles corporativos de detección, prevención y corrección de código malicioso o virus informático.

Cualquier conexión o intento de conexión por medios no autorizados se podrá catalogar como ataque o incidencia, con las respectivas consecuencias que recaen sobre el autor de ésta.

4.- Control del Uso adecuado de los Medios Tecnológicos

El quebrantamiento por parte de un empleado de cualquiera de las reglas establecidas en la presente Política puede generar daños muy importantes a los intereses y a la reputación de la Empresa.

Además, este hecho constituye a su vez un incumplimiento por parte del empleado de sus obligaciones legitimando a **SeH** para exigir al trabajador el cese inmediato en sus actuaciones y para adoptar cualquier otra medida que proceda, incluido el despido procedente, de conformidad a lo establecido en la normativa interna así como en la legislación vigente.

Por todo ello, con la finalidad última de vigilar y comprobar la aplicación por los de las reglas, medidas y recomendaciones de seguridad sobre los Medios Tecnológicos establecidas en esta Política, de poder sancionar o reclamar a aquéllos que incurran en conductas prohibidas, así como para poder acreditar ante los órganos judiciales u otras autoridades nacionales tanto la implantación de controles preventivos o la localización de tales conductas, como la realización de las mismas por los empleados o profesionales, la entidad podrá acceder y controlar todos los Medios Tecnológicos, siempre de conformidad con la Ley aplicable y vigente en cada momento.

Por los motivos expuestos, **SeH** podrá aplicar las siguientes medidas de control:

- Herramientas de control automatizadas para analizar y detectar los usos y comportamientos abusivos, indebidos o ilícitos por parte de los empleados cuando éstos traten información considerada como confidencial o sensible para la entidad. Esta monitorización se podrá realizar a través de cualquier software o sistema de

información que resulte idóneo para ello, incluyendo programas informáticos que permitan la captura de imágenes o visualización de la actividad llevada a cabo por el empleado en el Medio Tecnológico o, incluso, la posibilidad de llevar cabo el control remoto de dichos Medios Tecnológicos.

- Búsquedas automáticas de las conductas prohibidas en la presente Política, que podrán incluir controles tendentes a monitorizar la información procesada en los equipos y otros Medios Tecnológicos que hayan sido utilizados por los trabajadores.

- En el caso de que existan indicios razonables de que un empleado ha desatendido las previsiones de esta Política o ha incurrido en conductas prohibidas o en normas nacionales y vigentes en cada momento, **SeH** podrá, a través del departamento correspondiente, realizar accesos específicos a los Medios Tecnológicos utilizados por el empleado siempre y cuando se respeten las obligaciones, prohibiciones y/o limitaciones establecidas por la legislación vigente en cada momento.

5.- Procedimiento de acceso a Medios Tecnológicos

SeH podrá llevar a cabo la ejecución de las medidas de control sobre los empleados, establecidas en la presente Política, así como aquellas acciones necesarias para la continuidad del negocio. En este sentido, se podrán dar varias circunstancias para el acceso al correo de los empleados, por ejemplo:

- **En el supuesto de que un empleado no se encuentre físicamente en las instalaciones de la Organización y la continuidad del negocio requiera que sea necesario acceder a su cuenta de correo electrónico o sistema de información**. En este caso, **SeH** podrá autorizar, a través del Departamento de Informática, bien el redireccionamiento del buzón de correo del empleado a, o bien, el acceso exclusivamente durante el plazo de ausencia, a la dirección o direcciones de su correo electrónico o de cualquier otro sistema de información utilizado y de ser posible con la autorización previa y por escrito del empleado o profesional en cuestión. De manera previa al acceso, se recomienda realizar una copia de respaldo del buzón de correo.

- Cuando existan indicios suficientes de que un empleado ha incumplido las estipulaciones de la presente Política, y/o demás normativa interna existente y aprobada por **SeH**. En este caso, el Comité de Compliance notificará por escrito al Departamento de Informática, para acceder al buzón de correo del empleado o a cualquier otro sistema de información utilizado por el empleado, indicando: ***(i)*** que se trata de un posible incumplimiento de la Política o

normativa interna aprobada; ***(ii)*** que será necesario acceder al contenido del buzón de correo o del cualquier otro sistema de información que utilice, y si es posible delimitarlo, al existente entre dos fechas determinadas; ***(iii)*** si se considera necesario conservar evidencia electrónica del acceso y cuestiones que en su caso pudieran detectarse durante el proceso, por resultar conveniente su utilización en procedimientos judiciales posteriores, para actuar en consecuencia conforme a la normativa interna.

En función del caso, se podrá: ***(i)*** indicar al empleado el incumplimiento detectado de la Política e instarle a que deje de realizar las acciones infractoras; ***(ii)*** interrumpir la conexión a la red corporativa del empleado y/o su acceso al correo corporativo o sistema de información; ***(iii)*** solicitar/exigir al empleado la devolución del dispositivo a través del cual se haya producido el supuesto incumplimiento, con la finalidad de obtener pruebas que permitan acreditar la ejecución de acciones contrarias a la presente Política.

A través de la presente Política se informa de que toda la información que circula por la red, así como por el correo electrónico de las cuentas administradas por **SeH**, podrá ser monitorizada y sujeta a controles y reportes sobre su uso, en los que se puede contener información como: nombre de usuario, fecha de accesos, hora de accesos, bytes transferidos, almacenamiento de ficheros, acceso a los servidores, sitios visitados, tiempo de navegación por la red, etc.

6.- Consecuencias del Incumplimiento de la Presente Política

Para que la facultad de control del uso de Medios Tecnológicos asumida por la Empresa a través de la presente Política pueda ser considerada efectiva en la consecución de la finalidad perseguida, resulta preciso determinar las consecuencias que se derivarán del incumplimiento de las reglas, medidas y recomendaciones establecidas en esta Política por parte de los empleados o profesionales a los que se dirige la misma.

Cuando existan indicios suficientes o cuando se haya demostrado el incumplimiento real y efectivo de alguna de las estipulaciones contenidas en la Política, **SeH** estará legitimada para realizar alguna de las acciones que se enuncian a continuación:

- Podrá solicitar al empleado el cese definitivo de la actividad a través de la cual se haya producido el incumplimiento de la presente Política.

- **SeH** queda facultada para bloquear el acceso, interrumpir la conexión y recuperar los dispositivos, equipos y demás Medios Tecnológicos que se

hubieran utilizado o se estuvieran utilizando por los empleados para el desarrollo de su actividad laboral.

- **SeH** podrá adoptar todas aquellas medidas disciplinarias resulten de aplicación al caso concreto de que se trate, teniendo en cuenta el tipo de incumplimiento que se haya producido pudiendo constituir despido disciplinario, sin perjuicio de los daños y perjuicios irrogados como consecuencia de dicho incumplimiento.

- **SeH** facultada para iniciar todas las acciones legales que considere oportunas, de conformidad con la legislación nacional vigente, derivadas del incumplimiento por el empleado o profesional de la presente Política.

El conocimiento, observancia y respeto de la presente Política es vinculante para todos los empleados de la Organización, cuando de forma directa o indirecta, accedan o hagan uso de los Medios Tecnológicos facilitados por la Empresa.

Segura e Hijos
desde 1985

Avda. Tenerife, 16 – San Sebastián de los Reyes – 28703 Madrid – tel.: 91 652 39 00 – fax: 91 654 76 96 – e-mail: sanse@seguraehijos.es Camino de la Carrera ,10 –Fuente el Saz del Jarama – 28140 Madrid – tel.: 91 620 06 11 –fax: 91 620 06 36 – e-mail: fuentesaz@seguraehijos.es

www.seguraehijos.es

Madrid, xx de xxxxxxx de xxxxxx

Estimado Sr. xxxxxxxxxxxx

Por medio de este escrito, le comunicamos que la empresa pone a su disposición el material acordado, consistente en:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Como Ud. sabe, se trata de material de la empresa, que pone a su disposición para que Ud. pueda trabajar con más flexibilidad fuera de las oficinas de la empresa.

Por ello, Ud. deberá custodiarlo con especial diligencia y de acuerdo con la Política de Uso de Medios Tecnológicos que se acompaña como Anexo I al presente documento y que usted declara reconocer.

Atentamente;

SEGURA E HIJOS, S.A.

Recibí en XXXXXXX, a XX de XXXXXXXX de XXXX

XXXXXXXXXXXXXX

Política de Protección de Datos de Segura e Hijos, S.A.

POLÍTICA DE PROTECCIÓN DE DATOS CON CLIENTES DE SEGURA E HIJOS, S.A.

SEGURA E HIJOS, S.A. cumple, en el tratamiento de los datos de carácter personal de sus Clientes, con la legislación vigente en España y en la Unión Europea.

Para ello adopta las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos personales facilitados, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos.

A continuación, en cumplimiento de lo dispuesto en la normativa de protección de datos vigente, se le informa sobre los términos y condiciones del tratamiento de datos efectuado por **SEGURA E HIJOS, S.A.**

1. ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE SUS DATOS?

El responsable es y será la sociedad **SEGURA E HIJOS, S.A.** (en lo sucesivo, "*SEH"*), con CIF: A-78144524 y domicilio social Avenida Tenerife núm. 16, 28703, San Sebastián de los Reyes, Madrid Esta sociedad tiene por actividad el comercio al por mayor de madera, materiales de construcción y aparatos sanitarios.

2. ¿CON QUÉ FINALIDADES TRATAMOS SUS DATOS Y BAJO QUÉ LEGITIMACIÓN?

El tratamiento de sus datos persigue las siguientes finalidades:

Finalidad 1: Emisión de presupuestos y propuestas comerciales a potenciales clientes.

Con carácter previo a una relación contractual con cualquier cliente, SEH puede solicitar sus datos personales con el fin de poder elaborar y remitir una oferta o propuesta de servicios o un presupuesto.

Los datos personales que se recopilan a tales efectos son los datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) del potencial cliente para su incorporación a una base de datos de contactos de potenciales clientes.

Estos datos podrán ser archivados en formato físico y/o informático y entrarán a formar parte de una base de datos propiedad de SEH, en la que se incluye a todos los solicitantes de servicios que todavía no han formulado un encargo en firme a la Empresa.

Nuestro personal accede y consulta esa base de datos para elaborar ofertas, propuestas o presupuestos, enviarlos al potencial cliente por medios físicos o telemáticos y hacer seguimiento hasta la confirmación o rechazo por parte del potencial cliente.

Para la realización de este tipo de tratamientos, SEH solicita el consentimiento expreso, libre e informado del titular de los datos.

En caso de que el potencial cliente no acepte el presupuesto, la oferta o propuesta remitida y no se produzca finalmente una contratación con la Empresa, los datos serán tratados durante el tiempo imprescindible para el fin para el que fueron recopilados, de conformidad con el APARTADO 6.

Finalidad 2: Realización de las prestaciones propias de la compraventa y/o suministro de productos.

Con motivo de ´la relación jurídica entre SEH y cualquier cliente, es necesario que la empresa desarrolle diferentes tratamientos de datos

- La recopilación y el archivo físico y electrónico de sus datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) para su incorporación a una base de datos de contactos, que podrá incluir categorías por clientes.

- La consulta de los datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) almacenados para el envío de comunicaciones relacionadas con el curso de la relación contractual o para el intercambio de documentación.

- La consulta de los datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) almacenados para la emisión y envío de facturas y otros documentos económicos vinculados la relación contractual con el Cliente.

- El intercambio físico y/o telemático de información y documentación con terceros profesionales vinculados a la prestación del servicio (v.g. transportistas).

Para la realización de estos tratamientos, SEH se basa en la existencia de una relación contractual con el Cliente, de tal forma que no recabará consentimiento. No obstante, informa debidamente al Cliente de su Política de Protección de Datos a través de su página web y en todas las comunicaciones dirigidas a él que, por su naturaleza, así lo exijan.

Finalidad 3: Envío de publicidad sobre nuevos productos y promociones de la Empresa.

Dentro de esta finalidad se engloba el uso de los datos personales de clientes potenciales, clientes actuales y antiguos clientes para enviarles comunicaciones comerciales relacionadas con nuevos productos o servicios que pudieran ser de su interés.

La información comercial puede ser remitida por cualquier canal (mensajes de texto, correos electrónicos, llamadas telefónicas, correo postal…) y puede ser genérica o personalizada.

Para la realización de este tipo de tratamiento, SEH recaba previamente el consentimiento expreso, libre, informado de los

titulares de datos personales a los que pretenda remitir comunicaciones comerciales.

En cualquier momento se permite al titular de los datos y destinatario de las comunicaciones comerciales oponerse al envío de nuevas comunicaciones. El interesado puede hacer uso de este derecho por correo postal a la dirección arriba expuesta.

Finalidad 4: Desarrollo de acciones comerciales sobre productos y servicios ofrecidos por terceras empresas dedicadas a la producción y/o venta de material de construcción.

En caso de que preste su consentimiento, SEH podrá desarrollar acciones comerciales con el objetivo de hacerle llegar, por cualquier canal, ofertas y promociones de terceras empresas dedicadas a la producción y/o venta de materiales de construcción o del sector inmobiliario.

De nuevo, en cualquier momento se permite al titular de los datos y destinatario de las comunicaciones comerciales oponerse al envío de nuevas comunicaciones. El interesado puede hacer uso de este derecho por correo postal a la dirección arriba expuesta o en la dirección datospersonales@seguraehijos.es.

Finalidad 5: Gestión de financiación de las compras con entidades financieras.

Previo consentimiento por su parte, intercambio de los datos identificativos, de contacto, económicos y de compras del Cliente con AVANCA u otra entidad financiera para que el Cliente pueda financiar el importe de su compra.

Finalidad 6: Conservar los datos una vez finalizado el contrato

SEH conserva sus datos una vez finalizado el contrato, por un plazo máximo de diez (10) años con el objetivo de poder responder de cualquier reclamación de índole civil, administrativo y penal que pudiera derivarse de la relación jurídica mantenida con el Cliente, así como para el cumplimiento de las obligaciones legales que nos resultan de aplicación por la normativa vigente en materia fiscal, de prevención de blanqueo de capitales y penal.

Para la realización de este tipo de tratamiento, la Empresa no recaba ningún tipo de consentimiento, habida cuenta de la existencia de un interés legítimo en el mejor ejercicio de su derecho de defensa ante cualquier tipo de reclamación, así como la existencia de obligaciones legales de carácter fiscal, sociolaboral y de prevención de blanqueo de capitales.

Finalidad 7: Funcionamiento de página web
Aunque en estos momentos no dispone de ella, SEH podrá a disposición de potenciales clientes, clientes actuales y antiguos clientes una página web con el objetivo de poder ofrecerles información sobre los servicios y productos que la Empresa ofrece en el mercado y facilitarles la comunicación con nosotros.

Para el correcto funcionamiento de la página web, la empresa recabará información anónima sobre los visitantes (véase APARTADO 3):

El usuario debe ser consciente de que el contenido distribuido a través de las funciones de compartir y de las integraciones con terceros puede llevar a que se muestre una parte de su información personal fuera del sitio web. Por ejemplo, cuando se comparten contenidos, comentarios o votaciones en redes sociales (Facebook, Google+ o Twitter). Esta información no quedará almacenada en el sitio web y por ello, SEH no puede ser responsable de la información que el usuario revelar a través de estas vías.

Para la realización de estos tratamientos, recabará el consentimiento expreso, libre e informado la primera vez que el usuario acceda a la página web.

Finalidad 8: Gestión de perfiles en redes sociales

SEH podrá utilizar las direcciones de correo electrónico y números de teléfono de sus potenciales clientes, clientes actuales y antiguos clientes como criterios de búsqueda de posibles contactos en redes sociales en los que la Empresa tiene perfil corporativo.

El uso de esos datos no constituye una comunicación de datos a las empresas que gestionan dichas redes sociales, pues éstas no almacenan los datos.

Para este tipo de tratamiento, SEH recaba el consentimiento expreso, libre e informado de los titulares de los datos personales que van a ser utilizados.

Finalidad 9: Cámaras de seguridad

SEH utiliza cámaras de video que recogen y graban imágenes en el interior de sus instalaciones con el único objetivo de mantener un control sobre el estado a las instalaciones de la Empresa y el acceso a éstas por parte de personal ajenas a su personal.

Para la realización de este tratamiento, SEH no recaba consentimiento expreso de los titulares de los datos recopilados, pues existe un interés legítimo en establecer medidas de seguridad en el interés de sus instalaciones. No obstante, informa debidamente a cualquier persona que acceda a sus instalaciones de su Política de Protección de Datos a través de carteles informativos situados al lado de las cámaras.

Finalidad 10: Comunicar los datos de impago de la deuda a sistemas comunes de información crediticia

En caso de no atender puntualmente a sus obligaciones económicas frente a SEH y resultando de ello una deuda cierta, vencida y exigible y previo requerimiento previo de pago se procederá a la comunicación de sus datos identificativos y los datos relativos a la deuda pendiente de pago a las entidades responsables de sistemas comunes de información crediticia (p.ej., BADEXGUG, ASNEF, Fichero de Incidencias Judiciales, etc.), de acuerdo con la legislación vigente.

3. ¿QUÉ TIPO DE DATOS TRATAMOS?

Para las finalidades expuestas en el apartado anterior se trata el conjunto de datos del cliente que podemos dividir en las siguientes fuentes y categorías:

a) Datos proporcionados de forma directa por el cliente:

Datos proporcionados de forma directa por el cliente, ya sea en el momento de solicitud del servicio a través de la cumplimentación de los formularios a tal efecto habilitados como los facilitados a lo largo de la relación contractual a través de distintos medios como, por ejemplo, correos electrónicos, SMS, etc. El Cliente se responsabiliza de su veracidad y actualización.

b) Datos obtenidos de otras fuentes distintas del propio cliente:

Datos obtenidos de fuentes distintas del cliente, ya sea por contar con su consentimiento o por cualquier otra habilitación legal (interés legítimo, cumplimiento de una obligación legal…). Estas fuentes son:

- Fuentes accesibles al público.
- Organismos de la Administración Pública (p.ej., Tesorería General de la Seguridad Social (TGSS), Agencia Estatal de Administración Tributaria (AEAT), etc.) o Judicial.
- Sistemas comunes de información crediticia (p.ej., BADEXGUG, ASNEF, Fichero de Incidencias Judiciales, etc.).
- Ficheros de protección de identidad o detección fraudulenta de datos.
- Información proporcionada por otras empresas de servicios jurídicos en procesos de sustitución, previa concesión de venia.
- Información proporcionada por órganos administrativos y judiciales con motivo de desarrollo de encargos consistentes en la representación del Cliente.

c) Datos derivados del desarrollo de la relación:

Datos proporcionados de forma indirecta por el Cliente al derivar de la propia relación jurídica existente entre él y SEH.

Dentro de esta categoría se incluyen el histórico de pagos o de productos contratados, los datos de navegación

d) Datos obtenidos a través de nuestra página web:

A.- Datos de Navegación anónima a través de las páginas web.

SEH recaba información anónima acerca de los visitantes de la página, lo que significa que dicha información no puede ser asociada a un usuario concreto e identificado.

Los datos que se conservan son:

1. El nombre de dominio del proveedor (ISP) que les da acceso a la red. Por ejemplo, un usuario del proveedor XXX sólo estará identificado con el dominio xxx.es. De esta manera, podemos elaborar estadísticas sobre los países y servidores que visitan más a menudo nuestra web.

2. La fecha y hora de acceso a nuestra web. Ello nos permite averiguar las horas de mayor afluencia, y hacer los ajustes precisos para evitar problemas de acceso.

3. El número de visitantes diarios de cada sección. Ello nos permite conocer las áreas de mayor interés y aumentar y mejorar su contenido, con el fin de que los usuarios obtengan un resultado más satisfactorio.

B.- Uso de IP´s Black List

Adicionalmente y con el objetivo de proteger a los usuarios de la página web de malas prácticas existentes en internet (spam, robots, etc.) también recibimos la dirección del protocolo de Internet ("IP") de tu ordenador o el servidor proxy que utilizas para acceder a la red y se coteja con "listas negras" de IPs gestionadas por servicios especializados, como por ejemplo Honeypot. En caso de que tu dirección IP esté incluida en dichas listas, no podrás acceder a los servicios que proporciona nuestra web.

Esta información es tratada de manera anónima, sin asociarla a un usuario concreto e identificado, de manera que, si tu IP es rechazada, puedes acceder al servicio cambiando de IP.

La dirección IP no se almacena una vez realizadas estas comprobaciones.

D.- Información proporcionada a través del formulario de contacto.

Datos proporcionados de forma directa por el usuario de la página web al cumplimentar el formulario de contacto. El usuario se responsabiliza de su veracidad y actualización.

e) Datos obtenidos a través de las cámaras de seguridad.

Las cámaras recogen imágenes de las personas que acceden a las instalaciones de la Empresa.

4. ¿A QUIÉN COMUNICAMOS SUS DATOS?

Los datos personales tratados por SEH para alcanzar las finalidades detalladas anteriormente podrán ser comunicados, entre otros, a los siguientes destinatarios en función de la base legitimadora de la comunicación.

En virtud de lo anterior, en el siguiente cuadro se detallan las comunicaciones previstas y la base legitimadora que la ampara:

DESTINATARIO	TIPO DE DATOS	HABILITACIÓN

	COMUNICADOS	LEGAL
Empresas subcontratadas por SEH para la ejecución de la relación jurídica	Datos identificativos y de contacto	Desarrollo de la relación contractual
Otras empresas del sector de la producción y venta de material constructivo y del sector inmobiliario	Datos identificativos y de contacto	Consentimiento
Agencia Tributaria / SEPBLAC	Datos de carácter identificativo e histórico de pagos/abonos.	Cumplimiento obligación legal.
AVANCA u otras entidades financieras	Datos identificativos, de contacto, económicos, contenido de la compra.	Consentimiento
Diseñadores de interiores externos	Datos identificativos y de contacto	Consentimiento
Empresas externas que puedan desarrollar proyectos de obras con productos o materiales adquiridos a SeH	Datos identificativos y de contacto	Consentimiento

5. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES.

SEH le informa de que no realiza transferencias internacionales con sus datos personales.

6. ¿POR CUÁNTO TIEMPO CONSERVAREMOS SUS DATOS?

Los datos personales recopilados de clientes potenciales se conservarán el tiempo imprescindible para cumplir con la finalidad con que fueron obtenidos.

En caso de que el potencial cliente no contrate finalmente con SEH, sus datos serán conservados durante un (1) año, con el objetivo de que la Empresa pueda realizar un análisis sobre el perfil de aquellos clientes que rechazan las ofertas o presupuestos que se les remiten. Finalizado ese periodo, los datos personales serán destruidos.

Finalizado ese periodo de tratamiento de un (1) año, los datos serán conservados durante el periodo que la normativa nacional establezca para la prescripción de infracciones administrativas en materia de protección de datos personales.

Transcurrido ese periodo de prescripción, SEH cancelará sus datos personales. No obstante, previo consentimiento del titular, podrán conservarse con carácter indefinido los datos identificativos y de contacto para el envío de comunicaciones comerciales.

Los datos personales de los clientes serán conservados mientras se mantenga la relación contractual con el cliente y con posterioridad a la misma, durante un periodo de diez (10) años para la cobertura de las responsabilidades civiles derivadas de la prestación del servicio y el cumplimiento de las obligaciones legales en materia fiscal, de prevención de blanqueo de capitales y penal.

Durante ese periodo, previo consentimiento del titular, los datos podrán utilizarse por SEH para el envío de comunicaciones comerciales.

En cualquier caso, si al finalizar la relación contractual existieran litigios pendientes derivados del ejercicio de acciones de impugnación de las facturas emitidas por SEH o tendentes a lograr el cobro de éstas, los datos podrán conservarse durante la tramitación de éstos, en tanto no recaiga resolución definitiva –fecha en la que se procederá a su bloqueo y posterior borrado-, si bien sólo podrán utilizarse a fines probatorios.

Finalizado ese periodo de tratamiento de diez (10) años, los datos serán conservados durante el periodo que la normativa nacional establezca para la prescripción de infracciones administrativas en materia de protección de datos personales.

Transcurrido ese periodo de prescripción, SEH cancelará sus datos personales. No obstante, previo consentimiento del titular, podrán conservarse con carácter indefinido los datos identificativos y de contacto para el envío de comunicaciones comerciales.

En lo que respecta a imágenes recogidas por nuestras cámaras de videovigilancia, dichas imágenes se borrarán automáticamente en el plazo de un (1) mes desde que fueran almacenadas, salvo que tuvieran que ser conservados por un plazo mayor para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

7. ¿CUÁLES SON SUS DERECHOS?

La normativa de protección de datos le confiere una serie de derechos en relación con el tratamiento de datos que implican nuestros servicios que podemos resumir en los siguientes:

- Derecho de acceso: Conocer qué tipo de datos estamos tratando y las características del tratamiento que estamos llevando a cabo.

- Derecho de rectificación: Poder solicitar la modificación de sus datos por ser éstos inexactos o no veraces.

- Derecho de portabilidad: Poder obtener una copia en un formato interoperable de los datos que estén siendo tratados.

• Derecho a la limitación del tratamiento en los casos recogidos en la Ley.

• Derecho de supresión: Solicitar la supresión de sus datos cuando el tratamiento ya no resulte necesario.

• Derecho de oposición: Solicitar el cese en el envío de comunicaciones comerciales en los términos antes señalados.

• Derecho a revocar el consentimiento prestado, siendo su petición procesada en el plazo aproximado de 10 días.

• Derecho a interponer una reclamación frente a la autoridad de control (en España la AEPD).

Puede ejercitar sus derechos mediante correo postal a la dirección Avenida Tenerife núm. 16, 28703, San Sebastián de los Reyes, Madrid o en la dirección protecciondatos@seguraehijos.es indicando el derecho a ejercitar y acompañando la documentación requerida.

En la página web de la AEPD puede encontrar una serie de modelos que le ayudarán en el ejercicio de sus derechos.

POLÍTICA DE PROTECCIÓN DE DATOS CON TRABAJADORES DE SEGURA E HIJOS, S.A.

SEGURA E HIJOS, S.A. cumple, en el tratamiento de los datos de carácter personal de sus trabajadores, con la legislación vigente en España y en la Unión Europea.

Para ello adopta las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos personales facilitados, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos.

A continuación, en cumplimiento de lo dispuesto en la normativa de protección de datos vigente, se le informa sobre los términos y condiciones del tratamiento de datos efectuado por SeH.

1. ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE SUS DATOS?

El responsable es y será la sociedad SEGURA E HIJOS, S.A. (en lo sucesivo, "SEH"), con CIF: A-78144524 y domicilio social en Avenida Tenerife núm. 16, 28703, San Sebastián de los Reyes, Madrid. Esta sociedad tiene por actividad el comercio al por mayor de madera, materiales de construcción y aparatos sanitarios.

2. ¿CON QUÉ FINALIDADES TRATAMOS SUS DATOS Y BAJO QUÉ LEGITIMACIÓN?

El tratamiento de sus datos persigue las siguientes finalidades:

Finalidad 1: Selección de candidatos para puestos de trabajo en la empresa

Con carácter previo a una relación contractual con cualquier trabajador, SeH puede solicitar sus datos personales con el fin de poder considerar su candidatura para la provisión de un puesto de trabajo.

Los datos que se recopilan a tales efectos son los datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) del candidato.

Estos datos podrán ser archivados en formato físico y/o informático y entrarán a formar parte de una base de datos propiedad de SeH en la que se incluye a todos los candidatos que todavía no son trabajadores de la Empresa.

Nuestro personal accede y consulta esa base de datos hacer seguimiento del candidato.

Para la realización de este tipo de tratamientos, SeH solicitará el consentimiento expreso, libre e informado del titular de los datos.

En caso de que el candidato no se transforme en trabajador de la Empresa, los datos serán tratados durante el tiempo imprescindible para el fin para el que fueron recopilados, de conformidad con el APARTADO 6.

Finalidad 2: Realización de la relación laboral.

Con motivo de ´la relación jurídica entre SeH y cualquier trabajador, es necesario que la empresa desarrolle diferentes tratamientos de datos. Entre otros:

- La recopilación y el archivo físico y electrónico de sus datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) para su incorporación a una base de datos de trabajadores.
- La consulta de los datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) almacenados para el envío de comunicaciones relacionadas con el curso de la relación contractual.
- La formalización de altas y bajas ante la Seguridad Social.
- La emisión y abono de nóminas, así como la autoliquidación de las cotizaciones ante la Seguridad Social y de las retenciones en concepto de IRPF ante la Agencia Tributaria.
- La consulta de los datos identificativos (nombre, apellidos y DNI) y de contacto (teléfono, fax, correo electrónico, etc.) almacenados para la emisión y envío de nóminas y otros documentos económicos vinculados la relación contractual con el Trabajador.
- La consulta de los datos identificativos del trabajador para la gestión de su formación con entidades externas que organizar/imparten formación.
- La consulta de los datos identificativos del trabajador para la gestión de la prevención de riesgos laborales con entidades externas que organizar/imparten formación.

Finalidad 3: Conservar los datos una vez finalizado el contrato

SeH conserva sus datos una vez finalizado el contrato, por un plazo

máximo de diez (10) años con el objetivo de poder responder de cualquier reclamación de índole civil, administrativo y penal que pudiera derivarse de la relación jurídica mantenida con el Trabajador, así como para el cumplimiento de las obligaciones legales que nos resultan de aplicación por la normativa vigente en materia fiscal, de prevención de blanqueo de capitales y penal.

Para la realización de este tipo de tratamiento, la Empresa no recaba ningún tipo de consentimiento, habida cuenta de la existencia de un interés legítimo en el mejor ejercicio de su derecho de defensa ante cualquier tipo de reclamación, así como la existencia de obligaciones legales de carácter fiscal, sociolaboral y de prevención de blanqueo de capitales.

Finalidad 4. Cámaras de seguridad

SeH utiliza cámaras de video que recogen y graban imágenes en el interior de sus instalaciones con el único objetivo de mantener un control sobre el estado a las instalaciones de la Empresa y el acceso a éstas por parte de personal ajenas a su personal.

Para la realización de este tratamiento, SeH no recaba consentimiento expreso de los titulares de los datos recopilados, pues existe un interés legítimo en establecer medidas de seguridad en el interés de sus instalaciones. No obstante, informa debidamente a cualquier persona que acceda a sus instalaciones de su Política de Protección de Datos a través de carteles informativos situados al lado de las cámaras.

3. ¿QUÉ TIPO DE DATOS TRATAMOS?

Para las finalidades expuestas en el apartado anterior se trata el conjunto de datos del trabajador que podemos dividir en las siguientes fuentes y categorías:

a) Datos proporcionados de forma directa por el trabajador:

Datos proporcionados de forma directa por el trabajador, ya sea en el momento de iniciarse los contactos con la empresa, a través de la cumplimentación de los formularios a tal efecto habilitados como los facilitados a lo largo de la relación contractual a través de distintos medios como, por ejemplo, correos electrónicos, SMS, etc. El Trabajador se responsabiliza de su veracidad y actualización.

b) Datos obtenidos de otras fuentes distintas del propio Trabajador:

Datos obtenidos de fuentes distintas del Trabajador, ya sea por contar con su consentimiento o por cualquier otra habilitación legal (interés legítimo, cumplimiento de una obligación legal…). Estas fuentes son:

- Fuentes accesibles al público.
- Organismos de la Administración Pública (p.ej., Tesorería General de la Seguridad Social (TGSS), Agencia Estatal de Administración Tributaria (AEAT), etc.) o Judicial.
- Sistemas comunes de información crediticia (p.ej., BADEXGUG, ASNEF, Fichero de Incidencias Judiciales, etc.).
- Ficheros de protección de identidad o detección fraudulenta de datos.
- Información proporcionada por otras empresas de servicios jurídicos en procesos de sustitución, previa concesión de venia.
- Información proporcionada por órganos administrativos y judiciales con motivo de desarrollo de encargos consistentes en la representación del Cliente.

c) Datos derivados del desarrollo de la relación:

Datos proporcionados de forma indirecta por el Trabajador al derivar de la propia relación jurídica existente entre él y SeH.

d) Datos obtenidos a través de las cámaras de seguridad.

Las cámaras recogen imágenes de las personas que acceden a las instalaciones de la Empresa.

4. ¿A QUIÉN COMUNICAMOS SUS DATOS?

Los datos personales tratados por SeH para alcanzar las finalidades detalladas anteriormente podrán ser comunicados, entre otros, a los siguientes destinatarios en función de la base legitimadora de la comunicación.

DESTINATARIO	TIPO DE DATOS COMUNICADOS	HABILITACIÓN LEGAL
Agencia Tributaria y Seguridad Social	Datos de carácter identificativo e histórico de pagos/abonos, nóminas, seguros sociales, etc.	Cumplimiento obligación legal.

5. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES.

SeH informa de que no realiza transferencias internacionales con sus datos personales.

6. ¿POR CUÁNTO TIEMPO CONSERVAREMOS SUS DATOS?

Los datos personales recopilados de candidatos se conservarán el tiempo imprescindible para cumplir con la finalidad con que fueron obtenidos.

En caso de que el candidato no se transforme en trabajador de la Empresa, sus datos serán conservados durante un (1) año, con el objetivo de que la Empresa pueda realizar un análisis sobre el perfil de aquellos candidatos que finalmente son rechazados por SeH o que rechazan las ofertas de trabajo que les hace la Empresa.

Finalizado ese periodo de tratamiento de un (1) año, los datos serán conservados durante el periodo que la normativa nacional establezca para la prescripción de infracciones administrativas en materia de protección de datos personales.

Transcurrido ese periodo de prescripción, SeH cancelará sus datos personales.

Los datos personales de los trabajadores serán conservados mientras se mantenga la relación contractual con el trabajador y con posterioridad a la misma, durante un periodo de diez (10) años para la cobertura de las responsabilidades civiles derivadas de la prestación del servicio y el cumplimiento de las obligaciones legales en materia fiscal, de prevención de blanqueo de capitales y penal.

En cualquier caso, si al finalizar la relación contractual existieran litigios pendientes entre el trabajador e SeH, en tanto no recaiga resolución definitiva –fecha en la que se procederá a su bloqueo y posterior borrado-, si bien sólo podrán utilizarse a fines probatorios.

Finalizado ese periodo de tratamiento de diez (10) años, los datos serán conservados durante el periodo que la normativa nacional establezca para la prescripción de infracciones administrativas en materia de protección de datos personales.

Transcurrido ese periodo de prescripción, SeH cancelará sus datos personales.

En lo que respecta a imágenes recogidas por nuestras cámaras de videovigilancia, dichas imágenes se borrarán automáticamente en el plazo de un (1) mes desde que fueran almacenadas, salvo que tuvieran que ser conservados por un plazo mayor para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

7. ¿CUÁLES SON SUS DERECHOS?

La normativa de protección de datos le confiere una serie de derechos en relación con el tratamiento de datos que implican nuestros servicios que podemos resumir en los siguientes:

- Derecho de acceso: Conocer qué tipo de datos estamos tratando y las características del tratamiento que estamos llevando a cabo.
- Derecho de rectificación: Poder solicitar la modificación de sus datos por ser éstos inexactos o no veraces.
- Derecho de portabilidad: Poder obtener una copia en un formato interoperable de los datos que estén siendo tratados.
- Derecho a la limitación del tratamiento en los casos recogidos en la Ley.
- Derecho de supresión: Solicitar la supresión de sus datos cuando el tratamiento ya no resulte necesario.
- Derecho de oposición: Solicitar el cese en el envío de comunicaciones comerciales en los términos antes señalados.
- Derecho a revocar el consentimiento prestado, siendo su petición procesada en el plazo aproximado de 10 días.
- Derecho a interponer una reclamación frente a la autoridad de control (en España la AEPD).

Puede ejercitar sus derechos mediante correo postal a la dirección Avenida Tenerife núm. 16, 28703, San Sebastián de los Reyes, Madrid o mediante correo electrónico a la dirección datospersonales@seguraehijos.es indicando el derecho a ejercitar y acompañando la documentación requerida.

En la página web de la AEPD puede encontrar una serie de modelos que le ayudarán en el ejercicio de sus derechos.

PROTOCOLO CONTROL VEHÍCULOS

El usuario de cualquier vehículo destinado al transporte de personas o mercancías que sea titularidad de la Sociedad deberá cumplimentar diariamente al inicio y a la finalización de la jornada laboral un parte de incidencias sobre el estado y contenido del vehículo conforme al modelo Anexo I.

Adicionalmente y cuando se trate de vehículos de uso exclusivo por un solo usuario, éste firmará el documento de recepción de vehículo (Anexo II) aceptando la Política de Uso de Vehículos de la Empresa (Anexo III).

Segura e Hijos
MATERIALES DE CONSTRUCCIÓN

MATERIALES DE CONSTRUCCION
PAVIMENTOS Y REVESTIMIENTOS

Parte de trabajo Día [redacted]

Camión [redacted]

San Sebastián de los Reyes [redacted]

MATERIALES SERVIDOS

Cantidad	Clase de Materiales	Procedencia	Destino
[redacted]			

Incidencias detectadas en el vehículo al inicio de la jornada de trabajo:

(Estado anormal del vehículo, contenido imprevisto o inapropiado en la cabina o en el espacio de carga)

Firma_____

Hora_____

Nombre_____

Incidencias detectadas en el vehículo al finalizar la jornada de trabajo:
(Estado anormal del vehículo, contenido imprevisto o inapropiado en la cabina o en el espacio de carga)

Firma_____

Hora_____

Nombre_____

ENTREGA DE VEHÍCULO DE EMPRESA DE SEGURA E HIJOS, SA.

(A rellenar por el trabajador)

D/Dª_____, con DNI _____ y domicilio en _____, como trabajador de Segura e Hijos, S.A. recibo en el día de hoy

(A rellenar por la Empresa)

El vehículo _____ *(MARCA)*, _____ *(Modelo)*, matrícula _____.

Dicho vehículo se entrega con naturaleza _____ *(funcional o permanente, de acuerdo con la Política)*.

En el momento de la entrega del vehículo, el Trabajador reconoce que le hace entrega de copia de la Política de Uso de Vehículos de la Empresa, que declara conocer y de cuyo contenido he sido debidamente informado.

En cumplimiento de lo establecido en el Reglamento General de Protección de Datos (RGPD) se pone en conocimiento del Trabajador que, con motivo del presente documento, sus datos personales serán objeto de tratamiento bajo las siguientes condiciones:

INFORMACIÓN BÁSICA RGPD	
1. Responsable del tratamiento	Segura e Hijos, S.A.
2. Finalidad del tratamiento	Ejecución de la relación laboral
3. Legitimación	Existencia de una relación jurídica
4. Destinatarios	No se prevén cesiones de datos a terceros, salvo en cumplimento de una obligación legal.
5. Derechos	Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
6. Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en www.seguraehijos.es/protecciondedatos.

En San Sebastián de los Reyes, a ____ de _____ de 20___

Firma del trabajador

Firma de la empresa

POLITICA DE USO DE VEHICULOS CORPORATIVOS
TITULO: USO DE VEHICULOS CORPORATIVOS

INDICE DE CONTENIDOS

1.- PROPOSITO

Los principales objetivos de este procedimiento son establecer una adecuada política para el uso, manejo y administración de los vehículos de la compañía, asignados al personal con relación a su cargo dentro de la organización o en virtud de sus funciones dentro de la empresa, donde se busca el correcto manejo y cuidado de los mismos según los parámetros establecidos en la presente política: responsabilidades, límites en su uso, cuidado y manejo en caso de daños o accidentes.

2.- ALCANCE

Esta política aplica para todos los colaboradores que trabajan para Segura e Hijos, S.A. y que en virtud de su cargo o con ocasión de sus labores y funciones, les sean asignados de manera total o parcial el uso de vehículos corporativos.

3.- RESPONSABLES

Todo el personal que le sean asignados vehículos de la empresa o que en virtud de sus funciones, cargos o actividades dentro de la compañía manipulen, conduzcan o utilicen de cualquier manera el parque automotor de Segura e Hijos, S.A.

4.- OBJETIVOS

- Definir políticas que regirán el uso, cuidado y parámetros generales de tenencia por parte del personal, con relación a los vehículos de la compañía.

- Asegurar la integridad y responsabilidad en el uso o manejo de los vehículos de la empresa designados para el uso del personal.

- Informar a todos los colaboradores objeto del alcance de esta política, de las directrices de la compañía con relación al uso de estos recursos físicos de la misma.

5.- DISPOSICIONES GENERALES

- Bajo ninguna circunstancia el vehículo podrá ser prestado a una persona ajena a la empresa.

- Será obligatoria para la utilización de cualquier vehículo disponer del carnet vigente necesario para cada categoría de vehículo. Sin dicho permiso en vigor el usuario NO podrá conducir ningún vehículo de la empresa.

- Sólo se podrá prestar el vehículo de uso permanente a una persona de la empresa, con la autorización del nivel Directivo o Gerencial.

- Los casos especiales serán tratados por la Dirección de Recursos Humanos de la empresa junto con los demás niveles directivos que correspondan.

6.- PÓLITICA DE USO DE VEHÍCULOS DE USO FUNCIONAL:

6.1 Para el uso de un vehículo de uso funcional dentro de la empresa, el trabajador deberá tener experiencia en manejo de ese tipo de vehículos y tener su carnet de conducir vigente.

6.2 La asignación de un vehículo de uso funcional significa que el trabajador tendrá la responsabilidad de mantener en adecuadas condiciones de higiene el mismo y deberá cuidar del mantenimiento preventivo de forma permanente.

6.3 El uso del cinturón de seguridad y el acatamiento de las normas de circulación vigentes es obligatorio. Si el trabajador es multado por la falta de uso del cinturón o por violación de las normas de circulación, será su responsabilidad pagar la multa y se le podrá suspender el uso del vehículo.

6.4 El uso del teléfono móvil está prohibido mientras se está conduciendo. Si el empleado es multado por el uso del teléfono móvil mientras conduce, será su responsabilidad pagar la multa y se le podrá suspender el uso del vehículo.

6.5 El consumo de bebidas embriagantes o con alcohol están prohibidas en horas laborables y mientras se conduce el vehículo. Si el empleado es multado por dicha conducta, será su responsabilidad pagar la multa y se le podrá suspender el uso del vehículo.

6.6 El incumplimiento de las condiciones descritas en los puntos anteriores, además del pago de las sanciones administrativas impuestas, así como la remoción del vehículo de uso funcional para el desarrollo de sus labores; podrá según el caso y a consideración del área de Recursos Humanos, significar el inicio de un procedimiento disciplinario, el cual después de agotar las etapas del debido proceso podrá dar lugar a sanciones disciplinarias e incluso a la terminación del contrato de trabajo con justa causa.

6.7 El uso de estos vehículos de uso funcional, estará limitado exclusivamente al desarrollo de las funciones propias del área o en actividades inherentes a la empresa o su personal, por ende, el uso de los mismos será solo dentro de los horarios, destinos o distancias determinados por la empresa dentro de sus cronogramas de actividades previamente validados y autorizados por los responsables.

6.8 Por lo cual todos los vehículos de uso funcional de la compañía, deberán ser retornados a las instalaciones de la empresa o el lugar designado por esta, estando prohibido el uso de carácter personal o el resguardo en sitios diferentes sin previa autorización expresa de la compañía dentro de sus niveles directivos.

7.- PÓLITICA DE USO DE AUTOMOVILES DE USO PERMANENTE:

7.1 Tienen derecho al uso de vehículos de uso permanente los cargos: Directivos o Gerenciales determinados por los Directores o Gerentes del proyecto, así como otras personas que específicamente pueda designar la Dirección.

7.2 Las mismas políticas de los puntos 6.2 al 6.7 del capítulo anterior, se aplican a los vehículos de uso permanentes.

7.3 El criterio de asignación del vehículo de uso particular, estará relacionado con el nivel del cargo dentro de la organización, así como el desarrollo de funciones de especial relevancia que impliquen el reconocimiento de este beneficio.

7.4 Los trabajadores que sean beneficiarios de esta asignación de vehículo de uso permanente deberán establecer las medidas de cuidado, uso racional y economía a favor de los intereses de Segura e Hijos, S.A.

7.5 Teniendo en cuenta que este tipo de asignación de vehículo de uso permanente, implica un manejo libre del mismo en días hábiles como no hábiles, para uso

institucional y personal, se deberá velar por el trabajador que el resguardo del mismo fuera de las instalaciones de la empresa cumpla con los mínimos criterios de seguridad necesarios para garantizar la integridad del bien de la empresa.

8. RESPONSABILIDADES DE LOS USUARIOS.

8.1 Criterios generales:

- Tener en cuenta las responsabilidades descritas en las políticas de vehículos de uso funcional y permanente, descritas anteriormente.

- Cumplir en todo momento con las normas de circulación vigentes en cada punto geográfico en el que se utilice el vehículo.

- Asumir de forma personal y completa, todo coste derivado de sanciones administrativas impuestas por incumplimiento de dicha normativa.

- Mantener indemne a Segura e Hijos, S.A. en todo momento y lugar frente cualquier obligación pecuniaria derivada de sanciones, multas, condenas e indemnizaciones derivadas del mal uso del vehículo o de cualquier accidente generado en el mismo que involucre a terceros.

- Cumplir con las normas y directrices de Segura e Hijos, S.A., así como los procedimientos y controles de seguridad dispuestos por este, por medio del área de Prevención de Riesgos Laborales.

- Informar de manera inmediata de cualquier novedad o situación relevante con relación al vehículo asignado o en uso, con el fin de que la compañía tome las medidas o inicie las actuaciones pertinentes.

- Reportar de manera oportuna al área responsable sobre el rendimiento del vehículo, con el fin de realizar mantenimiento correctivo y preventivo con la suficiente antelación.

- Autorizar los descuentos en sus retribuciones que correspondan para reponer cualquier suma de dinero que se genere con ocasión del manejo irregular u omisivo del vehículo asignado y que por ende recaiga sobre su haber como empleado.

- En el supuesto de que el vehículo deba reparase por un mal uso del mismo será el trabajador quien deberá asumir de su propio peculio todos y cada uno de los gastos correspondientes a la reparación del vehículo.

- Se entenderá dentro de las normas internas de la empresa como falta calificada como grave, el uso inadecuado por parte del trabajador del vehículo asignado ya sea de uso funcional o permanente, el uso del vehículo de uso funcional fuera de la jornada laboral, el uso del vehículo de uso funcional durante los fines de semana, que el vehículo de uso funcional o permanente sea utilizado por una persona diferente al trabajador al que se le asignó el vehículo, utilizar el vehículo de uso funcional o permanente bajo influencia de sustancias alucinógenas o bebidas alcohólicas y no guardar el vehículo de uso funcional después de la jornada de trabajo en el aparcamiento que la empresa designe a tales efectos.

  Tales conductas podrán implicar sanciones disciplinarias severas para el trabajador o incluso la terminación del contrato de trabajo con justa causa.

8.2 En caso de Accidente o Robo:

- En caso de accidente o robo de un vehículo, el usuario responsable del mismo deberá reportarlo de inmediato al área administrativa y al área de seguros de la compañía; con el fin de dar aviso a la compañía de seguros correspondiente, así como al área jurídica y al área de recursos humanos con el fin de llevar un control y seguimiento del incidente.

- De la misma manera en situaciones de accidentes, se solicitarán los servicios de reparación o mantenimiento propios de la aseguradora respectiva. Segura e Hijos, S.A. no responderá por el valor objetos depositados en el interior del vehículo por robo de éste.

- Además de los avisos indicados anteriormente, también se deberá informar al respectivo jefe inmediato sobre esta situación.

- Durante el tiempo que un vehículo esté en reparación, no hay lugar a la asignación de un nuevo vehículo a no ser que exista la aprobación expresa de la Dirección de la Empresa.

9.- INDICIOS DE MAL USO DEL AUTOMOVIL CORPORATIVO.

Dentro de las diferentes actuaciones que pueden presentarse en eventos adversos en el uso de estos vehículos, se tienen las siguientes como indicios de su mal manejo, sin que sean taxativas, sino meramente enunciativas, existiendo muchas otras conductas que deriven en la responsabilidad directa del colaborador o empleador usuario del vehículo:

- Que el trabajador lo utilice para fines diferentes al desempeño de su cargo, cuando el vehículo es de uso funcional y no particular.

- Que el trabajador lo utilice en horario diferente a la jornada laboral, cuando el mismo no está asignado de forma permanente.

- Que el vehículo sea utilizado por una persona diferente al trabajador sin autorización expresa de los cargos autorizados para designar estos usos.

- Que el vehículo sea utilizado por el trabajador bajo influencia de sustancias alucinógenas o bebidas alcohólicas.

- Que el vehículo sea utilizado durante el fin de semana, cuando el mismo es de uso funcional y no es de asignación permanente.

10.- LIBERALIDAD DE LA EMPRESA Y CARÁCTER NO SALARIAL.

Cuando el vehículo asignado sea de carácter funcional, éste se asimila a una herramienta de trabajo dispuesta por la empresa para el desarrollo de las actividades de la compañía, por ende, su uso y mantenimiento está regulada por las directrices internas de la Empresa, y en ningún caso puede tomarse como retribución de los trabajadores.

Por lo que respecta a los vehículos de uso permanente, se trata de una mera liberalidad en cuya virtud el trabajador podrá utilizar el vehículo asignado hasta el momento que así lo disponga la empresa.

Segura e Hijos, S.A. podrá de manera unilateral y sin previo aviso solicitar la entrega del vehículo al trabajador. Lo anterior no se entenderá como una desmejora de las condiciones del mismo.

Política de respeto de los DDHH de Segura e Hijos, S.A.

21 de febrero de 2023

ÍNDICE

El órgano de administración de **SEGURA E HIJOS, S.A.** (la "**Sociedad**") tiene atribuida la competencia de aprobar y actualizar las políticas corporativas que contienen las pautas que rigen la actuación de la Sociedad.

En el ejercicio de estas responsabilidades y, consciente de que el respeto a los DD.HH. es una parte fundamental sobre la que se asienta el propósito y los valores de la Sociedad y un aspecto indisolublemente ligado a la Agenda 2030 de Naciones Unidas para el Desarrollo Sostenible, el órgano de administración aprueba esta *Política de respeto de los DD.HH.* (la "**Política**") que ha sido elaborada teniendo en cuenta los estándares internacionales más exigentes.

Finalidad

La finalidad de esta Política es formalizar el compromiso de la Sociedad con los DD.HH. reconocidos en la legislación nacional e internacional, así como definir los principios que aplicará la Sociedad para la debida diligencia en materia de DD.HH., de conformidad con los convenios de la Organización Internacional del Trabajo (incluido el convenio 169), los Objetivos de Desarrollo Sostenible (ODS) aprobados por la Organización de las Naciones Unidas, el *Código ético* de la Sociedad, así como los documentos y textos que puedan sustituir o complementar a los anteriormente referidos.

Principios básicos de actuación

Para la consecución de los objetivos y compromisos señalados, la Sociedad asume y promueve los siguientes principios básicos de actuación que deben presidir su actuación en todos los ámbitos:

a. identificar los potenciales impactos que las operaciones y actividades realizadas por la Sociedad, directamente o a través de un tercero, pueden generar a los DD.HH.;

b. disponer de un sistema de diligencia debida que identifique las situaciones y actividades de mayor riesgo de contravención de los DD.HH., con el objetivo de desarrollar mecanismos de prevención y mitigación de dicho riesgo, así como de reparación de los impactos en caso de que se materializaran;

c. evaluar periódicamente la eficacia del sistema de diligencia debida mediante indicadores de seguimiento;
d. comunicar el resultado de la evaluación de la eficacia del sistema de diligencia debida en la información pública periódica, disponible en la página web corporativa de la Sociedad;

e. promover una cultura de respeto de los DD.HH. y acciones destinadas a la sensibilización de los profesionales en esta materia en toda la Sociedad;

f. disponer de mecanismos de denuncia y reclamación, con suficientes garantías y con procedimientos adecuados de resolución, para atender los potenciales casos de conculcación de los DD.HH. Estos mecanismos deberán ser suficientemente comunicados, tanto a los profesionales de la Sociedad, como a las personas y organizaciones ajenas a la Sociedad. A estos efectos, se definirán procedimientos de reporte interno adecuados sobre los asuntos comunicados, con el objetivo de hacer posible la evaluación de los sistemas de debida diligencia; y

g. adoptar a la mayor brevedad posible las medidas que procedan en caso de detectar una conculcación de los DD.HH. en las instalaciones de la Sociedad, e informar de ello a las autoridades competentes para que emprendan las acciones oportunas cuando dicha conculcación pueda ser constitutiva de una infracción administrativa, penal o de cualquier otra índole.

Marco normativo de DD.HH.

Además de esta *Política*, también forman parte del marco normativo de la Sociedad sobre el respeto de los DD.HH.:

a. las políticas sociales, que atienden determinadas necesidades y expectativas de los Grupos de interés de la Sociedad y que, en particular, cubren distintos asuntos directamente relacionados con los DD.HH., tales como seguridad y salud laboral, igualdad de oportunidades y conciliación o calidad;

b. la *Política de protección de datos personales*, que garantiza el derecho a la protección de los datos de todas las personas físicas que se relacionan con la Sociedad, asegurando, en particular, el respeto del derecho al honor y a la intimidad en el tratamiento de las diferentes tipologías de datos personales; y

Además de lo ya establecido en estas políticas, la Sociedad asume explícitamente el compromiso de:

a. rechazar el trabajo infantil y el trabajo forzoso u obligatorio;

b. respetar la libertad de asociación y negociación colectiva;

c. respetar el derecho a circular libremente dentro de cada país;

d. no discriminar por ninguna condición;

e. respetar los derechos de las minorías étnicas y de los pueblos indígenas en los lugares donde desarrolle su actividad, y favorecer un diálogo abierto que integre distintos marcos culturales;

f. respetar el derecho al medioambiente de todas las comunidades en las que opera, considerando sus expectativas y necesidades; y

Relación con los Grupos de interés

En cuanto a la relación de los Grupos de interés de la Sociedad con los DD.HH., se ha de tener en cuenta:

a. en cuanto al equipo humano: los profesionales de la Sociedad deberán mostrar un estricto respeto a los DD.HH. reconocidos en la legislación nacional e internacional en el desarrollo de su actividad y, en particular, velarán por el cumplimiento de esta *Política* y del marco normativo de DD.HH. de la Sociedad. Se espera de todos los profesionales de la Sociedad que actúen como una primera línea de defensa de los DD.HH., informando sobre cualquier posible impacto a estos o sobre cualquier incumplimiento de las políticas corporativas de la Sociedad;

b. en cuanto a los proveedores: deberán mostrar igualmente un estricto respeto a los DD.HH. reconocidos en la legislación nacional e internacional en el desarrollo de su actividad. La Sociedad considera que sus proveedores son un aliado clave para el cumplimiento de esta *Política* y que, por tanto, asumen una responsabilidad compartida con la Sociedad. En particular, los proveedores y sus profesionales deberán: **(i)** adoptar las medidas necesarias para eliminar toda forma o modalidad de trabajo forzoso u obligatorio; **(ii)** rechazar expresamente el empleo de mano de obra infantil en su organización; **(iii)** respetar la libertad de asociación sindical y el derecho a la negociación colectiva de sus profesionales, evitando toda práctica discriminatoria en materia de empleo y ocupación; y **(iv)** fijar los salarios de sus profesionales de acuerdo con las leyes aplicables, respetando los salarios mínimos, horas extra y beneficios sociales;

c. en cuanto a la sociedad en general: la Sociedad, en su operativa, deberá reforzar el respeto a los derechos de las minorías étnicas y de los pueblos indígenas en los lugares donde desarrolle su actividad; y

La Sociedad podrá contar con asesoramiento especializado externo para adaptar los procedimientos operativos de la Sociedad a los principios básicos de actuación recogidos en esta *Política*, así como, en su caso, para acometer su seguimiento y la actualización de su contenido.

El órgano de administración de la Sociedad recibirá información periódica sobre las medidas y procedimientos adoptados en la Sociedad para implementar y dar seguimiento a lo dispuesto en esta *Política*.

* * *

Esta *Política* fue aprobada inicialmente por el órgano de administración de la Sociedad el 13 de febrero de 2023.

Política marco de RRHH de Segura e Hijos, S.a.

21 de febrero de 2023

ÍNDICE

El órgano de administración de **SEGURA E HIJOS, S.A.** (la "**Sociedad**") tiene atribuida la competencia de aprobar y actualizar las políticas corporativas, las cuales contienen las pautas que rigen la actuación de la Sociedad.

En ejercicio de estas responsabilidades, y consciente de que el equipo humano es un activo estratégico y que los profesionales de la Sociedad son el elemento clave para alcanzar el propósito y poner en práctica sus valores corporativos, el órgano de administración aprueba esta *Política marco de recursos humanos* (la "***Política***").

Finalidad

La finalidad de esta Política es definir, diseñar y difundir un modelo de gestión de recursos humanos de la Sociedad que permita atraer, impulsar, fidelizar y retener el talento. Además, tiene como finalidad fomentar el crecimiento personal y profesional de todas las personas que pertenecen al equipo humano de la Sociedad, haciéndoles partícipes de su proyecto de éxito empresarial y garantizándoles un puesto de trabajo digno y seguro en un entorno diverso e inclusivo.

El equipo humano determina, de manera fundamental, la diferencia entre las empresas competitivas y las que no lo son, así como la diferencia entre las que crean valor de forma sostenible y las que van perdiendo paulatinamente su capacidad de generar riqueza.

Se considera que son principios clave para la conservación del capital humano el diseño y la implantación de unos marcos de gestión de recursos humanos y de relaciones laborales que hagan partícipes a todos los profesionales del éxito de la Sociedad, que promuevan su desarrollo económico y social, contribuyendo con ello al cumplimiento del octavo de los Objetivos de Desarrollo Sostenible (ODS) aprobados por la Organización de las Naciones Unidas, y que favorezcan la competitividad y la eficiencia empresarial.
Esta *Política* establece las pautas que deben regir las relaciones laborales en la Sociedad y sirve de referencia para definir los objetivos de la Sociedad en la gestión de los recursos humanos. En particular, establece las pautas en cuanto a: **(i)** la selección de sus profesionales; **(ii)** la creación de un empleo estable y de calidad en un entorno diverso e inclusivo; **(iii)** la construcción de una relación estable con los profesionales; **(iv)** la seguridad y salud en el trabajo; **(v)** la conciliación de la vida personal y laboral; así como **(vi)** la gestión y promoción del talento y la formación.

La gestión de los recursos humanos y de las relaciones laborales debe venir presidida por el respeto a los DD.HH. y laborales reconocidos en la legislación nacional e internacional, a la diversidad e inclusión, a la igualdad de oportunidades y no

discriminación, así como por la alineación de los intereses de los profesionales con los objetivos estratégicos de la Sociedad.

Principios generales de actuación

Para la consecución de los objetivos señalados, la Sociedad asume y promueve los siguientes principios generales de actuación que deben presidir la gestión de su capital humano:

a. un marco de relaciones laborales adecuado y de mecanismos pactados para la adaptación de la organización a los requerimientos empresariales y sociales, favoreciendo los objetivos de competitividad y eficiencia empresarial;

b. el diseño de una oferta laboral de valor, que favorezca la selección, contratación, promoción y retención del talento, compuesta por una retribución competitiva y un entorno de trabajo diverso e inclusivo, que facilite la conciliación de la vida personal y laboral e impulse el crecimiento profesional del equipo humano de la Sociedad. Este crecimiento profesional debe estar basado en criterios objetivos de desempeño, en la igualdad de oportunidades;

c. la definición como objetivo estratégico del desarrollo de las relaciones laborales basadas en la igualdad de oportunidades, en especial entre géneros, la no discriminación y la consideración de la diversidad e inclusión en todas sus variables, de conformidad con la *Política de igualdad, diversidad e inclusión*. Asimismo, deberán impulsarse medidas para facilitar la integración de colectivos desfavorecidos y con distintas capacidades, así como para lograr un entorno favorable que facilite a los profesionales la conciliación de la vida personal y laboral, respetando la legislación vigente en cada país y siguiendo las mejores prácticas internacionales;

d. la consolidación de empleos estables y de calidad;

e. la valoración de la aportación de todos los profesionales a la creación de valor de la Sociedad y a su crecimiento;

f. la garantía de que los procesos de selección, contratación y promoción de la Sociedad velen por que todos sus profesionales sean personas honorables e idóneas, alineadas con los principios recogidos en el *Código ético*, valorándose su trayectoria y rechazándose a quienes, por sus antecedentes, carezcan de la idoneidad exigible. Todo ello, sin perjuicio del respeto de la identidad y convicciones individuales, según establece la *Política de igualdad, diversidad e inclusión*; y

g. un entorno de trabajo que sea seguro y saludable en la Sociedad, así como en sus ámbitos de influencia.

Instrumentos

Para la consecución de los objetivos señalados, la Sociedad cuenta con los siguientes instrumentos:

a. políticas de recursos humanos: esta *Política* y la *Política de igualdad, diversidad e inclusión*;

b. la dirección responsable de la implantación, seguimiento y verificación del cumplimiento de la *Política de igualdad, diversidad e inclusión*;

c. convenios colectivos o acuerdos equivalentes específicos para regular los aspectos relacionados con la gestión de los recursos humanos, así como los mecanismos específicos de seguimiento establecidos;

d. programas de formación que favorecen el desarrollo del capital intelectual y la promoción de los profesionales dentro de la Sociedad;

e. un programa específico de formación y seguimiento del personal directivo que fomenta la promoción interna y asegura la sucesión ordenada en la alta dirección y en los demás puestos clave de la Sociedad; y

f. programas y procesos de prevención de riesgos laborales y un sistema global de seguridad y salud en el trabajo.

Principios básicos de actuación en relación con la igualdad, diversidad e inclusión

La *Política de igualdad, diversidad e inclusión* desarrolla los objetivos y principios de la Sociedad en estas materias, que pueden sintetizarse en los siguientes:

a. respetar la diversidad entre sus profesionales, promoviendo la no discriminación;

b. desarrollar el principio de igualdad de oportunidades, cuyo cumplimiento constituye uno de los pilares esenciales del desarrollo profesional y conlleva el compromiso de practicar y demostrar un trato equitativo que impulse la

progresión personal y profesional del equipo humano, evitando, entre otras cuestiones, que los profesionales con vínculos familiares o personales análogos ocupen puestos que dependan directamente -jerárquica o funcionalmente- de los profesionales con los que estén vinculados; y

c. promover la igualdad de género, en especial, en lo que se refiere al acceso al empleo, a la formación, a la promoción profesional y a las condiciones de trabajo.

La Sociedad vela por que los procesos relacionados con la selección, la contratación, la gestión de las relaciones laborales, la formación y la promoción de los profesionales en los que se emplee la inteligencia artificial y, especialmente, los algoritmos que se utilicen no adolezcan de sesgos que vulneren dichos objetivos y principios, ni imposibiliten su verificación por limitaciones de transparencia y/o trazabilidad de los resultados.

Principios básicos de actuación en relación con la selección y contratación de profesionales

Tal y como se desarrolla en la *Política de igualdad, diversidad e inclusión*, los principios básicos de actuación en relación con la selección y contratación son:

a. favorecer el acceso de los jóvenes a su primer empleo mediante programas de becas y otros acuerdos;

b. presentar a los candidatos una propuesta laboral de valor, atractiva e integral que favorezca la selección y la contratación de los mejores profesionales;

c. favorecer la contratación de profesionales de colectivos excluidos y de personas con distintas capacidades;

d. la propuesta de valor de la Sociedad debe estar basada en la igualdad de oportunidades, la diversidad y la inclusión y compuesta por una retribución competitiva, un entorno de trabajo saludable, diverso e inclusivo, el proyecto empresarial, el balance de la vida personal y laboral y la conciliación;

e. promover que las contrataciones de sus profesionales se realicen mediante contratos estables; y

f. homogeneizar las condiciones laborales y los beneficios obtenidos por los profesionales a tiempo parcial y a tiempo completo.

Principios básicos de actuación en relación con la gestión y la promoción del talento y la formación

La gestión y la promoción del talento son aspectos clave para mejorar la posición de la Sociedad frente a sus competidores y persiguen la definición de un marco para desarrollar un sistema de gestión de la calidad global, que afecta a todos los profesionales de la entidad.

Con carácter general, el órgano de administración de la Sociedad, en el proceso de análisis y deliberación previo a la adopción de sus acuerdos, tiene en especial consideración el impacto que sus decisiones pueden tener en la estrategia de gestión y promoción del talento de la Sociedad.

Además, la Sociedad trabaja continuamente para configurar una oferta de valor dirigida a sus profesionales, que favorezca la selección, contratación, promoción y retención del talento.

Uno de los aspectos fundamentales de la gestión global del talento en la Sociedad es el fomento de la formación con arreglo a los siguientes principios básicos de actuación:

a. el establecimiento de un marco conceptual en el que se incluyen todas las acciones formativas diseñadas para impulsar la cualificación del equipo humano, adaptándola a un entorno de trabajo diverso e inclusivo, multicultural, permeable a los cambios culturales, creando valor para la Sociedad y favoreciendo el desarrollo sostenible de los negocios de la Sociedad;

b. la puesta en marcha de programas y planes de formación que favorezcan el perfeccionamiento profesional para el desempeño del puesto de trabajo, la adecuación a los cambios tecnológicos y organizativos, la adaptación del equipo humano a las exigencias de la Sociedad y una mayor capacidad de desarrollo profesional. En particular, estos programas y planes de formación han de facilitar procesos de actualización de conocimientos y reconversión continua de habilidades, de forma que tecnologías, innovación y formación compongan un triángulo interactivo cuyo funcionamiento fomente la competitividad sostenible de la Sociedad;

c. la concepción de la formación como un elemento clave de cualificación y desarrollo profesional, y como puerta de las oportunidades de promoción dentro de la Sociedad;

d. los programas de formación han de contener, en la medida de lo posible, aspectos relacionados con el respeto a los DD.HH., la diversidad inclusiva, y que fomenten una cultura de comportamiento ético, sin sesgos excluyentes o discriminatorios. Dichos programas han de ser integrales, de forma que los

aspectos técnicos, sociales y humanos se consideren en su conjunto para que los profesionales desarrollen en su trabajo no solo las mejores cualificaciones, sino también los principios y valores que la Sociedad quiere defender ante la sociedad; y

Principios básicos de actuación en relación con las evaluaciones del desempeño y desarrollo

Las evaluaciones de los profesionales y la comunicación de su resultado a los evaluados son un aspecto fundamental para su desarrollo profesional. Los principios básicos de actuación relativos a este ámbito son:

a. Procurar la realización periódica de evaluaciones del desempeño de los profesionales de la Sociedad basadas en criterios objetivos;

b. comunicar su resultado al evaluado, de forma que se favorezca su desarrollo profesional; y

c. evitar que en los procesos de evaluación o revisión salarial participen directamente profesionales que sean familiares o que tengan una vinculación personal análoga con los profesionales afectados.

Principios básicos de actuación en relación con el sistema retributivo

La Sociedad considera prioritario que el sistema retributivo favorezca la consolidación de su capital humano, como principal factor diferenciador respecto de sus competidores. Los principios básicos de actuación que deben guiar el sistema retributivo de la Sociedad son:

a. favorecer la atracción, contratación y permanencia de los mejores profesionales;

b. guardar coherencia con el posicionamiento estratégico de la Sociedad y con su desarrollo;

c. reconocer y recompensar la dedicación, la responsabilidad y el desempeño de todos sus profesionales;

Principios básicos de actuación en relación con la conciliación de la vida personal y laboral

Lograr la efectiva conciliación entre la vida personal y laboral de los profesionales es una prioridad de la Sociedad, que lleva a cabo a través de los siguientes principios básicos de actuación:

a. implantar medidas de conciliación que favorezcan el respeto de la vida personal y familiar de los profesionales y faciliten el mejor equilibrio entre esta y las responsabilidades laborales;

b. atender con las debidas medidas de conciliación, entre otras, las situaciones de personas solteras, casadas o en pareja de hecho, divorciadas, separadas, en viudedad, en convivencia con una pluralidad de personas, con o sin hijos, y con cualesquiera otras circunstancias familiares o afectivas particulares, incluyendo la vinculación específica que se origina con animales de compañía, como seres vivos dotados de sensibilidad.

Principios básicos de actuación en relación con el respeto a la vida privada y a la desconexión digital

Las dinámicas organizativas más recientes, así como la implantación de las nuevas tecnologías, fomentan la eficiencia organizativa, pero al mismo tiempo difuminan los límites entre el tiempo de dedicación al trabajo y la vida privada. Para la Sociedad, tal y como consta en esta *Política,* es prioritario que sus profesionales puedan desarrollar de forma plena su vida personal, de manera compatible con, y enriquecedora de, su actividad laboral.

A estos efectos, esta *Política establece* unas pautas que permiten la efectiva separación de los ámbitos personal y laboral, con especial atención a la desconexión de los dispositivos digitales, sin que se favorezca o discrimine a los profesionales, y ello en base a los siguientes principios básicos de actuación:

a. promover unas adecuadas pautas de desconexión digital que tengan como objetivo fomentar el respeto del tiempo de descanso y facilitar que el profesional pueda desarrollar plenamente su vida personal fuera del horario de trabajo y con las menores interferencias posibles de sus obligaciones profesionales, que solo han de darse en situaciones de justificada necesidad; y

b. fijar los criterios de desconexión que deberán tener en cuenta la situación específica de los distintos colectivos de profesionales, incluyendo, en particular: **(i)** aquellos que han de mantener una especial disponibilidad por su nivel de responsabilidad o por su posición de alerta para atender necesidades impredecibles; y **(ii)** aquellos que desarrollan, total o predominantemente, sus tareas a distancia, y en especial en sus domicilios.

En este último caso, deben definirse criterios que, sin perjuicio de las facultades empresariales de control del trabajo y de la flexibilidad horaria requerida, aseguren el pleno respeto a la vida personal y la desconexión de las responsabilidades laborales.

Las pautas de desconexión han de ser diversas en función de las responsabilidades de los distintos colectivos del equipo humano y han de abarcar los múltiples y variados instrumentos digitales de comunicación e información suministrados a los profesionales para el desempeño del trabajo, particularmente, dispositivos móviles, ordenadores y tabletas habilitados para el trabajo en remoto o en los que se reciba el correo profesional.

Sistema global de seguridad y salud en el trabajo

Reconociendo la importancia que tienen los riesgos de seguridad y salud en el trabajo, el órgano de administración de la Sociedad se compromete a desarrollar las acciones necesarias para proporcionar condiciones seguras y saludables para la prevención de lesiones y deterioro de la salud física o mental, relacionados con el trabajo, apropiadas y adaptadas al propósito, tamaño y contexto de cada organización y a la naturaleza especifica de los riesgos para los profesionales en la Sociedad, contribuyendo con ello a la consecución del tercero y octavo de los Objetivos de Desarrollo Sostenible (ODS) aprobados por la Organización de las Naciones Unidas.

Todo ello de modo que los diferentes niveles de la organización sean conscientes de la importancia de la seguridad y salud en el trabajo en la planificación y posterior desarrollo de las actuaciones de la Sociedad, y de que todos los profesionales contribuyan con su trabajo diario al cumplimiento de los objetivos que se adopten en este campo.

Ética en el trabajo

El órgano de administración de la Sociedad ha aprobado un *Código ético* que recoge los principios básicos de actuación exigibles a todos los profesionales y personal directivo de la Sociedad, cualquiera que sea su nivel jerárquico, su ubicación geográfica o funcional.

* * *

Esta *Política* fue aprobada inicialmente por el órgano de administración de la Sociedad el 13 de febrero de 2023.

Política de igualdad, diversidad e inclusión de Segura e Hijos, S.A.

21 de febrero de 2023

ÍNDICE

El órgano de administración de **SEGURA E HIJOS, S.A.** (la "**Sociedad**") tiene atribuida la competencia de diseñar, evaluar y revisar de aprobar y actualizar las políticas corporativas que establecen las pautas que rigen la actuación de la Sociedad.

En el ejercicio de estas responsabilidades, consciente de su compromiso con el equipo humano como principal activo estratégico y clave de su éxito empresarial, el órgano de administración de la Sociedad aprueba esta *Política de igualdad, diversidad e inclusión* (la "**Política**").

Finalidad

La finalidad de esta Política es lograr un entorno favorable que facilite y potencie la igualdad de oportunidades, la no discriminación, la diversidad y la inclusión de los profesionales de la Sociedad, apostando, en consecuencia, por un modelo de gestión de personas comprometido con la excelencia profesional y la calidad de vida, todo ello de conformidad con la legislación vigente en España y siguiendo las mejores prácticas internacionales, incluyendo lo dispuesto en los Objetivos de Desarrollo Sostenible (ODS) aprobados por la Organización de las Naciones Unidas en estos ámbitos.

La igualdad de oportunidades constituye uno de los pilares esenciales del progreso profesional y su desarrollo implica un trato equitativo para impulsar la progresión personal y profesional del equipo humano de la Sociedad.

En cuanto a la diversidad, esta engloba el conjunto de características que hacen a las personas únicas y singulares, es decir, la riqueza que cada persona aporta gracias a su variedad, incluyendo condiciones visibles y no visibles.

La inclusión, por su parte, se refiere a cómo se valoran las diferencias entre los individuos y se generan oportunidades para que todos puedan desplegar su máximo potencial. Esto es, la estrategia consciente que pone el foco en desarrollar las estructuras, sistemas, procesos y cultura que generan respeto a las particularidades de todas las personas en el seno de una organización, fomentando, asimismo, un sentimiento de pertenencia que hace que se sientan valoradas y parte de un grupo o comunidad.

Principios básicos de actuación en relación con la igualdad de oportunidades

Para la consecución de los objetivos y compromisos señalados en materia de igualdad de oportunidades, la Sociedad asume y promueve los siguientes principios básicos de actuación que deben presidir el desarrollo de sus relaciones laborales:

a. garantizar la calidad del empleo como medio fundamental para promover la igualdad de oportunidades y la no discriminación, fomentando el mantenimiento de puestos de trabajo estables y de calidad, con contenidos ocupacionales que garanticen una mejora continua de las aptitudes y competencias de los profesionales;

b. desarrollar el principio de igualdad de oportunidades en el trabajo, cuyo cumplimiento constituye uno de los pilares esenciales del desarrollo profesional, y que conlleva el compromiso de practicar y demostrar un trato equitativo que impulse la progresión personal y profesional del equipo humano de la Sociead en los siguientes ámbitos:

- promoción, desarrollo profesional y compensación: valorar aquellos conocimientos y habilidades necesarios para realizar el trabajo, a través de la evaluación de objetivos y desempeño.

  En particular, tanto en la realización de propuestas individuales de objetivos, como en la valoración del desempeño y, en su caso, del incremento salarial, se considerarán criterios de igualdad de oportunidades, de no discriminación y de respeto a la diversidad. En este sentido, se promoverá un trato equitativo que impulse la progresión personal y profesional del equipo humano de la Sociedad, de forma que se reconozcan los conocimientos y las habilidades necesarias para cada puesto de trabajo, la aportación de los profesionales a la creación de valor, así como la dedicación y responsabilidad en el desempeño de sus funciones;

- selección: elegir a los mejores profesionales por medio de herramientas y sistemas de selección basados en los conocimientos y las capacidades de los candidatos;

- contratación: no establecer diferencias salariales de carácter discriminatorio y asegurar una adecuada integración del profesional a la compañía, grupo de trabajo y puesto;

- formación: asegurar la formación y la capacitación de cada profesional en los conocimientos y habilidades que se requieren para el adecuado desarrollo de su trabajo;

- apoyo a los profesionales con capacidades diferentes, promoviendo su ocupación efectiva;

- impulso de una comunicación transparente, alentando la innovación y concediendo al profesional la autonomía necesaria en el ejercicio de sus funciones; y

- eliminación de cualesquiera actuaciones contrarias a la igualdad de oportunidades.

c. promover la igualdad de género dentro de la Sociedad, cumpliendo con la legislación vigente y siguiendo las mejores prácticas internacionales, así como lo dispuesto en este ámbito en el quinto de los Objetivos de Desarrollo Sostenible (ODS) aprobados por la Organización de las Naciones Unidas y, en particular, en lo que se refiere al acceso al empleo, a la formación, a la promoción profesional y a las condiciones de trabajo, y, a estos efectos:

- reforzar el compromiso de la Sociedad con la igualdad de género tanto en la organización como en la sociedad y fomentar la sensibilización sobre este tema en los dos ámbitos;

- garantizar el principio de igualdad de oportunidades en el desarrollo profesional, removiendo los obstáculos que puedan impedir o limitar la carrera por razón de género;

- analizar medidas de acción positiva para corregir las desigualdades que se presenten y para fomentar el acceso del género menos representado a cargos de responsabilidad en los que tengan escasa o nula representación;

- potenciar mecanismos y procedimientos de selección y desarrollo profesional que faciliten la presencia del género menos representado con la cualificación necesaria en todos los ámbitos de la organización en los que su representación sea insuficiente.

- procurar una representación equilibrada en los diferentes órganos y niveles de toma de decisiones, garantizando la participación en condiciones de igualdad de oportunidades en todos los ámbitos de consulta y de decisión de la Sociedad;

- fomentar la organización de las condiciones de trabajo con perspectiva de género, permitiendo la conciliación de la vida personal y laboral de todos los profesionales que trabajan en la Sociedad para favorecer esa igualdad de género, velando por la eliminación de todas las discriminaciones por motivo de género;

- proteger la gestación, el parto y el postparto como situaciones específicas del colectivo profesional femenino, evitando que ello pueda repercutir negativamente en su carrera profesional;

d. homogeneizar las condiciones laborales y los beneficios obtenidos por los profesionales a tiempo parcial y a tiempo completo;

e. respetar, en el establecimiento de las condiciones de trabajo, el principio de igualdad de condiciones laborales para los trabajos que representan una misma exigencia y un mismo valor;

f. excluir los prejuicios que puedan existir respecto a personas cuya condición social, cultural o educativa no respondan a modelos considerados tradicionalmente de referencia o habituales y que pueden condicionar indebidamente el progreso profesional basado en el mérito y la capacidad de las personas; y

Principios básicos de actuación en relación con la diversidad y con la promoción de la inclusión

Para la consecución de los objetivos y compromisos señalados en relación con la diversidad y con la promoción de la inclusión, la Sociedad asume y promueve los siguientes principios básicos de actuación que deben presidir el desarrollo de sus relaciones laborales:

a. garantizar la no discriminación entre sus profesionales por cualesquiera condiciones o circunstancias que sean dignas de tutela;

b. promover que todos los profesionales de la Sociedad aporten sus conocimientos, experiencias y habilidades, con independencia de cualesquiera condiciones o circunstancias personales o sociales;

c. fomentar un sentido de inclusión en la Sociedad que persiga que todo profesional se considere parte del proyecto empresarial. Con ello se pretende que los valores, principios y objetivos de la Sociedad sean asumidos como propios por el equipo humano y que su contribución a ellos se perciba como componente esencial del desarrollo no solo profesional, sino también personal;

d. reconocer la convivencia de diversas generaciones como una fuente de enriquecimiento continuo, por sus capacidades y enfoques diversos, tanto para los profesionales como para los distintos negocios y áreas corporativas, y como contribución decisiva para la adecuación de los servicios que la Sociedad presta a las necesidades de las comunidades en las que opera;

e. tomar en consideración que determinadas limitaciones en capacidades físicas y/o intelectuales que pueden ser un obstáculo para el desarrollo de algunas tareas representan, por el contrario, un valor añadido significativo en otros

desempeños. En todo caso, no identificar tales circunstancias, de manera preliminar y sin fundamentación, como obstáculos para la debida integración en el trabajo;

f. fomentar la información y la comunicación con las distintas comunidades en las que opera el la Sociedad para que ésta sea reconocida como un lugar idóneo para el desarrollo profesional de sus diversos colectivos como consecuencia de sus prácticas inclusivas;

g. garantizar que los procesos de selección y contratación se asienten sobre criterios neutros y objetivos de mérito y capacidad, al mismo tiempo que se establezcan acciones específicas para fomentar la inclusión de los colectivos con menor facilidad de acceso al mercado laboral;

h. asegurar que las decisiones en materia de promoción profesional, así como de desarrollo profesional, se fundamenten en criterios equitativos, eliminando en todas las decisiones empresariales al respecto, motivos o consecuencias perjudiciales para la diversidad, promoviendo la debida inclusión de todos los colectivos de profesionales;

i. asegurar que, en la formación de cada profesional, con independencia del colectivo al que pertenezca, se le dote de los conocimientos, aptitudes y habilidades suficientes para el adecuado desarrollo de su trabajo, al mismo tiempo que se prevean en dicha formación acciones específicas desde la perspectiva de la aceptación de la diversidad y del rechazo a la discriminación;

j. fomentar el uso de lenguaje inclusivo en cualquier tipo de comunicación corporativa, interna o externa, y erradicar, en todo caso, el empleo de lenguaje discriminatorio;

k. preservar un ambiente libre de acoso laboral, especialmente el que tenga como intencionalidad o fundamento la discriminación directa o indirecta, asegurando la instauración de canales de denuncia ágiles y eficaces;

l. desarrollar, de forma constante, políticas de sensibilización de los profesionales que prestan servicios en la Sociedad, especialmente de los que desempeñan responsabilidades directivas, para que valoren y fomenten la aportación que la diversidad representa para la Sociedad;

m. incorporar en los programas de liderazgo comportamientos que favorezcan una mejor toma de decisiones y una cultura basada en la diversidad, así como una estrategia de comunicación interna y que logre transmitir la naturaleza plural e inclusiva de la Sociedad;

n. en línea con la *Política de respeto de los DD.HH.*, garantizar los derechos de libertad sindical recogidos en la normativa internacional, a efectos de preservar la opción de cada persona en su relación con las organizaciones sindicales y la actuación de estas en la defensa de sus legítimos intereses; y

o. velar por que los procesos relacionados con la selección, la contratación, la gestión de las relaciones laborales, la formación y la promoción de los profesionales en los que se emplee la inteligencia artificial y, especialmente, los algoritmos que se utilicen, no adolezcan de sesgos que vulneren, por su diseño o por el resultado de su implementación efectiva, los objetivos y compromisos de la Sociedad en materia de diversidad y de promoción de la inclusión, ni imposibiliten su verificación por limitaciones de transparencia y/o trazabilidad de los resultados.

Instrumentos

Para la consecución de los objetivos establecidos en esta Política, la Sociedad cuenta con una dirección responsable, dependiente de la Dirección de Recursos Humanos de la Sociedad, que se ocupa de la implantación, el seguimiento y verificación del cumplimiento de esta *Política*.

* * *

Esta Política fue aprobada inicialmente por el órgano de administración el 13 de febrero de 2023 como *Política de igualdad, diversidad e inclusión.*

Segura e Hijos
desde 1965

POLÍTICA DE CALIDAD Y MEDIOAMBIENTE

SEGURA E HIJOS, como empresa dedicada al suministro y venta de materiales de construcción, ferretería, cocina, baño, mobiliario, decoración y jardinería, se compromete a satisfacer los requisitos y expectativas de los clientes y otras partes interesadas, por lo que la Dirección establece los siguientes principios:

- Establecemos objetivos que nos permitan evaluar la mejora continua de nuestros productos y servicios, con el fin de reducir, en la medida de lo posible, los impactos ambientales generados.
- Promovemos el desarrollo profesional y personal de nuestros colaboradores y garantizamos su competencia técnica.
- Nos comprometemos a que se determinen los requisitos del cliente y se cumplan con el propósito de aumentar la satisfacción de los mismos.
- Fomentamos la cooperación y el respeto mutuo con los empleados a fin de mejorar el funcionamiento de nuestra compañía y que los clientes reciban la mejor atención por nuestra parte.
- Garantizamos el correcto estado de las instalaciones y de los equipos necesarios para que estén en correspondencia con nuestra actividad.
- Realizamos un análisis de los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Realizamos un análisis del contexto y de los procesos relevantes de la organización, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Realizamos un análisis de riesgos, adecuados al contexto de la organización, con el fin de adoptar medidas para minimizarlos.
- Cumplimos con todos los requisitos de la legislación aplicable a nuestra actividad, los compromisos adquiridos con nuestros clientes y todas aquellas normas internas o pautas de actuación a los que voluntariamente nos sometemos.
- Prevenimos la contaminación mediante la reducción, en la medida que sea técnica y económicamente viable, los residuos, vertidos y emisiones generados por nuestras actividades, así como otros impactos que nuestra actividad pudiera producir sobre el medio.
- Trabajamos de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar sus actuaciones medioambientales, que repercutan en una mayor eficiencia ambiental de nuestra actividad.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento.

Madrid, 10 de noviembre de 2020

Segura e Hijos

P.P.
Demetrio Segura
Director General

MANUAL DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO

[NORMAS DE PROCEDIMIENTO Y CONTROL PARA LA PREVENCIÓN DEL BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO]

ÍNDICE

1. PREÁMBULO

La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (en adelante, "**Ley 10/2010**"), que entró en vigor el 30 de abril de 2010, tiene por objeto la protección de la integridad del sistema financiero y de otros sectores de actividad económica e impone a los sujetos obligados determinadas obligaciones con el fin de prevenir e impedir que sus servicios sean utilizados para actividades de blanqueo de capitales y de la financiación del terrorismo. El Consejo de Ministros aprobó el 30 de abril de 2014 el Real Decreto 304/2014, de 5 de mayo, que desarrolla el Reglamento de la Ley 10/2010 (en adelante, "**Reglamento**").

SEGURA E HIJOS, S.A. con N.I.F. número A-78144524 (**en adelante, "SEGURA"** o la "**Sociedad**") considera imprescindible cumplir con los más altos estándares en materia regulatoria, y en particular, en relación con la prevención del blanqueo de capitales.

En este sentido, SEGURA asume funciones de "prevención y vigilancia", así como el diseño de políticas y procedimientos internos para tratar de evitar e impedir la utilización del sector de la economía en el que actúa para blanquear dinero o financiar el terrorismo.

La Sociedad es consciente del riesgo de blanqueo de capitales a través de los servicios a prestar y bienes a comercializar y se compromete a cumplir escrupulosamente la normativa vigente y, por este motivo, aplicará el siguiente Manual de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo (en adelante el "**Manual**" o las "**Normas**") que será de obligado conocimiento y cumplimiento por todo el personal y profesionales que presten sus servicios en o para la Sociedad.

Asimismo, el principio de "Conoce a tu Cliente", según el cual los sujetos obligados deben solicitar determinada información y documentación antes de establecer relaciones comerciales con un potencial cliente, ha demostrado ser el instrumento preventivo más eficaz en la lucha contra el blanqueo de capitales y la financiación del terrorismo. Por ello, el establecimiento y regulación de esta obligación es uno de los principales objetivos de este Manual, junto con el diseño de las políticas y procedimientos internos.

A efectos aclaratorios, se hace constar expresamente que el término "cliente" utilizado en este Manual debe entenderse en sentido amplio, englobando a todas las personas físicas o jurídicas que operen con la Sociedad-

2. DEFINICIONES

- **Bienes que proceden de una actividad delictiva o de la participación en una actividad delictiva**. Según el artículo 1.2. de la Ley 10/2010, todo tipo de activos cuya adquisición o posesión tenga su origen en un delito, tanto materiales como inmateriales, muebles o inmuebles, tangibles o intangibles, así como los documentos o instrumentos jurídicos con independencia de su forma, incluidas la electrónica o la digital, que acrediten la propiedad de dichos activos o un derecho sobre los mismos, con inclusión de la cuota defraudada en el caso de los delitos contra la Hacienda Pública.

- **Blanqueo de capitales**. Según el artículo 1.2. de la Ley 10/2010:

  - ✔ La conversión o la transferencia de bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva, con el propósito de ocultar o encubrir el origen ilícito de los bienes o de ayudar a personas que estén implicadas a eludir las consecuencias jurídicas de sus actos.

  - ✔ La ocultación o el encubrimiento de la naturaleza, el origen, la localización, la disposición, el movimiento o la propiedad real de bienes o derechos sobre bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva.

  - ✔ La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de la recepción de los mismos, de que proceden de una actividad delictiva o de la participación en una actividad delictiva.

  - ✔ La participación en alguna de las actividades mencionadas en las letras anteriores, la asociación para cometer este tipo de actos, las tentativas de perpetrarlas y el hecho de ayudar, instigar o aconsejar a alguien para realizarlas o facilitar su ejecución.

  Existirá blanqueo de capitales aun cuando las conductas descritas en los apartados precedentes sean realizadas por la persona o personas que cometieron la actividad delictiva que haya generado los bienes.

  Se considerará que hay blanqueo de capitales aun cuando las actividades que hayan generado los bienes se hubieran desarrollado en el territorio de otro Estado.

- **Financiación del terrorismo**. Según el artículo 1.3 de la Ley 10/2010, el suministro, el depósito, la distribución o la recogida de fondos o bienes, por cualquier medio, de forma directa o indirecta, con la intención de utilizarlos o con e l conocimiento de que serán utilizados, íntegramente o en parte, para la comisión de cualquiera de los delitos de terrorismo tipificados en el Código Penal.

Se considera que existe financiación del terrorismo aun cuando el suministro o la recogida de fondos o bienes se hayan desarrollado en el territorio de otro Estado.

- **Titular Real**. Según el artículo 4.2. de la Ley 10/2010 y el artículo 8 del Reglamento:

  - ✔ La persona o personas físicas por cuya cuenta se pretenda establecer una relación de negocios o intervenir en cualesquiera operaciones.

  - ✔ La persona o personas físicas que en último término posean o controlen, directa o indirectamente, un porcentaje superior al 25 % del capital o de los derechos de voto de una persona jurídica, o que por otros medios ejerzan el control, directo o indirecto, de la gestión de una persona jurídica. Se exceptúan las sociedades que coticen en un mercado regulado de la Unión Europea o de Países Terceros Equivalentes.

  - ✔ La persona o personas físicas que sean titulares o ejerzan el control del 25% o más de los bienes de un instrumento o persona jurídicos que administre o distribuya fondos, o, cuando los beneficiarios estén aún por designar, la categoría de personas en beneficio de la cual se ha creado o actúa principalmente la persona o instrumento jurídicos. Cuando no exista persona física que posea o controle directa o indirectamente el 25% o más de los bienes mencionados en el apartado anterior tendrán la consideración de Titular Real la persona o personas físicas en última instancia responsables de la dirección y gestión del instrumento o persona jurídicos o incluso a través de una cadena de control o propiedad.

  - ✔ La persona o personas físicas que posean o controlen un 25% o más de los derechos de voto de un Patronato. De tratarse de una fundación o asociación se tendrá en cuenta los acuerdos estatutarios para identificar al Titular Real. Si no existiera tal previsión estatutaria tendrán la consideración de Titulares Reales los miembros del Patronato y en el caso de asociación los miembros del órgano de representación o Junta Directiva.

- **Cliente:** La persona física o jurídica que vaya a ser la destinataria o beneficiaria última de los servicios o bienes que comercializa la Sociedad.

- **Director del OCI**: Será el administrador designado por el órgano de gobierno de la Sociedad, conforme a lo establecido en las presentes Normas.

- **Empleados:** Todos los empleados que presten servicios de forma permanente para la Sociedad y estén unidos a la Sociedad por una relación laboral.

- **GAFI**: El Grupo de Acción Financiera de la OCDE (**www.fatf-gafi.org**), que es un órgano intergubernamental cuyo propósito es el desarrollo y la promoción de políticas, tanto a nivel nacional como a nivel internacional, para combatir el blanqueo de capitales y la financiación del terrorismo.

- **OCI**: Órgano de Control Interno, cuya composición y funcionamiento se regulan en el apartado cinco de estas Normas.

- **Países Terceros Equivalentes**: Según el artículo 1.4. de la Ley 10/2010, Estados, territorios o jurisdicciones que, por establecer requisitos equivalentes a los de la legislación española, se determinen por la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. La calificación como País Tercero Equivalente de un Estado, territorio o jurisdicción se entenderá en todo caso sin efecto retroactivo.

  En la fecha en la que se dictan estas Normas, el listado de Países Terceros Equivalentes consta en la Resolución de 10 de agosto de 2012, de la Secretaría General del Tesoro y Política Financiera, por la que se publica el Acuerdo de 17 de julio de 2012, de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, por el que se determinan las jurisdicciones que establecen requisitos equivalentes a los de la legislación española de prevención del blanqueo de capitales y de la financiación del terrorismo (BOE 23/08/12) (**Anexo I**).

  No obstante, estas jurisdicciones solo se considerarán como Países Terceros Equivalentes en la medida en que el GAFI no los haya identificado como países "no-cooperantes" o como países con deficiencias estructurales en materia de prevención del blanqueo de capitales y de la financiación del terrorismo.

- **Personas con Responsabilidad Pública** (en adelante, "**PRP**"): Las personas físicas que desempeñen o hayan desempeñado en los últimos dos (2) años, funciones públicas importantes en España, otros Estados miembros de la Unión Europea o en terceros países, así como sus familiares más próximos y personas reconocidas como allegados. A estos efectos se entenderá:

  - ✔ Por personas físicas que desempeñen o hayan desempeñado funciones públicas importantes: Los jefes de Estado, jefes de Gobierno, ministros, secretarios de Estado o subsecretarios; los parlamentarios; los magistrados de tribunales supremos, tribunales constitucionales u otras altas instancias judiciales cuyas decisiones no admitan normalmente recurso, salvo en circunstancias excepcionales, con inclusión de los miembros equivalentes del Ministerio Fiscal; los miembros de tribunales de cuentas o de consejos de bancos centrales; los embajadores y encargados de negocios; el alto personal militar de las Fuerzas Armadas; y los miembros de los órganos de administración, de gestión o de supervisión de empresas de titularidad pública.

    Estas categorías comprenderán, en su caso, cargos desempeñados a escala comunitaria e internacional. Ninguna de estas categorías incluirá empleados públicos de niveles intermedios o inferiores.

- ✔ Por familiares más próximos: El cónyuge o la persona a quien se halle ligado de forma estable por análoga relación de afectividad, así como los padres e hijos, y los cónyuges o personas ligadas a los hijos de forma estable por análoga relación de afectividad.

- ✔ Por personas reconocidas como allegados: Toda persona física de la que sea notorio que ostente la titularidad o el control de un instrumento o persona jurídicos conjuntamente con alguna de las personas mencionadas en la letra a), o mantenga otro tipo de relaciones empresariales estrechas con las mismas, u ostente la titularidad o el control de una persona o instrumento jurídicos que notoriamente se haya constituido en beneficio de las mismas.

- **PEP:** Tendrá el mismo significado que Persona con Responsabilidad Pública.

- **SEPBLAC**: Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

3. NORMATIVA INTERNA APLICABLE

La normativa interna aplicable en materia de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo es la siguiente:

- Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.

- Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.

- Ley 12/2003, de 21 de mayo, sobre prevención y bloqueo de la financiación del terrorismo.

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- Resolución de 10 de agosto de 2012, de la Secretaría General del Tesoro y Política Financiera, por la que se publica el Acuerdo de 17 de julio de 2012, de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, por el que se determinan las jurisdicciones que establecen requisitos equivalentes a los de la legislación española de prevención del blanqueo de capitales y de la financiación del terrorismo (BOE 23/08/12).

- Orden EHA/2444/2007, de 31 de julio, por la que se desarrolla el Reglamento de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, aprobado por Real Decreto 925/1995, de 9 de junio, en relación con el informe de experto externo sobre los procedimientos y órganos de control interno y comunicación establecidos para prevenir el blanqueo de capitales.

- Orden EHA/1464/2010, de 28 de Mayo, que modifica el artículo único de la Orden ECO/2652/2002 para incluir a la República Islámica de Irán en la relación de países y territorios establecida en el mismo.

- Orden ECO/2652/2002, de 24 de octubre, por la que se desarrollan las obligaciones de comunicación de operaciones en relación con determinados países al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

También resultan aplicables las siguientes normas comunitarias:

- La Directiva 2005/60/CE, del Parlamento Europeo y del Consejo de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo.

- La Directiva 2006/70/CE, de la Comisión, de 1 de agosto de 2006, por la que se establecen disposiciones de aplicación de la Directiva 2005/60/CE del Parlamento Europeo y del Consejo en lo relativo a la definición de "personas del medio político", y los criterios técnicos aplicables en los procedimientos simplificados de diligencia debida con respecto al Cliente, así como en lo que atañe a la exención por razones de actividad financiera ocasional o muy limitada.

- La Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) nº 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión.

- La Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.

Son igualmente de aplicación:

- Los Convenios Internacionales en la materia de los que el Reino de España es signatario y las Resoluciones del Consejo de Seguridad de las Naciones Unidas, siempre que hayan sido adoptadas de acuerdo con los procedimientos establecidos en el capítulo VII de la Carta Constitutiva.

- Las recomendaciones del GAFI, así como los estándares internacionales emitidos por este organismo u otros organismos internacionales especializados en la materia (Grupo Egmont, Banco Central Europeo, Banco Internacional de Pagos, Banco Mundial, Fondo Monetario Internacional, entre otros).

4. ÁMBITO DE APLICACIÓN

4.1 Objetivo

De acuerdo con el artículo 2.1, apartado l) de la Ley 10/2010, las personas que comercien profesionalmente con bienes en los términos del artículo 38 del mismo texto legal estarán sujetas a las obligaciones derivadas de este último precepto de la citada Ley.

Por tanto, estas normas deberán ser aplicadas en los supuestos en los que la Sociedad intervenga directa o indirectamente en operaciones de comercio de bienes respecto de las transacciones en que los cobros o pagos se efectúen por personas físicas no residentes en España en los que se cumplan al mismo tiempo los siguientes dos (2) requisitos:

a) Importe superior a DIEZ MIL EUROS (10.000,00.-€) o su contravalor en moneda extranjera.

b) Utilización de los medios de pago previstos en el artículo 34.2 de la Ley: envíos postales, envíos por mensajería, equipaje no acompañado o carga en contenedores, por importe igual o superior a 10.000 euros o su contravalor en moneda extranjera

4.2 Subjetivo

Las presentes Normas deberán ser aplicadas por todo el personal al servicio de la Sociedad. También serán de obligado cumplimiento en las sucursales y filiales en las que SEGURA tenga una participación mayoritaria, así como por parte de las compañías o personas contratadas por SEGURA para prestar servicios esporádicos o permanentes de comercialización de sus productos inmobiliarios, debiéndose éstos subrogar en la totalidad de obligaciones impuestas en las presentes Normas.

A tal fin, los contratos que SEGURA suscriba para la subcontratación de su propia actividad con terceros y que no se refieran a servicios que impliquen la asunción de las obligaciones establecidas en el artículo 8 de la Ley 10/2010, contendrán una cláusula específica cuyo modelo se adjunta como **Anexo II**. Y ello, sin perjuicio de que la Sociedad, en todo caso, deberá hacer un seguimiento y control de las actividades de la empresa subcontratada que se adapte al nivel de riesgo existente en función de las características concretas de la relación entre las partes. Esos mismos contratos contendrán cláusulas de posible terminación de la relación contractual en caso de incumplimiento grave o sistemático de los procedimientos previstos en las presentes Normas.

La Sociedad mantendrá una relación completa y actualizada de empresas subcontratadas para el desarrollo de su propia actividad que incluirá todos los datos necesarios para su adecuada identificación y localización.

En el caso en que sí se incluyan servicios que impliquen la asunción de las obligaciones establecidas en el artículo 8 de la Ley 10/2010 se impondrá a la empresa subcontratada el

cumplimiento de las obligaciones impuestas en las presentes Normas, así como por la Ley 10/2010 en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, durante toda la vigencia del contrato suscrito con SEGURA y se añadirá la cláusula siguiente y se le entregará una copia del Manual:

> "[La entidad subcontratada] será responsable de aplicar, respecto a las operaciones efectuadas al amparo de este contrato, las medidas normales de diligencia debida mencionadas en el Art. 8 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (en adelante LPCFT). Las medidas normales de diligencia debida consisten en la identificación formal del adquiriente del producto, la identificación, en su caso, del titular real de la relación de negocio, así como la obtención de información/documentación sobre el propósito o índole de dicha relación, la cual pondrá a disposición de [La Sociedad].
>
> A la firma del presente contrato [La Sociedad] hace entrega del Manual de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo de [La Sociedad] que [La entidad Comercializadora/comercial/agente] recibe, cuyas normas y procedimientos se obliga a aplicar, de acuerdo con las funciones encomendadas en el presente contrato. [La Sociedad] le hará entrega de cualesquiera actualizaciones que de dichas Normas acontezca durante la vigencia del presente contrato. En caso de incumplimiento grave o sistemático de los procedimientos previstos en las presentes Normas, [La Sociedad] podrá terminar la relación contractual con el Agente."

4.3 Aprobación y entrada en vigor

El presente Manual de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo será aprobado por el Órgano de Control Interno de SEGURA por unanimidad. No obstante, su entrada en vigor no tendrá lugar hasta su ratificación por los cualquiera de los dos (2) administradores solidarios de SEGURA.

El estudio de su cumplimiento le corresponderá asimismo al Órgano de Control Interno, que propondrá las modificaciones y actualizaciones que considere necesarias, que en todo caso, deberán ser aprobadas por el Consejo de Administración por mayoría simple.

4.4 Disponibilidad

El presente Manual debe estar a disposición de todos los empleados, directivos, agentes y colaboradores de SEGURA.

Además, el Manual está a disposición del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y se podrá remitir voluntariamente al mismo, a efectos de que por éste se determine la adecuación de las medidas de control interno establecidas o que se propongan establecer. El OCI o el Consejo de Administración decidirán qué versiones del Manual deben ser enviadas al SEPBLAC.

5. ÓRGANOS DE CONTROL INTERNO

5.1 Órgano de Administración

Los administradores solidarios de SEGURA de forma colegiada son los supervisores e impulsores de las Políticas de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo de SEGURA. Sus funciones en esta materia se resumen en:

- Aprobación de las políticas en materia de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Aprobación de las altas y bajas en la composición de los miembros del Órgano de Control Interno (en adelante, "**OCI**").

- Nombramiento del Representante ante el Servicio Ejecutivo.

- Ser informado de las principales deficiencias y recomendaciones propuestas en el informe de experto externo en el plazo máximo de tres (3) meses desde la fecha de emisión de dicho informe y adoptar las medidas necesarias para solventar las deficiencias identificadas.

- Adoptar y dotar, en su caso, las medidas necesarias para solventar las deficiencias identificadas en el informe anual de experto externo, y/o en los informes que se emitan semestralmente desde el departamento de Auditoría Interna de la Sociedad.

5.2 Órgano de Control Interno

El OCI será el órgano encargado de la aplicación de las políticas y procedimientos establecidos en las presentes Normas, actuando con independencia funcional de los distintos órganos de la Sociedad. No obstante, dependerá jerárquicamente del órgano de administración de la Sociedad.

5.2.1 Composición del Órgano de Control Interno

El OCI estará integrado por tres (3) miembros que deberán ser elegidos de entre los empleados de SEGURA que ostenten cargos de administración o dirección en la misma, recayendo, asimismo, en uno de ellos el cargo de Representante Principal de la entidad ante el SEPBLAC.

El OCI estará compuesto por los siguientes miembros:

- D. Demetrio Segura Martín
- Dª. Paloma García xxxxxxx
- D. Jesús Redondo Martín

El Consejo de Administración de la Sociedad será el órgano encargado del nombramiento de los miembros que componen el OCI, así como de la destitución de cualquiera de ellos, debiendo, en este caso, motivarse dicho cese en el cargo.

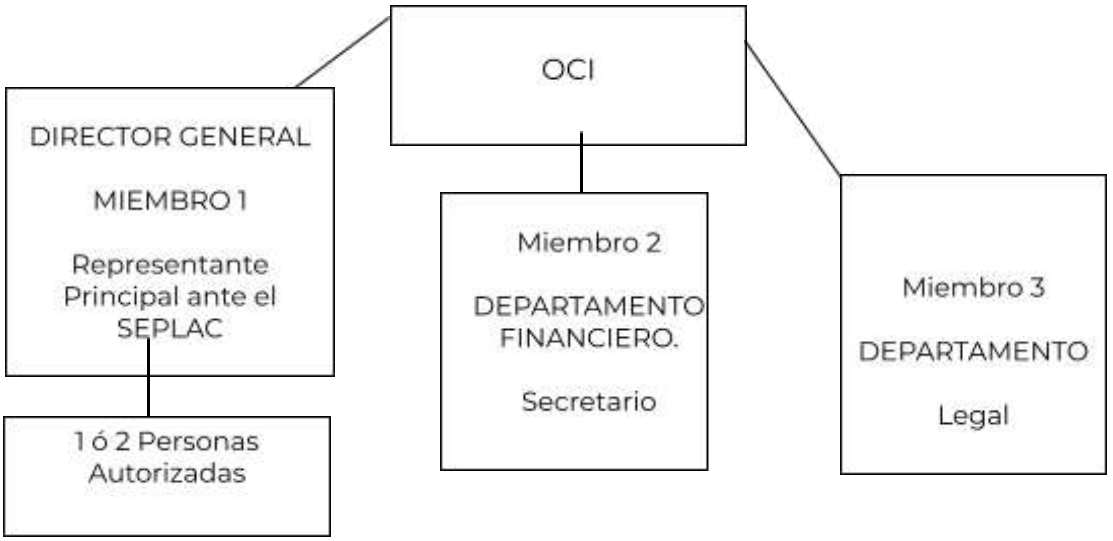
El Representante Principal de SEGURA ante el SEPBLAC podrá nombrar una o dos personas autorizadas para asistirle en sus funciones.

El OCI nombrará como Secretario del OCI a la persona del Departamento Financiero designada como miembro. El Secretario del OCI se encargará de asistir a sus miembros en el cumplimiento puntual de las obligaciones de recepción de solicitudes de los empleados y/o colaboradores de SEGURA, así como en todas aquellas cuestiones que tanto el OCI como el Representante Principal de la entidad consideren necesario.

El Secretario designará, si así se requiriera, al personal auxiliar o Unidad Técnica (en adelante, "personal auxiliar") que le asista en el ejercicio de sus funciones. Dicho personal auxiliar contará con formación adecuada en materia de análisis para la prevención del blanqueo de capitales y/o la financiación del terrorismo. En el supuesto de que la Sociedad supere en volumen de negocios anual la cifra de 50 millones de Euros o su balance general anual excediera de 43 millones de Euros, contará con un personal auxiliar con dedicación exclusiva en la materia objeto de las presentes Normas.

El personal auxiliar se encargará del cumplimiento puntual de las obligaciones de archivo y conservación de la documentación relativa a la obtención de los registros públicos y/o privados correspondientes, de la información de Clientes que los empleados y/o colaboradores de SEGURA requieran, así como de aquellas cuestiones administrativas que el OCI o el Secretario consideren necesarios.

Estructura orgánica del OCI:



La dirección para notificaciones a los miembros del OCI, su Secretario y el personal auxiliar será:

Correo electrónico: oci@seguraehijos.es

5.2.2 Competencias del Órgano de Control Interno

Las competencias del OCI son las siguientes:

- Establecer la estrategia global de la Sociedad sobre prevención del blanqueo de capitales y de la financiación del terrorismo.

- Coordinar a todos los empleados, directivos, agentes y colaboradores que por razón de su actividad en la Sociedad puedan verse involucrados en las anteriores actividades.

- Vigilar todas las actuaciones de la Sociedad que pudieran estar relacionadas con el blanqueo de capitales y/o la financiación del terrorismo.

- Vigilar la permanente actualización del sistema, la práctica de pruebas que examinen su solidez y fiabilidad, la realización de cursos y reuniones de coordinación en esta materia, y el cumplimiento por parte de los agentes, comisionistas o intermediarios, de aquellos aspectos de las presentes Normas que les sean de aplicación.

- En cumplimiento de lo establecido en el Reglamento de desarrollo de la Ley 10/2010, analizar con criterios de seguridad, rapidez, eficacia y coordinación, tanto en la comunicación interna, como la que fuere pertinente al SEPBLAC, aquellas operaciones de riesgo, anormales, inusuales y potencialmente indicativas de actividades de blanqueo de capitales y/o financiación del terrorismo, detectadas por los empleados, colaboradores o por las aplicaciones informáticas, que, en su caso, existieren implantadas en la Sociedad, especialmente diseñadas al efecto o por cualquier otro medio.

- Proponer el nombramiento y contratación del experto independiente.

- Proponer ante órgano de Administración de SEGURA el nombramiento de Representante Principal ante el SEPBLAC.

- Velar por el cumplimiento de las siguientes obligaciones en materia de blanqueo de capitales y/o financiación del terrorismo:

    - ✔ Examinar con especial atención cualquier operación que por razón de su cuantía o naturaleza pueda estar particularmente relacionada con el blanqueo de capitales y/o la financiación del terrorismo.

    - ✔ Comunicar al SEPBLAC cualquier operación o hecho respecto del que existan indicios razonables de que está relacionado con el blanqueo de capitales y/o la financiación de actividades terroristas, así como cualquier petición que reciban en la que el ordenante, emisor, titular, beneficiario o destinatario sea una persona o entidad vinculada a organizaciones terroristas o exista algún indicio racional de que está relacionado con ellas.

- ✔ Facilitar a la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y a sus órganos de apoyo la información que requieran en el ejercicio de sus facultades.

- ✔ Procurar, en lo posible, que no se lleva a cabo ninguna operación sobre la que pudieran existir indicios de estar relacionada con el blanqueo de capitales y/o la financiación de actividades terroristas, sin haber efectuado previamente la comunicación prevista al SEPBLAC.

- ✔ No revelar al Cliente ni a terceros que se ha transmitido información al SEPBLAC o que se está examinando alguna presunta operación de estas características.

- ✔ Establecer procedimientos y órganos adecuados de control interno y de comunicación, a fin de prevenir e impedir la realización de operaciones relacionadas con personas y entidades vinculadas a organizaciones terroristas.

- Informar puntualmente al órgano de administración de la Sociedad en materia de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, y, en todo caso, siempre que dicho órgano así lo requiera.

En cuanto a las competencias del Secretario, éste tiene la obligación de informar –a la mayor brevedad- al OCI acerca de cualquier operación sospechosa de blanqueo de capitales y/o de financiación del terrorismo de la que tenga constancia o noticia, y que le hubieran trasmitido las sucursales, filiales o participadas sujetas al ámbito de aplicación objetiva y subjetiva de las presentes Normas. Ello, con el fin de que el citado Órgano, pueda analizar la operación y decidir sobre la necesidad de que el Representante Principal de la entidad ante el SEPBLAC comunique la operación sospechosa al citado Servicio Ejecutivo.

Asimismo, el Secretario informará al OCI de la Sociedad acerca de cualquier cuestión que estime relevante en materia de Prevención del Blanqueo de Capitales y/o de Financiación del Terrorismo y que considere oportuno elevar y someter al citado Servicio, mediante la remisión de un informe provisional.

5.2.3 Reuniones del Órgano de Control Interno

El OCI se reunirá siempre que las circunstancias así lo demanden y, al menos, una vez cada tres (3) meses, debiendo asistir obligatoriamente a tales reuniones la totalidad de sus miembros, el Representante Principal, la persona o personas autorizadas por el mismo y el Secretario de dicho OCI. Las decisiones que se adopten por el OCI lo serán por mayoría absoluta.

El Secretario del OCI será el encargado de convocar las reuniones del OCI y de proponer el Orden del Día de las reuniones, debiéndose ratificar el mismo previamente por el Representante Principal de la entidad ante el SEPBLAC.

En dichas reuniones se podrá analizar cualquier cuestión que los asistentes consideren oportuno, y, en concreto deberán:

- Analizar toda incidencia comunicada incluidas las de posible detección de operación sospechosa.

- Analizar la eficacia y efectividad de los procedimientos implantados en la Sociedad para detección de operaciones sospechosas.

- Promover cualquier medida de mejora y/o modificación atendiendo a los cambios legislativos o por cualesquiera otras circunstancias que se estimen pertinentes.

- Analizar cualquier medida que el OCI establezca que se deba implantar en la Sociedad, adoptando los medios necesarios a estos efectos.

De las reuniones celebradas por el OCI se levantará un Acta con las conclusiones alcanzadas, la cual será redactada por el Secretario, debiendo ser firmada por todos los asistentes al final de la reunión. En el mismo Acta se consignarán los asistentes y se incluirá un apartado denominado "Requerimientos de Información", en el que se detallará, lo más posible, los requerimientos de información que hubiera recibido la Sociedad tanto del SEPBLAC como de cualquier otro organismo, así como la respuesta dada por la Sociedad al mismo. De las Actas aprobadas se guardará oportuno archivo por plazo de diez años.

Por motivos de urgencia de las materias a tratar cabe la convocatoria de una reunión extraordinaria del OCI tanto por parte del Representante Principal de la Sociedad ante el SEPBLAC, como por parte de cualquier miembro del mencionado Órgano, así como por el órgano de administración.

En la convocatoria de la reunión extraordinaria la persona convocante deberá exponer los motivos de la urgencia de la reunión y de la necesidad o no de asistencia de todos los miembros que componen el OCI.

La convocatoria podrá realizarse por correo electrónico, fax o cualquier otro medio que deje constancia documental tanto de su envío por el convocante como de su recepción por el convocado.

Por su contenido, los asuntos, deliberaciones y acuerdos del OCI están sujetos al deber de confidencialidad, sin perjuicio de las comunicaciones que se acuerde emitir o de la puesta en conocimiento de la Autoridad Judicial y/o Gubernativa de cuantos actos e informaciones fueran requeridos por aquéllas o de obligada o conveniente comunicación de acuerdo con lo establecido en el presente Manual para la salvaguarda de su responsabilidad.

Toda comunicación de asuntos, informes, datos o acuerdos en materias tratadas por el OCI o de su competencia, incluirá una mención expresa al destinatario sobre su deber de confidencialidad al respecto de la información y/o documentación trasladada.

5.2.4 Procedimientos internos

El OCI será el responsable y tendrá la obligación de examinar cualquier tipo de operación que, atendiendo a los criterios de la Ley 10/2010 y normativa de desarrollo, pudiera tener la consideración de sospechosa, con independencia de que el Cliente sea persona física o jurídica.

Los empleados, directivos, agentes o colaboradores que quieran someter al juicio del OCI una operación, por considerar que existen indicios de estar relacionada con el blanqueo de capitales y/o la financiación del terrorismo, así como cualquier cuestión relacionada con la identificación de Clientes o el examen de cualesquiera operaciones, se dirigirán al mismo a través del Coordinador Interno mediante comunicación escrita, y, en todo caso, en un plazo no superior a cuarenta y ocho (48) horas, cumplimentando el Modelo que se adjunta como **Anexo III**, adjuntando la documentación necesaria para su análisis.

En el caso de las sucursales, filiales o participadas, que se hallen dentro del ámbito de aplicación del presente Manual, la comunicación -que deberá cumplir los mismos requisitos formales- será remitida por el empleado o colaborador en un plazo no superior a a cuarenta y ocho (48) horas, al Coordinador Interno. A su vez, el Coordinador Interno se encargará de remitir la comunicación con la documentación adjunta al OCI.

Una vez recibida la comunicación por el OCI, ésta será remitida, si fuera necesario, al Secretario del OCI, quien emitirá un informe provisional en el plazo máximo de diez (10) días hábiles que será sometido a votación en reunión del OCI.

El OCI estudiará pormenorizadamente el informe provisional emitido por su Secretario de la comunicación efectuada por el empleado o colaborador de la Sociedad y de la documentación anexa a la misma, determinando la necesidad o no de proceder a comunicar una operación, hecho o incluso una mera tentativa sospechosa de estar vinculada con el blanqueo de capitales y/o la financiación del terrorismo al SEPBLAC. En todo caso, el OCI siempre deberá comunicar toda operación que muestre una falta de correspondencia ostensible con la naturaleza, volumen de actividad o antecedentes operativos de los Clientes, si no se apreciara justificación económica, profesional o de negocio para la realización de dicha operación.

La decisión adoptada por el OCI en cuanto a la comunicación o no de una operación sospechosa de estar relacionada con el blanqueo de capitales y/o la financiación del terrorismo se plasmará en un informe escrito definitivo.

Dicho informe definitivo será oportunamente comunicado al empleado o colaborador que formuló la consulta en el plazo máximo de veinte (20) días hábiles, desde la recepción por el OCI de la comunicación del empleado o colaborador, debiendo informarle del curso dado a su comunicación y de las concretas actuaciones a seguir.

Se guardará archivo de todo lo actuado, adjuntándose copia al expediente del Cliente.

5.3 Representante Principal ante el SEPBLAC

El cargo de Representante Principal de la entidad ante el SEPBLAC deberá ser desempeñado por quien ostente una posición de dirección o cargo de administración en SEGURA.

Dicho nombramiento deberá ser aprobado por mayoría simple en el seno del Consejo de Administración u órgano de administración de SEGURA, y el cargo tendrá que ser debidamente aceptado.

El nombramiento del Representante Principal será notificado al SEPBLAC mediante carta, a la que se adjuntará:

- Certificación del Acta del órgano de administración en el que se aprobó y aceptó el nombramiento del Representante Principal de la entidad ante el SEPBLAC.

- Fotocopia del DNI del Representante.

- Currículum vitae del representante en el que se acredite tener conocimientos en materia de Prevención del blanqueo de Capitales y de la Financiación del Terrorismo.

- Formulario F22 debidamente cumplimentado.

Se adjunta a las presentes Normas como **Anexo IV**, Modelo de comunicación al SEPBLAC de nombramiento de Representante Principal.

Las filiales y participadas sujetas al ámbito de aplicación objetiva y subjetiva de las presentes Normas, seguirán el mismo procedimiento de nombramiento de sus respectivos Representantes Principales ante el SEPBLAC.

5.3.1 Funciones del Representante Principal ante el SEPBLAC

Son funciones del Representante Principal ante el SEPBLAC:

- Ostentar la representación de la Sociedad en las comunicaciones existentes entre la misma y la Comisión de Prevención del Blanqueo de Capitales y sus órganos de apoyo y otras autoridades.

- Formar parte del OCI de la Sociedad como miembro del mismo, presidiendo las reuniones.

- Potestad de control del cumplimiento de las competencias y funciones que tiene atribuidas el OCI.

- Comparecer en la totalidad de procedimientos administrativos o judiciales relacionados con las comunicaciones que en materia de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo se hayan efectuado a la Comisión de Prevención del Blanqueo de Capitales y sus órganos de apoyo y otras autoridades.

- Coordinar las actividades a realizar por la Sociedad en la Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo y promover las mejoras necesarias.

- Seguimiento y estudio de las modificaciones normativas en materia de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, así como de las técnicas y métodos más novedosos en la detección de las operaciones sospechosas de estar relacionadas con el blanqueo de capitales y/o la financiación del terrorismo.

- Asistencia a las reuniones a las que sea convocado por el SEPBLAC con finalidad consultiva o informativa.

- Ratificación del Orden del Día de las reuniones del OCI propuesto por el Secretario del OCI.

- Mantener informado puntualmente al Consejo de Administración de cualquier circunstancia que pudiera alterar o determinara la necesidad de modificar la política de prevención del blanqueo de capitales y/o de la financiación del terrorismo.

Todas las funciones del Representante Principal de la entidad ante el SEPBLAC son delegables. Las funciones y atribuciones de la persona o personas autorizadas por el Representante Principal de la entidad ante el SEPBLAC serán las designadas por éste en el momento de su nombramiento, debiendo constar éstas por escrito.

En caso de delegación, se mantiene la responsabilidad del Representante ante el SEPBLAC.

5.4 Persona Autorizada por el Representante Principal

Con el fin de asegurar en todo momento la posibilidad de comunicación entre el SEPBLAC y SEGURA, y teniendo en cuenta la condición del Representante Principal, que ostenta además cargo de administración o dirección en la Sociedad, podrá ser nombrada por éste una persona autorizada para que actúe en su nombre ante dicho Servicio.

La designación de la persona autorizada por el Representante Principal de la entidad deberá hacerse en soporte escrito y deberá estar firmada por ambas personas, Representante Principal y autorizado, comunicando éste su aceptación en el cargo.

El Representante Principal podrá autorizar hasta un máximo de dos personas, y su nombramiento tendrá duración indefinida.

El Representante Principal procederá a comunicar al SEPBLAC la identidad de la persona a quien concede la facultad de obrar en su nombre, quien igualmente deberá comunicar su aceptación. Por cada persona que autorice o apodere deberá enviar al SEPBLAC un formulario F22-6 debidamente cumplimentado y firmado.

Se adjunta modelo de comunicación por el Representante Principal de persona autorizada ante el SEPBLAC como **Anexo V**.

Asimismo, deberá comunicarse por el Representante Principal inmediatamente al SEPBLAC cualquier modificación en la condición de la persona autorizada, tanto su revocación, sustitución u otras circunstancias, mediante carta firmada por dicho Representante, desplegando plenos efectos desde su recepción por dicho Servicio.

Los actos realizados por la persona o personas autorizadas se entenderán hechos por el propio Representante Principal, tanto a efectos internos como externos.

6. POLÍTICA DE ADMISIÓN DE CLIENTES

La Sociedad dispone de una política expresa de admisión de Clientes que es de obligado cumplimiento para las personas físicas y jurídicas referidas en el apartado 4.2 del presente Manual.

La política de admisión de Clientes de la Sociedad se ha elaborado teniendo en cuenta un enfoque de riesgo basado, tanto en las características de sus clientes como en la actividad social desarrollada.

6.1 Clientes no admitidos

Por motivos del control del riesgo de blanqueo de capitales y de la financiación del terrorismo, no serán clientes de SEGURA aquellas personas que se incluyan en alguna de las siguientes categorías:

- Personas incluidas en las listas de terroristas u otras listas oficiales, en los que se detecte o pueda haber indicios de riesgo de blanqueo de capitales (ver procedimiento detallado sobre análisis de listas terroristas en el apartado 6.3).

  A tales efectos, se adjunta listado de personas, grupos y sociedades consideradas por la Unión Europea como relacionadas con actividades terroristas como **Anexo VI.**

- Personas sobre las que se disponga de alguna información de la que se deduzca que pueden estar relacionadas con actividades delictivas, especialmente aquellas supuestamente vinculadas al narcotráfico, al terrorismo o al crimen organizado.

- Personas que tengan negocios cuya naturaleza haga imposible la verificación de la legitimidad de las actividades o la procedencia de los fondos.

- Personas que rehúsen facilitar la información o la documentación requerida o se sospechara de la veracidad de la misma.

- Personas que rehúsen entregar la documentación que permita realizar una plena identificación del titular real, o que habiéndola entregado se nieguen a que la Sociedad obtenga una copia de su documento identificativo.

- Personas que aporten a la Sociedad documentos manifiestamente falsos o que susciten serias dudas sobre su legalidad, legitimidad, no manipulación, etc.

- Personas que rehúsen facilitar información o la documentación requerida relativa tanto para obtener la verificación de las actividades declaradas o la procedencia de los fondos, como acerca del propósito y naturaleza de la relación comercial con SEGURA.

- Clientes cuya actividad comercial esté sujeta a la concesión de autorización administrativa para operar (en especial la explotación de casinos, máquinas de juego, apuestas u otros juegos de azar, cambio de moneda o divisas y gestión de transferencias) y que no dispongan de dicha autorización administrativa.

- Clientes que soliciten abrir o mantener cuentas anónimas o con nombres ficticios, en los que no quede registrado el titular real.

- Bancos Pantalla ("Shell Banks"), es decir entidades financieras con actuación en países o territorios donde no tengan presencia física y que no pertenezcan a un Grupo Financiero regulado. Esta prohibición se hace extensiva a las entidades financieras que operen con ellos, y específicamente, a las que mantengan cuentas de corresponsalía con los citados bancos-pantalla.

- Personas a las que no se puedan aplicar las medidas de diligencia debida descritas en este Manual. Cuando se aprecie esta imposibilidad en el curso de la relación de negocios, la Sociedad pondrá fin a la misma, procediendo a realizar el examen especial de operaciones. La negativa a establecer relaciones de negocio, a ejecutar operaciones o la finalización de la relación de negocios por imposibilidad de aplicar las medidas de diligencia debida no conllevará, salvo que medie enriquecimiento injusto, ningún tipo de responsabilidad para SEGURA.

- Personas jurídicas cuya estructura de propiedad o de control no pueda determinarse y en especial, sociedades nacionales o extranjeras cuyas acciones estén representadas mediante títulos al portador. No obstante, de manera excepcional, se podrá admitir este tipo de clientes siempre y cuando lo autorice de manera expresa y personalizada el OCI.

6.2 Clientes admitidos

Las personas no consideradas en el apartado anterior podrán ser admitidas como clientes en el momento en el que se apliquen las medidas de diligencia debida en cuanto a identificación formal, identificación del titular real y conocimiento del propósito e índole de la relación de negocios.

No obstante, será sometido al control del OCI al inicio de la relación de negocio, o previamente si el empleado, directivo, agente o colaborador de la Sociedad observan elementos de riesgo, todos aquellos clientes considerados de riesgo medio y alto (tal y como se definen en el apartado 6.4 de este Manual).

6.3 Chequeo de Terroristas

La Sociedad chequeará periódicamente las listas oficiales de terroristas.

Esta revisión se realizará con carácter mensual se revisará por el personal del OCI. En caso de coincidencia positiva se informara al Consejo de Administración, y, además, en el caso de que se detecte algún indicio de riesgo de blanqueo de capitales se remitirá la información al Servicio Ejecutivo.

6.4 Tipología de Clientes atendiendo al riesgo que presentan

La política de admisión de clientes es gradual e incluye una descripción detallada de aquellos que implican un mayor riesgo de blanqueo de capitales y financiación del terrorismo. Esta clasificación se hace en base a distintos parámetros, tal y como se describe detalladamente a continuación:

- Se consideran **Clientes de riesgo alto**, aquéllos que, tras efectuar los exámenes previos y obligatorios recogidos en las presentes Normas, se tengan indicios de poder estar relacionados con el Blanqueo de Capitales y/o la Financiación del Terrorismo y, por tanto, se haya dirigido comunicación al OCI para que autorice la suscripción o no de la operación, y en cualquier caso todos aquellos que reúnan las características descritas en los **Anexos VII** y **VIII** de las presentes Normas. En concreto:

  - ✔ Personas físicas o jurídicas con nacionalidad de territorios designados o paraísos fiscales o países no cooperantes.
  - ✔ Personas físicas o jurídicas cuya actividad es de alto riesgo (Se adjunta descripción como **Anexo VIII**).
  - ✔ Personas con Responsabilidad Pública extranjeras.
  - ✔ Personas físicas o jurídicas que por su operativa así lo determine el OCI.

  En estos casos, además de las medidas normales de diligencia debida, se aplicarán las medidas reforzadas descritas en el apartado 7.3 de las presentes Normas, se obtendrá la autorización del OCI con carácter previo a ejecutar la operación con el Cliente, y se adoptarán las medidas adecuadas para determinar el origen del patrimonio y de los fondos con los que se llevará a cabo la operación.

- Se consideran **Clientes de riesgo medio** y, por tanto, no existirá con respecto a los mismos la obligación de obtener la autorización previa y por escrito del OCI para concluir una operación con estos, todos aquellos que no reúnan las características descritas en los **Anexos VII** y **VIII** de las presentes Normas. En concreto:

  - ✔ Personas jurídicas de nacionalidad no UE.
  - ✔ Personas físicas o jurídicas residentes en un país no UE.
  - ✔ Personas físicas o jurídicas cuya actividad es de riesgo medio. Se adjunta descripción como **Anexo IX**).
  - ✔ Personas con Responsabilidad Pública nacionales.

  En estos casos se aplicarán las medidas normales de diligencia debida y en caso de detectarse a raíz de aplicar estas medidas cualquier indicio de estar la operación relacionada con el blanqueo de capitales y/o la financiación del terrorismo, se procederá de inmediato a la aplicación de las medidas reforzadas previstas en el apartado 7.3 de las presentes Normas.

- Se consideran **Clientes de riesgo bajo** el resto de Clientes que no reúnen las anteriores características, y en particular, los descritos en el apartado 7.2 del

presente Manual. Les será de aplicación las medidas simplificadas de diligencia debida para concluir una operación con éstos.

El empleado y/o colaborador en todo caso deberá acreditar documentalmente y archivar conforme a lo recogido en el apartado 7.4 de las presentes Normas, la documentación acreditativa de la aplicación de estas excepciones.

Asimismo, será obligatorio actualizar toda la información recabada en la primera toma de contacto con el Cliente si ocurriera algún hecho público notorio relacionado con el mismo que incida en la tipología de Cliente, y en cualquier caso, con anterioridad a la firma de cualquier nuevo documento con el mismo.

7. MEDIDAS DE DILIGENCIA DEBIDA

La Sociedad ha adoptado medidas de diligencia debida de identificación formal de sus clientes.

No obstante, podrá determinar el grado de aplicación de las anteriormente citadas medidas en función del riesgo. A tales fines, la Sociedad ha establecido medidas de diligencia debida de carácter normal, simplificada y reforzada.

Se deberán aplicar siempre medidas de diligencia reforzada a Clientes de riesgo alto y cuando concurran indicios de blanqueo de capitales o de financiación del terrorismo, con independencia de cualquier excepción, exención o umbral, o cuando existan dudas sobre la veracidad o adecuación de los datos obtenidos con anterioridad. En estos casos siempre, y si es posible de forma previa, se debe informar al OCI, proporcionando toda la información disponible y los indicios que se tienen.

Las medidas de diligencia debida se aplicarán en función del riesgo, tanto a los nuevos Clientes como a los Clientes existentes. SEGURA no establecerá relaciones de negocio ni ejecutarán operaciones cuando no puedan aplicar las medidas de diligencia debida. Cuando se aprecie la imposibilidad en el curso de la relación de negocios, se pondrá fin a la misma, procediendo a realizar el examen especial al que se refiere el apartado 8.2 del Manual.

7.1 Medidas normales de diligencia debida de carácter normal:

7.1.1 Identificación formal del Cliente

El empleado, directivo, agente y/o colaborador identificará a cuantas personas físicas o jurídicas pretendan establecer relaciones de negocio (incluidos los minoristas oficiales y los no oficiales), antes de suscribir cualquier documento generador de obligaciones para las partes intervinientes.

En todo caso, los empleados, directivos, agentes y/o colaboradores se abstendrán de concluir relaciones de negocio o realizar operaciones con Clientes personas físicas y/o jurídicas que no hayan sido debidamente identificadas. A tal efecto serán de obligatoria cumplimentación por cada empleado o colaborador los modelos que a efectos de identificación del Cliente se anexan a las presentes Normas como **Anexos X** y **XI**.

En el caso de **personas físicas**, se exigirá al Cliente que facilite:

- La siguiente información:

  ✔ Nombre y dos apellidos
  ✔ Número de Documento Nacional de Identidad (DNI) o pasaporte

  En el caso de ciudadanos de nacionalidad extranjera se exigirá:

  ✔ Tarjeta de Residencia, la Tarjeta de Identidad de Extranjero o el Pasaporte
  ✔ El documento, carta o tarjeta oficial de identidad personal expedido por las autoridades de algún país de la Unión Europea

- ✔ Documento de identidad expedido por el Ministerio de Asuntos Exteriores y de Cooperación para el personal de las representaciones diplomáticas y consulares de terceros países en España

Excepcionalmente, los sujetos obligados podrán aceptar otros documentos de identidad personal expedidos por una autoridad gubernamental siempre que gocen de las adecuadas garantías de autenticidad e incorporen fotografía del titular.

- ✔ Fecha de expedición y fecha de caducidad del documento de identificación
- ✔ Fecha de nacimiento
- ✔ Género (Masculino / Femenino)
- ✔ Nacionalidad
- ✔ País de residencia (Domicilio, Código Postal, Localidad)
- ✔ Dirección de email (opcional)
- ✔ Teléfono fijo (opcional) y/o Teléfono móvil (con carácter obligatorio)
- ✔ Propósito de la relación negocial a suscribir con la Sociedad
- ✔ Actividad empresarial o profesional desarrollada

- La siguiente documentación en vigor que, en todo caso, deberá facilitar en copia o remitir escaneada:

  - ✔ Documento de identificación fehaciente de la persona física (DNI, Pasaporte, permiso de residencia expedido por el Ministerio del Interior, NIE) en los términos que se expondrán en el apartado 7.1.3 del Manual.
  - ✔ Declaración expresa del Cliente justificativa de la profesión/actividad desarrollada.

En el caso de **personas jurídicas**, se exigirá al Cliente:

- La siguiente información:

  - ✔ Denominación social y forma jurídica
  - ✔ Domicilio, Código Postal, Localidad
  - ✔ Objeto social
  - ✔ Actividad empresarial o profesional desarrollada
  - ✔ Identidad de sus administradores.

  En el caso de personas jurídicas de nacionalidad española, será admisible, a efectos de identificación formal, certificación del Registro Mercantil, aportada por el Cliente u obtenida mediante consulta telemática.

- La siguiente documentación en vigor que, en todo caso, deberá ser facilitada en copia o remitir escaneada y cuya vigencia deberá acreditarse mediante una declaración responsable del Cliente:

- ✔ Documento fehaciente acreditativo de su denominación social y forma jurídica. A estos efectos, se solicitará la escritura de constitución de la sociedad y los estatutos.
- ✔ N.I.F.
- ✔ Poder o documento público otorgado a favor de la persona/as que actúe/en nombre de la persona jurídica. Será admisible la comprobación mediante certificación del Registro Mercantil Provincial aportada por el cliente u obtenida mediante consulta telemática.

o jurídica, deberá aportar al menos un documento de los señalados en el **Anexo XII**.

7.1.2 Comprobación

En el caso de que el Cliente sea una persona jurídica, la Sociedad obtendrá información comercial de la actividad a la que se dedica, y verificará la veracidad de la información societaria y comercial facilitada por el Cliente, a través de los registros públicos y/o privados correspondientes

7.2 Medidas simplificadas de diligencia debida

Habida cuenta del ámbito objetivo de aplicación de las presentes Normas (artículo 38 de la Ley), no procede la aplicación de medidas simplificadas a ningún cliente.

7.3 Medidas reforzadas de diligencia debida

Habida cuenta del ámbito objetivo de aplicación de las presentes Normas (artículo 38 de la Ley), no procede la aplicación de medidas reforzadas a ningún cliente.

8. COMUNICACIÓN INTERNA. EXAMEN ESPECIAL.

8.1 Comunicación de los empleados o colaboradores al OCI

Los empleados, directivos, agentes y/o colaboradores que consideren que, tras la identificación del Cliente y del examen de la operación en la que intervengan, existen indicios o certeza de que aquél o la operación están relacionados con el blanqueo de capitales y/o la financiación del terrorismo, deberán comunicarlo inmediatamente por escrito al OCI.

La comunicación incluirá los datos que permitan identificar al sujeto, los hechos u operaciones, la cuantía, el lugar y las fechas. La comunicación al OCI contendrá copia de los documentos de identificación y descripción de la operación sospechosa. Se realizará de forma inmediata por los empleados o colaboradores a su conocimiento, aun cuando no haya sido concluida finalmente la operación. El notificante guardará copia de la comunicación hecha al OCI.

La comunicación será confidencial y los medios por los que se enviará la notificación escrita al OCI por el empleado o colaborador, podrán variar según los casos (correo electrónico, valija interna, etc.).

En caso de duda, y como criterio general, el empleado o colaborador consultará con el OCI cualquier operación sospechosa o inusual que, en su opinión, pudiera tener relación con el blanqueo de capitales y/o la financiación del terrorismo. La consulta se efectuará utilizando los mismos cauces que para la comunicación de una operación sospechosa, debiendo indicar en el documento tal circunstancia.

Se adjunta como **Anexo III** el modelo de comunicación interna al OCI de operaciones sospechosas de estar relacionadas con el Blanqueo de Capitales y/o la Financiación del Terrorismo.

8.2 Examen Especial.

Una vez que el OCI haya recibido una comunicación de incidencia se acusará recibo al empleado o colaborador comunicante y se procederá a su inmediato análisis o comprobación para determinar la relación de los hechos u operaciones con el blanqueo de capitales y/o la financiación del terrorismo.

La decisión adoptada se reflejará en un informe escrito al que se unirá copia de toda la documentación analizada y se archivará y guardará conforme se indica en el apartado 7.4 de las presentes Normas. El informe deberá contener los oportunos razonamientos de la decisión adoptada, que podrá observar la necesidad de comunicar la operación sospechosa al SEPBLAC.

Además, el informe deberá contener los siguientes apartados:

- Relación e identificación de las personas físicas o jurídicas que participen en la operación y el concepto de su participación en ella.

- La actividad conocida de las personas físicas o jurídicas que participen en la operación, y la correspondencia entre la actividad y las operaciones realizadas.

- Relación de las operaciones y fechas a las que se refieran, con indicación de su naturaleza, moneda en que se realice, cuantía, lugar o lugares de ejecución, finalidad e instrumentos de pago o cobro utilizados.

- Las gestiones realizadas para investigar las operaciones sospechosas.

- Exposición de las circunstancias de toda índole de las que pueda inferirse el indicio o certeza de vinculación con el blanqueo de capitales y/o la financiación del terrorismo, o que pongan de manifiesto la falta de justificación económica, profesional o de negocio para la realización de las actividades.

- Descripción de las medidas tomadas en relación con los sujetos intervinientes en la operativa con indicios de estar relacionados con el blanqueo de capitales y/o la financiación del terrorismo comunicada. En caso de haber continuado con la relación de negocios, expresión de los motivos de haberse adoptado tal decisión, identificando la persona, órgano o departamento de la Sociedad que lo hubiera adoptado.

- Cualesquiera otros datos o circunstancias relevantes para la prevención del blanqueo de capitales y la financiación del terrorismo.

- Propuesta de comunicación por indicios al SEPBLAC.

8.3 Gestión

De la decisión adoptada sobre el curso dado a su comunicación, se informará cumplidamente por el OCI al empleado o colaborador comunicante, y ello, en un plazo no superior a veinte (20) días hábiles desde la recepción de la comunicación efectuada por el empleado o colaborador.

En el supuesto de que habiendo dado traslado un empleado, directivo, agente o colaborador de la Sociedad de una comunicación de operación sospechosa de estar vinculada con el blanqueo de capitales y/o la financiación del terrorismo, no se informara a éste del curso dado a la misma transcurrido el plazo de veinte (20) días mencionado en el párrafo anterior -desde la recepción de la comunicación por parte del OCI-, podrá el empleado, directivo, agente o colaborador dirigir dicha comunicación directamente al SEPBLAC. De lo actuado se guardará expediente conforme se indica en el apartado 7.4 anterior.

9. COLABORACIÓN CON LA COMISIÓN DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y SUS ÓRGANOS DE APOYO

El OCI de SEGURA, a través de su Representante Principal ante el SEPBLAC, colaborará facilitando toda la documentación e información que la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, sus órganos de apoyo u otras autoridades legalmente competentes les requieran para el ejercicio de sus competencias.

Asimismo, la Sociedad colaborará con la mencionada Comisión y con las autoridades legalmente competentes comunicándoles por propia iniciativa o por requerimiento previo, cualquier hecho u operación que le haya sido notificado previamente por el personal de SEGURA, sus directivos, agentes o colaboradores, respecto de la cual exista indicio o certeza de que está relacionado con el blanqueo de capitales y/o la financiación del terrorismo.

9.1 Comunicación por iniciativa propia

El procedimiento que se habrá de seguir para efectuar las mencionadas comunicaciones por iniciativa propia, será el indicado en el apartado 8 de las presentes Normas.

La comunicación será confidencial y contendrá, como mínimo, la información a la que alude el informe de Examen Especial del apartado 8.2 del Manual.

Se adjunta como **Anexo XII** el Modelo de comunicación de operación sospechosa de blanqueo de capitales y/o financiación del terrorismo al SEPBLAC. En todo caso, cabe consultar el Modelo de Formulario F19 en la página web **www.sepblac.es**.

9.2 Comunicación a requerimiento del SEPBLAC

El procedimiento que seguir en el caso de recepción por la Sociedad de un requerimiento de información del SEPBLAC o de cualquier otro órgano o autoridad legalmente competentes, respecto de la que exista la obligación legal de contestar, será el siguiente:

- El empleado o colaborador que reciba el requerimiento, lo enviará inmediatamente al OCI, debiéndo quedar siempre copia del documento enviado.

- El OCI analizará el requerimiento y acordará la respuesta que se deba emitir, pudiendo recabar el correspondiente informe previo del Secretario, conforme al apartado 5.2.2 de las presentes Normas.

  El OCI analizará el requerimiento y propondrá la respuesta que se deba emitir en un plazo no superior a diez (10) días. A tales fines, el OCI goza de autoridad para obligar al personal sujeto a estas Normas a facilitar la información que le sea requerida y, en particular, que hubiera sido requerida por el SEPBLAC en el ejercicio de sus competencias o por cualquier otro órgano o autoridad respecto de la que exista la obligación legal de contestar.

- El OCI emitirá respuesta al SEPBLAC, órgano o autoridad legalmente competentes, requirente a través de su Representante Principal.

- En el supuesto de que se hubiera fijado un plazo de contestación en el requerimiento recibido por la Sociedad menor a diez (10) días, el OCI deberá emitir la respuesta a la mayor rapidez posible y, en todo caso, dentro del plazo otorgado a tal efecto por el SEPBLAC, organismo u autoridad competente, para que el Representante Principal ante el SEPBLAC pueda enviar la respuesta en plazo.

En todo caso, el OCI procederá a mantener un archivo por fechas y por los plazos que se indican en el apartado 7.4 anterior, de los requerimientos de información del SEPBLAC y cualesquiera otros órganos y autoridades legalmente competentes, en el que se incluirá toda la documentación relacionada con el citado requerimiento: requerimiento recibido, respuesta dada, informes internos emitidos relacionados con tal requerimiento, personal que intervino en su diligenciado, etc.

9.3 Comunicación directa por el personal de la Sociedad

El personal de la Sociedad podrá comunicar directamente al SEPBLAC las operaciones de que tuviera conocimiento y respecto de las cuales estimen que concurren indicios o certeza de estar relacionadas con el blanqueo de capitales y/o la financiación del terrorismo, en los casos en que, habiendo sido puestas de manifiesto internamente, el OCI no hubiese informado al comunicante del curso dado a su comunicación en el plazo de diez (10) días hábiles desde que se efectuó la misma.

A tales efectos, utilizará el formulario que se adjunta como **Anexo IV** a las Normas.

9.4 Confidencialidad sobre datos y operaciones que presenten indicios de estar relacionadas con el blanqueo de capitales

Las personas sujetas a estas Normas no revelarán al Cliente, ni a terceros, que se ha comunicado información al SEPBLAC, o que se está examinando o puede examinarse alguna operación por si pudiera estar relacionada con el blanqueo de capitales y/o con la financiación del terrorismo.

Esta prohibición no incluirá la revelación a las autoridades competentes incluidas -en su caso- los órganos centralizados de prevención, o la revelación por motivos policiales en el marco de una investigación penal.

9.5 Protección de datos de carácter personal

A efectos del cumplimiento de la normativa aplicable, la Empresa creará una base de datos de carácter personal con los siguientes datos y características

a) Finalidad del tratamiento y usos previstos: gestión y registro de la información sobre blanqueo de capitales, especialmente los relativos a la conservación de los documentos de identidad y conocimiento de las personas físicas.
b) Personas sobre las que se pretende obtener datos personales o que están obligadas a suministrarlos: aquellas personas físicas y jurídicas y sus representantes que deseen utilizar los servicios de la Sociedad.

c) Procedimiento de recogida de datos: declaraciones y manifestaciones de dichas personas y fotocopias de los documentos que acrediten la aplicación de las medidas de diligencia debida.

d) Tipos de datos:

- Datos de carácter identificativo.
- Datos de características personales.
- Datos relativos a la actividad económica.

b) Cesiones previstas de datos personales:

- A la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y sus órganos de apoyo, para el cumplimiento de los fines encomendados a dicho Servicio.
- A las autoridades judiciales, fiscales y administrativas competentes en materia de prevención de blanqueo de capitales y financiación del terrorismo.
- A aquellas entidades financieras domiciliadas en la Unión Europea o terceros países equivalentes, con las que exista un acuerdo previo formalizado.

c) Responsable del tratamiento: SEGURA E HIJOS, S.A.

d) Ejercicio de los derechos de acceso, rectificación, cancelación, oposición, portabilidad y limitación: los derechos de acceso, rectificación, cancelación, oposición, portabilidad y limitación podrán ser ejercidos, en su caso, conforme a lo previsto en la Política de Privacidad de la Sociedad.

Conforme a lo establecido en el artículo 32 bis:

- El tratamiento de datos personales que resulte necesario para el cumplimiento de las obligaciones establecidas en el Capítulo II de esta ley se encuentra amparado por lo dispuesto en el artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 6.1 c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no precisando del consentimiento del interesado.
- Los datos recogidos por los sujetos obligados para el cumplimiento de las obligaciones de diligencia debida no podrán ser utilizados para fines distintos de los relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo sin el consentimiento del interesado, salvo que el tratamiento de dichos datos sea necesario para la gestión ordinaria de la relación de negocios.
- Con carácter previo al establecimiento de la relación de negocios o la realización de una transacción ocasional, los sujetos obligados deberán facilitar a los nuevos clientes la información requerida en los artículos 13 y 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y en el artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre. Dicha información contendrá, en particular, un aviso general sobre las obligaciones legales de los sujetos obligados con respecto al tratamiento de datos personales a efectos de prevención del blanqueo de capitales y la financiación del terrorismo.

- Los sujetos obligados deberán realizar una evaluación de impacto en la protección de datos de los tratamientos a los que se refiere este artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos.

10. DEBER DE ABSTENCIÓN DE EJECUCIÓN

Las personas sujetas a las presentes Normas que aprecien indicios o evidencias de que una operación en la que estén interviniendo pudiera estar relacionada con el blanqueo de capitales y/o con la financiación del terrorismo, se abstendrán de continuar y lo notificarán inmediatamente al OCI. No podrán proseguir con la operación hasta que, en su caso, dicho Órgano lo autorice por escrito. Esta autorización, o, en su caso, la abstención para la ejecución de ésta, deberá ser emitida en un plazo no superior a diez (10) días hábiles.

De todo el proceso se guardará absoluta confidencialidad, tanto por los empleados, directivos, agentes y colaboradores, como por el OCI.

En el supuesto de que el OCI informe al empleado, directivo, agente o colaborador por escrito de que debe abstenerse de realizar la operación, le informará igualmente en el documento, y, en su caso, le explicará también de forma oral, la forma en que debe proceder con el Cliente, a fin de no levantar sospechas del motivo por el que la operación finalmente no se ejecuta.

Si, en opinión del OCI dicha abstención no fuera posible o pudiera dificultar la investigación y persecución de los beneficiarios de la operación de blanqueo y/o de financiación del terrorismo, entonces podrá autorizar que continúe la operación al empleado, notificando formalmente de la misma el representante al SEPBLAC inmediatamente después de su ejecución o realización.

La comunicación al SEPBLAC deberá exponer los motivos que justificaron la ejecución de la operación sospechosa, así como la información a la que alude el informe de Examen Especial del apartado 8.2 del Manual.

11. PROHIBICIÓN DE REVELACIÓN

Las personas sujetas a las presentes Normas tienen la obligación de guardar secreto acerca de las comunicaciones e informaciones mantenidas con el OCI y, en su caso, con el SEPBLAC.

La prohibición de revelación abarca tanto la información que se haya comunicado, la que pueda estarse examinando en la actualidad o cualquier operación que pudiera ser examinada en un futuro, por su posible relación con el blanqueo de capitales y/o con la financiación del terrorismo. Queda exenta de dicha prohibición la revelación a las autoridades competentes y aquella realizada por motivos policiales en el marco de una investigación penal.

La comunicación de buena fe de información a las autoridades competentes con arreglo a las presentes Normas, no constituye violación de las restricciones que sobre divulgación de información se hubieran impuesto por vía contractual o mediante disposición legal, reglamentaria o administrativa.

12. FORMACIÓN DE EMPLEADOS

Periódicamente, el OCI establecerá un Plan de Formación Anual con motivo de la participación de los empleados en cursos específicamente orientados a la detección de las operaciones que pudieran estar relacionadas con el blanqueo de capitales y/o la financiación del terrorismo, y a su instrucción en los procedimientos a seguir en tales casos.

Los planes de formación se deberán ir adaptando hacia las nuevas formas de operar de las personas relacionadas con el blanqueo de capitales y/o la financiación del terrorismo, según se vayan conociendo a través de las publicaciones emitidas por el GAFI, el SEPBLAC, u otros órganos nacionales e internacionales relacionados con la lucha contra el blanqueo de capitales y/o la financiación del terrorismo, así como por la propia experiencia adquirida por SEGURA.

El OCI convocará a los empleados, que por razón del desempeño de su cargo se vean afectos a esta normativa, para su participación en los cursos de formación anuales establecidos.

Sin perjuicio de lo anterior, el OCI podrá convocar a los cursos de formación, a empleados de otros departamentos o incluso a personas que no sean empleados de SEGURA y/o de sus filiales o participadas, que con motivo de la relación comercial o de cualquier otra índole, mantenida con éstos se vean afectos a esta normativa.

Es de obligado cumplimiento para cada empleado convocado por el OCI a los cursos de formación, la cumplimentación del Modelo de control de asistencia al Plan Anual de Formación (**Anexo XIV**), que deberá ser entregado al comienzo de cada sesión de formación al personal auxiliar habilitado al efecto.

Asimismo, se efectuará una evaluación de los contenidos impartidos con el fin de garantizar el aprovechamiento de los mismos, tomando las acciones oportunas en caso de ser necesario que deberán ser ejecutadas por el OCI.

Al finalizarse el Plan Anual de Formación se realizará un registro-memoria acreditativo de la asistencia y comprensión de contenidos, cuya copia deberá ser consignada oportunamente por la Sociedad conforme a lo establecido para el resto de documentación en materia de prevención del blanqueo de capitales y/o de la financiación del terrorismo.

Por último, periódicamente y siempre que las circunstancias lo aconsejen, bien por cambios normativos, cambios en los procedimientos internos o para servir de actualizaciones, el Representante Principal de la Sociedad ante el SEPBLAC, circulará documentos específicos en la materia entre los empleados y colaboradores a su servicio afectos al presente Manual.

13. EXAMEN DE LAS MEDIDAS DE CONTROL INTERNO POR EL OCI Y POR EXPERTO EXTERNO

El OCI elaborará con carácter anual un Informe o Memoria Explicativa, que contenga las actuaciones e información estadística más relevantes que en materia de prevención del blanqueo de capitales y/o de la financiación del terrorismo se hayan producido en el periodo considerado (ej. cambios significativos en los procedimientos, implantación de nuevas aplicaciones informáticas, datos estadísticos sobre el número de alertas, de operaciones objeto de análisis especial, de comunicaciones realizadas al SEPBLAC, solicitudes de información, cumplimiento de la normativa interna por la Sociedad y sus filiales o entidades con participación mayoritaria de la Sociedad, proceso de implantación de mejoras indicadas o sugeridas por los expertos externos respecto del sistema de prevención interno de la sociedad, etc.)

Igualmente, y de conformidad con lo establecido en la Ley 10/2010, de 28 de abril, y en la Orden del Ministerio de Economía y Hacienda EHA/2444/2007, de 31 de julio, por la que se desarrolla el Reglamento de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, aprobado por Real Decreto 925/1995, de 9 de junio, en relación con el informe de experto externo sobre los procedimientos y órganos de control interno y comunicación establecidos para prevenir el blanqueo de capitales, SEGURA deberá someter al examen de experto externo, sus medidas, procedimientos y órganos de control interno.

Este examen deberá efectuarse con una periodicidad anual, por personas de reconocido prestigio en la materia, y siempre que las mismas no hubieran prestado o presten en la actualidad cualquier otra clase de servicios retribuidos durante los tres años anteriores o posteriores a la emisión del informe.

Los resultados del examen deberán describir detalladamente las medidas de control interno existentes, valorándose su eficacia operativa y pudiendo proponerse, en su caso, eventuales rectificaciones o mejoras.

El informe se elevará en el plazo máximo de tres (3) meses desde la fecha de emisión al órgano de administración de SEGURA, que adoptará las medidas necesarias para solventar las deficiencias identificadas.

El informe externo se conservará por el OCI y estará a disposición de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias durante los cinco años siguientes a la fecha de emisión.

14. DIVULGACIÓN DE NORMAS Y ANEXOS

Las personas sujetas a las presentes Normas tienen obligación de conocerlas, de cumplirlas y de colaborar con el OCI en tal cumplimiento.

Para el efectivo cumplimiento de las anteriores obligaciones, SEGURA difundirá estas Normas y hará entrega de una copia completa y actualizada a todos los empleados y colaboradores de la Sociedad, junto con todos sus Anexos. Y ello, con el fin de prevenir que la misma sea utilizada como mecanismo para realizar actividades de blanqueo de capitales y/o financiación del terrorismo. Se adjunta como **Anexo XV** documento de acuse de recibo por el empleado y/o colaborador al servicio de la Sociedad acreditativo de la entrega del Manual y sus Anexos.

Las posteriores modificaciones de las presentes Normas y sus Anexos, serán notificadas a todos los empleados, directivos, agentes y colaboradores mediante un comunicado, haciéndoles llegar una nueva versión completa cuando la importancia de los cambios lo justifique, o mediante comunicado interno que permita el debido conocimiento de los cambios operados en estas Normas, por aquéllos sometidos a las mismas. De esta nueva entrega, en su caso, del Manual también se acusará recibo por parte de la Sociedad utilizando el mismo **Anexo XV**.

El OCI de SEGURA habilitará un espacio en el sistema informático interno en el que se pondrá a disposición de todos los empleados las presentes Normas y sus Anexos, en formato electrónico, donde se encontrarán debidamente actualizadas.

Asimismo, la Sociedad entregará a los terceros proveedores contratados por la Sociedad que presten algún tipo de servicio en materia de prevención del blanqueo de capitales y/o de la financiación del terrorismo, copia del Acta aprobada del OCI donde se recoja un listado de las concretas competencias asumidas por los terceros en la mencionada materia. Se adjunta como **Anexo XV** documento de acuse de recibo por el proveedor de la Sociedad acreditativo de la entrega del citado acta.

El contenido de estas Normas se divulgará en seminarios o reuniones con el personal y colaboradores involucrados en las operaciones que constituyan el ámbito objetivo de su aplicación.

Igualmente, todo el personal y colaboradores serán informados de que su identidad será preservada en las comunicaciones que éstos mantengan con el OCI en relación con la aplicación de las presentes Normas.

15. INFORME DE AUTOEVALUACIÓN DEL RIESGO ANTE EL BLANQUEO DE CAPITALES Y LA FINANCIACIÓN DEL TERRORISMO

En cumplimiento de las recomendaciones sobre las medidas de control interno para la Prevención del Blanqueo de Capitales y/o la Financiación del Terrorismo, así como de la normativa reglamentaria que desarrolla la Ley 10/2010, la Sociedad evaluará anualmente los niveles de riesgo relevante para el blanqueo de capitales y/o la financiación del terrorismo en el Informe de Autoevaluación que se adjunta como **Anexo XV**, con las correspondientes Fichas anexas al Informe, debiendo ser evaluado en su conjunto por la Sociedad y sus miembros.

ANEXO I: RELACIÓN DE PAÍSES TERCEROS EQUIVALENTES

Resolución de 10 de agosto de 2012, de la Secretaría General del Tesoro y Política Financiera, por la que se publica el Acuerdo de 17 de julio de 2012, de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, por el que se determinan las jurisdicciones que establecen requisitos equivalentes a los de la legislación española de prevención del blanqueo de capitales y de la financiación del terrorismo.

(BOE núm. 202 Jueves 23 agosto 2012)

A los efectos previstos en los artículos 1.4, 4.2, 8.2, 9.1, 10.2, 12.1 y 24.2 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, en su sesión de 17 de julio de 2012, ha determinado, de conformidad con los criterios acordados por los Estados miembros del Comité comunitario de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, creado por el artículo 41 de la Directiva 2005/60/CE, que **las siguientes jurisdicciones establecen requisitos equivalentes a los de la legislación española: Australia, Brasil, Canadá, Corea del Sur, Estados Unidos, Hong Kong, India, Japón, México, Singapur, Sudáfrica y Suiza**.

La lista no es aplicable a los Estados miembros de la Unión Europea y del Espacio Económico Europeo, que se benefician de iure de reconocimiento mutuo. La lista incluye, asimismo, a los territorios y jurisdicciones integrados en las delegaciones ante el Grupo de Acción Financiera de **Francia (Mayotte, Nueva Caledonia, Polinesia Francesa, Saint Pierre-et-Miquelon y Wallis-et-Futuna) y del Reino de los Países Bajos (Aruba, Curasao, Sint Maarten, Bonaire, Sint Eustatius y Saba)**.

La presente Resolución se entiende sin perjuicio de la aplicación en función del riesgo por los sujetos obligados de las medidas de diligencia debida, de conformidad con lo establecido en el artículo 7.1 de la Ley 10/2010. En particular, los sujetos obligados no aplicarán medidas simplificadas de diligencia debida cuando concurran indicios de blanqueo de capitales o de financiación del terrorismo. Asimismo, los sujetos obligados aplicarán medidas reforzadas de diligencia debida en aquellas situaciones que por su propia naturaleza puedan presentar un riesgo más elevado de blanqueo de capitales o de financiación del terrorismo.

Madrid, 10 de agosto de 2012.–El Secretario General del Tesoro y Política Financiera, P.D. (Resolución de 23 de abril de 2012), el Subdirector General de Inspección y Control de Movimientos de Capitales, Juan Manuel Vega Serrano.

ANEXO II: CLÁUSULAS DE OBLIGADO CUMPLIMIENTO POR TERCEROS QUE CONTRATEN CON LA SOCIEDAD EN MATERIA DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO

[La entidad subcontratada] se compromete a cumplir con todas las obligaciones que le sean exigibles de conformidad con la normativa de prevención del Blanqueo de Capitales y de la Financiación del Terrorismo aplicable al sector inmobiliario, vigente durante la duración del presente contrato.

A los expresados fines, se subrogará en la totalidad de obligaciones impuestas por [la Sociedad], para dar cumplimiento a los deberes que derivan de la Ley de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, Reglamentos que la desarrollan, y normativa sobre la materia vigente en cada momento.

En especial, pero no limitadas, a la obligación de conocimiento y cumplimiento de las Normas de Procedimiento y Control para la Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo aplicables a [la Sociedad], así como a la obligación de comunicación inmediata al Órgano de Control Interno de la precitada entidad, de cualesquiera hechos con relevancia en la prevención del blanqueo de capitales de los que tenga conocimiento su personal (agentes y/o comerciales y/o representantes, etc.) durante la prestación de sus servicios a [la Sociedad].

A la firma del presente contrato [La Sociedad] hace entrega de las mencionadas Normas de Procedimiento y Control para la Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo aplicables a [la Sociedad], que [La entidad Comercializadora] recibe. [La Sociedad] le hará entrega de cualesquiera actualizaciones que de dichas Normas acontezca durante la vigencia del presente contrato.

[La entidad subcontratada] se obliga a dar a conocer a su personal (agente, comercial) la referida normativa, así como a que dicho personal asista a cursos de formación anual y continúa sobre la materia. [La Sociedad] podrá requerir a [La entidad subcontratada] la exhibición de la correspondiente documentación acreditativa de haber obtenido dicho personal los conocimientos necesarios en materia de prevención del Blanqueo de Capitales y de la Financiación del Terrorismo en el sector inmobiliario, así como de la formación continua recibida.

El incumplimiento de cualesquiera obligaciones en materia de prevención del Blanqueo de Capitales y de la Financiación del Terrorismo aplicables a [La Sociedad] por [la entidad comercializadora] y/o sus comerciales y/o agentes, facultará a [La Sociedad] a dar por resuelto el presente contrato sin necesidad de previo aviso.

[La entidad subcontratada] estará obligada a indemnizar a [la Sociedad] por todos los daños y perjuicios que le ocasione el incumplimiento de las obligaciones contenidas en la presente cláusula y exigibles de conformidad con la normativa referida. Dicha indemnización comprenderá pero no estará limitada al abono por [La entidad subcontratada] a [La Sociedad] del importe íntegro de cualquier sanción que le pudiera, en su caso, serle impuesta por el Servicio Ejecutivo de Prevención de Blanqueo de Capitales del Banco de España y/o por cualquier otra Autoridad administrativa y/o judicial con competencias en la indicada materia, como consecuencia de cualquier incumplimiento de ésta o de su personal, de la normativa de prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, así como de la totalidad de los gastos, daños y perjuicios que las actuaciones inspectoras y sancionadoras de estos organismos le hubiesen podido

ocasionar a [la Sociedad], tanto desde un punto de vista material, como desde un punto de vista de imagen corporativa, en el mercado y frente a los clientes.

ANEXO III: FORMULARIO DE COMUNICACIÓN INTERNA DE OPERACIÓN SOSPECHOSA DE BLANQUEO DE CAPITALES

FORMULARIO DE COMUNICACIÓN DE OPERACIÓN SOSPECHOSA DE BLANQUEO DE CAPITALES

Empleado / Colaborador	
Nombre y apellidos:	
Cargo:	
Departamento:	
Teléfono:	
E-mail:	
Datos del Cliente	
Nombre:	
Dirección:	
País de Residencia:	
Detalles sobre su identificación obtenidos	
Persona Física	

RELACIÓN DE LAS OPERACIONES

Operación	
Objeto de la operación:	

Fecha de ejecución (identificando la persona, órgano o departamento de la Sociedad que hubiera adoptado la decisión de continuar con la relación de negocios):	
Moneda:	
Cuantía:	
Lugar o lugares de ejecución:	
Finalidad:	
Instrumentos de retirada o cobro utilizados:	

(A) Razón de la comunicación:	
Indicios. Se debe acompañar copia de toda la documentación relevante.	
No identificó correctamente	

Fecha: Firma:	

Nota: no se revelarán al cliente ni a terceros las actuaciones que estén realizando en cumplimiento de la normativa sobre Prevención del Blanqueo de Capitales. Se debe adoptar las precauciones necesarias para que la comunicación no esté en ningún momento al alcance del cliente.

ANEXO IV: MODELO DE COMUNICACIÓN DE REPRESENTANTE PRINCIPAL DE LA SOCIEDAD ANTE EL SEPBLAC

SEGURA E HIJOS, S.A.
Avenida de Tenerife núm. 16,
San Sebastián de los Reyes
28703 (MADRID)

Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

BANCO DE ESPAÑA
Alcalá, 48
28.014 MADRID

Ref. Comunicación de nombramiento de representante ante el SEPBLAC de la Sociedad SEGURA E HIJOS, S.A.

Madrid, a __ de __ de 202_

Muy señores nuestros:

En cumplimiento de lo ordenado en la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, la Sociedad **SEGURA E HIJOS, S.A.**, con CIF A-78144524, domicilio en Avenida de Tenerife núm. 16, San Sebastián de los Reyes, 28703 (MADRID), y que tiene por objeto social, con carácter general, el comercio al por mayor de madera, materiales de construcción y aparatos sanitarios, acompaña para su conocimiento:

i. Certificaciónn del órgano de administración de la Sociedad que recoge el acuerdo de nombramiento y aceptación de D._____ como representante de la Sociedad ante el SEPBLAC

ii. Fotocopia del DNI.

iii. Currículum Vitae.

iv. Formulario F22 debidamente rellenado y firmado.

Atentamente,

_____
D.
Representante Principal

ANEXO V: MODELO DE COMUNICACIÓN DE PERSONA AUTORIZADA POR EL REPRESENTANTE PRINCIPAL DE LA SOCIEDAD ANTE EL SEPBLAC

D._____
Representante Principal de
SEGURA E HIJOS, S.A.
Avenida de Tenerife núm. 16,
San Sebastián de los Reyes
28703 (MADRID)

Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

BANCO DE ESPAÑA
Alcalá, 48
28.014 MADRID

Ref. Comunicación de nombramiento por el representante Principal de la Sociedad SEGURA E HIJOS, S.A. de persona autorizada.

Madrid, a __ de __ de 202_

Muy señores nuestros:

En cumplimiento de lo ordenado en la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, por medio de la presente y en mi condición de Representante Principal de la sociedad **SEGURA E HIJOS, S.A.**, con CIF A-78144524, domicilio en Avenida de Tenerife núm. 16, San Sebastián de los Reyes, 28703 (MADRID), les participa el nombramiento de D._____ como persona autorizada por mi parte ante el SEPBLAC.

Se adjunta a la presente comunicación la siguiente documentación:

v. Fotocopia del DNI de la persona autorizada.

vi. Formulario F22-6 debidamente rellenado y firmado.

Atentamente,

_____
D.
Representante Principal

ANEXO VI: LISTADO DE PERSONAS, GRUPOS Y SOCIEDADES CONSIDERADAS POR LA UNION EUROPEA COMO RELACIONADAS CON ACTIVIDADES TERRORISTAS

(Posición común 2001/931/PESC del Consejo, de 27 de diciembre de 2001, sobre la aplicación de medidas específicas de lucha contra el terrorismo)

Esta lista se corresponde con la actualización efectuada por la DECISIÓN (PESC) 2019/25 DEL CONSEJO de 8 de enero de 2019 por la que se modifica y actualiza la lista de personas, grupos y entidades a los que se aplican los artículos 2, 3 y 4 de la Posición Común 2001/931/PESC sobre la aplicación de medidas específicas de lucha contra el terrorismo y se deroga la Decisión (PESC) 2018/1084.

A. Personas

BDOLLAHI Hamed (alias Mustafa Abdullahi), nacido el 11.8.1960 en Irán. Número de pasaporte: D9004878.

2. AL-NASSER, Abdelkarim Hussein Mohamed, nacido en Al Ihsa (Arabia Saudí), nacional de Arabia Saudí.

3. AL YACOUB, Ibrahim Salih Mohammed, nacido el 16.10.1966 en Tarut (Arabia Saudí), nacional de Arabia Saudí.

4. ARBABSIAR Manssor (alias Mansour Arbabsiar), nacido el 6.3.1955 o el 15.3.1955 en Irán. Nacional de Irán y de EE.UU. Número de pasaporte: C2002515 (Irán). Número de pasaporte: 477845448 (EE.UU.). Número de documento nacional de identidad: 07442833; fecha de caducidad: 15.3.2016 (permiso de conducción estadounidense).

5. ASADI Assadollah, nacido el 22.12.1971 en Teherán (Irán), nacional de Irán. Número de pasaporte diplomático iraní: D9016657.

6. BOUYERI, Mohamed (alias Abu ZUBAIR, alias SOBIAR, alias Abu ZOUBAIR), nacido el 8.3.1978 en Ámsterdam (Países Bajos).

7. EL HAJJ, Hassan Hassan, nacido el 22.3.1988 en Zaghdraiya, Sidón (Líbano), nacional de Canadá. Número de pasaporte: JX446643 (Canadá).

8. HASHEMI MOGHADAM Saeid, nacido el 6.8.1962 en Teherán (Irán), nacional de Irán. Número de pasaporte: D9016290; fecha de caducidad: 4.2.2019.

9. IZZ-AL-DIN, Hasan (alias GARBAYA, Ahmed, alias SA-ID, alias SALWWAN, Samir), Líbano, nacido en 1963 en el Líbano, nacional del Líbano.

10. MELIAD, Farah, nacido el 5.11.1980 en Sydney (Australia), nacional de Australia. Número de pasaporte: M2719127 (Australia).

11. MOHAMMED, Khalid Shaikh (alias ALI, Salem, alias BIN KHALID, Fahd Bin Abdallah, alias HENIN, Ashraf Refaat Nabith, alias WADOOD, Khalid Adbul), nacido el 14.4.1965 o el 1.3.1964 en Pakistán. Número de pasaporte: 488555.

12. ŞANLI, Dalokay (alias Sinan), nacido el 13.10.1976 en Pülümür (Turquía).

13. SHAHLAI Abdul Reza (alias Abdol Reza Shala'i, alias Abd-al Reza Shalai, alias Abdorreza Shahlai, alias Abdolreza Shahla'i, alias Abdul-Reza Shahlaee, alias Hajj Yusef, alias Haji Yusif, alias Hajji Yasir, alias Hajji Yusif, alias Yusuf Abu-al-Karkh), nacido hacia 1957 en Irán. Direcciones: 1) Kermanshah, Irán, 2) Base militar de Mehran, provincia de Ilam, Irán.

14. SHAKURI Ali Gholam, nacido hacia 1965 en Teherán (Irán).

15. SOLEIMANI Qasem (alias Ghasem Soleymani, alias Qasmi Sulayman, alias Qasem Soleymani, alias Qasem Solaimani, alias Qasem Salimani, alias Qasem Solemani, alias Qasem Sulaimani, alias Qasem Sulemani), nacido el 11.3.1957 en Irán. Nacional de Irán. Número de pasaporte: 008827 (diplomático iraní), expedido en 1999. Rango: General de División.

B. Grupos y Sociedades

1. «Organización Abu Nidal» — «OAN» (otras denominaciones: «Consejo Revolucionario de Al Fatah», «Brigadas Revolucionarias Árabes», «Septiembre Negro» y «Organización Revolucionaria de los Musulmanes Socialistas»).

2. «Brigada de los Mártires de Al-Aqsa».

3. «Al-Aqsa e.V».

4. «Babbar Jalsa».

5. «Partido Comunista de las Filipinas», incluido el «Nuevo Ejército del Pueblo» — «NEP» («New People's Army» — «NPA»), Filipinas.

6. «Dirección de la Seguridad Interior del Ministerio de Inteligencia y Seguridad iraní».

7. «Al Gama al Islamiya» (otras denominaciones: «Al-Gama'a al-Islamiyya») («Grupo Islámico» — «GI»).

8. «İslami Büyük Doğu Akıncılar Cephesi» — «IBDA-C» («Frente de Guerreros del Gran Oriente Islámico»).

9. «Hamás», incluido «Hamas-Izz al-Din al-Qassem».

10. «Ala militar de Hizbulá» [otras denominaciones: «Ala militar de Hezbolá», «Ala militar de Hizbulah», «Ala militar de Hizbolah», «Ala militar de Hezbalah», «Ala militar de Hisbolah»,

«Ala militar de Hizbu'llah», «Ala militar de Hizb Allah», «Consejo de la Yihad» (y todas las unidades bajo su mando, incluida la Organización de Seguridad Exterior)].

11. «Hizbul Muyahidín» — «HM».

12. «Khalistan Zindabad Force» — «KZF» («Fuerza de Jalistán Zindabad»).

13. «Partido de los Trabajadores del Kurdistán» — «PKK» (otras denominaciones: «KADEK», «KONGRA-GEL»).

14. «Tigres para la Liberación de la Patria Tamil» — «LTTE».

15. «Ejército de Liberación Nacional».

16. «Palestinian Islamic Jihad» — «PIJ» («Yihad islámica para la liberación de Palestina»).

17. «Frente Popular de Liberación de Palestina» — «FPLP».

18. «Frente Popular de Liberación de Palestina» — «Comando General» (otras denominaciones: «FPLP – Comando General»).

19. «Devrimci Halk Kurtuluș Partisi-Cephesi» — «DHKP/C» (otras denominaciones: «Devrimci Sol» («Izquierda revolucionaria») o «Dev Sol») («Ejército/Frente/Partido Revolucionario de Liberación Popular»).

20. «Sendero Luminoso» — «SL».

21. «Teyrbazen Azadiya Kurdistan» — «TAK» (otras denominaciones: «Halcones de la Libertad del Kurdistán»).

ANEXO VII: RELACIÓN DE PARAÍSOS FISCALES

Anguila, Bahrein, Barbados, Bermuda, Dominica, Fiji, Gibraltar, Guam, Guernsey, Isla de Man, Islas Caimán, Islas Malvinas, Islas Marianas, Islas Salomón, Islas Turcas y Caicos, Islas Vírgenes Británicas, Islas Vírgenes de Estados Unidos de América, Jersey, Palaos, Samoa, Samoa Americana, Seychelles, Trinidad y Tobago y Vanuatu.

ANEXO VIII: CATÁLOGO DE EJEMPLOS DE CLIENTES DE RIESGO ALTO

A título de ejemplo, se considerarán como Clientes de riesgo alto los que se encuentren en alguna de las categorías siguientes:

1. Por sus antecedentes públicos o notorios: personas físicas o personas jurídicas cuyos consejeros hubieran sido condenados por delitos relativos a:

    - el blanqueo de capitales;
    - el tráfico de estupefacientes;
    - el terrorismo;
    - la participación en grupos criminales organizados (ver Anexo X)
    - el tráfico de armas;
    - el tráfico ilegal de personas;
    - las detenciones ilegales y el secuestro;
    - la prostitución y la explotación de menores;
    - el cohecho, la malversación, los sobornos y la corrupción;
    - la extorsión;
    - el robo;
    - el tráfico de objetos robados y el tráfico ilegal de objetos;
    - la falsificación de moneda;
    - la falsificación y la piratería de productos;
    - el contrabando;
    - el fraude; o
    - las insolvencias punibles.

2. Por su país de origen: personas o Sociedades domiciliadas en (i) paraísos fiscales, cuya lista figura en el Anexo VIII, con independencia de si se han firmado acuerdos de intercambio de información en materia tributaria o convenios para evitar la doble imposición con cláusula de intercambio de información; (ii) cualesquiera otros países que tuvieran la consideración de “no-cooperantes” según el GAFI o que presenten, según el mismo, deficiencias estructurales en materia de prevención del blanqueo de capitales y de la financiación del terrorismo y cuya lista se recoge al final del presente anexo; o (iii) en Estados donde se tiene conocimiento de la existencia de organizaciones criminales particularmente activas (por ejemplo, tráfico de drogas, actividades terroristas, delincuencia organizada o tráfico de seres humanos).

3. Por su actividad: personas o sociedades dedicadas a actividades relacionadas con:

    - sellos, joyas, piedras y metales preciosos;
    - antigüedades y objetos de arte;
    - casinos;
    - comercialización de árboles, bosques naturales o animales con oferta de restitución posterior, en uno o varios pagos, de todo o parte del precio pagado en todo caso;

- Sociedades sin ánimo de lucro (asociaciones y fundaciones), salvo cuando se trate de clientes habituales o conocidos, o de Sociedades cuya actividad y buen nombre sean públicamente reconocidos;
- Personas con Responsabilidad Pública; o
- Depósito, custodia, transferencia o transporte de medios de fondos y medios de pago, siempre que no se trate de Sociedades Financieras, según la definición contenida en estas Normas.

4. Lista de países o territorios no cooperantes (PTNC), según recoge la Orden EHA/1464/2010, de 28 de mayo, por la que se modifica la Orden ECO/2652/2002, de 24 de octubre:

   - Egipto.
   - Filipinas.
   - Guatemala.
   - Indonesia.
   - Myanmar (antigua Birmania).
   - Nigeria.
   - Ucrania.
   - República Islámica de Irán.

5. Países y territorios identificados por GAFI con deficiencias en materia de prevención del blanqueo de capitales y financiación del terrorismo:

   - Argelia
   - Ecuador
   - Etiopía
   - Indonesia
   - Myanmar
   - Pakistán
   - Siria
   - Turquía
   - Yemen
   - Albania
   - Angola
   - Argentina
   - Cuba
   - Irak
   - Kenia
   - Kuwait
   - Kirguistán
   - Rep. Dem. Popular Lao
   - Mongolia
   - Namibia
   - Nepal
   - Nicaragua

- Papua Nueva Guinea
- Sudán
- Tayikistán
- Tanzania
- Uganda
- Zimbabwe
- Afghanistan
- Camboya

ANEXO IX: CATÁLOGO DE ACTIVIDADES DE RIESGO MEDIO

- Pequeñas firmas de abogados.
- Agencias de viajes.
- Marchantes de arte.
- Distribuidores de automóviles, barcos y piezas usadas.
- Bróker.
- Asesorías contable y fiscal.
- Negocios que mueven gran cantidad de dinero en efectivo.
- Distribuidores de electrónica de consumo, en especial, equipos de informática.
- Agencias de empleo eventual (ETTs).
- Compraventa de ganado.
- Inmobiliario.
- Distribuidor de joyas, piedras y metales preciosos.
- Almacenes de pieles.
- Fundaciones u organismos sin ánimo de lucro.

ANEXO X: EXPEDIENTE "CONOZCA A SU CLIENTE"

MODELO DE OBLIGADO CUMPLIMIENTO

IDENTIFICACIÓN CLIENTE PERSONA FÍSICA (interno)

1. **DATOS INTERNOS**

☐ Cliente Nuevo
☐ Modificación de datos anteriores

Fecha primer contacto cliente y modo de contacto:

Fecha de apertura del expediente del Cliente:

Fecha de modificación de datos de Clientes históricos en caso de establecimiento de nueva relación de negocios:

Nombre y Apellidos del empleado/colaborador:

Cargo ocupado en la empresa:

DNI/Otros indicar:

2. DATOS RELATIVOS AL CLIENTE PERSONA FÍSICA Y A LA OPERACIÓN

a) Descripción de la operación:

b) Importe de la operación:

c) Datos de identificación personal del Cliente:

- Nombre y dos Apellidos:
- DNI / Otros (ver apartado 7.1.1.1 de las Normas):
- Fecha de expedición y fecha de caducidad:
- Fecha de nacimiento:
- Género (Masculino/Femenino):
- Nacionalidad:
- Domicilio:
- País de Residencia:
- Teléfonos de contacto:
- E-mail:
- Profesión:
- Antecedentes con la Sociedad:
- Propósito de la relación negocial a suscribir con la Sociedad:

d) Comprobación obligatoria:

- Fecha en la que se coteja que el cliente no figura en la lista pública de terroristas (ver **Anexo VI**):
- Fecha en la que se ha cotejado que el cliente no reside en alguno de los países que figuran en las listas de Estados de Alto Riesgo/Paraíso Fiscal/Estado no cooperante (ver **Anexos VII** y **VIII**):
- Fecha en la que se ha cotejado que el cliente no es PRP o PEP (ver apartado 7.1.1.3 de las Normas):

e) Documentación que obligatoriamente ha de acompañar a este impreso:

- Fotocopia de DNI/Otros en vigor del Cliente.
- Contrato(s) original(s) objeto de la operación suscrita con el Cliente.
- Documentación justificativa de la profesión/actividad desarrollada por el Cliente (véase **Anexo XII** del presente Manual).

Indicar expresamente si no se adjunta algún documento y el motivo de ello:

3. DATOS RELATIVOS A LA OPERACIÓN CONCLUIDA

a) Descripción de la operación:

b) Importe de la operación:

c) Modo de pago y fecha:

d) Motivos del cese de la relación con el Cliente, en su caso:

4. OTRAS INCIDENCIAS

Incidencias destacables:

Fecha y nombre del empleado:

DNI/Otros indicar:

ANEXO XI: EXPEDIENTE "CONOZCA A SU CLIENTE"

MODELO DE OBLIGADO CUMPLIMIENTO

IDENTIFICACIÓN CLIENTE PERSONA JURÍDICA (interno)

1. DATOS INTERNOS

☐ Cliente Nuevo
☐ Modificación de datos anteriores

Fecha primer contacto con el cliente y modo de contacto:

Fecha de apertura del expediente:

Fecha de modificación de datos de Clientes históricos en caso de establecimiento de nueva relación de negocios:

Nombre y Apellidos del Empleado/colaborador comercial:

Cargo ocupado en la empresa:

DNI/Otros indicar:

2. DATOS RELATIVOS AL CLIENTE PERSONA JURÍDICA Y A LA OPERACIÓN

a) Descripción de la operación:

b) Importe de la operación:

c) Datos de identificación personal del Cliente:

- Denominación social:
- CIF:
- Domicilio:
- Teléfonos de contacto:
- E-mail:
- Actividad empresarial:
- Órgano de control y dirección:
- Antecedentes con la empresa:

d) Comprobación obligatoria:

- Fecha en la que se coteja que el cliente no figura en la lista pública de terroristas (ver **Anexo VI** de las Normas):

- Fecha en la que se coteja que el cliente no reside en alguno de los países que figuran en las listas de Estados de Alto Riesgo/Paraíso Fiscal/Estado no cooperante (ver **Anexos VII** y **VIII** de las Normas):
- Fecha en la que se coteja que el cliente no es PRP o PEP (ver apartado 7.1.1.3 de las Normas):

e) Identificación de la persona física que contrata en nombre de la Sociedad:

- Nombre y dos Apellidos:
- DNI/Otros indicar (en vigor):
- Fecha de expedición y fecha de caducidad:
- Fecha de nacimiento:
- Género (Masculino/Femenino):
- Nacionalidad
- Domicilio:
- País de Residencia:
- Teléfonos de contacto:
- E-mail:
- Profesión:
- Antecedentes con la empresa:
- Propósito de la relación negocial a suscribir con la Sociedad:

f) Documentación en vigor que obligatoriamente ha de acompañar a este impreso:

- Fotocopia de la escritura de constitución de la sociedad Cliente y de los estatutos.
- Contrato(s) original(s) objeto de la operación suscrita con el Cliente.
- Documentación justificativa de la profesión/actividad desarrollada por el Cliente (véase **Anexo XII** del presente Manual).
- Fotocopia del poder que la persona física que actúa en nombre del Cliente exhibe para celebrar la operación.
- Fotocopia del DNI (otros indicar) en vigor de la persona física que representa al Cliente.
- Documento que describa la estructura de propiedad y control del Cliente a los fines de identificar al Titular Real (ver definiciones y apartado 7.1.2 de las Normas).
- Declaración expresa del Cliente de que los datos consignados en la documentación aportada están en vigor.

3. DATOS RELATIVOS A LA OPERACIÓN CONCLUIDA

a) Descripción de la operación:

b) Importe de la operación:

c) Modo de pago y fecha:

d) Motivos del cese de la relación con el Cliente, en su caso:

4. OTRAS INCIDENCIAS

Incidencias destacables:

Fecha:

ANEXO XII: CATÁLOGO DE OPERATIVA SOSPECHOSA DE BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO COMERCIO PROFESIONALDE BIENES

Introducción y marco normativo

La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, establece la condición de sujetos obligados para los promotores inmobiliarios y quienes ejerzan profesionalmente las actividades de agencia, comisión e intermediación en la compraventa de bienes inmuebles.

Indicadores y ejemplos de posibles operaciones de riesgo

A. POR LAS CARACTERÍSTICAS DE LOS INTERVINIENTES

1. Personas físicas.

a. Operaciones en las que intervengan personas domiciliadas en paraísos fiscales o territorios de riesgo, cuando el medio de pago utilizado por las mismas reúna alguna de las características incluidas en este documento.

b. Operaciones que se realicen a nombre de menores de edad, personas mayores de 70 años o que presenten signos de discapacidad mental o con evidentes indicios de falta de capacidad económica para tales adquisiciones.

c. Operaciones en las que intervengan personas que ocupen o hayan ocupado puestos políticos preeminentes, altos cargos o asimilados en países generalmente no democráticos, incluyendo su entorno familiar próximo.

d. Operaciones en las que intervengan personas que están procesadas o condenadas por delitos o resultase ser público o notorio o se tuviera sospecha de su presunta relación con actividades delictivas, siempre que las mismas permitan un enriquecimiento ilícito y que puedan ser consideradas como subyacentes del delito de blanqueo, así como aquellas operaciones realizadas por personas relacionadas con las anteriores (por ejemplo. por lazos familiares, profesionales, de origen, en las que exista coincidencia en el domicilio o coincidencia de representantes o apoderados, etc.).

e. Operaciones en las que intervengan personas con domicilio desconocido o de mera correspondencia (por ejemplo. apartado de correos, sedes compartidas, despachos profesionales, etc.), o con datos supuestamente falsos o de probable no certeza.

f. Varias operaciones en las que participa un mismo interviniente o aquellas realizadas por grupos de personas relacionadas entre sí (por ejemplo, por lazos familiares, por lazos profesionales, por personas de una misma nacionalidad, por

personas en las que exista coincidencia en el domicilio o coincidencia de representantes o apoderados, etc.).

2. Personas jurídicas

a. Operaciones en las que intervengan personas jurídicas domiciliadas en paraísos fiscales o territorios de riesgo, cuando el medio de pago utilizado por las mismas reúna alguna de las características detalladas en este documento.

b. Operaciones en las que intervengan personas jurídicas, de reciente constitución, cuando el importe sea elevado con relación a su patrimonio.

c. Operaciones en las que intervengan personas jurídicas cuando no parezca que exista relación entre las características de la operación y la actividad realizada por la empresa compradora o bien cuando esta no realice ninguna actividad.

d. Operaciones en las que intervengan personas jurídicas cuyos propietarios ocupen o hayan ocupado puestos políticos preeminentes, altos cargos o asimilados en países generalmente no democráticos, incluyendo su entorno familiar próximo.

e. Operaciones en las que intervengan Fundaciones, Asociaciones Culturales y Recreativas y en general, entidades sin ánimo de lucro, cuando no correspondan las características de la operación con los objetivos de la entidad.

f. Operaciones en las que intervengan personas jurídicas que, aun estando registradas en España, están constituidas principalmente por ciudadanos extranjeros o no residentes en España.

g. Operaciones en las que intervengan personas jurídicas con domicilio desconocido o de mera correspondencia (por ejemplo, apartado de correos, sedes compartidas, despachos profesionales), o con datos supuestamente falsos o de probable no certeza.

h. Varias operaciones en las que participa un mismo interviniente. Así como aquellas realizadas por grupos de personas jurídicas que puedan estar relacionadas entre sí (por ejemplo, por lazos familiares de sus propietarios o apoderados, por lazos profesionales de los mismos, por coincidencia en la nacionalidad bien de las personas jurídicas o de sus propietarios o apoderados, por coincidencia en el domicilio bien de las personas jurídicas o de sus propietarios o apoderados, por coincidencia de propietario, representantes o apoderados, por la similitud de nombres de personas jurídicas, etc.).

i. Operaciones en las que intervengan personas jurídicas cuya única actividad conocida sea la inversión en inmuebles como mera tenencia de los mismos.

3. Comportamiento de los intervinientes, bien sea persona física o jurídica:

a. Operaciones en las que existan indicios o certeza de que los intervinientes, no actúan por cuenta propia, intentando ocultar la identidad del cliente real.

b. Operaciones que se inician a nombre de una persona y que se formalizan finalmente a nombre de un tercero (por ejemplo, venta o transmisión de titularidad de la compra u opción de compra de un inmueble que no ha sido entregado todavía a su propietario, operaciones de reserva de inmuebles en fase de obra y que subrogan a terceros en sus derechos, etc.).

c. Operaciones en las que los intervinientes:

    - No demuestran demasiado interés por las características de los bienes (p.e. calidades de construcción, plazos de entrega, etc.) que son objeto de la operación.

    - No muestran demasiado interés en obtener un mejor precio por la operación, ni en mejorar los planes de pago.

    - Muestran gran interés en realizar la operación muy rápidamente, sin que exista causa que lo motive.

    - Muestran un gran interés en operaciones relativas a inmuebles situados en determinadas zonas, sin importarles el precio que fuese necesario pagar.

d. Operaciones en las que los intervinientes no sean residentes en España:

    - Tienen como única finalidad la inversión de capital (por ejemplo, no muestran interés en residir, aunque sea temporalmente, en el bien adquirido, etc.)

    - Muestran interés en grandes operaciones (por ejemplo, adquirir grandes solares para la posterior construcción de viviendas, compra de edificios completos, establecer negocios relacionados con actividades de ocio, etc.).

e. Operaciones en las que cualquiera de los pagos se efectúe por un tercero distinto de los intervinientes, especialmente si tienen origen en un país extranjero o un territorio designado.

4. Intermediarios:

a. Operaciones realizadas a través de intermediarios, cuando los mismos actúen por cuenta de grupos de personas físicas, que puedan estar relacionadas entre sí (por ejemplo, por lazos familiares, por lazos profesionales, por personas de una misma nacionalidad, por personas en las que exista coincidencia en el domicilio, etc.).

b. Operaciones realizadas a través de intermediarios, cuando los mismos actúen por cuenta de grupos de personas jurídicas, que puedan estar relacionadas entre sí. (por ejemplo, por lazos familiares de sus propietarios o apoderados, por lazos profesionales de los mismos, por coincidencia en la nacionalidad bien de las personas jurídicas o de sus propietarios o apoderados, por coincidencia en el domicilio bien de las personas jurídicas o de sus propietarios o apoderados, por coincidencia de propietario, representantes o apoderados, por la similitud de nombres de personas jurídicas, etc.).

c. Operaciones realizadas a través de intermediarios, cuando los mismos sean ciudadanos extranjeros o no residentes en España.

d. Operaciones realizadas a través de intermediarios, cuando los mismos actúen por cuenta de ciudadanos extranjeros o no residentes en España.

B. POR LAS CARACTERÍSTICAS DE LOS MEDIOS DE PAGO UTILIZADOS.

a. Operaciones en las que se utilicen los medios de pago previstos en el artículo 34.2 de la Ley.

C. POR LAS CARACTERÍSTICAS DE LA OPERACIÓN

a. Operaciones en las que se haya incluido una cláusula con un contrato de arras y finalmente no se haya formalizado la operación.

b. Operaciones sobre unos mismos bienes o derechos, muy cercanas en el tiempo (por ejemplo, compra e inmediata transmisión de bienes) y que suponen un incremento o disminución significativo del precio respecto al valor de adquisición.

c. Operaciones formalizadas por un valor significativamente diferente (muy superior o inferior) al real de los bienes transmitidos.

d. Operaciones relativas a promociones inmobiliarias en municipios o zonas de alto riesgo a juicio de la propia empresa (por ejemplo, por tener un alto porcentaje de personas de origen extranjero, zonas en las que haya sido aprobado un nuevo plan de desarrollo urbanístico, zonas cuyo número de inmuebles construidos en relación con el número de habitantes sea superior a la media, etc.).

e. Operaciones formalizadas mediante contrato privado en los que no exista intención de elevarlo a público, o aunque dicha intención exista, no sea elevado finalmente.

ANEXO XIII: FORMULARIO DE COMUNICACIÓN DE OPERACIÓN SOSPECHOSA AL SEPBLAC (F19-1)

COMUNICACIÓN DE OPERATIVA SOSPECHOSA AL SEPBLAC (F19-1)

Sujeto obligado:	
Número de documento identificativo del sujeto obligado:	
Nombre del Representante: Principal:	
Referencia de la comunicación:	
Fecha de la comunicación:	

Identificación de los intervinientes en las operaciones:

(Condición de los intervinientes: titular, autorizado, apoderado, avalista, etc., y consignar la identificación completa de cada uno de ellos).

Conocimiento de los intervinientes en las operaciones:

(Incluir las informaciones acerca del cliente, en su caso, la correspondencia entre la actividad declarada y la actividad real y la coherencia entre la actividad y las operaciones que realizan).

Descripción de las operaciones:

(Descripción clara, precisa y detallada de las operaciones, acompañada, en los casos que se considere necesario, de gráficos o resúmenes explicativos, en el formato que se determine).

Indicios de blanqueo de capitales:

Gestiones y comprobaciones realizadas:

(Es conveniente señalar todas las gestiones y comprobaciones realizadas. El SEPBLAC, al valorarlas, tendrá en cuenta el grado de dificultad y exhaustividad con que se hayan efectuado. Precisar si se ha decidido o no por el OCI continuar adelante con la operación sospechosa y motivo de la toma de tal decisión).

Documentación remitida (relación de documentos que se adjuntan):

_____

El Representante Principal

ANEXO XIV: MODELO DE CONTROL DE ASISTENCIA AL PLAN ANUAL DE FORMACIÓN

Control de asistencia al Curso de Formación en materia de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo SEGURA E HIJOS, S.A.
Apellidos (2):
Nombre:
Empresa:
Puesto:
Teléfono:
Correo electrónico:

Datos del curso
Denominación:
Fecha:
Lugar:
Duración:

ANEXO XV: ACUSE DE RECIBO DEL MANUAL Y DE SUS ANEXOS

En el presente acto se hace entrega del Manual de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo aprobado por SEGURA E HIJOS, S.A., actualizado a fecha:

Nombre:
Empresa:
Puesto:
Teléfono:
Correo electrónico:

Recibí fecha:

_____

Nombre completo y Firma Colaborador

Datos del proveedor
Apellidos (2):
Nombre:
Empresa:
Puesto:
Teléfono:
Correo electrónico:

En el presente acto se hace entrega de copia del Acta aprobada del OCI de SEGURA ADAPTA II NUEVA PROMOCIÓN, S.L.U. en la que se recogen las facultades concretas que, en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, son de obligado cumplimiento por la Sociedad (proveedor) desde la firma del presente documento hasta la conclusión del contrato de prestación de servicios suscrito entre ambas Sociedades con fecha ___ de _____ de _____.

Recibí fecha:

_____
Nombre completo y Firma (proveedor)

ANEXO XVI: INFORME DE AUTOEVALUACIÓN DEL RIESGO ANTE EL BLANQUEO DE CAPITALES Y LA FINANCIACIÓN DEL TERRORISMO

El presente Informe de Autoevaluación del Riesgo (en adelante, "Informe") ante el Blanqueo de Capitales y/o la Financiación del Terrorismo, tiene por objeto determinar aquellos elementos de riesgo que pueden afectar a las actividades realizadas por la compañía SEGURA E HIJOS, S.A., por la posible exposición de la referida Sociedad ante el Blanqueo de Capitales y/o la Financiación del Terrorismo. El presente Informe se emite en estricto cumplimiento de las medidas de control interno para la Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo –Artículo 33.1.m, 33.1.n, y 33.2 del Real Decreto 304/2014, de 5 de mayo, que aprueba el Reglamento para la Prevención del Blanqueo de Capitales y la Financiación del Terrorismo.

1. Datos identificativos de SEGURA E HIJOS, S.A. como sujeto obligado:

La compañía SEGURA E HIJOS, S.A. tiene domicilio social en Avenida de Tenerife núm. 16, San Sebastián de los Reyes, 28703 (MADRID).

La Sociedad cuenta con personal propio y está constituida en un único centro de operaciones. En la actualidad, no cuenta con filiales, sucursales, agentes, ni Sociedades situadas fuera del territorio nacional, lo que no obsta a que pueda contar con ellas en un futuro.

2. Actividades, productos y servicios ofrecidos por SEGURA E HIJOS, S.A.:

El objeto de la Sociedad es el comercio al por mayor de madera, materiales de construcción y aparatos sanitarios.

Verificado el objeto social de la Sociedad se confirma que su actividad se encuentra expuesta mínimamente al Blanqueo de Capitales y/o la Financiación del Terrorismo, motivo por el que se han establecido e implantado estrictos mecanismos de control y prevención internos.

3. Sistemas o canales utilizados para el ingreso, movimiento y transmisión de los fondos:

[*]

4. Tipologías de los clientes y actuaciones de los clientes que puedan suponer un mayor riesgo de blanqueo de capitales y de la financiación del terrorismo:

[*]

5. Zonas geográficas de actividad del sujeto obligado:

La Sociedad basa su operativa en el Estado español con personal propio. Por el momento, no ejerce actividad social alguna a través de sucursales, agentes o sociedades situadas fuera del territorio nacional, por lo que a fecha de la presente autoevaluación no se estima la existencia de un riesgo potencial en materia de prevención del blanqueo y/o de la financiación del terrorismo.

6. **Procedimiento establecido para que el propio documento o informe de evaluación del riesgo sea periódicamente revisado y actualizado:**

Siguiendo las recomendaciones del SEPBLAC sobre las medidas de control interno para la prevención de blanqueo de capitales y de la financiación de terrorismo, se adjuntan las siguientes Fichas de Autoevaluación, cuyo examen y valoración habrá de efectuarse con carácter anual por la Sociedad y sus miembros:

Ficha de Autoevaluación de Riesgos derivados de la Actividad de **SEGURA E HIJOS, S.A..**: La Ficha analiza en tres niveles (bajo, medio, alto) el tipo de riesgo derivado de la actividad desarrollada por la Sociedad, según la percepción de la propia Sociedad. Será de obligado cumplimiento hacer constar la información mentada en la Ficha.

Ficha de Autoevaluación del Sistema de Prevención del Blanqueo de Capitales y/o la Financiación del Terrorismo: La Ficha analiza, una vez valorados los riesgos que se pudieren derivar de la actividad desarrollada por la Sociedad, la real exposición de la misma ante el blanqueo de capitales y/o la financiación del terrorismo, según la percepción que la propia Sociedad, o sus miembros, pueda tener al respecto. Será de obligado cumplimiento hacer constar la información mentada en la Ficha, y ello según lo prevenido en las recomendaciones sobre las medidas de control interno para la prevención de blanqueo de capitales y/o de la financiación del terrorismo.

FICHA DE RIESGOS DERIVADOS DE LA ACTIVIDAD DESARROLLADA POR SEGURA ADAPTA II NUEVA PROMOCIÓN, S.L.U.

ACTIVIDAD DESARROLLADA POR SEGURA E HIJOS, S.A.	EVENTUALES RIESGOS DERIVADOS DE LA ACTIVIDAD, ALGUNOS EJEMPLOS	RIESGO ANTE BC/FT
Estructura de Propiedad y Control de la Sociedad	Complejidad de la estructura de propiedad o control	
	Composición del Órgano de Administración, OCI, [Comité de Auditoría] y resto de departamentos.	
	Filiales o sucursales de la sociedad	
	Actuación a través de agentes u otros mediadores	
Actividades, productos o servicios ofrecidos por el sujeto obligado	Servicios que facilitan el ingreso o movimiento internacional de activos o fondos	
	Productos propicios al anonimato	
	Relaciones de negocio y operaciones no presenciales o a distancia, realizadas a través de medios telefónicos, electrónicos o telemáticos.	
	Negocios con personas con responsabilidad pública, zonas geográficas de alto riesgo, u otros considerados como parte del sujeto.	
	Clientes con nacionalidad de países considerados de mayor riesgo en materia de prevención	
Sistemas o canales utilizados para el ingreso, movimiento y transmisión de fondos	Transferencias nacionales o internacionales	
	Operaciones a distancia y no presenciales	
Tipología de clientes	Clientes de riesgo bajo	
	Clientes de riesgo medio	
	Clientes de riesgo alto	

Actuaciones de los clientes que puedan suponer un mayor riesgo de BC/FT	Dificultades en la aplicación de las medidas impuestas por el Manual de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo	
	Realización de operaciones sin sentido lógico o económico aparente	
	Transacciones en las que es difícil determinar el origen de los fondos	
Zonas geográficas de actividad del sujeto obligado	Paraísos fiscales	
	Países sujetos a sanciones financieras internacionales	
	Países con altos índices de corrupción	
	Países con regulaciones deficientes en materia de BC/FT	
Procedimiento establecido para que el propio Informe de Autoevaluación sea periódicamente revisado y actualizado	Auditoría externa	

Valoraciones

	Riesgo Bajo
	Riesgo Medio
	Riesgo Alto

FICHA DE AUTOEVALUACIÓN DEL SISTEMA DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y/O DE LA FINANCIACIÓN DEL TERRORISMO

En el marco de la guía sobre recomendaciones de control interno de prevención del blanqueo de capitales y/o de la financiación del terrorismo emitida por el SEPBLAC, es de obligado cumplimiento adaptar la presente Ficha o Modelo de Autoevaluación a la realidad de la actividad desarrollada por la Sociedad, así como al riesgo al que la misma pudiera estar expuesta.

		Valoraciones
Gobernanza	Involucración Órgano de Administración: información proporcionada y periódica	
	Composición del OCI	
	Representante ante el SEPBLAC o persona autorizada	
Diligencia debida	Política de aceptación de clientes	
	Catalogación de clientes en función del riesgo	
	Procedimiento de identificación: titularidad real	
	Realización de expedientes: actividad, origen de los fondos	
	Conservación de documentos: digitalización	
	Procedimientos de contratación	
	Gestión del conocimiento	
Detección, Análisis y Comunicación		
	Gestión de alertas	
	Canales de comunicación interna	
	Procesos de análisis especial	
	Comunicación al SEPBLAC	
Revisiones	Control interno	
	Auditoría externa	

Valoraciones

	Cumplimiento satisfactorio
	Grado de avance sustantivo en el proceso de implantación de medidas
	Necesidad de mejoras