

CONDICIONES GENERALES PARA LA PRESTACIÓN DE SERVICIOS EN RÉGIMEN DE SUBCONTRATACIÓN PARA SAREB

Las condiciones que seguidamente se detallan (las “**Condiciones**”) serán de plena aplicación y exigibilidad en la relación contractual que, en su caso, pudiera existir por su parte, en calidad de subcontratista (el “**Subcontratista**”) con ALISEDA SERVICIOS DE GESTIÓN INMOBILIARIA, S.L.U. como Gestor (el “**Gestor**”) de la SOCIEDAD DE GESTIÓN DE ACTIVOS PROCEDENTES DE LA REESTRUCTURACIÓN BANCARIA, S.A. (el “**Cliente**” o “**Sareb**”) bajo el Contrato para el Servicio Global de gestión de Activos de Sareb (el “**Contrato SMO II**”), para la prestación de servicios en régimen de subcontratación para dicha entidad (los “**Servicios Subcontratados**” y, el correspondiente contrato al amparo del cual se subcontraten los mismos, el “**Contrato**”, del que forman parte inseparable las presentes Condiciones). En adelante el Gestor y el Subcontratista serán denominados las “**Partes**”.

CONDICIONES:

1. ESTÁNDAR DE DILIGENCIA

El Subcontratista prestará los Servicios Subcontratados con la adecuada profesionalidad, confidencialidad, lealmente y de buena fe. En concreto, en la prestación de los Servicios Subcontratados el Subcontratista se obliga a actuar con la diligencia de un ordenado comerciante y un empresario leal, haciendo uso de los mejores recursos técnicos, humanos y materiales disponibles en cada momento que procedan para la adecuada prestación y ejecución de los Servicios Subcontratados de acuerdo con las mejores prácticas comerciales en España, cumpliendo los más estrictos y más altos estándares de calidad en la prestación y ejecución de los Servicios Subcontratados (el “**Estándar de Diligencia**”).

En particular, el Subcontratista prestará los Servicios Subcontratados con el objetivo de preservar y maximizar el valor de los activos del Cliente gestionados, en su caso, minimizando los riesgos para el Gestor y el Cliente y evitando, en todo momento, los conflictos de interés que pudieran derivarse en la prestación de los mismos.

El Subcontratista prestará los Servicios Subcontratados a su riesgo y ventura y, salvo lo expresamente previsto de otra forma, bajo su exclusiva responsabilidad, realizando todas las actuaciones que sean pertinentes para cumplir el Estándar de Diligencia, a fin de satisfacer plenamente las necesidades, requerimientos y expectativas del Cliente en los términos aquí previstos.

En aplicación del principio de buena fe contractual, el Subcontratista corregirá cualquier deficiencia advertida en la prestación de los Servicios Subcontratados, tan pronto como le sea puesta de manifiesto por el Gestor o detectada por el propio Subcontratista, debiendo comunicarla previamente al Gestor, para confirmar y consensuar la manera y procedimientos de dicha corrección.

En caso de que para la prestación de los Servicios Subcontratados, el Subcontratista deba realizar algún tipo de seguimiento o control sobre el presupuesto anual del Cliente o preste servicios relacionados con la entrega de activos inmobiliarios a la Administración General del Estado o la entidad pública correspondiente, el Subcontratista deberá dar traslado al Gestor de toda la información detallada del estado de dicho presupuesto o traslado de activos, así como el cumplimiento o incumplimiento probable, en su caso, de las dificultades o elementos que impidan o dificulten su consecución.

Asimismo, el Subcontratista en ningún momento actuará de tal forma que su actuación pueda tener un impacto negativo en la buena imagen y/o reputación del Cliente o el Gestor.

El Subcontratista se compromete en todo momento y mediante los mecanismos y formatos que se consideren necesarios, a facilitar a las personas designadas por el Gestor y/o el Cliente, en su caso, toda aquella información y documentación que el Cliente solicite, bien para disponer de pleno conocimiento de las circunstancias en las que se desarrollan los trabajos correspondientes al servicio objeto del Contrato, o bien para solucionar eventuales problemas que pudieran producirse.

El Subcontratista atenderá diligentemente cualquier Instrucción de Sareb y contestará con el nivel de diligencia previsto para la prestación de los Servicios Subcontratados cualquier cuestión, inquietud o pregunta que le pueda ser planteada por el Gestor y/o Sareb en relación con las actividades, Servicios Subcontratados y nivel de cumplimiento a que se refiere Contrato y velará porque sus subcontratistas cumplan con la misma obligación.

2. SEGURIDAD DE LA INFORMACIÓN

El Subcontratista deberá adoptar y cumplir las medidas y requisitos de seguridad (las "**Medidas de Seguridad de la Información**") que se detallan en el **Anexo 1** (Medidas de Seguridad de la Información) para la prestación de los Servicios Subcontratados. A tal efecto, el Subcontratista deberá establecer las medidas técnicas y organizativas descritas en el referido Anexo encaminadas a asegurar la integridad, confidencialidad y disponibilidad de la información tratada, obtenida y generada en el marco de la prestación de los Servicios Subcontratados, debiendo acreditar el Subcontratista al Cliente y/o al Gestor la implantación de las mismas. Asimismo, el Subcontratista deberá dar a conocer a sus empleados las Medidas de Seguridad de la Información y las consecuencias de su incumplimiento.

El cumplimiento de las Medidas de Seguridad por parte del Subcontratista (y sus empleados) tiene carácter esencial para el Gestor y el Cliente teniendo su incumplimiento la consideración de Supuesto de Resolución Anticipada, sin perjuicio de la eventual reclamación por daños y perjuicios que pueda realizarse al Subcontratista.

3. CONFIDENCIALIDAD

3.1 Preservación de Información Confidencial

Salvo por lo que respecta a los comunicados de la Información Confidencial expresamente autorizados de conformidad con la Cláusula 3.2 (Excepciones) siguiente, el Subcontratista mantendrá y tratará como privada y confidencial: (i) los específicos términos y condiciones del presente documento; y (ii) la Información Confidencial.

Las Partes no podrán revelar los específicos términos y condiciones del presente documento o la Información Confidencial a ninguna persona distinta de aquellas que integren su órgano de administración o su alta dirección, o de quienes participen en condición de asesor legal, contable, financiero o de otra especialidad, o de aquellos empleados que vayan a participar en la ejecución de los Servicios Subcontratados (respecto de asesores y empleados y subcontratistas únicamente se revelarán las secciones del Contrato y la Información Confidencial que sea necesaria para la ejecución de sus funciones), a no ser que sean requeridas para ello por cualquier órgano regulador, inspector o supervisor o instancia judicial o arbitral. Las Partes asumen la obligación de asegurar que las personas a las que se les facilite acceso al Contrato y a Información

Confidencial asumen como propias las obligaciones de confidencialidad previstas en la presente Cláusula.

A los efectos de esta Cláusula, "Información Confidencial" significa, a título meramente enunciativo pero no exhaustivo, toda aquella información de las Partes técnica o comercial, secretos de empresa, estudios, programas, conocimientos, know-how, la información relativa a la estratégica comercial y datos de análoga naturaleza pertenecientes a cualquiera de las Partes, o relativos a sus productos, servicios subcontratados, actividades, planes, estrategias, valor neto contable de los Activos Gestionados, situación financiera, presupuestos o a cualquier otro aspecto de su actividad empresarial, que no quepa razonablemente considerar en el dominio público y que haya sido proporcionada por las Partes en el marco del contrato, incluyendo la información confidencial contenida en cualquier análisis, recopilación, estudio, resumen, extracto o documentación de todo tipo elaborada por cualquiera de las Partes, a partir de Información Confidencial revelada por la otra.

3.2 Excepciones

En el caso de que cualquiera de las Partes resulte legalmente obligada a hacer pública la totalidad o parte de la Información Confidencial, o en caso de que sea requerida para ello por cualquier órgano regulador, inspector o supervisor o instancia judicial o arbitral, la Parte obligada notificará por escrito a la otra Parte tal circunstancia, a la mayor brevedad y en la medida que sea legalmente posible, indicando la Información Confidencial que le ha sido requerida divulgar.

Sin perjuicio de lo anterior y en todo caso, Sareb estará facultada para proporcionar cualquier Información Confidencial que sea requerida por los organismos a cuya supervisión se encuentra sometida, así como la que resulte necesaria para dar cumplimiento a los deberes de transparencia que le imponga la legislación vigente en cada momento, sin necesidad de consulta previa con el Subcontratista.

3.3 Comunicados de prensa

El Subcontratista no podrá emitir ningún tipo de nota de prensa, comunicado de naturaleza publicitaria, comercial o análoga, cualquiera que sea el medio de divulgación, relativo al Contrato o a los Servicios Subcontratados (sin perjuicio de las comunicaciones que puedan ser necesarias para la operativa de la prestación de los Servicios subcontratados) sin contar con el acuerdo previo por escrito de Sareb respecto de su contenido, antes de proceder a su emisión o divulgación.

No obstante lo anterior, las Partes acuerdan que podrán emitir cualquier comunicado, sin contar con la autorización de la otra Parte, a las autoridades u organismos competentes (incluyendo los organismos competentes en materia de mercados de valores y de carácter bursátil), siempre que ello fuera requerido por la legislación que le resultara de aplicación a cada una de ellas.

3.4 Vigencia

La obligación de confidencialidad de las Partes permanecerá en vigor durante toda la vigencia del Contrato y una vez extinguido éste por cualquier causa, por un plazo adicional de dos (2) años.

4. PROTECCIÓN DE DATOS

Las Partes se comprometen a cumplir con todas las obligaciones en materia de protección de datos que se derivan de la siguiente Normativa: (i) el RGPD; (ii) la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (la "**LOPDGDD**"), y (iii) cualquier otra normativa relativa a protección de datos que pueda devenir obligatoria en el futuro.

En el **Anexo 2** (Protección de Datos) se detallan las obligaciones a cumplir por el Subcontratista en materia de protección de datos.

En todo caso, formará parte del Contrato los términos y condiciones del contrato específico de sub-encargo del tratamiento (el "**Contrato de Sub-Encargo de Tratamiento**") que se adjunta como **Anexo 2(bis)** (Contrato de Sub-Encargo de Tratamiento), de obligado cumplimiento y aceptación por las Partes con la firma del Contrato, y que recoge y desarrolla las pautas de actuación por parte del Subcontratista y del Encargado del Tratamiento de conformidad con el artículo 28 RGPD.

En consecuencia, las Partes serán responsables de cualquier incumplimiento, derivado del contrato, así como, del Contrato de Sub-Encargo de Tratamiento o de la Normativa de protección de datos, que le sea imputable.

5. RIESGO PENAL Y BLANQUEO DE CAPITAL

El Subcontratista se compromete a cumplir durante toda la vigencia del Contrato con las obligaciones detalladas en el **Anexo 3** (Riesgo penal y blanqueo de capitales).

Las obligaciones del Subcontratista en relación con las obligaciones detalladas en el **Anexo 3** (Riesgo penal y blanqueo de capitales) tienen carácter esencial para el Cliente bajo el Contrato SMO II, teniendo su incumplimiento la consideración de supuesto de resolución anticipada de la relación contractual con el Gestor, sin perjuicio de la eventual reclamación por daños y perjuicios que pueda realizarse al Subcontratista, y, por tanto, tendrá igualmente dicha consideración a los efectos del Contrato.

6. PROPIEDAD INTELECTUAL

6.1 Propiedad Intelectual del Cliente y el Gestor

Todos los trabajos e información generados durante el desarrollo del Contrato serán propiedad del Gestor o de Sareb, según corresponda, que será titular de todos los derechos de propiedad intelectual e industrial de la totalidad de los trabajos y de sus resultados con las limitaciones previstas en el Texto Refundido de la Ley de Propiedad Intelectual, aprobado por RDL 1/1996, de 12 de abril y la Ley 24/2015, de 24 de julio, de Patentes, y su normativa complementaria y de desarrollo.

Los integrantes del equipo del Subcontratista que hayan participado en el Contrato se comprometerán expresamente mediante documento escrito a no divulgar información relacionada con el mismo durante su duración.

Las Partes acuerdan que el Contrato no implicará la cesión, licencia, sublicencia o derecho de uso general sobre marcas, nombres comerciales o cualesquiera otros derechos intelectuales o industriales que sean propiedad del Cliente o el Gestor, ostentando el Cliente o el Gestor, según corresponda, el derecho de uso exclusivo de conformidad con la normativa de aplicación. El Subcontratista reconoce la propiedad exclusiva del Cliente o el Gestor sobre sus derechos intelectuales o industriales. Dicha propiedad sobre derechos

intelectuales, industriales y operaciones comprende, entre otros, pero no limitados a, marcas, sistemas de información informáticos, listas diagramas, informes, manuales, materiales de apoyo y cualesquiera otros elementos complementarios a los programas, aplicaciones y/o desarrollos.

El Subcontratista manifiesta conocer la relevancia que tiene para el Cliente la utilización de la marca "Sareb" por el Subcontratista y por ello el Subcontratista no podrá usar la marca "Sareb" sin autorización expresa y escrita, y en el caso de ser autorizado deberá ajustarse a los términos y condiciones establecidos para ello.

6.2 Propiedad Intelectual generada durante la ejecución del Contrato

Las Partes acuerdan expresamente que la Propiedad Intelectual que se genere o pueda generarse durante la ejecución de los Servicios Subcontratados será en todo caso propiedad exclusiva del Cliente, que ostentará todos los derechos sobre la misma (incluidos los derechos de explotación) y los explotará de la forma que considere más apropiada, con facultad de cesión a terceros, en todo el mundo, por el máximo período de tiempo permitido legalmente, sin perjuicio de los derechos irrenunciables reconocidos a los autores e inventores en la correspondiente normativa aplicable.

A estos efectos, el Subcontratista reconoce y acepta expresamente al Cliente como único y válido titular de la mencionada Propiedad Intelectual y asume la obligación de firmar y autorizar cualquier documento y a llevar a cabo cualquier acto que sea necesario para garantizar la titularidad de la Propiedad Intelectual del Cliente, incluyendo el registro de la misma si así se solicita. El Subcontratista garantiza asimismo que se asegurará de que su personal firme también todos los documentos y lleven a cabo todos los actos que sean necesarios a tal efecto, siendo totalmente responsable frente al Cliente en el supuesto de que dichos actos no lleguen a llevarse a cabo.

Adicionalmente, el Subcontratista se obliga a prestar su plena colaboración al Cliente, en caso de que sea necesaria, para acreditar que el Cliente es el legítimo titular de la mencionada Propiedad Intelectual y, si así lo solicita el Cliente, el Subcontratista aportará asimismo la documentación firmada por sus representantes, su personal y/o los subcontratistas del Subcontratista, en su caso, en relación con la transmisión de la Propiedad Intelectual a favor del Cliente.

En caso de que el Subcontratista incumpla alguno de los términos de la presente Cláusula y/o no preste su plena colaboración y/o no aporte la documentación mencionada anteriormente, deberá exonerar y mantener indemne al Cliente frente a cualquier responsabilidad que pueda derivarse, en particular, frente a cualquier reclamación de titularidad y/o de daños y perjuicios que pueda surgir en relación con la Propiedad Intelectual mencionada.

El Subcontratista asume expresamente la obligación de asegurar la puesta a disposición y entregar toda la Propiedad Intelectual mencionada al Cliente, a petición del Gestor y en el plazo que el Cliente determine. En todo caso, la puesta a disposición y entrega de la Propiedad Intelectual se llevará a cabo en un soporte adecuado en formato electrónico editable y que permita al Subcontratista explotar la Propiedad Intelectual de manera independiente y sin recibir ayuda o asistencia adicional.

Las obligaciones y compromisos para el Subcontratista contenidas en la presente Cláusula no darán derecho al Subcontratista a solicitar ningún tipo de remuneración adicional al reconocer expresamente ambas Partes que la contraprestación por las

mismas queda incluida en sus honorarios.

A efectos aclaratorios, las Partes hacen constar expresamente que, como excepción a lo anterior será titularidad del Gestor:

- a) La Propiedad Intelectual del Gestor previa a la Fecha de Entrada en Vigor.
- b) La Propiedad Intelectual sobre los desarrollos tecnológicos en las plataformas del Gestor posteriores a la Fecha de Entrada en Vigor, siempre y cuando dichos desarrollos no estén basados en Propiedad Intelectual del Cliente.
- c) La Propiedad Intelectual sobre nuevas plataformas o herramientas de gestión que pueda crear el Gestor, siempre y cuando dichas plataformas o herramientas de gestión no estén basadas en Propiedad Intelectual del Cliente.
- d) La Propiedad Intelectual sobre las marcas que haya registrado el Gestor y pueda utilizar eventualmente para prestar los Servicios subcontratados, siempre y cuando dichas marcas no incorporen marcas o denominaciones registradas por el Cliente.

7. INDEMNIDAD

El Subcontratista responderá, personal y directamente, frente al Gestor y el Cliente del cumplimiento de las obligaciones asumidas de la prestación de los Servicios Subcontratados, respondiendo de los actos y omisiones que efectúe, tanto él mismo como las personas que dependan laboralmente o bajo cualquier otra relación, y cualesquiera otras personas jurídicas, personas físicas o entidades que sean subcontratadas por el Gestor en su nombre para la prestación de los Servicios Subcontratados. La responsabilidad del Subcontratista por los Servicios Subcontratados será de aplicación, en relación con cada uno de los Servicios Subcontratados, desde que el Subcontratista deba comenzar a prestarlos conforme a lo establecido en el Contrato.

Como consecuencia de la responsabilidad asumida por el Subcontratista, éste asume un compromiso de indemnidad frente al Cliente y el Gestor respecto de cualquier coste, daño, perjuicio, responsabilidades, reclamaciones (incluyendo, sin carácter limitativo, honorarios de abogados, peritos, procuradores, etc.), o sanción derivada de la actuación de cualesquiera intervinientes en la prestación de los Servicios Subcontratados.

Indemnidad en caso de resolución total o parcial del Contrato:

El Subcontratista deberá mantener indemne al Gestor y al Cliente respecto de cualquier deuda, coste, daño, perjuicio, indemnización, responsabilidades, reclamaciones (incluyendo, sin carácter limitativo, honorarios de abogados, peritos, procuradores, etc.), penalidad o sanción derivados de los acuerdos, contratos o relaciones jurídicas con terceros suscritos por el Subcontratista. En ningún caso podrán repercutirse al Gestor o al Cliente deuda, coste, daño, perjuicio, indemnización, responsabilidades, reclamaciones, penalidad o sanción que el Subcontratista deba satisfacer a terceros a raíz de dichas resoluciones. La indemnidad se mantendrá también tras la finalización del Contrato si el hecho trae causa de su gestión.

8. CESIÓN DEL CONTRATO A FAVOR DEL CLIENTE

El Gestor en cualquier momento, a petición del Cliente, podrá ceder su posición contractual frente al Subcontratista en relación con los Servicios Subcontratados, sin necesidad del consentimiento previo del Subcontratista.

9. AUDITORIA INTERNA SAREB

El Subcontratista se compromete a llevar a cabo todas las actuaciones necesarias para que el Gestor pueda cumplir frente al Cliente con sus obligaciones en materia de Auditoría Interna. En este sentido el Subcontratista manifiesta aceptar y conocer el alcance del **Anexo 4** (Servicio de Auditoría Interna Sareb) donde se establecen las obligaciones del Gestor frente al Cliente en materia de Auditoría Interna, obligándose a cumplirlo *mutatis mutandi* en aquello que le sea de aplicación según la naturaleza de los Servicios Subcontratados, y muy especialmente, facilitará cuanta información y documentación sea necesaria, dando acceso tanto a sus instalaciones como a sus aplicaciones informáticas.

10. CÓDIGO DE CONDUCTA SAREB

El Subcontratista reconoce haber leído y aceptado en su totalidad y sin reservas la versión en vigor del código de conducta de Sareb, publicado en la web <https://www.sareb.es> (actualmente <https://www.sareb.es/wp-content/uploads/2024/05/pol-055-codigo-de-conducta-v40-240424.pdf>, sin perjuicio de ulterior modificación por parte de Sareb) (el “**Código de Conducta Sareb**”), asumiendo su obligación de conocer y dar cumplimiento estricto al contenido de dicho Código de Conducta Sareb en cualquier operación relacionada con los activos de Sareb.

Asimismo, el Subcontratista se obliga a adoptar las medidas internas necesarias para garantizar que tanto su personal como, en su caso, sus subcontratistas, conozcan y respeten el Código de Conducta de Sareb durante toda la vigencia del Contrato.

El Gestor y/o Sareb podrán requerir, cuando lo estimen oportuno, la acreditación del cumplimiento de estas obligaciones. El incumplimiento de lo dispuesto en esta cláusula podrá ser considerado causa suficiente para la resolución anticipada del Contrato, sin perjuicio de las acciones legales que pudieran corresponder.

El Subcontratista deberá trasladar, tanto a personal propio como subcontratado, por responsabilidad funcional o por cualquier otro motivo, dispongan de Información Reservada sobre activos de Sareb, la prohibición de adquirir, alquilar o participar por cuenta propia en operaciones sobre estos activos de Sareb. Dicha prohibición se hace extensiva a sus personas equiparadas.

Se considera persona equiparada al cónyuge o persona de análoga relación de afectividad, a quienes convivan o dependan económicamente y las personas jurídicas que, no siendo sociedades de capital cotizadas en bolsa, se encuentren participadas por alguna de las personas físicas citadas anteriormente.

Se entiende por Información Reservada cualquier información no pública, incluida aquella que con vocación de serlo no hubiera sido aún difundida por los cauces previstos para ello.

El Subcontratista deberá informar inmediatamente al Gestor y a Sareb de cualquier circunstancia que pueda implicar un conflicto de intereses que pueda afectar al Gestor y/o a Sareb, de manera que el Gestor y/o Sareb puedan tomar una decisión fundada en relación con la situación sobrevenida. Esta estipulación tiene carácter de obligación esencial, por lo que su incumplimiento se considera suficiente para instar la resolución inmediata del Contrato por parte del Gestor, sin perjuicio de la eventual reclamación por daños y perjuicios que pueda realizarse a la parte incumplidora.

El Subcontratista se obliga a mantener indemne al Gestor y a Sareb frente a cualesquiera daños que cualquier Conflicto de Interés o el incumplimiento de cualquier política u obligación detallada en este documento le pueda causar al Gestor y/o a Sareb.

En especial, el Subcontratista se obliga a no promover y/o fomentar operaciones en las que concurra Conflicto de Intereses, tal y como dicho concepto está expresamente descrito en el Contrato y en el Código de Conducta Sareb.

Asimismo, el Subcontratista se obliga expresamente a denunciar y a difundir la existencia del Buzón de Denuncias y trasladar la obligación de denunciar, incluso anónimamente, a través de la dirección <https://cdd.sareb.es>, cualquier actuación que:

- 1) Implique o pudiera llegar a implicar el incumplimiento de alguna de las obligaciones legales a las que Sareb se encuentra sujeta.
- 2) Suponga el incumplimiento de los compromisos u obligaciones contenidas en el Código de Conducta en todos aquellos ámbitos que resulten de aplicación.
- 3) De ser públicamente conocida en todos sus aspectos relevantes, pudiera cuestionar la integridad de Sareb o afectar adversamente a su reputación.

Para proceder a tramitar la denuncia, mediante un sistema bien confidencial o incluso, a elección del denunciante, anónimo, delegado en un tercero ajeno a las partes (en adelante, el “**Gestor de Denuncias**”), Sareb ha habilitado la dirección <https://cdd.sareb.es> que facilita la interacción con las personas comunicantes.

El contenido de la comunicación (pero no la identidad del denunciante) será remitido por el Gestor de Denuncias al Área de Cumplimiento y Control Interno de Sareb, encargado de la gestión de las denuncias.

En ningún caso, la existencia del buzón de denuncias deberá ser considerada como eximente de la obligación de comunicación al Gestor y/o a Sareb de las denuncias de empleados y terceros recibidas directamente por el Subcontratista y que puedan afectar a éstos o los Servicios Subcontratados.

Las denuncias recogidas por los canales habilitados al efecto por el Subcontratista, o por cualquier otro cauce, que afecten a Activos Gestionados de Sareb deberán ser puestas en conocimiento de Sareb.

11. RIESGO REPUTACIONAL

El Subcontratista deberá poner en conocimiento del Gestor con la mayor antelación posible cualquier hito, evento, suceso o circunstancia que implique un riesgo reputacional para ésta, incluido un riesgo reputacional “por contagio”.

El riesgo reputacional “por contagio” se considera un subtipo del riesgo reputacional tradicionalmente considerado (el derivado de actuaciones internas o externas que pudieran afectar a la imagen de la compañía), y se circunscribe exclusivamente a aquellos casos en los que la reputación de la sociedad puede verse afectada por el hecho de que el Gestor o el Cliente se vinculen contractualmente con personas que tienen su reputación deteriorada por su potencial o probada participación en hechos delictivos.

En consecuencia, el Subcontratista deberá adoptar las medidas necesarias con la finalidad de evitar el riesgo reputacional por contagio y, por tanto, que el Gestor y/o el Cliente no se vinculen de forma alguna con personas que estén inmersas o relacionadas con una situación procesal penal conocida, para lo que deberán verificar en bases públicas, entre otras actuaciones pertinentes, la situación procesal penal de cualquier ofertante o potencial contraparte del Cliente en el marco de la prestación de los Servicios Subcontratados, o sus titulares reales, administradores sociales o representantes, y comunicar al Gestor y/o Cliente con carácter previo a la firma del contrato la existencia de

un posible riesgo reputacional, para que la situación sea valorada por el Gestor y/o el Cliente. En todo caso, el Gestor y el Cliente se reservan la posibilidad de rechazar operaciones propuestas por el Subcontratista en aquellos casos en los que considere que dicha situación procesal penal representa un riesgo reputacional para el Cliente.

ANEXO 1 – MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

1.1 INTRODUCCIÓN

El presente Anexo describe las medidas y requisitos de seguridad que el Subcontratista debe cumplir en el marco de la prestación de los Servicios Subcontratados objeto del Contrato. Por ello, el Subcontratista se compromete y obliga al cumplimiento de todas las medidas de seguridad que se describen en este Anexo y que sean de aplicación, en función de los Servicios Subcontratados y de cómo se prestan los mismos.

El Subcontratista deberá implementar las garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de información, incluidos datos personales, la destrucción o el daño accidental debiendo establecer para ello aquellas medidas técnicas y organizativas descritas en el presente anexo encaminadas a asegurar la integridad, confidencialidad y disponibilidad de la información (incluidos los datos de carácter personal) tratada en el marco de los Servicios Subcontratados contratados y/o generada u obtenida como consecuencia de la prestación de los Servicios Subcontratados y la posibilidad de demostrar que estas medidas se han llevado a la práctica con justificación suficiente a requerimiento del Cliente.

Las normas de seguridad desarrolladas en el presente Anexo pueden ser sustituidas por otras que puedan proporcionar un nivel de seguridad equivalente, de conformidad con la legislación y estándares vigentes en cada momento.

Dado el carácter específico de ciertas normas de seguridad dentro del articulado del Reglamento (UE) 2016/679 de Protección de Datos (RGPD), algunas medidas tales como la formación del personal del Encargado del Tratamiento, los deberes de confidencialidad o la necesidad de disponer de un protocolo de actuación para comunicación de violaciones de seguridad, serán parte integral del Contrato y no únicamente de sus anexos, conforme a las disposiciones del art. 28 y ss. RGPD.

El Subcontratista manifiesta comprender los requisitos de seguridad de la información descritos en el presente anexo y asociados a las características de los Servicios Subcontratados, y se obliga a dar a conocer de forma comprensible a sus empleados tanto los requisitos de seguridad exigibles como las consecuencias de su incumplimiento.

Las medidas de seguridad que se establecen a continuación y que deberá implantar el Subcontratista, siempre irán referidas a la prestación de los Servicios Subcontratados o derivado del tratamiento de información del Cliente que implique esta prestación de Servicios Subcontratados. El Subcontratista debe cumplir aquellas obligaciones asociadas a una o varias características que identifiquen tanto a los Servicios, como a su información o su tecnología, desarrolladas a continuación:

1.2 NORMAS DE SEGURIDAD A CUMPLIR POR TODOS LOS PROVEEDORES

Estas normas de seguridad son de aplicación al Subcontratista (y a todos los subcontratistas que este pueda designar de acuerdo con lo previsto en el Contrato) que durante su prestación tenga capacidad de acceso, tratamiento, transmisión y/o almacenamiento de información del Cliente.

1.2.1 Políticas de Seguridad de la Información

- a) Poseer y cumplir una Política de Seguridad -basada en las buenas prácticas

reconocidas en el mercado-, actualizada y vigente durante la prestación de los Servicios Subcontratados, así como avalada por la Dirección de la Compañía.

- b) Cumplir y hacer cumplir las medidas aplicables del presente Anexo.
- c) Cumplir y respetar las características fundamentales de Seguridad de la Información: confidencialidad, integridad, disponibilidad y resiliencia.
- d) Adoptar las medidas de índole organizativa y técnica necesarias, que garanticen la Seguridad de la Información y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
- e) Llevar a cabo procedimientos de vigilancia de nuevos requisitos legales y de cumplimiento.

1.2.2 Obligaciones relativas a los requisitos de seguridad relacionados con la clasificación de la información

- a) Disponer de procedimientos y mecanismos de clasificación de la información, de acuerdo con requisitos legales, criticidad y sensibilidad de cada tipo de información.
- b) Clasificar, etiquetar y tratar la información acorde a las necesidades identificadas. Disponer de un sistema de etiquetado de soportes que permita su marcado y clasificación de su información.
- c) No divulgar información del Cliente y/o el Gestor a terceros no autorizados, así como, evitar la fuga de dicha información. Garantizar que no se publique o divulguen datos personales, a menos que se autorice expresamente.
- d) No utilizar los nombres comerciales u otros derechos de propiedad intelectual del Cliente o el Gestor, excepto cuando sea necesario para la prestación de los Servicios Subcontratados y contando con el previo consentimiento del Cliente.
- e) No divulgar información de los Servicios Subcontratados (naturaleza, herramientas de desarrollo, arquitectura, etc.) a otro personal del Subcontratista no autorizado, así como en los perfiles profesionales de sus trabajadores.
- f) Aplicar mecanismos de destrucción segura de la información en base a su clasificación, imposibilitando la recuperación de la información destruida sea cual sea el soporte destruido y el método utilizado.
- g) Asegurar, el Subcontratista, que todas las personas autorizadas para tratar datos personales estén debidamente informadas de la confidencialidad y hayan firmado cláusulas vinculantes.
- h) Guardar secreto respecto de los datos personales que tenga acceso y trate, durante la vigencia de los Servicios Subcontratados y después de finalizar sus relaciones con el responsable de tratamiento, durante los plazos máximos previstos en la legislación vigente.

1.2.3 Obligaciones relativas a las medidas de seguridad relacionadas con el control de accesos

- a) Implementar y mantener una segregación de las funciones de la totalidad de los empleados que repercuta en la definición de roles e incompatibilidades de funciones para un mismo usuario dentro de un proceso.
- b) Reportar cualquier baja de un empleado o finalización de su participación en los Servicios Subcontratados, al que se le haya dado permiso de acceso a las ubicaciones donde se prestan los Servicios Subcontratados.
- c) Adoptar medidas de formación y concienciación sobre la custodia y uso de la información de sus puestos de trabajo, la comunicación inmediata de la pérdida o robo.
- d) Garantizar y asegurar que el acceso a los datos personales se restrinja únicamente

a aquellos empleados que necesiten acceso para cumplir con las obligaciones del encargado de tratamiento.

1.2.4 Obligaciones relativas a la seguridad en la operativa

- a) Mantener identificada la información del Cliente, así como los posibles soportes utilizados para la prestación de los Servicios Subcontratados.
- b) Disponer de procedimientos actualizados que describan la operativa para los Servicios Subcontratados y ponerlos a disposición de los empleados en todo momento.

1.2.5 Obligaciones relativas a la seguridad física y del entorno

- a) Establecer unas medidas de seguridad adecuadas en caso de almacenar información sensible del Cliente en formato físico.
- b) Contar con normas de escritorio limpio para que los puestos de trabajo estén despejados de información confidencial o secreto, con independencia del formato en el que se materialice dicha información.

1.2.6 Obligaciones relativas a las medidas de seguridad relacionadas con los recursos humanos

- a) Adoptar las medidas necesarias para garantizar que se transmita correctamente las medidas de seguridad y confidencialidad especificadas en el presente documento, así con las relativas a continuidad de negocio y de presentación de los Servicios. Adicionalmente se deberán establecer mecanismos que verifiquen el cumplimiento de las medidas anteriormente indicadas.
- b) Garantizar mediante cláusulas contractuales con sus empleados, las funciones, términos y condiciones de desempeño, responsabilidades legales, la no divulgación de información y medios a su disposición.
- c) Asegurar que no se custodie ninguna información y se cancelen las autorizaciones otorgadas en la prestación de los Servicios cuando ya no se requiera para su desempeño profesional.
- d) Informar a sus empleados sobre las responsabilidades y obligaciones en lo que respecta a la seguridad y al deber de confidencialidad, y su vigencia después de la finalización de la relación contractual.
- e) Disponer de asignaciones formales de roles y funciones en materia de seguridad, evitando incompatibilidades para no concentrarse en mismas áreas o personas.
- f) Contar con perfiles cubiertos por profesionales debidamente cualificados, así como mantener actualizados los datos de contacto de aquellas personas de interés para los Servicios.
- g) Comunicar al Gestor, para su traslado al Cliente cuando proceda, con antelación suficiente a la fecha en que se produzca, cualquier cambio en las personas designadas por el Subcontratista de interés para los Servicios Subcontratados.

1.2.7 Obligaciones relativas a las medidas de seguridad relacionadas con la monitorización de seguridad

- a) Dar la facultad al Gestor y al Cliente de realizar revisiones que pudieran ser necesarias para garantizar el cumplimiento de las medidas de seguridad expresadas en el presente documento -relacionado al servicio prestado-, así como, para verificar la confidencialidad, integridad, resiliencia y disponibilidad de los Servicios Subcontratados.
- b) Durante la vigencia de los Servicios Subcontratados, dichas revisiones podrán

realizarse con periodicidad anual. Con carácter extraordinario, también se podrá llevar a cabo revisiones cuando se realicen modificaciones sustanciales.

- c) El alcance de la revisión podrá extenderse a cualquier aspecto relacionado con los Servicios, lo que implica el acceso libre y sin restricciones. La información obtenida será tratada como confidencial.
- d) El resultado de la revisión se acordará y se decidirán las acciones que proceda implantar para solventar las cuestiones planteadas, así como, quién deberá ser responsable de acometer las acciones correctoras.
- e) Cada revisión se efectuará previa notificación por escrito al Subcontratista con un preaviso mínimo de quince (15) días a su inicio, en el que el Gestor y/o el Cliente indicarán su objeto y justificación.
- f) Colaborar y proporcionar soporte en las investigaciones de cualquier tipo que se efectúen ante requerimientos o actividades supervisoras o inspectoras de los organismos y administraciones públicas.
- g) Asegurar la custodia y retención de los registros de auditoría -logs-, mediante los mecanismos necesarios, y durante el tiempo que determinen las regulaciones, o que establezcan el Gestor y/o el Cliente, si así lo consideran oportuno por el tipo de servicio.
- h) Habilitar, definir, documentar, implementar y revisar periódicamente las trazas de actividad de los usuarios del Subcontratista recogidas en los sistemas que dan soporte a los Servicios Subcontratados.
- i) Remitir los informes de auditorías que se realicen sobre los sistemas de información que prestan soporte al Cliente en caso de ser requeridos.

1.2.8 Obligaciones relativas a las medidas de seguridad relacionadas con la gestión de incidentes de Seguridad de la Información

- a) Informar inmediatamente al Gestor de cualquier amenaza que afecte a la seguridad de la información o a la reputación del Gestor o del Cliente, incluyendo la naturaleza de la violación de seguridad, número de registros, persona de contacto, posibles consecuencias y medidas adoptadas o propuestas para su remediación.
- b) Coordinar las actividades de respuesta y comunicación de incidentes con las partes interesadas internas y externas asegurando que los tiempos de actuación cumplan con los acuerdos de indisponibilidad.
- c) Disponer de un modelo para la comunicación eficaz de los eventos de seguridad entre los distintos participantes involucrados en el proceso de detección.

1.2.9 Obligaciones relativas a los aspectos de la gestión de la continuidad del negocio

- a) Disponer de un plan de continuidad de negocio, garantizando que la información no se revela a personas no autorizadas tanto en el proceso cotidiano del negocio como ante situaciones de emergencia.
- b) Revisar y probar las estrategias y planes de respuesta y recuperación de manera periódica, o siempre que se produzcan cambios relevantes, asegurando una respuesta adecuada y sin dilación ante crisis.
- c) Asegurar que, en caso de una situación de crisis o de un desastre, los requisitos de seguridad se mantienen como parte del plan de continuidad del negocio y de prestación de Servicios Subcontratados, y del proceso de recuperación ante desastres.
- d) Prestar servicios alternativos y seguros, tanto para procesos estándar como para los procesos que se activan en el plan de continuidad del negocio.
- e) Formar a las posibles partes implicadas, como puedan ser Operaciones, Seguridad,

- Sistemas, etc. en la gestión y respuesta de incidentes de seguridad de la información.
- f) Comunicar inmediatamente y mantener informados en todo momento al Gestor y, cuando proceda, al Cliente de las actuaciones y resultados del Plan de Continuidad de los Servicios Subcontratados.

1.2.10 Obligaciones relativas al cumplimiento legal y regulatorio

- a) Identificar los requisitos legales, contractuales y regulatorios que puedan aplicar sobre la utilización, gestión y uso de información.
- b) Cumplir en toda ubicación, infraestructura o sistema relacionado con los Servicios Subcontratados, la legislación vigente y aquellas normas aplicables, con relación a la información, sus plazos de conservación y su eliminación.
- c) Asegurar que el tratamiento de datos de carácter personal en un país fuera de la Unión Europea/Suiza deberá estar adherido a algún acuerdo (por ejemplo, Privacy Shield EU-US) entre la Unión Europea/Suiza y el país en cuestión que garantice un nivel adecuado de protección. En ningún caso, se procederá a realizar la transferencia sin la previa autorización por escrito del responsable de tratamiento.
- d) Asegurar que el tratamiento de datos de carácter personal en un país fuera de la Unión Europea/Suiza y sin estar adherido a algún acuerdo (por ejemplo, Privacy Shield EU-US) entre la Unión Europea/Suiza y el país en cuestión, se deberá regir por lo estipulado en los artículos 46, 47, 48 o 49 del RGPD. En ningún caso, se procederá a realizar la transferencia sin la previa autorización por escrito del responsable de tratamiento.
- e) Asegurar que se siguen las mejores prácticas de seguridad, de acuerdo con las últimas versiones de los requerimientos vigentes de regulaciones y estándares de seguridad sobre la información de los Servicios Subcontratados.

1.2.11 Obligaciones relativas a la devolución de los Servicios Subcontratados

- a) Adoptar las medidas que defina el Cliente encaminadas a limitar el acceso a la información por terceros que causen baja en los Servicios Subcontratados.
- b) Destruir toda información propiedad del Cliente, en caso de finalización del servicio salvo que el Gestor y/o el Cliente indique que requieren la devolución de la misma. Adicionalmente el Gestor y/o el Cliente podrán solicitar que el Subcontratista aporte un certificado de terceros que verifique la destrucción.
- c) Si, debido al cumplimiento de una obligación legal el Subcontratista debiera conservar la información, deberá comunicar y justificar debidamente este hecho al Gestor y/o al Cliente. Igualmente, la conservación de la información se limitará a los mínimos necesarios para el cumplimiento del deber legal.

1.2.12 Obligaciones relativas a la gestión de activos

- a) Contar con una política de uso aceptable y seguro de activos de información aceptada por los empleados del Subcontratista, así como, cumplir con todos aquellos procedimientos asociados que se trasladen desde el Gestor y/o el Cliente.
- b) Mantener un registro de información del Cliente que contenga el responsable, tipo de información, localización, clasificación, documento o soporte, número y formato de las copias y personas autorizadas.
- c) Adoptar las medidas de seguridad dirigidas a evitar la sustracción, pérdida o acceso indebido a la información en el caso de que se produzcan envíos con información entre el Gestor y/o el Cliente y el Subcontratista.
- d) Realizar un inventariado y gestión de activos, incluyendo un registro de propiedad de

los activos de asignación al personal al cargo, realizado según las necesidades de negocio y criticidad de los activos.

1.3 NORMAS DE SEGURIDAD ADICIONALES A CUMPLIR POR LOS SUBCONTRATISTAS CON COMPONENTE TECNOLÓGICA

Estas normas de seguridad adicionales son de aplicación a todo Subcontratista que durante la prestación de los mismos acceda, procese, transmita o almacene información en sistemas tecnológicos.

1.3.1 Obligaciones relativas a las políticas de seguridad de la información

- a) Disponer de cuadros de mando e indicadores de seguridad de la información para soportar la toma de decisiones en la prestación de los Servicios Subcontratados y consiga la involucración en comités de dirección.
- b) Implementar medidas de seguridad y mecanismos que permitan:
- c) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de sistemas y servicios de tratamiento de los datos personales;
- d) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico;
- e) Verificar, evaluar y valorar la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento de datos personales;
- f) Seudonimizar y cifrar los datos personales.

1.3.2 Obligaciones relativas a las medidas de seguridad relacionadas con el análisis y evaluación de riesgo

- a) Aplicar análisis de riesgos sobre los proyectos con tecnología asociada, que incluyan una adecuada previsión de los requisitos de seguridad, continuidad o protección de datos desde el inicio del mismo.
- b) Implementar procedimientos o metodologías para la evaluación del riesgo sobre la información y la tecnología.
- c) Tanto de manera periódica, como cuando se produzcan cambios relevantes, identificar y priorizar las respuestas a los riesgos tecnológicos definiendo umbrales y escalas de valoración.
- d) Identificar, analizar, gestionar y documentar de forma periódica, los eventos de riesgo y las amenazas que afecten a los activos tecnológicos que pongan en riesgo la consecución de objetivos.

1.3.3 Obligaciones relativas a los requisitos de seguridad relacionados con la clasificación de la información

- a) Aprobar e implementar un procedimiento formal de mantenimiento, eliminación y reutilización de activos tecnológicos, con base en la clasificación de la información, según los criterios establecidos.

1.3.4 Obligaciones relativas a las medidas de seguridad relacionadas con el control de acceso

- a) Dar cumplimiento a los requerimientos establecidos sobre control de acceso a la información tratada, definidos en el presente documento.
- b) Establecer un procedimiento de gestión de usuarios que especifique el tratamiento de las credenciales y privilegios del usuario, así como su anulación cuando se

extinga la relación del usuario con el Subcontratista, el Gestor o el Cliente, según corresponda.

- c) Realizar la gestión de usuarios de los Servicios Subcontratados de forma integrada.
- d) Contar con un procedimiento de control de accesos que incluya, entre otros:
 - La gestión de altas/bajas en el registro de usuarios asegurando que se asigna un identificador único;
 - La gestión de derechos y credenciales de acceso asignados a los usuarios;
 - La gestión de privilegios especiales según el impacto que puede derivar de un uso inadecuado;
 - La gestión de información confidencial de autenticación de usuarios;
 - La política de retirada de cancelación de accesos y credenciales;
 - La revisión periódica de la información de control registrada.
- e) Disponer de mecanismos para identificar a todos los usuarios administradores y sistemas asignados para administración.
- f) Asimismo, no permitir identificadores genéricos a ser utilizados por un individuo.
- g) Habilitar, definir, documentar, implementar y revisar periódicamente las trazas de actividad de los usuarios administradores.
- h) Disponer de una relación de usuarios y perfiles identificados de forma inequívoca y personalizada.
- i) Realizar revisiones periódicas de los privilegios de los usuarios, validando que los permisos asignados sean adecuados y actualizados, de acuerdo con el principio de menor funcionalidad.
- j) Garantizar que se den de alta usuarios en los sistemas con una cuenta asociada a una única persona a la que se asignarán credenciales de acceso sin que nadie las conozca salvo el propietario del identificador.
- k) Segmentar las aplicaciones y sistemas para proteger sus registros, garantizando que el acceso esté debidamente protegido.
- l) Asegurar que el acceso a las aplicaciones, servicios y sistemas se realiza mediante el uso de contraseñas, que se modifican de forma periódica, siguen formatos complejos y guardan un histórico de las mismas.
- m) Disponer de mecanismos de autenticación centralizados que no muestren la contraseña en claro, ni muestren información que pudiera ayudar a un intruso en caso de error de autenticación.
- n) Disponer de mecanismos seguros de autenticación, que garanticen el cambio de contraseña inicial tras el primer acceso de los usuarios a los sistemas y aplicaciones.
- o) Tener un procedimiento de distribución de contraseñas seguro que incluya la transmisión cifrada de las contraseñas si ésta se realiza a través de la red.
- p) Fijar un tiempo máximo de inactividad para la sesión, procediendo a invalidar la misma transcurrido el período de tiempo que se determine de inactividad.
- q) Mantener un registro de accesos, en el que se detalle usuario, fecha y hora, fichero e información accedida, tipo de acceso, y si ha sido autorizado o denegado. Revisar dichos accesos periódicamente.

1.3.5 Obligaciones relativas a la seguridad en la operativa

- a) Establecer políticas y procedimientos, e implementar medidas técnicas para inventariar, documentar y mantener los flujos de datos de aplicaciones y servicios distribuidos dentro de la infraestructura de red.
- b) Asegurar que los intercambios de información a través de sistemas o componentes hayan sido verificados según las necesidades del Subcontratista, del Gestor y del

Cliente, así como, la integridad del flujo de información.

- c) Configurar los sistemas de acuerdo con el principio de menor funcionalidad, de tal manera que se habiliten únicamente las funciones esenciales para llevar a cabo las tareas que son objetivo del diseño.
- d) Garantizar que los relojes de todos los sistemas de tratamiento de información involucrados están debidamente sincronizados con una única fuente precisa y acordada de tiempo.
- e) Restringir la instalación de software no homologado sin consentimiento explícito y realizar controles en los equipos sobre el software instalado.
- f) Garantizar la completa destrucción de la información del Gestor y/o Cliente contenida en los equipos, empleando los mecanismos necesarios para impedir la recuperación total o parcial de ésta por parte de un tercero.
- g) No permitir en ningún caso la impresión de información con datos reales propiedad de Sareb que no haya sido previamente autorizado por el responsable correspondiente.

1.3.6 Obligaciones relativas a la seguridad física y del entorno

- a) Proteger los sistemas tecnológicos de las amenazas y los riesgos ambientales, así como de las eventualidades de que se produzcan accesos físicos no autorizados al dispositivo, redes o periféricos.
- b) Contar con medios que garanticen la seguridad del cableado y cualquier otro medio por el que se pueda transmitir información, así como, estar correctamente identificados y etiquetados.
- c) Adoptar todas las precauciones y medidas encaminadas a la limitación de capacidades para usar medios de almacenamiento extraíbles.

1.3.7 Obligaciones relativas a las medidas de seguridad relacionadas con los recursos humanos

- a) Definir los roles y responsabilidades de los usuarios en aplicaciones. Revisar periódicamente los permisos de los usuarios con el fin de detectar y solventar asignaciones de funciones inadecuadas.
- b) Facilitar toda colaboración para mantener tareas de coordinación entre responsables de Seguridad del Subcontratista, del Gestor y, cuando proceda, del Cliente, o aquellas actividades necesarias para el seguimiento del desempeño de los Servicios Subcontratados.

1.3.8 Obligaciones relativas a las medidas relacionadas a la adquisición, desarrollo y mantenimiento de los sistemas de información

- a) Realizar pruebas de usuarios sobre las nuevas aplicaciones y sistemas para validar que cumplen todos los requerimientos funcionales, así como cualquier requerimiento en materia de seguridad.
- b) Disponer de un proceso formal para la adquisición de hardware o software que tenga en cuenta los requisitos de seguridad y de compatibilidad.
- c) Establecer los controles de seguridad adecuados en relación con la adquisición o desarrollo de nuevas aplicaciones o sistemas para la prestación de los Servicios Subcontratados.
- d) Disponer de una infraestructura tecnológica en la cual se establezcan medidas que permitan la separación lógica de información en aquellas infraestructuras que sean compartidas.

- e) Probar actualizaciones de software y nuevas licencias en entornos previos y aplicarlas antes de su puesta en producción.
- f) Evaluar la integridad de la información, su efectividad y efectos colaterales.
- g) Realizar revisiones de seguridad sobre cualquier componente del sistema incorporado en los Servicios Subcontratados en entornos diferentes al de producción.

1.3.9 Obligaciones relativas a las medidas relacionadas con la seguridad de las comunicaciones

- a) Disponer e implantar un mapa completo de la red, así como proporcionar al Gestor y/o al Cliente el detalle de las medidas de seguridad perimetral aplicadas sobre los Servicios Subcontratados.
- b) Identificar los requisitos y los niveles de servicio de comunicaciones a través de redes internas y externas en base a las características de los Servicios Subcontratados a prestar.
- c) Restringir el acceso a internet, de manera que el uso quede limitado a través de proxy.
- d) Disponer, en lo referente al intercambio de información a través de correo electrónico, de medidas de seguridad que protejan tanto el cuerpo del mensaje como los adjuntos.
- e) Establecer el cifrado de comunicaciones que se realicen a través de redes públicas y/o privadas y a través de las cuales viaje información, especialmente cuando se trate de información confidencial.
- f) Impedir el envío de información sensible a través de correo electrónico, sino realizarlo a través de pasarelas de comunicación destinadas a tal fin.
- g) En las comunicaciones con clientes, proteger las redes de comunicaciones por medios técnicos para controlar que se produzcan de manera que se asegure la integridad sobre la información enviada.

1.3.10 Obligaciones relativas a las medidas relacionadas con el cifrado y criptografía

- a) Disponer de un proceso de gestión de claves criptográficas que permita garantizar el ciclo de vida de las mismas, y las asegure frente al acceso y uso no autorizado.
- b) Almacenar cifradas las contraseñas y las credenciales para impedir su revelación o reutilización por terceras partes, en caso de ser extraídas.
- c) Contar con controles de cifrado, ya sea de terminales móviles, discos, portátiles, dispositivos externos, aplicaciones web, sistemas de transferencia de información, o correo electrónico.
- d) Garantizar que la información que se almacene en los dispositivos móviles esté en todo caso cifrada con un algoritmo fuerte y reconocido.
- e) Disponer de un servicio específico de intercambio de archivos, o bien mediante correo electrónico cifrado, para realizar los intercambios de archivos electrónicos entre el Gestor y/o el Cliente y el Subcontratista.
- f) Evitar el tratamiento de datos en dispositivos portátiles que no permitan su cifrado, con el fin de garantizar que dicha información no sea inteligible ni manipulada.
- g) Llevar a cabo seudonimización de datos reales y garantizar su integridad y confidencialidad.
- h) Distribuir y transmitir la información de carácter personal del Cliente de forma cifrada con el fin de garantizar que dicha información no sea inteligible ni manipulada. Evitar su tratamiento en dispositivos portátiles que no permitan su cifrado.

- i) Asegurarse de que, cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, se utilice un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido.

1.3.11 Obligaciones relativas a las medidas de seguridad relacionadas con la monitorización de seguridad

- a) Revisar los accesos a los servicios de red periódicamente, en especial los servicios de red externos.
- b) Almacenar logs y trazas de la incidencia al menos durante siete (7) días desde la notificación de la misma, y salvaguardar y aislar cuantas evidencias sean de utilidad para realizar una copia forense.
- c) Almacenar los logs con un formato y contenido adecuados para poder llevar a cabo la trazabilidad de los eventos.
- d) Permitir al Gestor y/o al Cliente, en caso de necesidad, realizar el análisis de los logs de los sistemas, trazas de los elementos de IDS, firewall y cualquier elemento de red y seguridad asociados a los Servicios.
- e) Aportar cualquier información requerida relativa a la seguridad de la información de los Servicios cuando se solicite, como: actividad de usuarios y sistemas, cambios efectuados, registro de eventos o alertas de seguridad.

1.3.12 Obligaciones relativas a las medidas de seguridad relacionadas con las amenazas informáticas

- a) Mantener y probar la adecuada y oportuna detección de cualquier tipo de evento anómalo que pueda afectar al objetivo y calidad de los Servicios Subcontratados.
- b) Facilitar información sobre amenazas potenciales para el Cliente desde foros y fuentes de intercambio de información.
- c) Realizar ciberejercicios de simulación de incidentes de seguridad de la información.
- d) Disponer de mecanismos de gestión de versiones y parches de sistemas y asegurar su distribución de forma centralizada, gestionando el estado de actualización de dichos sistemas y equipos.
- e) Disponer de sistema antivirus con actualización automática y diaria, firewall local activado y de un sistema de cierre automático de sesión en los equipos informáticos.

1.3.13 Obligaciones relativas a las medidas de seguridad relacionadas con la gestión de incidentes de seguridad de la información

- a) Seguir un proceso de gestión de incidentes y brechas de seguridad según marca la legislación vigente y las buenas prácticas del mercado reconocidas, colaborando en todo lo necesario con el Cliente para llevar a cabo dicha gestión y cumplir con sus obligaciones de información.
- b) Proporcionar al Gestor y/o al Cliente los recursos necesarios para el análisis de una incidencia y su subsanación.
- c) Garantizar la implantación de los requisitos de seguridad y de comunicar cualquier incidente que afecte al sistema de información contratado ya sea directa o indirectamente.
- d) Realizar un análisis técnico, en caso de incidente, para establecer el origen, la debilidad que se está explotando y toda aquella información necesaria, de cara a definir pautas de resolución del incidente.
- e) Realizar pruebas periódicas del plan de respuesta, y aplicar las lecciones aprendidas

de estas pruebas para la mejora del proceso.

- f) Informar de forma inmediata de los incidentes de seguridad, reportando y detallando el incidente en los tiempos estipulados por el Gestor y/o el Cliente, una vez que se ha producido.
- g) Notificar inmediatamente al Gestor y, cuando proceda, al responsable del tratamiento, y en cualquier caso antes del plazo máximo de setenta y dos (72) horas desde que se tenga conocimiento o se sospeche la existencia de un tratamiento ilícito de datos personales responsabilidad del Cliente, incluyendo toda la información relevante para la documentación y comunicación de la incidencia.
- h) Incluir en dicha notificación del Subcontratista al Gestor y, cuando proceda, al Cliente, al menos:
 - La naturaleza de la violación de la seguridad de los datos personales, categorías y número aproximado de interesados afectados y registros de datos personales afectados;
 - El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
 - Las posibles consecuencias de la violación de la seguridad de los datos personales.
 - Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

1.3.14 Obligaciones relativas a los aspectos de la gestión de la continuidad del negocio

- a) Establecer planes de recuperación de los sistemas que permitan el restablecimiento en el tiempo tolerable de indisponibilidad, según el tiempo objetivo de recuperación y el punto objetivo de recuperación.
- b) Disponer de un plan de continuidad de servicios de TI que contemple los sistemas y componentes que procesan información del Cliente, incluyendo otras ubicaciones y centros de procesamiento de datos.
- c) Conservar los planes de respuesta, de recuperación y el resto de documentación necesaria para gestionar un incidente/ crisis, en la ubicación destinada a tal efecto y conocida por todas las partes.
- d) Contar con un grupo definido para la gestión de crisis e incidentes con personal identificado con el suficiente nivel para coordinar un incidente que repercuta en la continuidad de los Servicios Subcontratados al Cliente.
- e) Revisar las estrategias y planes de respuesta y recuperación sobre sus principales subcontratistas o proveedores de segundo nivel.
- f) Realizar una evaluación de impacto en el negocio que determine las necesidades para seguir operando de forma normal en caso de contingencias o desastres.
- g) Analizar e identificar las necesidades sobre instalaciones alternativas ante una contingencia que suponga indisponibilidad de la ubicación principal.
- h) Contar con un plan de prevención de riesgos en el que se adopten medidas como el almacenamiento de datos distribuidos, sistemas de alimentación eléctrica de soporte, políticas de backups, duplicación de sistemas críticos o sistemas de seguridad pasivos.
- i) Disponer de los criterios de activación y ejecución del plan de recuperación, de cómo reorganizar al personal involucrado, cómo reestablecer los sistemas necesarios, o cómo recuperar los datos.
- j) Destinar los recursos suficientes, tanto en el plano humano como de equipamiento

(software y hardware), que garanticen la continuidad los niveles de calidad acordados.

1.3.15 Obligaciones relativas a las medidas de seguridad relacionadas a la gestión de respaldo de información

- a) Aplicar procesos para realizar copias de seguridad, periodicidad, sistemas de almacenamiento y custodia, procesos de restauración y registro de las acciones realizadas a lo largo del tiempo.

1.3.16 Obligaciones relativas a la subcontratación

- a) Mantener identificadas las empresas subcontratadas involucradas en los Servicios Subcontratados y trasladar los requerimientos de seguridad establecidos en el presente Anexo a las que el Subcontratista deberá garantizar que dan cumplimiento a los mismos.
- b) Gestionar adecuadamente los cambios en los servicios del subcontratista de segundo nivel que afecten a sistemas de Sareb para garantizar que las condiciones de seguridad y disponibilidad se mantienen.
- c) Monitorizar el cumplimiento de los requisitos depositados en el subcontratista de segundo nivel para detectar posibles eventos de seguridad que pueda afectar a su información. El Subcontratista responderá de cualquier incumplimiento y de las consecuencias de los posibles daños o perjuicios que pudiera causar al Cliente.

1.3.17 Obligaciones relativas a la finalización de los Servicios Subcontratados

- a) Proporcionar mecanismos de portabilidad de información, que facilite al Cliente la incorporación de los datos al sistema, permitiendo asegurar la integridad de los mismos.

1.3.18 Obligaciones relativas a la gestión de activos

- a) Gestionar, identificar e inventariar cualesquiera aplicaciones, bases de datos, sistemas operativos (software y hardware), según marcan los estándares de seguridad de la información y buenas prácticas.
- b) Catalogar los soportes tecnológicos, debiendo existir un registro de entrada, salida, utilizados, borrados. El traslado de los soportes informáticos deberá garantizar que no existan recuperaciones indebidas.
- c) No permitir el almacenamiento de cualquier tipo de información con datos reales propiedad del Cliente en dispositivos de almacenamiento de usuario a menos que Sareb lo haya autorizado expresamente.
- d) Proteger y gestionar los dispositivos móviles de forma remota. Implementar los controles y mecanismos de seguridad necesarios para proteger los dispositivos portátiles y móviles de la organización.
- e) Proteger toda la información a la que acceda y los soportes que la contengan contra accesos no autorizados, usos indebidos o deterioro, empleando para ello las medidas técnicas adecuadas.
- f) Contar con un procedimiento formal de mantenimiento, eliminación y reutilización de activos tecnológicos y la información tratada acorde a los requerimientos de los Servicios Subcontratados.
- g) Hacer uso de medidas físicas y lógicas necesarias para garantizar la irrecuperabilidad de documentación destruida de documentos o soportes electrónicos que contengan información del Cliente.

- h) Implementar los mecanismos de seguridad necesarios para que el Subcontratista realice una correcta administración y operación de los dispositivos de seguridad.

1.4 NORMAS DE SEGURIDAD ADICIONALES A CUMPLIR POR LOS SUBCONTRATISTAS QUE PRESTEN SERVICIOS CONECTADOS A LA RED DEL CLIENTE

Estas normas específicas de seguridad son de aplicación a todo Subcontratista que preste Servicios Subcontratados comunicándose con la red del Cliente. Se entiende por red del Cliente los puestos de trabajo, servidores y dispositivos de comunicación propiedad del Cliente, ubicados en sus instalaciones o conectándose a estos de forma telemática.

1.4.1 Obligaciones relativas a las medidas de seguridad relacionadas con el control de acceso

- a) Comunicar a sus empleados las normas e indicaciones de seguridad - expresados en el presente documento - aplicables a sus accesos a los sistemas del Cliente, debiendo vigilar su cumplimiento y seguimiento de forma adecuada.
- b) Utilizar los usuarios y credenciales emitidos por el Cliente para cada persona, con carácter intransferible, para acceder a los sistemas del Cliente, de forma local o remota.

1.4.2 Obligaciones relativas a las medidas relacionadas con la seguridad de las comunicaciones

- a) Aplicar las medidas de seguridad expresadas en el presente documento, los niveles de servicio y los requisitos de gestión de los servicios de red que se requieren para la prestación de los Servicios Subcontratados hacia el exterior a través de internet.
- b) Contar con una política de gestión de seguridad en las redes que deberá proponer mecanismos asociados a servicios en red y disponer de controles de red y políticas de segregación de redes.
- c) Garantizar que las comunicaciones entre su infraestructura y la del Cliente conserven la confidencialidad, integridad y disponibilidad de la información, limitándose a las necesidades de los Servicios Subcontratados.
- d) Implementar mecanismos de autenticación que garanticen la comunicación inequívoca.
- e) Proveer un sistema de comunicaciones con un nivel de seguridad equivalente al acceso local, de forma cifrada, autenticadas en cada extremo, ocultas hacia el exterior, solamente disponibles desde direcciones IP pertenecientes al Cliente y filtradas en cada extremo.

1.4.3 Obligaciones relativas a los aspectos de la gestión de la continuidad del negocio

- a) Garantizar que cuando el entorno se encuentre fuera de las dependencias del Cliente, la conexión a la misma sea consistente y segura proporcionando disponibilidad y protección frente a pérdida de datos.

1.5 NORMAS DE SEGURIDAD ADICIONALES A CUMPLIR POR LOS SUBCONTRATISTAS QUE PRESTEN LOS SERVICIOS SUBCONTRATADOS DESDE SUS PROPIOS SISTEMAS

Estas normas específicas de seguridad son de aplicación a todo Subcontratista que preste los Servicios Subcontratados en sus instalaciones o centros, utilizando puestos de trabajo,

servidores y dispositivos de comunicación de su propiedad.

1.5.1 Obligaciones relativas a las medidas de seguridad relacionadas con el análisis y evaluación de riesgos

- a) Analizar la necesidad y la idoneidad de permitir la operación de forma remota, evaluando las medidas específicas de seguridad para garantizar la confidencialidad de estas comunicaciones.

1.5.2 Obligaciones relativas a las medidas de seguridad relacionadas con el control de accesos

- a) Establecer procedimientos de acceso a sistemas de información y aplicaciones, inicio seguro de sesión, validación de parámetros de identificación, gestión de contraseñas y herramientas de administración.
- b) Implementar mecanismos de segregación para garantizar que la información del Cliente sea únicamente accesible por el interesado para el desarrollo de sus funciones, proporcionando un aislamiento efectivo.
- c) Garantizar la diferenciación de usuarios en los distintos entornos, de manera que los usuarios de los entornos no productivos sean distintos a los usados en entornos de producción.
- d) Limitar y registrar los privilegios asignados a los usuarios que gestionan los procesos offline para garantizar que no se producen modificaciones/eliminaciones no deseadas.
- e) Asegurar que existe un control de sesiones concurrentes de usuario independientemente del dispositivo desde el que se acceda.
- f) Asegurar el acceso de administradores a sistemas de información y/o a herramientas de administración de sistemas que prestan servicio a Sareb mediante canales cifrados, autenticación fuerte, tokens, etc.
- g) Garantizar el acceso a la información mediante mecanismos restrictivos, evitando el acceso no autorizado, siguiendo reglas de autenticación, autorización y gestión de cuentas aceptadas por la industria.

1.5.3 Obligaciones relativas a la seguridad en la operativa

- a) Definir un diagrama que detalle el flujo de datos en los procesos que se desarrollan dentro de su infraestructura tecnológica.
- b) Dimensionar los sistemas para hacer frente de manera dinámica a las fluctuaciones de volumen de transacciones.
- c) Monitorizar la capacidad de los sistemas para detectar fallos de disponibilidad.
- d) Garantizar que las transacciones que se ejecuten a través de un planificador se gestionen de manera segura, debiendo ser aprobadas por el usuario y monitorizadas a lo largo de su ciclo de vida.
- e) Disponer de procedimientos para controlar los cambios planificados y de emergencia sobre la configuración e instalación del software en explotación.
- f) Solamente crear ficheros temporales cuando resulte preciso para la realización de trabajos temporales o auxiliares y deber cumplir las mismas medidas de seguridad que los ficheros originales.
- g) Aplicar procedimientos de control de ficheros temporales, de manera que los ficheros generados sean eliminados y existan mecanismos para verificar que no queda información no controlada.

1.5.4 Obligaciones relativas a la seguridad física y del entorno

- a) Proteger las áreas que contienen información del Cliente, estableciendo un procedimiento de control que incluya controles físicos, perímetro de seguridad, protección contra amenazas externas o ambientales.
- b) Controlar y aislar recursos de tratamiento de información en el acceso a las instalaciones del Subcontratista, garantizando que se realice de forma individual y permita identificar a las personas con autorización.
- c) Solicitar la identificación visible y permanente del personal y registrar las entradas y salidas del mismo a las áreas de tratamiento de información.
- d) Proteger las áreas de sistemas tecnológicos con información del Cliente, estableciendo controles de autorización, acceso, perímetro de seguridad o protección contra amenazas externas o ambientales.

1.5.5 Obligaciones relativas a las medidas relacionadas con la seguridad de las comunicaciones

- a) Identificar las características de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red que se requieren para la prestación de los Servicios Subcontratados hacia el exterior a través de internet.
- b) Contar con una política de gestión de seguridad en las redes que proponga mecanismos de seguridad asociados a servicios en red y disponer de controles de red y políticas de segregación de redes.
- c) Implementar mecanismos de autenticación que garanticen la comunicación inequívoca.
- d) Aislar completamente la red interna, a partir de comunicaciones, sistemas y aplicaciones destinados al Servicio Subcontratado, del resto de su red, y de las otras redes que utilice el Subcontratista para otros clientes.
- e) Garantizar que los entornos compartidos estén aislados para que no se propague el efecto de un ataque, a nivel físico y/o lógico, es decir, a nivel de dispositivos de comunicación y líneas dedicadas.
- f) Implementar mecanismos de seguridad necesarios que permitan el almacenamiento cifrado de información del Cliente, tanto en servidores y unidades de almacenamiento como en copias de seguridad.

1.5.6 Obligaciones relativas a las medidas de seguridad relacionadas con la monitorización de seguridad

- a) Monitorizar actividades y acciones sobre la infraestructura tecnológica, red y plataforma con la finalidad de detectar potenciales eventos de seguridad como intrusiones, código malicioso, ataques de denegación de servicio y sustracción de información.
- b) Registrar y monitorizar la actividad de usuarios, con independencia de su perfil, de los sistemas involucrados directa o indirectamente, incluyendo sistemas intermedios de almacenamiento temporal.
- c) Las labores de administración a través de programas de asistencia remota deben quedar registrada, identificando unívocamente al administrador que se encarga de realizarla y las acciones llevadas a cabo.
- d) Realizar tareas de monitorización activa para la pronta gestión de alertas, notificando inmediatamente al Cliente sobre posibles violaciones de seguridad sobre los sistemas de información.
- e) Solventar las debilidades de control identificadas en las revisiones realizadas

siguiendo los planes de acción acordados.

- f) Emitir métricas que reflejen el grado de cumplimiento de las medidas de seguridad.
- g) Garantizar que toda la actividad realizada remotamente sobre sesiones de usuarios quede registrada, identificando unívocamente al administrador que se encarga de realizarla y las acciones llevadas a cabo.
- h) Disponer de un plan de gestión y auditoría que permita identificar las vulnerabilidades de los activos críticos con base en una planificación periódica y siempre que se produzcan cambios significativos.
- i) Contar con un registro de ubicaciones de sistemas de captación de imágenes y monitores de observación.
- j) Conservar las imágenes por el plazo máximo permitido por las legislaciones aplicables, salvo que su conservación resulte necesaria para investigar un hecho que haya afectado a la seguridad de las personas, bienes e instalaciones.

1.5.7 Obligaciones relativas a las medidas de seguridad relacionadas con los procesos de detección

- a) Garantizar que los eventos detectados que supongan una desviación significativa sobre los parámetros de la línea base generen una alerta que permita analizarlos y determinar si constituyen un ataque.
- b) Realizar pruebas de eficacia y eficiencia sobre los sistemas de detección para asegurar que éstos funcionan correctamente y que responden correctamente a su objetivo de diseño.
- c) Disponer de mecanismos de monitorización, registro y bloqueo de usuario ante intentos reiterados de acceso a los sistemas de manera fallida. Dichos intentos serán considerados eventos de detección.

1.5.8 Obligaciones relativas a las medidas de seguridad respecto a revisiones de Sistemas de Información

- a) Posibilitar la integración con módulos de terceros y aplicaciones instaladas localmente independientemente de dónde se encuentre alojada la solución.
- b) La arquitectura de la plataforma de administración deberá ser independiente de la configuración del centro de procesamiento de datos y la ubicación de este.

1.5.9 Obligaciones relativas a las medidas de seguridad relacionadas con las amenazas informáticas

- a) Garantizar que existan medios de protección frente a ataques de fuerza bruta o ataques de denegación de los Servicios Subcontratados prestados al Cliente.
- b) Implementar mecanismos automatizados y manuales para la detección y prevención de código malicioso.

1.5.10 Obligaciones relativas a las medidas de seguridad relacionadas con la gestión de incidentes de seguridad de la información

- a) Tener implementado un procedimiento de gestión de incidentes y brechas de seguridad que permita su identificación, tratamiento y notificación al órgano correspondiente según su naturaleza.
- b) Analizar y clasificar las alertas de los sistemas de detección y monitorización para determinar la existencia de uso indebido, incidentes y su impacto.
- c) Registrar las evidencias obtenidas durante el análisis de los incidentes de acuerdo con el principio cadena de custodia para asegurar su validez ante cualquier

procedimiento judicial, pericial, etc.

- d) Mantener un registro de incidencias y los procedimientos necesarios de recuperación de datos, con la finalidad de realizar tareas de aprendizaje y mejora continua. Reportar periódicamente el estado de la resolución de incidencias sobre sistemas asociados a los Servicios Subcontratados.
- e) Realizar todas aquellas actividades que sean necesarias para detener la propagación de un incidente, con el fin de evitar que se vean afectados nuevos activos o afectar a terceras partes conectadas.

1.5.11 Obligaciones relativas a las medidas de seguridad relacionadas a la gestión de respaldo de información

- a) Realizar copias de seguridad sobre la información, los registros, el software y los sistemas con el fin de ser capaces de recuperar un estado anterior de los mismos ante una contingencia.
- b) Realizar copias de seguridad con una periodicidad mínima semanal en un segundo soporte distinto del destinado a los usos habituales.
- c) Realizar pruebas periódicas de restauración de copias de seguridad sobre los sistemas para verificar que los procedimientos de copias y recuperación son adecuados.
- d) Controlar el acceso a las copias de seguridad y los sistemas que las gestionan y garantizar que permanecen inalteradas, restringiendo el acceso al personal mínimo necesario.
- e) Contar con un procedimiento de recuperación de datos cuya ejecución debe ser autorizada por el responsable del fichero.
- f) Almacenar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan.

1.5.12 Obligaciones relativas al cumplimiento legal y regulatorio

- a) Las actividades de monitorización de redes y sistemas del Cliente realizadas por el Subcontratista deberán respetar los derechos fundamentales y la privacidad de los usuarios.

1.6 NORMAS DE SEGURIDAD ADICIONALES A CUMPLIR POR LOS SUBCONTRATISTAS QUE DESARROLLEN SOFTWARE PARA EL CLIENTE

Estas normas específicas de seguridad son de aplicación a todos los Subcontratistas que presten Servicios Subcontratados de desarrollo y mantenimiento de software.

1.6.1 Obligaciones relativas a las medidas relacionadas a la adquisición, desarrollo y mantenimiento de los sistemas de información

- a) Garantizar que el ciclo de vida de desarrollo de sistemas se controla de principio a fin, garantizando que las distintas actividades incluidas en el ciclo se realicen conforme a la metodología definida.
- b) Incluir los requerimientos del usuario, las pruebas y la información técnica sobre medidas de seguridad en la documentación del sistema.
- c) Garantizar que la configuración de referencia de los sistemas se realice teniendo en cuenta la menor funcionalidad.
- d) Llevar a cabo actualizaciones de configuración de acuerdo con las mejores prácticas.

- e) Asegurar que los desarrollos de aplicaciones usen datos no reales o en su caso anonimizados o enmascarados que garantice que el proceso no es reversible.
- f) Garantizar la segregación física y lógica entre entornos de desarrollo, prueba y producción, y proponer mecanismos asociados a servicios en red, controles de red y políticas de segregación de redes.
- g) Garantizar que el proceso de subida a producción esté en todo momento controlado y aprobado por el usuario, y que durante dicho proceso se aplique una correcta segregación de funciones.
- h) Restringir el acceso al código fuente de las aplicaciones en entornos productivos a personal limitado e identificado, registrando la trazabilidad de las acciones que realizan.
- i) Probar los nuevos desarrollos o las modificaciones realizadas sobre el software existente en los Servicios Subcontratados prestados al Cliente.
- j) Poner a disposición del Gestor y/o del Cliente aquellos desarrollos de software hechos a medida por el Subcontratista para Sareb, incluyendo código fuente, código objeto, manuales o cualquier otra información relevante.
- k) Realizar un procedimiento para la gestión de cambios que pudieran ser necesarios realizar sobre aplicaciones o sistemas involucrados y disponer de módulos de control de errores.
- l) Definir las pruebas de seguridad en el ciclo de vida de desarrollo a todos los niveles de pruebas: unitarias, integradas, funcionales y de aceptación.
- m) Garantizar que las librerías se mantienen actualizadas y libres de vulnerabilidades conocidas que puedan poner en riesgo todas las aplicaciones desarrolladas con las citadas librerías.

1.7 NORMAS DE SEGURIDAD ADICIONALES A CUMPLIR POR LOS SUBCONTRATISTAS QUE OFREZCAN A SAREB SERVICIOS UBICADOS EN LA NUBE (CLOUD COMPUTING)

Estas normas específicas de seguridad son de aplicación a todo Subcontratista que presta servicios bajo infraestructura cloud.

1.7.1 Obligaciones relativas a las medidas de seguridad relacionadas con el análisis y evaluación de riesgo

- a) Realizar un análisis de riesgos en base a la ubicación geográfica de los servidores de datos que se alojen en infraestructuras cloud.
- b) Garantizar la ubicación de los datos en sistemas compartidos cloud, especialmente los considerados de carácter personal, y de la misma manera garantizar que se cumplen los requisitos legales y regulatorios tanto del país de origen como del país de destino.

1.7.2 Obligaciones relativas a los requisitos de seguridad relacionados con la clasificación de la información

- a) Asegurar que se implantan las medidas de seguridad más restrictivas en el tratamiento de la información en los sistemas cloud.

1.7.3 Obligaciones relativas a las medidas de seguridad relacionadas con el control de accesos

- a) Asegurarse de que existe segmentación del acceso a las sesiones y datos en arquitecturas compartidas cloud.

- b) Garantizar que, en los sistemas cloud, se tomarán las medidas necesarias para que exista un aislamiento y protección total de los recursos.

1.7.4 Obligaciones relativas a la seguridad en la operativa

- a) Garantizar en todo momento la integridad de todas las imágenes de las máquinas virtuales. Cualquier cambio realizado en las imágenes de las máquinas virtuales debe ser registrado.
- b) Proporcionar, si así se le solicita, información sobre el estado de actividad de las máquinas virtuales, así como de las versiones necesarias de los sistemas operativos que se ejecutan en ellas.

1.7.5 Obligaciones relativas a las medidas relacionadas a la adquisición, desarrollo y mantenimiento de los sistemas de información

- a) Proteger la información que se transmite estableciendo medidas relativas al desarrollo de una infraestructura de seguridad, implementando sistemas para almacenaje y transmisión de información, manteniendo compatibilidad con los sistemas, aplicando medidas de cifrado y controlando su acceso.
- b) Proporcionar la información técnica sobre los recursos que va a servir al Cliente, con el objetivo de que se puedan realizar test de compatibilidad de aplicaciones antes de la implementación.
- c) Garantizar que todos los sistemas software intervinientes en la prestación de servicios cloud están actualizados a la última versión disponible, mediante procedimientos de actualización periódica.
- d) Las aplicaciones multicliente, ya sean de propiedad o administradas, y el sistema de infraestructura y componentes de red, deberán estar diseñados, desarrollados, desplegados y configurados de tal manera que el acceso del Subcontratista y del Cliente esté adecuadamente separado del resto.

1.7.6 Obligaciones relativas a las medidas relacionadas con la seguridad de las comunicaciones

- a) Garantizar que las comunicaciones entre la infraestructura del Subcontratista y del Cliente se produce mediante mecanismos necesarios para la confidencialidad, integridad y disponibilidad de la información.
- b) Cifrar la información en sistemas compartidos cloud siempre que se almacene y se transmita.
- c) No almacenar las claves criptográficas en cloud, tanto por el Subcontratista como por el tercero que gestione los sistemas compartidos. La gestión y uso de claves deberán tener funciones segregadas.
- d) Informar al Gestor y, cuando proceda, al Cliente de los cambios dentro de los sistemas criptográficos si los datos de Sareb forman parte de los Servicios, y se tiene alguna responsabilidad compartida sobre la implementación del control.
- e) Usar protocolos de cifrado para las aplicaciones expuestas a Internet.

1.7.7 Obligaciones relativas a los aspectos de la gestión de la continuidad del negocio

- a) Disponer de una infraestructura que permita hacer frente de manera dinámica y óptima las fluctuaciones de volumen de transacciones, asegurando y manteniendo la calidad de los Servicios prestado.

1.7.8 Obligaciones relativas al cumplimiento legal y regulatorio

- a) Asegurar el cumplimiento legal de la infraestructura de sistemas compartidos dentro de las geografías donde se presta los Servicios Subcontratados, manteniendo la calidad de los Servicios Subcontratados acordado.

1.7.9 Obligaciones relativas a la subcontratación

- a) Fijar específicamente las condiciones y requisitos de seguridad de la información con los subcontratistas o proveedores de segundo nivel de sistemas compartidos cloud.

1.8 NORMAS DE SEGURIDAD ADICIONALES A CUMPLIR POR LOS SUBCONTRATISTAS QUE OFREZCAN AL CLIENTE SERVICIOS DE VIDEOVIGILANCIA

Estas normas de seguridad básicas son de aplicación por todo Subcontratista cuya prestación de servicios incluya tratamiento de datos personales por prestar servicios de videovigilancia.

1.8.1 Obligaciones relativas al cumplimiento legal y regulatorio

- a) Contar con un registro de ubicaciones de sistemas de captación de imágenes y monitores de observación.
- b) Conservar las imágenes por el plazo máximo permitido por las legislaciones aplicables, salvo que su conservación resulte necesaria para investigar un hecho que haya afectado a la seguridad de las personas, bienes e instalaciones.

ANEXO 2 – PROTECCIÓN DE DATOS

1.1 TRATAMIENTO DE DATOS PERSONALES EN RELACIÓN CON LA PRESTACIÓN DE LOS SERVICIOS SUBCONTRATADOS

En relación con los Servicios Subcontratados prestados en virtud del Contrato, que suponen el tratamiento de datos personales por el Subcontratista en nombre de Sareb, el Subcontratista se compromete a actuar como sub-encargado del tratamiento y de conformidad con el artículo 28 del RGPD, al cumplimiento de lo siguiente:

1.1.1 Finalidad del tratamiento e instrucciones

El Subcontratista se limitará a realizar las actuaciones que resulten necesarias para prestar los Servicios Subcontratados.

El Subcontratista tratará los datos únicamente de conformidad con las instrucciones dadas por Sareb, que seguirá siendo el responsable del tratamiento, tanto de aquellos datos a los que haya dado acceso al Subcontratista, como de aquellos que se hayan generado durante la prestación de los Servicios Subcontratados.

El Subcontratista no utilizará los datos personales a los que tenga acceso por Sareb para ninguna finalidad distinta de la prestación de los Servicios Subcontratados.

1.1.2 Registro de las actividades de tratamiento

El Subcontratista deberá mantener un registro, por escrito, de todas las actividades de tratamiento efectuadas por cuenta de Sareb, en los términos establecidos en el artículo 30.2 del RGPD.

1.1.3 Prohibición de cesión de datos personales

Los datos personales no serán cedidos a ninguna otra persona o entidad, ni siquiera para su conservación, salvo en los supuestos autorizados por la Normativa aplicable en cada momento y en favor de las entidades subcontratadas por el Subcontratista, en los términos y condiciones previstos en el Contrato y en el apartado 1.10 subsiguiente. En estos supuestos se deberá informar previamente de la cesión al Cliente.

1.1.4 Transferencias internacionales

Sareb no autoriza ni permite transferencias internacionales de datos fuera del territorio del Espacio Económico Europeo.

Si por determinadas circunstancias fuese absolutamente necesario para la correcta prestación de los Servicios Subcontratados, una transferencia internacional de datos, previo a la misma, el Subcontratista deberá solicitar autorización escrita al Cliente, que analizará si procede o no y, en su caso, solicitará la información que precise para su análisis.

1.1.5 Confidencialidad

El Subcontratista se compromete a observar la máxima reserva y confidencialidad acerca de los datos personales a los que tenga acceso, adoptando las medidas necesarias para evitar su revelación. Esta obligación seguirá en vigor de forma indefinida tras la finalización de la prestación de los Servicios Subcontratados.

El Subcontratista garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una

obligación de confidencialidad de naturaleza estatutaria.

Esta cláusula estará a lo establecido en la Condición 3 (*Confidencialidad*) de las presentes Condiciones.

1.1.6 Medidas de seguridad y notificación de violaciones de la seguridad de los datos

El Subcontratista deberá adoptar todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales responsabilidad de Sareb, e impedir su destrucción, alteración, pérdida, utilización o acceso no autorizados con arreglo a lo dispuesto en la Condición 2 (*Medidas de Seguridad de la información*), así como todas aquellas medidas necesarias para el cumplimiento de lo dispuesto en el artículo 32 del RGPD.

El Subcontratista deberá notificar al Cliente por los medios de comunicación convenidos, sin dilación indebida, y en cualquier caso antes del plazo de veinticuatro (24) horas, las violaciones de seguridad sufridas sobre los datos personales a su cargo de las que tenga conocimiento, incluyendo toda la información relevante para la documentación y comunicación de la incidencia.

1.1.7 Solicitud de información para evaluar el cumplimiento de las obligaciones en materia de protección de datos y auditorías

Siendo una obligación por parte del Cliente velar porque el Subcontratista reúna las garantías para el cumplimiento de las normas de protección de datos cuando se realice tratamiento de datos, previo al inicio de la prestación de los Servicios Subcontratados y durante la misma, el Cliente estará facultado para solicitar al Subcontratista toda la información que razonablemente sea necesaria para poder evaluar y valorar el grado de cumplimiento de sus obligaciones, así como para la realización de las auditorías por sí misma u otro auditor autorizado por él. Cualquier auditoría que el Cliente quiera realizar deberá ser comunicada al Subcontratista con diez (10) días de antelación, no pudiéndose realizar más de dos (2) auditorías en cada ejercicio, salvo que concurran circunstancias especiales que motiven la realización de auditorías o inspecciones extraordinarias.

1.1.8 Apoyo a Sareb con determinadas obligaciones en materia de protección de datos

El Subcontratista colaborará con Sareb y el Cliente en el cumplimiento de sus obligaciones en materia de medidas de seguridad, comunicación y/o notificación de violaciones de seguridad a las autoridades competentes o los interesados, y en la realización de evaluaciones de impacto relativas a la protección de datos y de consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

1.1.9 Solicitudes de acceso, rectificación, supresión, limitación, oposición, portabilidad y a no ser objeto de decisiones automatizada

El Subcontratista hará llegar al Cliente, todas las solicitudes de interesados para ejercitar sus derechos de acceso, rectificación, supresión, limitación, oposición, portabilidad y a no ser objeto de decisiones automatizadas de las que sea Responsable y dará el apoyo necesario para la correcta gestión de la solicitud. El Cliente informará, en su caso, al Subcontratista si debe gestionarlas o las atiende el Cliente directamente.

1.1.10 Subcontratación

El Subcontratista no podrá subcontratar con un tercero la realización de ningún

tratamiento de datos a los que tenga acceso y le hubiera encomendado el Cliente, salvo que haya obtenido por parte del Cliente una autorización previa y por escrito para ello.

Junto con la solicitud de autorización, el Subcontratista tendrá que comunicar al Cliente los datos del tercero a subcontratar: (i) datos identificativos, nombre, dirección, NIF y teléfono de contacto (ii) información y descripción de los Servicios Subcontratados que se vayan a recibir por la empresa subcontratada y (iii) descripción del tratamiento de datos personales que se vaya a realizar y los ficheros y datos a los que vaya a tener acceso para la prestación del servicio.

En cualquier supuesto de subcontratación, el contrato que se suscriba entre el Subcontratista y el tercer subcontratista debe dar cumplimiento a la normativa sobre protección de datos y, en particular, que contemple los mismos compromisos asumidos por el Subcontratista en virtud de lo aquí establecido.

El Subcontratista deberá incorporar al Contrato de Encargo del Tratamiento un listado con todos los proveedores que vayan a actuar como subsub-encargados del tratamiento, y por tanto presten Servicios Subcontratados al Subcontratista que impliquen el tratamiento de datos de carácter personal de Sareb para la verificación de que no existe incompatibilidad y en su caso adoptar las medidas oportunas para limitarla.

1.1.11 Deber de información

El Subcontratista solicitará, requerirá, recopilará, recogerá y tratará datos de carácter personal de los interesados en nombre de Sareb, que no habrán sido facilitados por esta última y que son necesarios para la correcta prestación de los Servicios Subcontratados. Por tanto, el Subcontratista lo hará informando a los interesados de todos los aspectos recogidos en el artículo 13 o 14 del RGPD, según corresponda.

El texto y el formato de los formularios de cumplimiento del deber de información y de recogida de consentimientos serán facilitados por el Cliente. Esto no obstante, las Partes procederán a modificar dicho texto en el supuesto de que dicha modificación sea necesaria para cumplir con la normativa de protección de datos aplicable en cada momento durante la vigencia del Contrato.

1.1.12 Destrucción de los datos

El Subcontratista se compromete una vez finalizada la prestación del Servicio correspondiente a mantener bloqueados los datos personales correspondientes a Sareb, durante el plazo de prescripción de las acciones que pudieran derivarse de la relación mantenida con el Cliente y/o los plazos de conservación previstos legalmente, y a devolver los datos al Cliente siguiendo las instrucciones para dicha devolución establecidos por el responsable de tratamiento. Una vez devueltos el Subcontratista deberá destruir aquella información que contenga datos de carácter personal que haya sido transmitida por el Cliente con motivo de la prestación de los Servicios Subcontratados. Una vez destruidos, emitirá un certificado de destrucción al Cliente donde se relacionará la información, soportes físicos y documentación destruidos. Igualmente, el Subcontratista se compromete a solicitar a sus colaboradores y subcontratados que traten datos de Sareb la devolución y destrucción de los datos finalizado el servicio. Al amparo de lo dispuesto en el art. 33.4 LOPDGDD, el Subcontratista, en tanto que sub-encargado del tratamiento, podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el Encargado del tratamiento. En tal caso, los datos objeto de conservación serán los imprescindibles.

1.1.13 Responsabilidad del Subcontratista

En el caso de que el Subcontratista destinara los datos a finalidades distintas a las previstas en el Contrato, los comunicara a terceros, los utilizara incumpliendo las estipulaciones del Contrato, o infringe lo establecido en el RGPD al determinar los fines y medios del tratamiento será considerado responsable del tratamiento con respecto a dicho tratamiento y deberá responder de cualesquiera consecuencias que pudieran derivarse de tales conductas, o infracción, debiendo mantener indemne a Sareby al Cliente por cualquier reclamación de terceros fundada en dicho incumplimiento y sin perjuicio de otras consecuencias que puedan proceder según el Contrato o la legislación aplicable.

ANEXO 2(bis) – CONDICIONES DE SUB-ENCARGO DE TRATAMIENTO EXPOSITIVOS

I.- Que el Gestor es una entidad dedicada a la prestación para terceros de servicios de gestión integral de activos financieros (principalmente, de créditos y préstamos con garantía hipotecaria) y de activos inmobiliarios, incluyendo su comercialización en venta o alquiler.

II.- Que el Proveedor es una entidad dedicada a la prestación de diversa tipología de servicios de gestión de activos.

III.- Que el Gestor tiene suscrito un contrato de prestación de servicios con SAREB, Proyecto SMO II, en relación con los activos gestionados, en el marco del cual podrá acceder y proceder al tratamiento de determinados datos titularidad SAREB.

IV.- Que, como consecuencia del expositivo III, el Gestor tiene suscrito un contrato de encargado de tratamiento con SAREB, en el que actúa en su condición de ENCARGADO DEL TRATAMIENTO, según lo dispuesto en la normativa sobre protección de datos de carácter personal, siendo SAREB el RESPONSABLE DEL TRATAMIENTO también a los efectos de dicha normativa.

V.- Que el Proveedor, como consecuencia de la prestación de los servicios que se detallan en el contrato principal del que este documento es anexo inseparable (en adelante, el “**Servicio**” o los “**Servicios**” y el “**Contrato Principal**”), podrá acceder y proceder al tratamiento de determinados datos titularidad de SAREB, actuando el Proveedor como SUB- ENCARGADO DEL TRATAMIENTO (los “**Servicios de Tratamiento**”).

VI.- Que, por la presente, se establece entre las partes una relación contractual por la cual el Proveedor ha asumido la prestación de los servicios objeto del Contrato Principal, siendo objeto del presente documento de condiciones de Sub-encargo de tratamiento, regular los términos y condiciones conforme a los cuales el Proveedor tratará los datos personales a los que tenga acceso con motivo de la prestación de servicios al amparo del Contrato Principal. El presente documento es colateral y vinculado al Contrato Principal del que trae causa.

VII.- Que con el fin de dar cumplimiento a la normativa de Protección de Datos Personales y, principalmente, al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, “**Reglamento general de Protección de datos**” o “**RGPD**”), ambas partes se obligan a cumplir lo dispuesto en las siguientes:

ESTIPULACIONES

1. Objeto.

El presente documento tiene por objeto definir las condiciones conforme a las cuales el Proveedor llevará a cabo el tratamiento de datos personales que resulten necesarios para la prestación del Servicio contratado por el Gestor de conformidad con lo dispuesto en el artículo 28 del RGPD, y el resto de normativa de protección de datos.

Dicho tratamiento se realizará sobre datos personales de los que el RESPONSABLE DEL TRATAMIENTO es titular (en adelante, los “**datos personales**”), con motivo de la prestación del Servicio, lo que implica el tratamiento de los datos de carácter personal vinculados a los activos y los generados fruto de la prestación del Servicio, que el Proveedor presta al Gestor, de conformidad con el Contrato Principal suscrito entre ambas entidades.

2. Obligaciones del Proveedor.

El Proveedor llevará a cabo el tratamiento de datos personales derivado de la prestación del Servicio contratado, de conformidad con las siguientes obligaciones:

2.1 Limitarse a realizar las actuaciones que resulten necesarias para prestar al Gestor el Servicio contratado, de conformidad con lo establecido en el Contrato Principal.

En concreto, se comprometerá a realizar el tratamiento de los datos personales ajustándose a las instrucciones que, en cada momento, le indique el Gestor, así como a lo dispuesto en la normativa que le resulte aplicable en materia de protección de datos personales, inclusive con respecto a las transferencias de datos personales a un tercer país o a una organización internacional en los términos y condiciones recogidos en la estipulación 10 siguiente.

Las actividades del tratamiento consistirán en: Cumplimiento y Control Interno, Gestión de proveedores, Negocio, Saneamiento Jurídico, Desarrollo Inmobiliario, Seguridad, Vivienda asequible y social.

El tratamiento consistirá en: recogida, estructuración, conservación, consulta, cotejo, supresión, comunicación, registro, modificación y limitación.

Las categorías de interesados a los que afecta el presente encargo de tratamiento son: clientes y usuarios, proveedores, personas de contacto, beneficiarios, cargos públicos.

Los tipos de datos a los que afecta el presente encargo de tratamiento son: datos de carácter identificativo, características personales, académicos y profesionales, información comercial, circunstancias sociales, detalles del empleo, transacciones de bienes o servicios, categorías especiales de datos.

Si el Proveedor considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición española o de la Unión Europea en materia de protección de datos, este informará inmediatamente al Gestor, quedando facultado el Proveedor a no llevar a cabo el tratamiento de los datos de conformidad con dicha instrucción mientras se acuerda una modificación de la misma que sea acorde con la norma.

2.2 Comprometerse a no realizar ningún otro tratamiento sobre los datos personales, ni a aplicar o utilizar los datos con una finalidad distinta a la prestación del Servicio establecida en el Contrato Principal y, en su caso, de sus correspondientes Anexos, ni a utilizarlos con fines propios.

2.3 Garantizar la formación y conocimiento necesarios en materia de protección de datos personales de las personas autorizadas para tratar datos personales así como el adecuado cumplimiento de las obligaciones que le corresponden en virtud del presente documento y de la normativa vigente en materia de protección de datos por parte de sus empleados, y, en su caso, de los subcontratistas que estén autorizados en función de lo establecido en la estipulación 9 siguiente.

2.4 Mantener un registro, por escrito, de todas las actividades de tratamiento efectuadas por cuenta del RESPONSABLE DEL TRATAMIENTO, que contenga:

- El nombre y los datos de contacto del Proveedor y del RESPONSABLE DEL TRATAMIENTO y, en su caso, de representante del Cliente o del Proveedor y, en su caso, del delegado de protección de datos.
- Las categorías de tratamientos efectuados por cuenta del RESPONSABLE DEL TRATAMIENTO.
- En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional, la documentación de garantías adecuadas.
- Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
 - La seudonimización y el cifrado de datos personales.
 - La capacidad de garantizar la confidencialidad, integridad,

disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2.5 Comprometerse a guardar bajo su control y custodia los datos personales suministrados por el Gestor a los que acceda con motivo de la prestación del Servicio y a no divulgarlos, transferirlos, o de cualquier otra forma comunicarlos, ni siquiera para su conservación a otras personas, excepto en los casos de subcontratación, en los términos y condiciones previstos en el Contrato Principal.

2.6 No revelar, transferir, ceder, o cualquier otra forma que implique comunicación, ni siquiera para su conservación, los ficheros y datos en ellos contenidos, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, a ningún tercero ajeno a las partes intervinientes de la relación jurídica aquí regulada, excepto a los subcontratistas, en los términos y condiciones previstos en el Contrato Principal.

A tal efecto, solo podrá permitir el acceso a los datos a aquellos empleados del Proveedor o en su caso del subcontratado, que tengan la necesidad de conocerlos para la correcta prestación de los Servicios de Tratamiento, con idénticas obligaciones a las establecidas en el presente documento, y aquellas de confidencialidad y secreto profesional.

2.7 En caso de que deba transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informar al Gestor de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

2.8 Dar apoyo al Gestor en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

2.9 Dar apoyo al Gestor en la realización de las consultas previas a la autoridad de control, cuando proceda.

2.10 Poner a disposición del Gestor toda la información necesaria para demostrar el cumplimiento de sus obligaciones en relación a la prestación de los Servicios objeto del Contrato Principal, así como para la realización de las auditorías o las inspecciones que realice el Gestor u otro auditor autorizado por él. El Gestor anunciará dichas auditorías o inspecciones con una antelación mínima de 10 días hábiles informando al Proveedor de la documentación e información a la que accederá durante la realización de las mismas. El Gestor se obliga a preservar la confidencialidad de toda la información o documentación a la que tenga acceso durante el transcurso de dichas auditoría o inspecciones.

2.11 En el supuesto de que el Proveedor solicite, requiera, recopile, recoja o trate datos de carácter personal de terceros interesados, que no hayan sido facilitados por el Gestor y que son necesarios para la correcta prestación de los Servicios de Tratamiento objeto del presente documento, lo hará informando a los interesados de todos los aspectos recogidos en el artículo 13 del RGPD actuando el Proveedor como SUB-ENCARGADO DEL TRATAMIENTO. Por tanto, los datos generados serán de Sareb y una vez finalizadas las relaciones entre las partes deberán ser devueltos al Gestor. El Proveedor mantendrá debidamente bloqueados los datos personales imprescindibles correspondientes al RESPONSABLE DEL TRATAMIENTO, durante el plazo de prescripción de las acciones que pudieran derivarse de la relación mantenida con el cliente y/o los plazos de conservación previstos legalmente, de forma previa a la destrucción de estos.

2.12 Designar cuando proceda un delegado de protección de datos y comunicar su identidad y datos de contacto al Gestor.

3. Seguridad de los datos personales.

3.1 El Proveedor implantará las medidas de seguridad y mecanismos establecidos en el artículo 32 del RGPD para:

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

3.2 Asimismo, el Proveedor deberá adoptar todas aquellas medidas técnicas y organizativas que, a tenor del análisis de riesgo efectuado por el Gestor, este considere que resultan necesarias para garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. En caso de que en un futuro se modificara el análisis de riesgo y, en su caso, las medidas técnicas y organizativas a implementar, ambas Partes acordaran el plazo de implementación de las mismas.

3.3 En anexo separado se recogerán las actividades de tratamiento que se han identificado para las que el Proveedor presta el servicio.

3.4 Sareb tiene establecido un modelo de control basado en normas y estándares internacionales, entre otras ISO/IEC 27002:2013, COBIT, NIST, comúnmente aceptados, de cara a una gestión adecuada del riesgo en el ámbito de la privacidad.

3.5 Igualmente, el Gestor podrá facilitar al SUB-ENCARGADO DEL TRATAMIENTO medidas de control específicas para los tratamientos que haga en nombre de Sareb.

3.6 Sin perjuicio de lo anterior, el Proveedor deberá hacer su propio análisis de riesgo y proponer al Gestor la adopción de medidas de seguridad adicionales o sustitutivas de las propuestas por este, siempre que de las mismas resulte un nivel de seguridad adecuado. En todo caso, la decisión final sobre la adopción e implantación de unas u otras medidas corresponden al Gestor.

4. Copias de datos.

El Proveedor se compromete a no copiar o reproducir la información y datos de carácter personal facilitados por el Gestor, salvo cuando sea necesario para su tratamiento y en los términos previstos en el presente Contrato de ENCARGADO DEL TRATAMIENTO, así como cuando esté previsto o sea necesario por disposición legal.

5. Notificación de violaciones de la seguridad de los datos.

5.1 El Proveedor deberá notificar al Gestor, mediante comunicación al DPO a la dirección de correo dpo@alisedainmobiliaria.com y al Departamento de Seguridad de la Información a la dirección de correo seguridad.informacion@alisedainmobiliaria.com sin dilación indebida, y en cualquier caso antes del plazo de 24 horas -desde que tuvo conocimiento de ellas-, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento -que afecten a SAREB y sus servicios-, incluyendo toda la información relevante para la documentación y comunicación de la incidencia.

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

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

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Toda aquella otra información que resulte relevante para el conocimiento de la violación de seguridad, sus efectos sobre los derechos y libertades de las personas, así como para cumplir con el deber de notificación a los interesados y al organismo regulador que la normativa de protección de datos imponga al RESPONSABLE DEL TRATAMIENTO.

5.2 Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

6. Deber de confidencialidad.

6.1 El deber de secreto y confidencialidad que se deriva del presente contrato obliga al Proveedor durante su vigencia y se extenderá, aun después de finalizar sus relaciones con el Gestor. Si se produjese una filtración de información ya fuese intencionada o accidental, que rompa con el principio de confidencialidad y/o secreto profesional, el Proveedor queda comprometido a comunicar al Gestor en el mismo momento que tenga conocimiento, y en su caso, a la mayor brevedad posible el hecho acontecido, todo ello sin perjuicio de otras consecuencias que pudieran proceder.

6.2 El Proveedor garantizará que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que el Gestor informará convenientemente.

6.3 El Proveedor mantendrá a disposición del Gestor la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

7. Deber de información.

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

8. Obligación de devolución de los datos y destrucción.

8.1 Una vez cumplida la prestación del servicio objeto del Contrato Principal, el Proveedor se compromete a devolver la documentación e información que contenga datos de carácter personal responsabilidad de SAREB y, seguidamente, a destruir dicha información obtenida con motivo de la prestación del Servicio, así como todas las copias de la misma que pudiera tener, y en todo caso a actuar conforme a las instrucciones e indicaciones del Gestor.

8.2 Una vez destruidos, emitirá un certificado de destrucción al Gestor mediante el que se garantice la indisponibilidad de los datos de carácter personal destruidos y donde se relacionará la información, soportes físicos y documentación destruidos conforme al modelo que se le facilitará a tales efectos.

8.3 No obstante, lo previsto en el párrafo anterior, el Proveedor podrá conservar los datos e información tratada, debidamente bloqueados, en el caso que pudieran derivarse responsabilidades de su relación con el Gestor o cuando se requiera en virtud del Derecho de la Unión o de los Estados miembro.

9. Subcontratación.

9.1 El Proveedor no podrá subcontratar con un tercero la realización de ningún tratamiento de datos a los que tenga acceso y le hubiera encomendado el Gestor, ni siquiera los datos que el Proveedor y fruto de la prestación de los Servicios de Tratamiento, haya generado, solicitado u obtenido de terceros interesados, salvo que haya obtenido por parte del Gestor una autorización previa y por escrito para ello.

9.2 En todo caso, los gastos que se deriven de la subcontratación de los Servicios de Tratamiento conforme a lo previsto en la presente estipulación 9 correrán por cuenta y cargo del Proveedor, exceptuando aquellos supuestos expresamente establecidos en contrario en el Contrato Principal o en el presente anexo, sin perjuicio del derecho del Proveedor a refacturar, cuando proceda, dichos gastos al Gestor, en los términos previstos en el Contrato Principal.

9.3 Junto con la solicitud de autorización el Proveedor tendrá que comunicar al Gestor los datos del tercero a subcontratar: (i) datos identificativos, nombre, dirección, NIF y teléfono de contacto (ii) información y descripción de los Servicios de Tratamiento que se vayan a recibir por la empresa subcontratada y (iii) descripción del tratamiento de datos que se vaya a realizar y los ficheros y datos a los que vaya a tener acceso para la prestación de los Servicios de Tratamiento.

9.4 El Proveedor, que también tiene la condición de Encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el Proveedor y las instrucciones que dicte el Gestor. Corresponde al Proveedor inicial regular la nueva relación de conformidad con el artículo 28 del RGPD, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad, etc.) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

9.5 En el caso de incumplimiento por parte del sub-encargado, el Proveedor inicial seguirá siendo plenamente responsable ante el RESPONSABLE DEL TRATAMIENTO en lo referente al cumplimiento de las obligaciones.

10. Transferencias internacionales.

10.1 EL RESPONSABLE DEL TRATAMIENTO no autoriza ni permite transferencias internacionales de datos fuera del territorio del Espacio Económico Europeo (“EEE”).

10.2 Si por determinadas circunstancias fuese absolutamente necesario para la correcta prestación de los Servicios de Tratamiento objeto del presente documento, una transferencia internacional de datos, previo a la misma, comunicación, acceso o uso de los datos personales deberá solicitar autorización escrita al Gestor para realizarla e informar de (i) los datos que van a salir fuera del territorio Español, (ii) Estado destinatario y en su caso tercero subcontratado o para el que se solicita la subcontratación, (iii) el destino y tratamiento que se le dará a los datos, y (iv) aquella otra información que solicite el Gestor por entenderla necesaria.

10.3 Las comunicaciones de datos fuera del territorio español, pero dentro del EEE, igualmente deberán ser previamente informadas al Gestor, indicando los motivos que justifican dicha transferencia.

10.4 El Proveedor estará sujeto al cumplimiento de las necesidades y obligaciones establecidas por las normas de Transferencias Internacionales de Datos en la legislación vigente en materia de privacidad que lo regule en cada momento.

10.5 Igualmente, si el Proveedor dispone de normas corporativas vinculantes aprobadas (“BCR”) seguirá aplicando la misma restricción, no pudiendo comunicar datos responsabilidad de Sareb fuera del EEE.

11. Derechos de los interesados.

El Proveedor debe trasladar al Gestor, sin dilación indebida, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo, dirigidas o que afecten a datos del RESPONSABLE DEL TRATAMIENTO.

12. Obligaciones del Gestor.

Corresponden al Gestor las siguientes obligaciones:

- Entregar al Proveedor los datos objeto de tratamiento de conformidad con lo establecido en el presente.
- Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el Proveedor.
- Realizar las consultas previas que corresponda.
- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del Proveedor.
- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

13. Responsabilidades.

13.1 El Proveedor se compromete a cumplir con las obligaciones establecidas en el presente Contrato y en la normativa vigente, en relación con el presente encargo de tratamiento. Adicionalmente garantiza el íntegro cumplimiento de las obligaciones de confidencialidad y custodia y será responsable de cualquier revelación no autorizada de los datos de carácter personal a terceras partes, así como de cualquier otro incumplimiento de las estipulaciones recogidas en el presente documento, estando, en su caso, obligado a resarcir de los daños y perjuicios ocasionados, directa o indirectamente, al Gestor.

13.2 Las obligaciones establecidas para el Proveedor en el presente documento serán también de obligado cumplimiento para sus empleados y subcontratistas, y por las que el Proveedor responderá frente al Gestor si son incumplidas.

13.3 En el caso de que el Proveedor destinara los datos a finalidades distintas a las previstas en el presente documento, los comunicara a terceros o los utilizara incumpliendo las estipulaciones del presente documento, deberá responder de cualesquiera consecuencias que pudieran derivarse de tales conductas, o infracción, debiendo mantener indemne al Gestor por cualquier reclamación de terceros fundada en dicho incumplimiento y sin perjuicio de otras consecuencias que puedan proceder según el presente documento, el Contrato Principal o la legislación aplicable.

13.4 De conformidad con lo establecido en el artículo 28.10 del RGPD y normativa de protección de datos, si el Proveedor infringe lo establecido en el RGPD al determinar los fines y medios del tratamiento será considerado responsable del tratamiento con respecto a dicho tratamiento.

13.5 En cuanto a la interpretación y resolución de controversias se estará a lo estipulado en el Contrato Principal.

13.6 En lo no previsto en este Contrato de Encargo de Tratamiento se estará a lo dispuesto en el Contrato Principal.

14. Notificaciones.

Cualquier notificación que se efectúe entre las partes se hará de la forma y a los

destinatarios establecidos de acuerdo con lo previsto en el Contrato Principal.

15. Extinción.

15.1 El presente documento es un Anexo al Contrato Principal, por lo que se extinguirá por las causas que allí se reflejen y en todo caso cuando se extinga dicho Contrato Principal:

- Por el transcurso de su plazo de duración (en su caso).
- Por la extinción o expiración de la prestación de los Servicios de Tratamiento que vincula a las partes.
- En caso de incumplimiento por alguna de las partes de las obligaciones asumidas en el presente documento.
- Por las demás causas previstas en el Contrato Principal.

15.2 Esta estipulación 15 (extinción) no supone modificación alguna del Contrato Principal, salvo en caso de contradicción con lo expresamente previsto en este documento, en cuyo caso regirá lo dispuesto en el Contrato Principal.

15.3 Se deberá actuar según lo estipulado en el Contrato Principal para la extinción de la relación objeto del presente y en su defecto, cuando se den las causas para la extinción, realizar una comunicación de la rescisión a la parte contraria.

15.4 Este documento no supone modificación alguna del Contrato Principal, salvo en caso de contradicción con lo expresamente previsto en este documento que regirá lo dispuesto en el Contrato Principal.

16. Entrada en vigor.

El presente Contrato entra en vigor en la fecha de su firma y estará vigente hasta la fecha de terminación de la relación de prestación del Servicio por parte del Proveedor a favor del Gestor, así como la extinción del Contrato Principal salvo y se hayan cumplido las obligaciones contempladas en el presente documento, con independencia de cualquier otra obligación de carácter legal que fuera aplicable a las partes tras la terminación de dicha relación.

ANEXO 3 - RIESGO PENAL Y BLANQUEO DE CAPITAL

1.1 RIESGO PENAL

En la prestación de los Servicios Subcontratados, el Subcontratista (en adelante, igualmente, el “**Proveedor**”) se obliga frente al Gestor y Sareb a realizar todo lo que sea necesario y suficiente para que todas las personas físicas y jurídicas que participen en la prestación de los Servicios Subcontratados cumplan la totalidad de las obligaciones establecidas por la normativa aplicable, y, en particular, lleven a cabo las actuaciones necesarias para que no pueda incurrirse ni por el Gestor ni por el Cliente, ni por ninguna persona jurídica o entidad en ningún delito previsto en el Código Penal.

Respecto a la responsabilidad penal, el Proveedor deberá prestar los Servicios Subcontratados cumpliendo con todas las obligaciones que como tal le son exigibles en materia penal, laboral, tributaria, o de cualquier otra índole y velando por el cumplimiento de dichas obligaciones por parte de cualesquiera personas físicas o jurídicas intervinientes en la prestación de los Servicios Subcontratados y a responder del cumplimiento de cualesquiera obligaciones establecidas por (a) el Código Penal con el objeto que no pueda incurrirse ni por el Proveedor ni por el Gestor y/o Sareb, ni por ninguna persona física o jurídica en delito alguno previsto en el mismo; (b) la normativa urbanística, de ordenación del territorio de dominio público y de seguridad; (c) la normativa relativa a recursos naturales y medio ambiente; (d) el cumplimiento de las órdenes expresas de la autoridad administrativa, de cualquier índole; y (e) en general, el cumplimiento de toda la normativa aplicable en la prestación de los Servicios Subcontratados, manteniendo indemne al Gestor y a Sareb y a sus representantes, administradores, directivos, encargados de Servicios Subcontratados y empleados de cualesquiera daños, reclamaciones o sanciones derivadas del incumplimiento de dichas obligaciones.

En virtud de lo anterior, el Proveedor se obliga a trasladar las obligaciones descritas en el apartado inmediatamente anterior y en los mismos términos a sus empleados, directivos, consejeros y terceros subcontratados, sean estas personas físicas o jurídicas y a efectuar los controles necesarios sobre el cumplimiento adecuado de la presente cláusula por parte de los mismos.

El Proveedor deberá:

- (a) Contar con medidas de vigilancia y control para la prevención, detección y gestión de los riesgos de naturaleza penal, de acuerdo con lo establecido en el artículo 31 bis del Código Penal.
- (b) Facilitar copia al Gestor de los Manuales Internos (o Procedimientos de Prevención de Riesgo Penal y/o sus actualizaciones) y cualesquiera evidencias sobre el cumplimiento de las medidas de prevención del riesgo penal solicitadas.
- (c) Realizar certificaciones por expertos independientes o empresas especializadas que valoren y acrediten que cuenta con un sistema de cumplimiento de prevención de riesgo penal eficaz y que cumple con los requisitos del Código Penal establecidos específicamente en el artículo 31 bis, así como la eficacia operativa del programa y facilitar copia a Sareb de la misma.
- (d) Velar de manera proactiva por el cumplimiento de dicho sistema de prevención realizando los controles oportunos.
- (e) Comunicar al Gestor, con carácter inmediato y en todo caso en el plazo

máximo de cuarenta y ocho (48) horas, cualquier dato o información de la que deba o pueda tener conocimiento y que pueda implicar la materialización de un riesgo de incumplimiento normativo de carácter penal, en el marco de la ejecución de los Servicios Subcontratados.

1.2 PREVENCIÓN DE BLANQUEO DE CAPITALS

1.2.1 Cumplimiento con la Normativa de PBCFT

El Proveedor se obliga a cumplir con la totalidad de la normativa aplicable en cada momento (ya sea europea, estatal, regional, local, recomendaciones de órganos reguladores o de cualquier otro tipo aplicable) a la prestación de los Servicios Subcontratados. Sin perjuicio de la generalidad de lo anterior y sin carácter limitativo, el Proveedor asume las siguientes obligaciones:

- (a) El Proveedor declara que conoce y cumple con las obligaciones reguladas por la Normativa PBCFT.
- (b) El Proveedor se compromete a cumplir cualquier normativa que pueda ser promulgada en el futuro para modificar, ampliar o sustituir a las anteriormente mencionadas. En consecuencia, el Proveedor se compromete a adoptar las medidas de control interno adecuadas en relación con el presente Contrato en su calidad de sujeto obligado bajo la Normativa PBCFT, para lo que deberá contar con herramientas propias de gestión del riesgo de blanqueo de capitales y de la financiación del terrorismo, y a emprender todas las acciones adecuadas para asegurarse de que sus empleados y/o colaboradores y/o subcontratistas sean conscientes en todo momento de la Normativa PBCFT, para que en todo momento se aseguren de su cumplimiento.
- (c) El Proveedor actuará cumpliendo puntualmente y con precisión, además de la Normativa PBCFT aplicable, los buenos usos y prácticas mercantiles y las Instrucciones en cada momento vigentes. Este deber incluirá, sin limitarse a ello, la adopción tanto de las medidas necesarias para cumplir con las obligaciones normativas que, en materia de PBCFT, se deriven para el Proveedor en su condición, como de aquellas otras que resulten igualmente necesarias para cumplir con las políticas y procedimientos desarrollados por Sareb en esta materia.
- (d) El Proveedor, con el objetivo de cumplir y hacer cumplir todos los procedimientos y políticas establecidos por Sareb para la gestión del riesgo de blanqueo, se compromete a volcar en las herramientas que se pongan a su disposición y que se conecten con las herramientas del Proveedor todos los datos necesarios para el chequeo de listas y el registro de las operaciones y la toma de datos y la conservación de la documentación soporte, salvo en los tipos de operaciones que no esté integrado el volcado de datos de sus aplicaciones en cuyo caso, deberán utilizar las aplicaciones que Sareb indique para volcar los datos necesarios.
- (e) Asimismo, el Proveedor deberá informar al Gestor de la apertura, en su caso, de una inspección en esta materia o de un expediente sancionador de los organismos supervisores, o si estuviera incurso en algún procedimiento de índole penal. Adicionalmente, deberá informar al Gestor del resultado de las anteriores actuaciones y de las notificaciones o solicitudes de colaboración que pudiera recibir del SEPBLAC o cualquier otro organismo regulador o supervisor, o de las autoridades competentes, y que estuviera

relacionada con la gestión de los activos de Sareb.

- (f) Facilitar copia de los Manuales Internos y Procedimientos de PBCFT (o sus actualizaciones), y de la parte de recomendaciones de los informes de Experto Externo en relación con el Proveedor (excluyendo las que afecten a otras sociedades del Grupo) o de cualquier otro examen realizado sobre la efectividad de los procedimientos implantados por el Proveedor y de los planes de remediación adoptados sobre las recomendaciones que se pudieran haber emitido.
- (g) Facilitar el plan de formación en materia de PBCFT aprobado anualmente, y certificado que acredite la formación impartida a sus empleados.
- (h) Acreditar la existencia de políticas y procedimientos adecuados para asegurar altos estándares éticos en la contratación de empleados, directivos y agentes.
- (i) Declarar a Sareb las entidades que componen su grupo a los efectos de PBCFT y sus actualizaciones.
- (j) Todo cambio o actualización en la normativa interna de PBCFT que afecte a la gestión de prevención de blanqueo de los activos de Sareb, será comunicado al Gestor antes de su aplicación.

1.2.2 Servicios Subcontratados de comercialización

El Proveedor deberá llevar a cabo las siguientes actuaciones:

- (a) Cumplirá con todas las obligaciones relativas a la PBCFT que se detallarán en las Instrucciones específicas emitidas por el Gestor.
- (b) Llevará a cabo la solicitud y recopilación de documentos requeridos según el nivel de riesgo del cliente y la operación, para su análisis y, en su caso, aprobación, y elevará, en los plazos establecidos, al Gestor para su sanción las operaciones que se detallarán en las Instrucciones específicas emitidas por el Cliente.
- (c) Establecerá controles que garanticen que todas las operaciones sujetas a la norma de prevención de blanqueo de capitales son analizadas en el momento oportuno, en cualquier caso, antes de asumir compromisos con los clientes, y siempre antes de su formalización.
- (d) Establecerá mecanismos para la comunicación inmediata al Gestor de operativas sospechosas de blanqueo de capitales o financiación del terrorismo.
- (e) Remitirá al Gestor, con la periodicidad que se establezca en las Instrucciones específicas emitidas por el Gestor, los datos y controles realizados en cada una de las ventas, en el que acredite el cumplimiento de estas obligaciones, incluida la verificación del chequeo de listas oficiales y listas internas de Sareb, recogiendo el resultado en la herramienta corporativa correspondiente.
- (f) Mantendrá y custodiará toda la documentación relacionada con activos de Sareb en todo momento, y la pondrá, a simple requerimiento, a disposición de Sareb durante los plazos legalmente establecidos para su salvaguarda.

ANEXO 4 – SERVICIO DE AUDITORÍA INTERNA

1. Directrices generales

El presente Pliego tiene por objeto regular las condiciones técnicas que debe cumplir el departamento de auditoría interna del Gestor, siendo dicho departamento un soporte a la función de auditoría interna de Sareb, garantizando la independencia, objetividad y calidad en la supervisión de los procesos, sistemas y controles internos relacionados con la gestión de Activos Sareb.

La función de auditoría interna del Gestor se estructurará como un servicio a la función de auditoría interna de Sareb y estará dotada de recursos suficientes para la adecuada realización de todas las actividades de auditoría interna requeridas, orientadas a evaluar la suficiencia, efectividad y eficiencia de los sistemas de control interno y procesos del Gestor, en los que descansa la administración y gestión de los Activos Sareb.

2. Descripción del Servicio

Comprende todos los servicios y actividades posibles orientadas a evaluar la suficiencia, efectividad y eficiencia de los sistemas de control interno y procesos del Gestor en los que descansa la administración y gestión de los Activos Gestionados.

La auditoría interna de Sareb elaborará anualmente, en colaboración con la auditoría interna del Gestor, un programa de supervisión que incluirá un calendario de actuaciones trimestrales, a realizar, con carácter general, por la auditoría interna del Gestor, junto con la estimación de horas previstas por actuación, pudiendo ser modificado por Sareb, en caso de que existan circunstancias que así lo requieran (el “**Programa de Supervisión**”).

El Programa de Supervisión también podrá contener auditorías que, en aplicación de la metodología de planificación de la auditoría interna de Sareb, se ejecuten directamente por la auditoría interna de Sareb, pudiendo contar, adicionalmente, con la colaboración de terceros, cuyo coste asumiría Sareb. El inicio de estos trabajos por la auditoría interna de Sareb será comunicado a la auditoría interna del Gestor con una antelación mínima de quince (15) días naturales antes de su inicio.

La auditoría interna de Sareb comunicará la aprobación del Programa de Supervisión a la auditoría interna del Gestor, así como las modificaciones que pudieran resultar necesarias sobre el mismo, con la mayor antelación posible. No obstante, y hasta que dichas comunicaciones tengan lugar, Auditoría Interna de Sareb determinará las actividades auditoras a realizar en el período.

Con la finalidad de cumplir con los objetivos planteados, las diferentes actuaciones auditoras a desarrollar en dicho Programa de Supervisión serán planificadas por la auditoría interna del Gestor, de acuerdo con el alcance de las mismas, y los objetivos planteados por la auditoría interna de Sareb. Cada actuación a desarrollar será comunicada por la auditoría interna del Gestor a auditoría interna de Sareb con una anticipación mínima antes de su inicio de un (1) mes.

La auditoría interna del Gestor, para documentar las actuaciones auditoras que se establezcan en el mencionado Programa de Supervisión, se compromete a:

- a) Utilizar la metodología de trabajo de Auditoría Interna de Sareb, que cumple con las Normas Internacionales de Auditoría Interna.
- b) Utilizar la misma aplicación que auditoría interna de Sareb utilice para documentar sus propias actuaciones auditoras. El coste total de uso de la aplicación (licencias, mantenimiento, etc.) será por cuenta del Gestor.

Cualquier actuación auditora debe de contar con su evaluación preliminar y programa de trabajo elaborado con un mínimo de quince (15) días de antelación sobre el inicio del trabajo de campo y conforme al Modelo y Metodología establecidos por Sareb; auditoría interna de Sareb podrá requerir las aclaraciones que considere oportunas y la posible modificación de alcances o incorporación de pruebas adicionales.

Los resultados de cada actuación deberán ser recogidos en el correspondiente informe, elaborado conforme al Modelo y Metodología establecidos por Sareb. Dicho informe deberá ser elaborado en un plazo máximo de quince (15) días desde la conclusión del trabajo de campo y su supervisión por Sareb, así como ser puesto a disposición de Sareb en un plazo máximo de dos (2) días desde la fecha de su emisión. Cualquier aspecto que a juicio de un observador imparcial pudiera poner de manifiesto la existencia de incidencias significativas en los procesos de gestión y administración de las operaciones de Sareb, o de riesgos significativos, deberá ser incluido en el Informe y ser puesto en conocimiento del área de auditoría interna de Sareb tan pronto como sea conocido.

La función de auditoría interna de Sareb podrá participar, a su criterio y sin limitaciones por parte del Gestor, en las actuaciones de auditoría ejecutadas por el Gestor, supervisando el trabajo de campo y con acceso a los documentos de trabajo y evidencias empleadas por la función de auditoría interna del Gestor, como parte de los medios necesarios para que Sareb ejerza su función supervisora.

La función de auditoría interna de Sareb, o terceros designados por ésta, se encuentra dotada de plena autoridad de acceso, sin restricciones, para poder examinar y evaluar:

- a) La efectividad y eficiencia de los sistemas de gestión y control de riesgos del Gestor que afecten a los Activos Sareb y los medios adoptados para su salvaguarda.
- b) La suficiencia e idoneidad de los controles internos del Gestor y, particularmente, de los asociados con:
 - 1. El cumplimiento de normas y estándares éticos;
 - 2. La prevención y detección tanto del fraude interno, como del uso impropio de los productos y servicios de Sareb; y
 - 3. La fiabilidad, efectividad e integridad de los sistemas y procesos de elaboración de la información financiera, no financiera y de gestión, incluida la relevancia, exactitud, exhaustividad, disponibilidad, confidencialidad y suficiencia de los datos en los que se base dicha información.
- c) La eficiencia y eficacia operativa con la que se desenvuelven las áreas y funciones del Gestor, en relación con los Servicios prestados en virtud del presente Contrato.
- d) Los procesos establecidos por el Gestor al objeto de asegurar la fiabilidad y suficiencia de la información suministrada a Sareb para fundamentar sus

decisiones y aquellos otros orientados a asegurar la adecuada ejecución de sus decisiones, así como el adecuado cumplimiento de los términos del presente Contrato.

- e) Las cuestiones que específicamente puedan ser requeridas por el consejo de administración, el comité de auditoría o por el primer ejecutivo de Sareb.

De considerarlo necesario en el ejercicio de la citada responsabilidad, además de poder realizar trabajos de auditoría directamente, la auditoría interna de Sareb podrá requerir la colaboración de las funciones de control del Gestor en la realización de revisiones sobre los aspectos citados relacionados con la administración y gestión de los Activos Gestionados o, alternativamente, llevar a cabo la revisión por sus propios medios. En particular, será necesaria la involucración de las funciones de control del Gestor para el seguimiento de las recomendaciones derivadas de sus actuaciones.

Adicionalmente, la auditoría interna de Sareb podrá requerir al Gestor la realización de una evaluación independiente al año, sobre la efectividad y suficiencia de aquellos elementos de su sistema de control interno en los que descansa la administración y gestión de los Activos Sareb, incluidos aspectos relacionados con los recursos y actividades de las áreas, unidades o departamentos que, con independencia de su denominación, desarrollen actividades propias de auditoría interna, cumplimiento y control de riesgos del Gestor (en adelante, “Funciones de Control”). Dicha evaluación deberá ser conducida conforme a los siguientes criterios:

- a) La elección del evaluador, que deberá contar con el visto bueno de Sareb.
- b) El marco contra el que llevar a cabo la evaluación deberá ser establecido con antelación a su realización y, al igual que el alcance de la evaluación, deberá contar con el visto bueno previo de Sareb.
- c) Los resultados de la evaluación deberán ser puestos en conocimiento del consejo de administración del Gestor o, en su caso, de su comisión de auditoría, y de la de Sareb. El informe de evaluación deberá identificar los riesgos derivados de eventuales deficiencias y debilidades del sistema de control interno del Gestor, conjuntamente con las correspondientes propuestas para su corrección.
- d) Los costes relativos a la evaluación independiente requeridos por Sareb al Gestor serán asumidos por éste.

El Gestor se compromete a facilitar, en todo lo posible, el eficaz desarrollo de las citadas revisiones, debiendo adoptar las medidas necesarias para facilitar el acceso del personal a cargo de la revisión, de Sareb o de terceros designados por ésta, a toda aquella información que resulte relevante al objeto de la revisión. Las consecuencias y posibles quebrantos de no atender en tiempo y forma los requerimientos razonables de Sareb o de terceros designados por ésta para el correcto desempeño de su labor supervisora le serán comunicadas al Gestor y habrán de ser asumidas por éste.

El Gestor facilitará a Auditoría Interna de Sareb los mejores accesos posibles en modo consulta a toda la información que necesite (los sistemas core y bases de datos complementarias) de los Activos Gestionados y los Servicios objeto del presente Pliego, sin restricciones y sin dependencia de terceras personas, incluido, cuando así lo requiera Sareb, espacio físico adecuado para que la auditoría interna de Sareb pueda desempeñar su función supervisora desde las instalaciones del Gestor, con acceso directo a las áreas

auditadas. En cualquier caso, se explorará la mejor forma de asegurar el acceso a la información de la cartera de Sareb por Auditoría Interna de Sareb.

Tras la conclusión de cualquiera de las actuaciones auditoras a las que se refiere el presente apartado, la auditoría interna de Sareb podrá hacer al Gestor las recomendaciones que crea oportunas para mejorar la eficiencia de los Servicios o solucionar cualquier defecto que se haya detectado en la prestación de los mismos. El Gestor se compromete a adoptar de buena fe las recomendaciones realizadas por Sareb y a efectuar un eficaz seguimiento de las mismas y velará porque sus socios u otros subcontratistas autorizados implementen igualmente aquellas recomendaciones que pudieran serles de aplicación.

El Gestor, para documentar el seguimiento de recomendaciones, se compromete a utilizar la misma aplicación que auditoría interna de Sareb utiliza para el seguimiento de recomendaciones. El coste total de uso de la aplicación (licencias, mantenimiento, etc.) serán por cuenta del Gestor.

Al objeto de mantener la necesaria independencia y una permanente actitud mental de objetividad: (i) la función de auditoría interna del Gestor desarrollará sus actividades libre de cualquier tipo de interferencia; (ii) el DAI no compartirá la función de DAI con la Dirección de otras unidades y/o ámbitos de control (Control Interno, Cumplimiento, etc.) (iii) los auditores internos del Gestor no tendrán responsabilidad directa en las operaciones ni autoridad sobre ninguna de las actividades y negocios que auditen; y (iv) los auditores internos no participarán en la implantación de controles internos, instalación de sistemas, preparación de registros o cualquier otra actividad que, a juicio de un observador imparcial, pudiera perjudicar la objetividad de juicio.

La función de auditoría interna del Gestor confirmará, anualmente, basándose en los cuatro aspectos anteriores, su independencia y objetividad a la dirección de auditoría interna de Sareb, y la prestación de los Servicios de Auditoría Interna deberá realizarse cumpliendo las directrices establecidas en la Política sobre Informes y Recomendaciones Vinculantes de Auditoría Interna de Sareb, que constituye el marco de gestión de los informes y recomendaciones de Auditoría Interna (calificación de los procesos, impacto de las recomendaciones y su proceso de gestión, etc.). A estos efectos, y con el objetivo de preservar la uniformidad de criterios, en caso de discrepancia entre la auditoría interna del Gestor y la auditoría interna de Sareb, Sareb podrá modificar la calificación global de la auditoría y la determinación de impactos de las recomendaciones de acuerdo con la Política anterior.

En la prestación de Servicios de Auditoría Interna, el Gestor deberá cumplir con los requerimientos del Marco Profesional para la Práctica de Auditoría Interna. La auditoría interna de Sareb tiene establecido, con carácter específico para la función, una declaración de principios y reglas de los auditores internos. El Gestor deberá adherirse anualmente mediante declaración jurada.

Sin menoscabo de cualquier otra obligación de información, el Gestor se obliga a poner en conocimiento de auditoría interna de Sareb, tan pronto como sea advertida, cualquier circunstancia de la que pudiera derivarse un riesgo de incumplimiento o cualquier aspecto que a juicio de un observador imparcial pudiera poner de manifiesto la existencia de incidencias significativas en los procesos de gestión y administración de los Activos Sareb, o de riesgos significativos.

En todo caso y siempre que su contenido tenga relación, directa o indirectamente, con los Servicios prestados sobre los Activos Sareb o con las relaciones de negocio que pudieran derivarse de su administración y gestión, el Gestor facilitará a Auditoría Interna de Sareb, con la inmediatez posible, una copia:

- a) De los informes de organismos supervisores y de la contestación que, en su caso, pudiera haber elaborado el Gestor;
- b) De los requerimientos de información de organismos oficiales y de la contestación a los mismos;
- c) De los informes de las Funciones de Control del Gestor;
- d) De las recomendaciones realizadas por los auditores y, en general, informes de expertos externos; y
- e) Adicionalmente, el Gestor se compromete a enviar mensualmente, durante los diez (10) primeros días del mes (el mecanismo de envío será definido por Auditoría Interna de Sareb):
 - 1. La plantilla cumplimentada de seguimiento del Programa de Supervisión; y
 - 2. El modelo cumplimentado de “confirmación de información remitida” para asegurar el envío de toda la documentación requerida.

El Gestor acepta y autoriza todas las actuaciones, requerimientos o visitas que cualquier autoridad reguladora o de supervisión lleve a cabo en las oficinas o instalaciones del Gestor, en el ejercicio de sus funciones en relación con los Servicios prestados en virtud de la presente licitación. El Gestor se compromete asimismo a cooperar con Sareb y con la autoridad reguladora y de supervisión de que se trate como sea preciso y conforme a las instrucciones dadas por Sareb para facilitar estos procedimientos. El Gestor velará porque sus socios u otros subcontratistas autorizados permitan igualmente la realización de actuaciones, requerimientos o visitas que cualquier autoridad reguladora o de supervisión lleve a cabo en sus oficinas o instalaciones, en el ejercicio de sus funciones en relación con los Servicios prestados en virtud de la presente licitación.