PROSEGUR

Documento de Soporte 3P a Condiciones Generales de Compra

ÁREA DE GESTIÓN DE MEDIOS - COMPRAS

1. Propietario

Director Corporativo de Gestión de Medios

2. Resumen

Marco normativo que regula las condiciones aplicables a cualquier tipo de contratación o pedido de Prosegur, en defecto de particularizarse por condiciones específicas pactadas por las partes y plasmadas en un contrato.

3. Elaboración y Aprobación

Elaborado por:	Área de Gestión de Medios - Compras				
Revisado por:	Área Legal Global				
Aprobado por:	Área Global de Compras	David Jose Gestal		Fecha:	23/06/2023
Sustituye a:	DS/GLO/GdM/COM/01 DS/GLO/GdM/COM/06	Edición:	03 02	Fecha:	31/03/2023 31/05/2022

4. Documentos Asociados

Código	Nombre
NG/GLO/GdM/COM/01	Norma General 3P de Compras

5. DEFINICIONES

Para mayor claridad y entendimiento de las presentes Condiciones Generales, se establecen las siguientes definiciones:

- Prosegur: Empresa del Grupo que actúa como parte compradora y/o contratante en cada Compra y/o Contratación.

- Filial se refiere a la entidad o conjunto de entidades ya sea inscrita o no, bajo el control común. Tal como se utiliza en esta definición, “control” (y las variantes utilizadas) significará la facultad, de forma directa o indirecta, de dirigir los intereses de otra entidad ya sea a título de propietaria, por contrato, o de otra forma.

- Compra: Operación en la que el importe corresponde mayoritariamente a las adquisiciones de bienes.

- Contratación: Operación en la que el importe mayoritariamente corresponde a la adquisición de obras y/o servicios, y por consiguiente aporte de mano de obra. Tanto una compra como una contratación podrán tener componentes de obras, bienes y de servicios. En el desarrollo de las presentes Condiciones los términos de compra y contratación se considerarán términos equivalentes.

- Pedido: Documento de carácter vinculante para las partes emitido por Prosegur al proveedor donde se fijan precios, plazos y condiciones para el aprovisionamiento de un bien o prestación de un servicio al que previamente se le ha adjudicado la compra o contratación. En ocasiones este documento reviste simultáneamente el carácter de contrato y el de solicitud de aprovisionamiento.

- Contrato: Acuerdo de carácter vinculante suscrito entre las partes donde se fijan precios, plazos y condiciones para la realización de una obra, subcontratación de la misma o prestación de un servicio.

- Condiciones Generales: Documento donde se establecen las bases del proceso de Compra de bienes y/o Contratación de obras y/o servicios y que son de aplicación a todo el Grupo Prosegur.

- Proveedor: La entidad que ha resultado adjudicataria de un Pedido.

- Contratista: La entidad que ha resultado adjudicataria de un Contrato.

- Condiciones Particulares: También denominado Petición de Oferta. Todo documento en el que se incluyen todos aquellos requisitos, de cualquier índole, necesarios para que el Proveedor/Contratista suministre el bien o realice las obras y servicios en forma y calidad requerida.

6. CONDICIONES GENERALES DE COMPRA Y CONTRATACIÓN

6.1. Validez y prelación de la documentación contractual

6.1.1. Las Condiciones Generales serán puestas en conocimiento de los Proveedores/Contratistas en el proceso de la gestión de Compra/ Contratación y que integrarán la documentación contractual que se establezca en el Pedido / Contrato, en todos sus términos y condiciones.

6.1.2. Estas Condiciones Generales podrán ser complementadas con Condiciones Particulares y/o los correspondientes Pedidos/ Contratos que se generen. En caso de discordancia entre los documentos que integren una Compra/ Contratación, lo particular prevalecerá sobre lo general siendo el orden de prelación el siguiente:

- Las eventuales modificaciones al Pedido / Contrato, expresamente convenidas por escrito y posteriores a su fecha de suscripción o emisión.
- El Pedido / Contrato y su documentación anexa.
- Las eventuales modificaciones a las especificaciones técnicas solicitadas
- Las especificaciones técnicas solicitadas.
- Las modificaciones a las Condiciones Particulares y/o Generales.
- Las Condiciones Particulares.
- Las Condiciones Generales
- Las aclaraciones realizadas por escrito por el Proveedor/Contratista, con posterioridad a su oferta que hayan resultado aceptadas por Prosegur.

6.1.3. No se aceptarán otras Condiciones Generales que sean propuestas por parte del Proveedor/Contratista distintas a las establecidas en el presente documento salvo aceptación expresa total o parcial de las mismas por Prosegur.

6.1.4. Serán nulas y sin valor las condiciones y especificaciones que el Proveedor/Contratista inserte en sus notas de entrega, facturas u otros documentos cruzados entre las partes, que contradigan las condiciones expresas establecidas en el Pedido/Contrato.

6.1.5. Los Contratos de obras y/o servicios se mantendrán en vigor mientras dure la ejecución de los trabajos objeto de los mismos, de acuerdo con lo establecido en la documentación contractual. Si se hubiera predeterminado una fecha de vencimiento y la duración de dichos trabajos superara esta fecha, el Contrato se entenderá tácitamente prorrogado por períodos mensuales sucesivos, salvo denuncia por escrito de cualquiera de las partes con una antelación mínima de quince días a dicha fecha de vencimiento o de cualquiera de las prórrogas.

No obstante, en el Contrato podrán incluirse las cláusulas que serán de aplicación en materia de cumplimiento de plazos de ejecución y de prórrogas de los mismos.

6.2. Sistema de evaluación y homologación de Proveedores

6.2.1. Prosegur utiliza una plataforma online gestionada por un proveedor externo a Prosegur (GoSupply Advanced Applications, S.L., en adelante “GoSupply”), para la precalificación, evaluación y homologación preliminar de sus Proveedores/Contratistas. Para la calificación y homologación definitiva de un Proveedor/Contratista se requiere como requisito obligatorio, el registro y participación

del Proveedor/Contratista en el proceso de análisis de riesgo de Proveedores que Prosegur tiene implementado a través de dicha plataforma.

6.2.2. El Proveedor/Contratista deberá estar calificado como apto en el proceso de análisis de Prosegur antes del inicio de cualquier suministro de servicios, bienes y/o materiales objeto de estas Condiciones Generales y/o del correspondiente Contrato/Pedido. Asimismo, el Proveedor/Contratista garantiza y se obliga a mantener las condiciones aprobadas en dicho análisis durante toda la vigencia de las presentes Condiciones Generales y/o del Contrato/Pedido correspondiente y para ello, se compromete a entregar a Prosegur la información y/o documentación actualizada que le sea solicitada de acuerdo a los criterios establecidos por Prosegur.

6.2.3. El Proveedor/Contratista queda informado y asume que Prosegur es ajeno a los servicios prestados por “GoSupply”, siendo responsabilidad del proveedor de esta plataforma los servicios de acceso y demás circunstancias asociadas al alta en la misma. Prosegur solo es receptor de la información que el Proveedor/Contratista incluya en la plataforma.

6.2.4. Para completar el proceso interno de precalificación, evaluación y homologación preliminar, Prosegur ha implantado el servicio de precalificación, evaluación y homologación preliminar de Proveedores/Contratistas, enfocado en la mejora constante de sus Proveedores/Contratistas con el fin de mejorar la sostenibilidad y calidad de los bienes y servicios comercializados a Prosegur. Este servicio de precalificación, evaluación y homologación preliminar, de contratación directa entre los Proveedores y Prosegur, es de obligado cumplimiento y conlleva el pago a Prosegur de una cuota anual, que será designada dependiendo del nivel de facturación anual del Proveedor/Contratista y de las categorías de productos y servicios a los que dedica su actividad. En todo caso, Prosegur determinará la categoría asignada al Proveedor/Contratista y la cuota anual correspondiente, que consisten en:

- Proveedor autónomo: 59€ anuales + IVA
- Proveedor básico: 99€ anuales + IVA
- Proveedor estándar: 199€ anuales + IVA
- Proveedor crítico: 299€ anuales + IVA

Estas cuotas y/o la propia categoría inicialmente asignada al Proveedor/Contratista podrán ser revisadas y actualizadas por Prosegur en cualquier momento y bajo su exclusivo criterio, comprometiéndose el Proveedor/Contratista a aceptar las nuevas cuotas y/o la nueva categoría asignada tan pronto como le sea comunicada por Prosegur.

6.2.5. El Proveedor/Contratista acepta que el pago de las cuotas anuales del servicio de precalificación, evaluación y homologación preliminar de Proveedores sea efectuado a Prosegur, mediante recibo domiciliado en la misma cuenta bancaria que el Proveedor/Contratista haya indicado a Prosegur para que Prosegur le efectúe los pagos de las facturas por obras, servicios o suministro de bienes y/o materiales prestados o entregados a Prosegur. Asimismo, en caso de devolución o imposibilidad de realizar el pago de conformidad con lo anteriormente indicado, Prosegur quedará facultada para descontar y/o compensar la cantidad correspondiente a dichas cuotas de las facturas pendientes de abono al Proveedor/Contratista.

6.3. Obligaciones y responsabilidades del Proveedor/Contratista

6.3.1. El Proveedor/Contratista se obliga a realizar las obras, servicios y suministro de bienes, conforme a lo que se recoge en el Pedido/Contrato y/o sus anexos y a cumplir todas las obligaciones de carácter técnico, administrativo, fiscal, laboral, legal y cualesquiera otras vinculadas a la relación contractual.

6.3.2. El Proveedor/Contratista deberá entregar toda la documentación que le sea requerida por Prosegur en el Pedido / Contrato, tanto en plazo como en cantidad, así como cualquier otra información o documento de cualquier índole que pudieran requerir las leyes, normas o reglamentaciones aplicables al suministro, obra o servicio.

6.3.3. El Proveedor/Contratista, ante el requerimiento de Prosegur, deberá justificar documentalmente el cumplimiento de las obligaciones a que se refieren los apartados anteriores. La falta de presentación o la presentación insuficiente de tal documentación justificativa constituirá un incumplimiento grave de sus obligaciones.

6.3.4. De acuerdo con la naturaleza del Pedido / Contrato, el Proveedor/Contratista nombrará a los responsables, dentro de su organización, del suministro de bienes y/o contratación de obras y/o servicios que se establezcan en las Condiciones Particulares del mismo, y comunicará tal designación al respectivo Coordinador de Prosegur.

6.3.5. El Proveedor/Contratista y en su caso, sus subcontratistas son responsables del pago puntual de los salarios, seguros sociales y de cualquier otra compensación o indemnización de naturaleza laboral o de cualquier otra índole que, por cualquier causa, deban recibir sus empleados y mantendrán indemne a Prosegur frente a cualquier reclamación derivada del incumplimiento de dicha obligación.

6.3.6. El Proveedor/Contratista y en su caso, sus subcontratistas, deberán cumplir las normas legales vigentes y otras como las de las Convenciones Fundamentales de la Organización Internacional del Trabajo relativas a derechos laborales y seguridad social.

El Proveedor/Contratista y en su caso, sus subcontratistas, deberán cumplir cuantas disposiciones relativas al Medio Ambiente, Prevención de Riesgos Laborales, y Seguridad e Higiene se hallaren vigentes y resulten de aplicación al Pedido / Contrato, deberá observar las políticas y procedimientos de Prosegur y, en cualquier caso, deberá respetar el Código Ético y de Conducta de Prosegur que se encuentra publicado en español y en inglés en los siguientes enlaces contenidos dentro de la página web de Prosegur:

- Código Ético y de Conducta de Prosegur - ES
- Code of Ethics and Conduct Prosegur – EN

6.3.7. El Proveedor/ Contratista y en su caso, sus subcontratistas será/n responsable/s e indemnizará/n y mantendrá/n indemne a Prosegur y al resto del Grupo Prosegur contra reclamaciones por daños directos, indirectos y/o consecuenciales, incluidos la pérdida de negocio, daños a la imagen o lucro cesante, pérdidas o destrucción de las propiedades de aquellos y/o de terceros o por muerte, enfermedad o lesiones del personal de aquellos y/o de terceros derivados de la ejecución por parte del Proveedor/Contratista y / o en su caso, sus subcontratistas de sus obligaciones contractuales o legales. Esta responsabilidad incluirá los honorarios legales y costas, sin que los montos de los Seguros que se suscriban al amparo de la Cláusula 2.10 constituyan un límite a su responsabilidad.

6.3.8. El Proveedor/Contratista y en su caso, sus subcontratistas responderá/n frente a Prosegur y frente al resto de Empresas del Grupo Prosegur, de cualesquiera daños directos, indirectos y/o consecuenciales, incluidos la pérdida de negocio, daños a la imagen y el lucro cesante que, tanto él/ellos como las personas de las que deba/n responder legal o contractualmente, pudiera/n ocasionar a Prosegur o a las empresas del Grupo Prosegur por daños, pérdidas o destrucción de las propiedades de ésta o por muerte, enfermedad o lesiones de su personal, y que tengan su causa en una acción u omisión en el cumplimiento de las obligaciones derivadas del Pedido / Contrato por parte del Proveedor/Contratista y en su caso sus subcontratistas o del personal de éstos. Esta responsabilidad incluirá los honorarios legales y costas, sin que los montos de los Seguros que se suscriban al amparo de la Cláusula 2.10. constituyan un límite a su responsabilidad.

6.3.9. El Proveedor/Contratista garantiza la indemnidad de Prosegur frente a eventuales reclamaciones de los trabajadores del Contratista afectos al cumplimiento del Pedido/Contrato o de sus subcontratistas, que serán defendidas o transadas por el Proveedor/Contratista, el cual, además, soportará los costes de defensa y las cantidades o declaraciones objeto de transacción o contenidas en sentencia condenatoria firme.

6.3.10. Asimismo, el Proveedor/Contratista garantiza la indemnidad de Prosegur frente a cualquier sanción administrativa o de cualquier otra índole que eventualmente le fuere impuesta a resultas, directa o indirectamente, de la ejecución del Pedido/Contrato.

6.3.11. En caso de incumplimiento por el Proveedor/Contratista de las obligaciones señaladas en los párrafos anteriores, Prosegur quedará facultado para deducir en la siguiente o siguientes certificaciones/facturas a abonar por Prosegur los importes a los que asciendan dichas reclamaciones o sanciones no atendidas por el Proveedor/Contratista, así como los gastos de defensa en que hubiera incurrido Prosegur, como consecuencia de dicho incumplimiento.

6.3.12. El régimen jurídico de responsabilidad al que se refiere este documento no resulta de aplicación a las responsabilidades que a cada una de las Partes les resultare exigible con arreglo a la ley de prevención de riesgos laborales o a la normativa que resulte de aplicación en esta materia y a sus normas reglamentarias de desarrollo, en cuyo caso será de aplicación el régimen legal y reglamentario establecido para dicha responsabilidad.

6.3.13. La responsabilidad fijada en la cláusula 6.3.8 se ampliará, y será igualmente exigible, durante el Período de Garantía.

6.3.14. En aquellos supuestos en que la condición de Proveedor / Contratista sea ostentada por una unión temporal de empresas, o cualquier entidad carente de personalidad jurídica propia distinta de la de sus componentes, la responsabilidad que pudiera derivarse del presente Pedido / Contrato frente a Prosegur será de carácter solidario de todas las personas o empresas que formen parte de las sociedades de que se trate.

6.3.15. Como consecuencia de lo anterior, y de acuerdo con lo establecido en los artículos 1.137 y 1.144 del Código civil español, Prosegur podrá dirigirse indistinta e individualmente contra cualquiera de las personas físicas o jurídicas que formen la unión temporal de empresas, o el ente carente de personalidad jurídica, para exigir el cumplimiento de todas las obligaciones que se derivan del Pedido / Contrato.

6.3.16. Prosegur, en ningún supuesto y bajo ningún concepto, podrá ser responsable por los daños directos, indirectos y/o consecuenciales que pueda sufrir el Proveedor/Contratista, derivados directa o indirectamente de la ejecución del Pedido / Contrato, incluyendo, pero no limitados a pérdidas de uso, pérdidas de beneficios e interrupciones de negocio.

6.3.17. Prosegur fomenta la contratación de proveedores que cumplen criterios de sostenibilidad y responsabilidad social corporativa, que promueven y suscriben los objetivos de desarrollo sostenible de las Naciones Unidas y que disponen de algún tipo de certificación ESG, bien a través de pertenencia a Índices sostenibles o a través de certificaciones en la materia. Prosegur promueve y fomenta que los proveedores y asociados con los que opera acepten los siguientes principios:

- Respetar las leyes aplicables de todas las jurisdicciones donde el Grupo Prosegur opera
- Operar como un empleador socialmente responsable que tenga el compromiso de:
    - pagar un sueldo digno a sus empleados siempre superior al salario mínimo Interprofesional
    - respetar la prevención del trabajo infantil y el trabajo forzoso,
    - respetar la no discriminación e igualdad de oportunidades,
    - respetar la libertad de asociación, el derecho a negociación colectiva y la eliminación de horas de trabajo excesivas.
- Ofrecer un entorno de trabajo seguro cumpliendo todos los estándares en seguridad y salud laboral.
- Utilizar prácticas sostenibles que respeten el medio ambiente, demandando a sus proveedores compromisos en:
    - Uso de energías renovables
    - Actuaciones encaminadas a la reducción de emisiones y agentes contaminantes que eviten el cambio climático
    - Respeto por la biodiversidad
  - Uso sostenible de recursos naturales
  - Reducción de residuos
- Respetar el Código Ético y de Conducta de Prosegur.

6.4. Obligaciones y responsabilidades de Prosegur

6.4.1. El pago de los bienes, obras y/o servicios en los precios y condiciones estipulados en el pedido/contrato según lo estipulado en las cláusulas 2.6 y 2.7.

6.5. Cesión del Pedido/Contrato y subcontratación

6.5.1. Las obras, bienes y servicios amparados por el Pedido / Contrato no podrán ser delegados o subcontratados, total o parcialmente, sin autorización previa, y por escrito, de Prosegur, subrogándose, en tal caso, expresamente el subcontratista en todas las condiciones de este documento.

6.5.2. Para la obtención de autorización previa de subcontratación, el Proveedor/Contratista exigirá al Subcontratista toda la documentación prevista en la Petición de Oferta y en estas Condiciones Generales, así como su compromiso escrito de cumplimiento de todas y cada una de las cláusulas del Pedido / Contrato y de su documentación anexa, debiendo hacer entrega inmediata de todo ello a Prosegur.

6.5.3. En caso de empleo de subcontratistas, el Proveedor/Contratista seguirá siendo el responsable principal ante Prosegur del cumplimiento de las obligaciones derivadas del Pedido/Contrato, aun cuando se trate de bienes, obras y/o servicios directamente suministrados/prestados por el subcontratista autorizado. Sin perjuicio de esto, Prosegur podrá en todo momento inspeccionar y vigilar los trabajos del subcontratista y el cumplimiento de sus obligaciones.

6.6. Condiciones económicas e impuestos

6.6.1. Los precios recogidos en el Pedido / Contrato y/o sus anexos, se entenderán fijos y no revisables hasta la total y correcta cumplimentación del Pedido / Contrato, salvo expresa indicación en contra, e incluirán toda clase de impuestos, cargas, gravámenes, tasas y arbitrios presentes o futuros, a excepción del Impuesto sobre el Valor Añadido o impuesto de similar naturaleza, que figurará por separado como partida independiente.

6.6.2. Como excepción adicional al párrafo anterior y en caso de aplicar retención de acuerdo con la Legislación aplicable, no se entenderá incluido dentro del precio el importe de retención que corresponda según la Legislación aplicable. De forma que, el Proveedor pagará el importe total de la factura al Cliente y pagará adicionalmente el importe de retención correspondiente a la Administración Fiscal del Proveedor. En caso de reducción de retención por aplicación de un Convenio para Evitar la doble imposición entre ambos países, el Cliente, a petición del Proveedor, le entregará previamente a realizar cualquier pago, un certificado de residencia fiscal en el sentido del Convenio, de forma que el Proveedor pueda pagar la retención que aplique según dicho Convenio. El Proveedor, una vez realizado el pago de la retención, aportará al Cliente un certificado de pago de dichas retenciones ingresadas.

6.6.3. No se pagarán bienes, obras y/o servicios no incluidos en el Pedido / Contrato si su ejecución no ha sido previamente ofertada por el Proveedor/Contratista, por escrito, y aceptada, también por escrito, por Prosegur, la correspondiente modificación del Pedido / Contrato.

6.6.4. El pago de anticipos a cuenta se efectuará, según sea cada caso, contra presentación del correspondiente aval bancario por el mismo importe a satisfacer, irrevocable y sin reservas, con carácter solidario, a primer requerimiento y con renuncia a los beneficios de excusión y división, y siempre y cuando tal pago de anticipos esté contemplado así, en el correspondiente Pedido / Contrato.

6.6.5. El pago del precio del Pedido / Contrato no implicará renuncia alguna a los derechos de Prosegur estipulados en el mismo.

6.6.6. El Proveedor/Contratista será responsable de cualquier diferencia de fletes, portes, tributos u cualesquiera otros gastos originados por el incumplimiento de las instrucciones de envío o de cualquier otra de las condiciones establecidas o aplicables al Pedido / Contrato.

6.6.7. Todos los impuestos que graven las operaciones comerciales a que estas Condiciones Generales se refieran, serán soportados por las partes de acuerdo a lo legalmente establecido. El contribuyente del impuesto es responsable, en cada caso, de la correcta tributación en lo que a sus obligaciones se refiere.

6.7. Forma de pago

6.7.1. Todos los pagos se realizarán a los 60 días naturales de fecha factura, a no ser que se haya pactado un plazo diferente entre las partes o que se establezca otro periodo de pago por imperativo legal. Las facturas se pagarán sólo si Prosegur posee documentos que demuestren la recepción conforme de los servicios realizados de acuerdo a lo establecido en el Pedido/Contrato. Para el caso de suministros de bienes se estará a lo establecido en los Incoterms y/o condiciones de entrega incluidas en el Pedido.

Se establece como medio habitual de pago la transferencia bancaria o el confirming.

6.7.2. El resto de condiciones de pago quedarán perfectamente definidas en el Pliego de Condiciones Particulares, así como en el Pedido / Contrato.

6.8. Aceptación del Pedido/Contrato

6.8.1. Aceptación del Contrato: La firma del Contrato por las Partes dará por supuesta la total aceptación del mismo.

6.8.2. Aceptación del Pedido: La firma o acuse de recibo en señal de aceptación del Pedido por parte del Proveedor/Contratista a Prosegur. En cualquier caso, la simple ejecución del Pedido por parte del Proveedor entraña la aceptación implícita del mismo por su parte y excluye toda excepción no aceptada por escrito por parte de Prosegur.

6.9. Plazos de entrega y ejecución

6.9.1. El plazo de entrega / ejecución que se establece en el Pedido / Contrato será firme, debiéndose de efectuar de acuerdo con las cantidades, fechas y lugares especificados en los programas de entrega/ ejecución definidos y suministrados por Prosegur

6.9.2. En caso de retraso en el plazo de entrega/ejecución fijado, Prosegur podrá aplicar las penalizaciones que se hayan establecido y/o en su caso resolver el Pedido / Contrato de acuerdo a lo estipulado en la cláusula 2.16.

6.9.3. Prosegur podrá cambiar los programas de entrega/ejecución, u ordenar la suspensión temporal de entregas programadas. A tal efecto buscará el acuerdo correspondiente y podrá solicitar el ajuste necesario del Pedido / Contrato.

6.10. Garantías

6.10.1. Las Garantías que, atendiendo a las características del bien, obra y servicio, podrán ser establecidas por Prosegur son las siguientes:

Garantía de fiel cumplimiento y de los bienes, obras y/o servicios al fin requerido. Se establecerá por el Proveedor/Contratista para garantizar el cumplimiento de todas sus obligaciones contractuales según Pedido/Contrato, desde el momento de la aceptación/firma del Pedido/Contrato, hasta la recepción definitiva por Prosegur de los bienes, obras y/o servicios requeridos. El requerimiento o no de dicha Garantía se establecerá en la Petición de Oferta y/o en el Pedido/Contrato correspondiente.

Dicha Garantía se establecerá a través del Modelo de Aval del Anexo II (emitido por un banco con rating mínimo BBB- de Standard & Poor o aprobado por el departamento de Tesorería de Prosegur) o bien seguro de caución (emitido por una aseguradora con rating mínimo BBB- de Standard & Poor o aprobada por el departamento de Seguros de Prosegur) o bien por una retención directa en factura.

6.10.2. El Proveedor garantiza que en el suministro de bienes éstos son de su plena propiedad, adecuados al fin que se destinan y de primera calidad y primer uso, así como que cumplen los requisitos de seguridad y calidad especificados en el Pedido. El Contratista garantiza que la realización de obras y/o servicios cumple los requisitos de seguridad y calidad especificados en el Contrato. Asimismo, el Proveedor/Contratista, garantiza el cumplimiento de la correspondiente legislación vigente, así como de las normas propias de Prosegur, y que en su cumplimiento se atendrá a los programas de trabajo/ ejecución establecidos.

6.10.3. El Proveedor/Contratista, garantiza igualmente que los bienes, obras y servicios, están libres de cargas y gravámenes a favor de terceros, carecen de defectos y son idóneos para su comercialización/utilización, así como que dispone de las patentes, licencias y demás derechos de propiedad industrial/intelectual necesarios para la realización de cuanto es objeto del Pedido / Contrato.

6.10.4. Retenciones en concepto de Garantía: Las retenciones en concepto de garantía se establecerán en el Pedido / Contrato.

6.10.5. El Período de Garantía de los bienes, obras y/o servicios suministrados/realizados por el Proveedor/Contratista será establecido en el Pedido / Contrato. En su defecto, será:

Para bienes, de 12 meses a partir de la fecha de la puesta en marcha o de 24 meses a partir de la fecha de la recepción conforme en destino o de la puesta a disposición, según Incoterm aplicable, lo que antes se produzca, si el Proveedor tuviera unas condiciones de mayor duración se atenderá a ellas.

Para contratos de obras y/o servicios, de 12 meses desde la fecha de firma del acta de recepción provisional.

Otros plazos podrán ser exigibles cuando así lo establezca la legislación aplicable y/o la naturaleza específica del suministro, obra y/o servicio de que se trate.

6.10.6. Durante el período de garantía serán por cuenta del Proveedor/Contratista todos los incumplimientos y/o daños, sin perjuicio de lo señalado al respecto en la Cláusula 6.3.16 y siguientes, que se originen por causa de incumplimiento o cumplimiento defectuoso o inadecuado por parte del Proveedor/Contratista de las condiciones contractuales aplicables al suministro, obra o servicio, así como en su caso, por los defectos de calidad de los materiales empleados.

El plazo de garantía se interrumpirá por el tiempo que se emplee en las respectivas reparaciones o sustituciones, las que a su vez serán garantizadas, a partir de su terminación, por igual tiempo al de la garantía inicial establecida.

6.10.7. Dichos incumplimientos o cumplimientos defectuosos o inadecuados del suministro, obra y/o servicio, o defecto de calidad de que se trate, cuando el Proveedor/Contratista no haya efectuado las pertinentes acciones rectificativas, o cuando no muestre la adecuada diligencia en la resolución de los problemas planteados, podrá dar lugar: a la retención por parte de Prosegur de los pagos pendientes; a la ejecución de la/s garantía/s económicas y/o bancarias e incluso al rechazo total o parcial del suministro, obra o servicio efectuados, con exigencia en este caso de la devolución de los importes satisfechos sin que dicha circunstancia pueda ser causa de reclamación alguna por parte del Proveedor/Contratista.

6.10.8. Prosegur descontará, en su caso, de las facturas pendientes de abono al Proveedor/Contratista las penalizaciones que fueren de aplicación.

Asimismo, para resarcirse de los gastos propios o de los gastos y costes derivados de contratar con terceros la reparación o la ejecución de lo incumplido o defectuosamente cumplido por el Proveedor/Contratista, y de cualquier otra deuda que mantenga el Proveedor/Contratista con Prosegur, podrá descontar tales importes de las facturas pendientes de abono al Proveedor/Contratista.

El pago o deducción de tales penalizaciones y gastos no relevará al Proveedor/Contratista de cualesquiera de sus demás obligaciones y responsabilidades que emanen del Pedido/Contrato.

6.10.9. Se considera automáticamente deuda del Proveedor/Contratista con Prosegur, cualquier cantidad que sea reclamada a esta última, por descubiertos o incumplimientos del Proveedor/Contratista en relación con salarios, con seguros sociales, con sus obligaciones fiscales y cualesquiera otras que puedan reclamarse a Prosegur con arreglo a normas legales o reglamentarias.

6.10.10. Las posibles deducciones efectuadas, de acuerdo con los apartados anteriores, serán totalmente independientes de la cantidad depositada en su caso como Garantía.

6.10.11. En el supuesto que el Proveedor pretenda dejar de fabricar el producto objeto de la Orden de Compra, éste deberá enviar notificación escrita con acuse de recibo dirigida al Departamento de Compras de Prosegur con un preaviso de seis meses antes de la fecha en que pretenda terminar la fabricación del producto. Dicha notificación deberá contener como mínimo: (i) identificación del producto; (ii) identificación de las Órdenes de Compra afectas al mismo; (iii) relación de los países afectados; y (iv) fecha en que se pretende terminar la fabricación del producto.

Desde la emisión de la Orden de Compra, el Proveedor garantiza el adecuado servicio técnico y la existencia de repuestos durante el plazo mínimo de diez (10) años en todos los países afectados y a partir de la fecha en el que el producto deje de fabricarse. El precio de los repuestos o de los productos y servicios se ofrecerá a Prosegur a un precio máximo equivalente al precio de contrato de los productos sustituidos; y con el mismo nivel de cumplimiento de los requisitos técnicos solicitados por Prosegur para el producto a reparar o sustituir.

En garantía de dicho compromiso, Prosegur se reserva el derecho de exigir al Proveedor un aval bancario a primer requerimiento conforme al modelo de Aval del Anexo II de este documento.

En incumplimiento por parte del Proveedor de dicha garantía o no tenga la capacidad para cumplirla, tendrá los siguientes efectos:

- La retención de cualquier pago pendiente por parte de Prosegur
- La ejecución del aval bancario
- La cancelación total o parcial de las Órdenes de Compra en curso, sin que ello suponga indemnización alguna a favor del proveedor.
- El derecho de Prosegur de poder reclamar todos los daños, perdidas, costes y gastos soportados (incluyendo honorarios de abogados) incurridos para poder atender por sus medios o a través de terceros las obligaciones incumplidas por parte del Proveedor.

Adicionalmente, el Proveedor, a su coste, deberá poner a disposición de Prosegur todos aquellos desarrollos software hechos a medida, incluyendo código fuente, código objeto, manuales y cualquier otra información relevante.

6.11. Seguros

6.11.1. Sin perjuicio de su responsabilidad según el Pedido / Contrato, y sin que esta cláusula limite la misma, el Proveedor / Contratista suscribirá y mantendrá en vigor a su cargo en todo momento durante la validez del Pedido / Contrato, y con compañías de reconocida solvencia financiera los seguros que se describen a continuación. Las coberturas y cantidades cubiertas en dichos seguros nunca serán inferiores a los obligatorios según las leyes vigentes. Su mantenimiento no variará las obligaciones de mantener indemne a Prosegur establecidas por el Pedido / Contrato.

6.11.1.1 Contratos de Obras y/o Servicios

a) Seguros de enfermedad y accidentes de trabajo de todos sus trabajadores asignados a los Trabajos, de acuerdo con la ley aplicable, incluyendo las leyes del estado de origen de los empleados expatriados.

b) Seguro de construcción/edificación, montaje y de daños a los equipos de construcción alquilados, arrendados o de propiedad del Contratista, con un límite no inferior a su valor de reposición. En el caso del seguro de construcción, será necesaria la contratación de la cobertura adicional de colindantes y preexistentes. En caso de siniestro, e independientemente de la causa, el Contratista renuncia de forma expresa al derecho de recurso contra Prosegur por cualquier daño o pérdida que sufran dichos bienes, comprometiéndose a comunicar por escrito a sus compañías aseguradoras esta renuncia a recurso.

c) Seguro de responsabilidad civil empresarial, incluyendo entre otras la responsabilidad civil patronal, profesional, productos, retirada de productos, post-trabajos y polución y contaminación con una cobertura igual al importe de las obras/servicios contratados en las Condiciones Particulares de cada Contrato y que como mínimo, será el de los importes estándares que figuran en el Anexo I.

En el caso de las pólizas de responsabilidad civil, si éstas son contratadas bajo el ámbito temporal de cobertura por ocurrencia, el Contratista deberá mantener en vigor dichas pólizas hasta el vencimiento del período de garantía o responsabilidad legal. Si las pólizas son contratadas bajo el ámbito temporal de cobertura por reclamación, el Contratista deberá mantener en vigor las pólizas como mínimo 2 (dos) años posterior al vencimiento del período de garantía o responsabilidad legal.

Dichos seguros incluirán a Prosegur como asegurado adicional, sin perder su condición de tercero.

d) Si fuera necesario para la ejecución de los trabajos la utilización de automóviles, maquinaria autopropulsada, maquinaria industrial, aeronaves o embarcaciones, seguro de responsabilidad civil, con un límite que será fijado por siniestro en las Condiciones Particulares de cada Contrato y que como mínimo, será el de los importes estándares que figuran en el Anexo I.

De ser necesaria la contratación de embarcaciones se exigirá cobertura de protección e indemnización (armador/fletador) con un club del Grupo Internacional.

Con independencia de lo anterior, podrá el Contratista suscribir los seguros complementarios que estime necesarios para la total cobertura de sus responsabilidades según el Contrato.

6.11.1.2 Pedidos de Bienes

a) Seguros de enfermedad y accidentes de trabajo de todos sus trabajadores asignados a los trabajos, de acuerdo con la ley aplicable, incluyendo las leyes del estado de origen de los empleados expatriados.

b) Seguro de transporte de los bienes y/o equipos objeto del Pedido, de acuerdo con las condiciones compra y del Incoterm que sea pactado en las Condiciones Particulares.

c) Seguro de responsabilidad civil empresarial, incluyendo entre otras la responsabilidad civil patronal, profesional, productos, retirada de productos, post-trabajos y polución y contaminación con una cobertura igual al importe de los bienes adquiridos que, como mínimo, será el que se determine en las Condiciones Particulares de cada Pedido.

En el caso de las pólizas de responsabilidad civil, si éstas son contratadas bajo el ámbito temporal de cobertura por ocurrencia, el Proveedor, deberá mantener en vigor dichas pólizas hasta el vencimiento del período de garantía o responsabilidad legal. Si las pólizas son contratadas bajo el ámbito temporal

de cobertura por reclamación, el Proveedor deberá mantener en vigor las pólizas como mínimo dos (2) años posterior al vencimiento del período de garantía o responsabilidad legal.

Dichos seguros incluirán a Prosegur como asegurado adicional, sin perder su condición de tercero.

Con independencia de lo anterior, podrá el Proveedor suscribir los seguros complementarios que estime necesarios para la total cobertura de sus responsabilidades según el Pedido.

6.11.2. Antes de la entrega de los bienes o del comienzo de obras/servicios, el Proveedor/Contratista deberá entregar a Prosegur un certificado de los seguros contratados. Este certificado quedará incorporado al Contrato/Pedido como Anexo. La no entrega del certificado facultará a Prosegur para resolver el Contrato/Pedido por causa imputable al Proveedor/Contratista.

6.11.3. Prosegur, en todo momento, podrá solicitar al Proveedor/Contratista la entrega del original de las pólizas, o copias legitimadas, de los seguros que tenga contratados, así como recibos o justificantes de encontrarse al corriente de pago de las primas correspondientes. El Proveedor/Contratista queda obligado a la entrega de todo ello en un plazo no superior a siete (7) días.

6.11.4. El Proveedor/Contratista queda obligado a informar por escrito a Prosegur, y de cualquier incidencia que afecte a la vigencia y condiciones de los seguros contratados.

6.11.5. En cualquier caso, Prosegur nunca será responsable por límites, deducibles o limitaciones en el condicionado de las pólizas del Proveedor/Contratista.

6.11.6. En todos los seguros a que se refiere la cláusula 2.10.1., se incluirá una mención por la que se exima de responsabilidad y no repetición de la entidad aseguradora contra Prosegur.

6.11.7. El Proveedor/Contratista, bajo su exclusiva responsabilidad, requerirá, en su caso, a los subcontratistas para que mantengan la misma política de responsabilidades y seguros requerida al Proveedor/Contratista. Ello no eximirá al Proveedor/Contratista de su responsabilidad frente a Prosegur.

6.11.8. En función del alcance o naturaleza del Contrato/Pedido, Prosegur se reserva el derecho de:

- Solicitar límites por siniestro superiores a los establecidos en el Anexo I,
- Solicitar coberturas o seguros adicionales no incluidos el apartado 2.10.1

6.12. Sanciones por incumplimiento

6.12.1. Las sanciones o penalizaciones por incumplimiento del Proveedor/Contratista, se establecerán en el Pliego de Condiciones Particulares y en el Pedido / Contrato estando sujetas en su defecto a la legislación mercantil vigente.

6.12.2. En el caso de que no se especifiquen en las condiciones particulares del Pedido / Contrato, se aplicarán las siguientes penalizaciones cuando se produzca un incumplimiento objetivo de las obligaciones del Proveedor/Contratista:

- Entrega de Materiales: Penalización hasta el 10 % semanal

- Retraso en la ejecución de obras o prestación de servicios: Penalización hasta el 5% semanal.

6.13. Cesión de derechos y créditos

6.13.1. Los Pedidos / Contratos y los créditos y/o facturas emergentes de estas relaciones jurídicas no podrán ser cedidos/as, total o parcialmente, ni constituirse prendas sobre ellas, sin la previa y expresa autorización de Prosegur, por escrito de acuerdo a la forma que se establezca.

6.13.2. Prosegur podrá ceder, sin consentimiento previo del Proveedor/Contratista, parte o la totalidad de sus derechos y obligaciones bajo el Pedido / Contrato a favor de cualquier sociedad del Grupo Prosegur o como consecuencia de cualquier operación societaria que comporte una sucesión, total o parcial, de los derechos y obligaciones correspondientes.

6.14. Inspecciones/Activaciones

6.14.1. El Proveedor/Contratista deberá realizar por su cuenta y a su costa, las inspecciones necesarias previas a la entrega de los bienes, obras o servicios para asegurar que se cumplen todos los requisitos especificados en el Pedido / Contrato.

Con el objeto de agilizar las gestiones para el cumplimiento del plazo de entrega, el Proveedor deberá contar con un sistema de control para el seguimiento de sus suministradores de materiales, componentes y servicios que afecten al/los bien/es objeto del Pedido.

El Proveedor/Contratista deberá inspeccionar mediante Organismo de Control competente, aquellos bienes sujetos a requisitos legales (reglamento técnico, seguridad, medio ambiente, etc.) y/o según se especifique en las condiciones contractuales del Pedido /Contrato.

6.14.2. Prosegur se reserva el derecho de efectuar inspecciones de los bienes, objeto del Pedido / Contrato y exigir cuantos ensayos sean necesarios, que serán de cuenta del Proveedor, tanto en las instalaciones del Proveedor como en las de sus suministradores.

Para ello PROSEGUR, designará inspectores quienes tendrán libre acceso a los talleres y procesos de fabricación, sin que esta inspección disminuya la responsabilidad del Proveedor.

6.14.3. El Proveedor/Contratista realizará revisiones semestrales de aquellas instalaciones o talleres temporales dentro de las instalaciones de Prosegur o de sus clientes. Del resultado de estas inspecciones y revisiones, el Proveedor/Contratista deberá informar a Prosegur.

6.14.4. Cuando en el Pedido / Contrato se requiera la entrega a Prosegur de documentación (planos, especificaciones, etc.) la misma deberá ser previamente firmada por el Proveedor/Contratista en calidad de aprobación. Prosegur se reserva el derecho de verificar la veracidad de la documentación e información entregada por el Proveedor/Contratista donde ésta se encuentre o donde Prosegur se lo indique o solicite. Para ello Prosegur podrá designar inspectores quienes tendrán libre acceso a la documentación acreditativa sin que esta inspección disminuya la responsabilidad del Proveedor/Contratista.

6.15. Entrega y envío de los bienes

6.15.1. Todo bien suministrado deberá ser adecuadamente embalado para evitar cualquier desperfecto. Prosegur no admitirá ningún cargo por embalaje si no ha sido previamente convenido. No se embalarán conjuntamente bienes correspondientes a diferentes Pedidos / Contratos.

6.15.2. Todos los envíos irán acompañados de un albarán o justificante de entrega en el que se indique la cantidad, descripción del producto, número del Pedido/Contrato, referencia del Proveedor/Contratista, y relación de bultos, realizando la distribución del documento según se especifique en el Pedido /Contrato y /o Condiciones Particulares.

6.15.3. Todos los bultos serán marcados exteriormente con el destino de la mercancía y número de Pedido/Contrato correspondiente, así como indicaciones para la manipulación o precauciones a adoptar en los casos necesarios.

6.15.4. Para los bienes que por su naturaleza sean entregados en envases discretos (por ejemplo, productos de laboratorio), el Proveedor deberá atenerse a las siguientes instrucciones:

a) Cada envase irá identificado con el número de lote, fabricación y fecha
b) No se incluirá en una misma entrega, bienes correspondientes a más de dos lotes, salvo comunicación previa del Proveedor a Prosegur, y aceptación por escrito de ésta.
c) El Proveedor notificará las limitaciones de caducidad del bien, en los casos en que éstas existan, haciendo figurar en los envases la fecha límite del empleo del mismo.
d) Normas de identificación, marcaje, transporte y manipulación establecidas en la ficha de seguridad y aquellas específicas en caso de mercancías peligrosas.

6.15.5. Para los bienes que por su naturaleza sean entregados en cisternas, el Proveedor deberá cumplir y hacer cumplir lo siguiente:

a) Las obligaciones y responsabilidades del expedidor y del cargador, tanto en la contratación, como en las operaciones de carga, siguen lo dispuesto en la legislación aplicable (Ley de Ordenación del Transporte Terrestre, Acuerdo ADR, etc.).
b) El transportista asume la ejecución de las operaciones materiales de carga en las instalaciones de Prosegur.
c) El transportista está obligado al estricto cumplimiento de las normas del centro de carga (en la doble vertiente de operación y de seguridad).
d) El Proveedor será siempre responsable ante Prosegur y ante terceros por los daños y perjuicios que se pudieran causar con ocasión de las operaciones de carga en el interior del centro de carga (acción negligente o inadecuada).
e) Previo a facilitar el acceso al transporte a las instalaciones, el Proveedor deberá justificar a Prosegur en el lugar de entrega que los transportes de MMPP disponen de la siguiente documentación en vigor:

- Seguro(s)
- ITV
- Permiso de conducción y ADR del conductor
- Certificado ADR de tractora y cisterna
- EPI del conductor
- Paneles naranja y etiquetas de peligro.
- Carta de porte ADR
- EPI a utilizar por el conductor según normativa vigente.

6.15.6. La sola recepción por parte de Prosegur de un envío o expedición de bienes del Proveedor no podrá ser considerada como aceptación final de los mismos, los que quedarán sujetos a revisión posterior. Prosegur tiene la facultad de reclamar por defectos y/o vicios de calidad o cantidad, etc. debiendo el Proveedor tomar las medidas necesarias para satisfacer tales reclamaciones.

6.15.7. Para la entrega del suministro será de aplicación el Incoterm (última edición) definido en el Pliego de Condiciones Particulares, así como en el correspondiente Pedido.

6.15.8. Prosegur se reserva el derecho de devolver los bienes, a costa del Proveedor, en el caso de no ajustarse a las especificaciones y cantidades solicitadas.

6.16. Recepción de las obras, bienes y/o servicios

6.16.1. Recepción Provisional: Concluidas las obras y/o servicios, entregada toda la documentación requerida, si la ejecución ha sido correcta, con todos los ensayos y pruebas de instalación realizadas con éxito, Prosegur elaborará un acta de recepción provisional en la que se indique la conformidad o no, del cumplimiento con las condiciones establecidas en el Pedido / Contrato relativas a los trabajos realmente ejecutados, fechas de puesta a disposición, calidad, correcto funcionamiento y cualquier otra observación. A partir de la firma de dicha acta provisional comenzará a contar el plazo de garantía que se haya establecido. Dicha acta provisional será firmada en aceptación por el Contratista.

6.16.2. Si las obras y/o servicios realizados presentan algún defecto, Prosegur dará un plazo al Contratista para su rectificación. De no efectuarse ésta en el plazo indicado, Prosegur podrá realizarla por sí misma o por terceros, con cargo a la cantidad retenida como garantía, o a cargo del Contratista por el importe de las obras y/o servicios no cubiertos por la garantía retenida.

6.16.3. Recepción definitiva: Una vez cumplido el plazo de garantía establecido para las obras y/o servicios y siempre y cuando no existan reclamaciones de Prosegur pendientes de resolver por el Contratista se producirá la recepción definitiva de las obras y/o servicios. Prosegur viene obligado a reintegrar al Contratista el importe, en su caso, de los fondos de garantía y de reparo no afectados a pagos a su cargo.

6.16.4. El Contratista volverá a rehacer, a su costa, aquellos trabajos que resulten defectuosos debido a errores u omisiones del Contratista. Asimismo, será a su costa los gastos de reparación, modificación o reemplazo de materiales necesarios para corregir dichos errores u omisiones.

6.16.5. La entrega de bienes, obras y servicios y la disposición del correspondiente documento de entrega o albarán, no supone que Prosegur haya aceptado la calidad de las obras bienes y/o servicios entregados. Independientemente de los plazos de garantía especificados para cada producto, obra o servicios, Prosegur dispone de quince (15) días naturales para verificar la calidad de las obras s bienes y/o servicios entregados y proceder a su devolución, a cargo del Proveedor/Contratista, en el caso de que no cumplan con las especificaciones de calidad o técnicas requeridas según el Pedido/Contrato.

6.16.6. En el caso de que la entrega de bienes, obras y/o servicios no se hubiera realizado en su totalidad, Prosegur sólo estará obligado a abonar al Proveedor/Contratista el precio de las obras bienes y/o servicios que han sido correctamente entregados y aceptados por Prosegur. Ello sin perjuicio del derecho de Prosegur a exigir el cumplimiento por el Proveedor/Contratista de su obligación de entrega de las restantes obras, bienes y /o servicios o la cancelación del Pedido/Contrato respecto a éstos, y, en todo caso, a ser indemnizado por los daños sufridos.

6.17. Resolución del Pedido/Contrato

6.17.1. El Pedido / Contrato se extinguirá por resolución o por vencimiento del mismo.

6.17.2. Rescisión del Pedido / Contrato por causa del Proveedor/Contratista.

6.17.2.1 Además de las establecidas legalmente, Prosegur, se reserva la facultad de resolver el Pedido / Contrato por las causas que, a título de ejemplo y no de modo limitativo, se relacionan a continuación:

a) La venta o transmisión inter vivos o mortis causa de la empresa del Proveedor/Contratista o su transformación en otra entidad jurídica, por los medios legalmente establecidos, sin la aprobación por escrito de Prosegur.

b) El incumplimiento, por parte del Proveedor/Contratista, de cualquiera de las cláusulas u obligaciones contenidas en las presentes Condiciones Generales, el Pedido/Contrato o cualquiera de los documentos contractuales que sean firmados por las partes.

c) El haberse alcanzado el máximo de penalizaciones aplicables según lo establecido en el Pedido/Contrato.

d) El incumplimiento de la legislación vigente, por parte del Proveedor/Contratista.

e) La existencia de embargos y retenciones de créditos decretados por órganos judiciales o administrativos de carácter ejecutivo (Agencia Estatal, Tributaria, Seguridad Social, etc.) o la disolución de la sociedad del Proveedor/Contratista.

f) El quedar pendiente de ejecución / entrega, más del 20% de las obras, bienes y servicios, cuando haya vencido el plazo establecido en el Pedido / Contrato.

g) En caso de siniestro o accidente que ocasione daños a las personas, bienes o al medio ambiente.

h) Existencia de inexactitudes graves en la información ofrecida por el Proveedor/Contratista, especialmente en lo relativo a la calidad, prevención de riesgos laborales, seguridad e higiene, sistemas de gestión medioambiental, condiciones y cumplimiento de requisitos laborales.

i) Incumplimiento de las normas éticas y de conducta de Prosegur.

j) Incumplimiento de las obligaciones de confidencialidad.

k) Cuando se detecte un caso de conflicto de interés entre el Proveedor/Contratista con algún empleado de Prosegur y tal situación no haya sido comunicada y expresamente autorizada con anterioridad.

l) Cuando el Proveedor/Contratista, sus accionistas o sus directivos, estén involucrados en casos de fraude, corrupción o en la comisión de cualquier otro tipo de delito.

6.17.2.2 Cuando concurra alguna de las causas anteriores, el Pedido / Contrato quedará resuelto y sin efecto desde la fecha en que Prosegur comunique su decisión en tal sentido al Proveedor/Contratista o, en su caso, a sus causahabientes.

6.17.2.3 En los casos en que proceda la resolución del Pedido / Contrato, Prosegur podrá adoptar todas o algunas de las siguientes medidas:

a) Suspender los pagos pendientes

b) Ejecutar las garantías que el Proveedor/Contratista tuviere constituidas.

c) Retener en prenda los bienes y elementos del Proveedor/Contratista que estuvieran en poder de PROSEGUR.

6.17.3. Rescisión del Pedido / Contrato por voluntad de Prosegur

6.17.3.1 Prosegur se reserva el derecho de dejar sin efecto el Pedido / Contrato de forma unilateral en cualquier momento, justificando y comunicando por escrito su decisión y comunicándosela al Proveedor/Contratista con una antelación mínima de 30 (treinta) días a la fecha en la que deba surtir efecto la resolución.

6.17.4. La solicitud de declaración de concurso, quiebra, suspensión de pagos o el inicio de cualquier procedimiento de insolvencia, del Proveedor/Contratista con arreglo a las leyes o normas que en cada caso resulten de aplicación , facultará a Prosegur para, en el plazo de 30 (treinta) días contados desde que tuviera conocimiento de la existencia de dicha solicitud, exigir al Proveedor/Contratista que acredite en un plazo de 10 (diez) días contados desde la recepción por el mismo del requerimiento realizado al efecto por Prosegur los siguientes extremos:

- Que cuenta con los medios materiales y personales necesarios y suficientes para continuar ejecutando los trabajos contratados (personal, medios técnicos, etc.).

- Que cuenta con los medios económicos necesarios para ejecutar hasta su finalización los trabajos contratados, a cuyo fin presentará ante Prosegur un aval bancario solidario, a primer requerimiento y con renuncia expresa a los beneficios de excusión y división, por el importe total de los trabajos contratados pendientes de ejecución incrementado en un 25 % de dicha cantidad, para garantizar el cumplimiento por el Proveedor/Contratista de la totalidad de sus obligaciones contractuales.

Si dentro del citado plazo de 10 (diez) días, el Proveedor/Contratista no acreditara todos los extremos a que hace referencia el presente apartado, Prosegur quedará facultada para resolver el Pedido/ Contrato, con derecho a ser indemnizada por el Proveedor/Contratista por todos los daños y perjuicios que dicha resolución contractual le irrogare.

6.18. Fuerza Mayor

6.18.1. Ninguna de las partes será considerada responsable por el incumplimiento de sus obligaciones derivadas del Pedido / Contrato en tanto en cuanto la ejecución de las mismas se retrase o se hiciese imposible como consecuencia de Fuerza Mayor.

A estos efectos, se considerarán causas de Fuerza Mayor aquellos fenómenos naturales, accidentes inevitables, pandemias, incendio, revuelta o motín popular, actos de guerra, por imposición, norma, orden o acto de cualquier gobierno o agencia gubernamental, así como de cualquier otra autoridad competente, o cualquier otra causa de similar naturaleza imprevisible, o que previsible, fuera inevitable, irresistible o independiente de la voluntad de las partes y que escape a su control.

No obstante, lo establecido en el párrafo anterior, no podrá invocarse como causa de Fuerza Mayor la suspensión de las obligaciones contractuales causada por el personal del Proveedor/Contratista o sus Subcontratistas.

6.18.2. La suspensión de las obligaciones contractuales durará en tanto en cuanto permanezca la causa que haya originado la fuerza mayor. La parte que sufra ésta deberá ponerlo inmediatamente en conocimiento de la otra y efectuar los esfuerzos que sean razonables para resolver la causa de la suspensión en el plazo más corto posible.

Si la causa de fuerza mayor tuviera una duración superior a un mes, Prosegur se reserva el derecho de cancelar el Pedido / Contrato con el abono al Proveedor / Contratista de las cantidades adeudadas por la realización de los trabajos de obra, prestación de servicios o entrega de los bienes que hasta el momento de la resolución se hayan llevado a cabo por parte del Proveedor/Contratista, sin que esta

resolución de derecho al cobro de cantidad adicional alguna o penalización o indemnización a favor del Proveedor/Contratista.

6.19. Propiedad Intelectual e Industrial

2.19.1. Garantías del Proveedor en relación con los servicios, productos, Entregables y Desarrollos Ad Hoc para Prosegur.

2.19.1.1. El Proveedor garantiza sin excepción la plena y pacífica explotación y uso de los servicios, productos, Entregables, y Desarrollos Ad Hoc para Prosegur, puestos a disposición de Prosegur en todo el mundo, así como (i) que los servicios, productos, Entregables y Desarrollos Ad Hoc para Prosegur no infringen ni infringirán la normativa vigente ni ningún Derecho de Propiedad Intelectual e Industrial o similar de terceros y que no tienen reclamación, demanda o litigio alguno; (ii) que está suficientemente autorizado para el suministro de los servicios, productos, Entregables y Desarrollos Ad Hoc para Prosegur, y que no mantiene con ningún tercero acuerdo que le impida, total o parcialmente, la ejecución del contrato al que se obliga; (iii) a obtener y asumir el coste de las licencias, cesiones, y Derechos de Propiedad Intelectual e Industrial con el alcance obligatorio para asegurar la explotación plena y pacífica por parte de Prosegur. En cumplimiento de la anterior garantía, el Proveedor exime a Prosegur de toda responsabilidad por infracciones relacionadas con la explotación y usos de los servicios, productos, Entregables y Desarrollos Ad Hoc para Prosegur provistos por el Proveedor en que pudiera Prosegur incurrir.

Así, el Proveedor deberá obtener el previo consentimiento expreso y por escrito de Prosegur para incorporar a los servicios, productos, Entregables y Desarrollos Ad Hoc para Prosegur, cualquier elemento propiedad de un tercero y/o que pueda estar protegido por Derechos de Propiedad Intelectual e Industrial de terceros.

2.19.1.2. El Proveedor garantiza a Prosegur y viene obligado a acreditar documentalmente ante éste, si le fuere requerido, que dispone de los Derechos de Propiedad Intelectual e Industrial precisos para la realización de cuanto es objeto de este Contrato.

2.19.1.3. El Proveedor se obliga a notificar a Prosegur cualquier información que tenga de reclamación de terceros en relación con los Derechos de Propiedad Intelectual e Industrial sobre los servicios, productos, Entregables y/o los Desarrollos Ad Hoc para Prosegur, o que pueda afectar a los derechos de Prosegur, y se inhibirá de iniciar cualquier acción sin el consentimiento previo y por escrito de Prosegur.

2.19.2. Indemnización.

En el supuesto de que se interpusiese alguna reclamación, judicial o extrajudicial, contra Prosegur, relacionada con la infracción de los Derechos de Propiedad Intelectual e Industrial empleados por el Proveedor o como consecuencia de cualquier acción, reclamación o procedimiento, público o privado, que se inicie por causa de actuaciones, tanto por acción como por omisión, llevadas a cabo o permitidas por el Proveedor o por cualquiera de sus directivos, agentes o empleados, en relación con el cumplimiento de las obligaciones aquí

referidas, el Proveedor exime a Prosegur de toda responsabilidad e indemnizará a Prosegur por los daños y perjuicios sufridos, comprometiéndose a mantenerle indemne, así como a sus consejeros, directivos y empleados de cualquier pérdida, responsabilidades, daños y perjuicios, gastos y costes (incluyendo costes legales) incurrido por Prosegur así como cualquier daño causado a terceros, garantizando a Prosegur poder continuar usando los Derechos de Propiedad Intelectual e Industrial causantes de la reclamación o poniendo a su disposición otros distintos que permitan la continuación de los servicios, productos o el contrato.

2.19.3. Derechos de Propiedad Intelectual e Industrial de Prosegur.

19.3.1 Se entenderá por Derecho/s de Propiedad Intelectual e Industrial cualquier derecho de propiedad intelectual e industrial o de naturaleza similar sobre cualesquiera resultados que sean o puedan ser objeto de protección conforme a la normativa al efecto. El Proveedor se obliga a respetar los Derechos de Propiedad Intelectual e Industrial y cualquier otro de naturaleza análoga titularidad de Prosegur, y reconoce que nada de lo dispuesto en este documento es una transferencia, cesión o licencia sobre tales en favor del Proveedor. El Proveedor reconoce que sólo podrá usar los Derechos de Propiedad Intelectual e Industrial de Prosegur con su instrucción expresa y consentimiento por escrito, y únicamente en el marco de la ejecución del contrato, obligándose a respetar las instrucciones de Prosegur.

2.19.3.2 En concreto, el Proveedor no podrá usar la denominación, nombre comercial, logotipo o marcas de Prosegur, ni podrá usarlos o utilizar la aceptación de cualquier oferta, ni la suscripción o ejecución del presente Contrato, ni la prestación de los servicios referidos en los mismos, como referencia para la adquisición de nuevos clientes o captación de negocio ni para mantener un cierto nivel profesional.

2.19.4. Titularidad de los Derechos sobre potenciales Desarrollos Ad Hoc del Proveedor para Prosegur.

2.19.4.1. En el hipotético caso de que fruto de la relación entre las partes, el Proveedor deba realizar un Desarrollo Ad Hoc para Prosegur, Prosegur será titular exclusivo, sin límite geográfico ni temporal, de todos los Derechos de Propiedad Intelectual e Industrial sobre dichos Desarrollos Ad Hoc que el Proveedor, o cualquier persona a la que el Proveedor haya contratado al efecto, haya desarrollado para Prosegur como fruto de la relación aquí regulada.

En el caso de que la titularidad de los Derechos de Propiedad Intelectual e Industrial sobre los Desarrollos Ad Hoc para Prosegur, no pudiera atribuirse de forma originaria a Prosegur de conformidad con la legalidad vigente, entonces, por virtud del presente documento, el Proveedor cede a Prosegur la titularidad sobre todos los Derechos de Propiedad Intelectual e Industrial, con carácter exclusivo, y con la máxima amplitud permitida en Derecho, es decir, por toda la duración de los Derechos de Propiedad Intelectual e Industrial cedidos, para todo el mundo y para cualquier modalidades de explotación, aunque no fuera el sector de actividad habitual de Prosegur. En consecuencia, Prosegur podrá ejercitar libremente y en la forma que considere los Derechos de Propiedad Intelectual e Industrial de los Desarrollos Ad Hoc, incluyendo su explotación, transmisión, cesión, licencia a terceros, y todo ello en los términos y condiciones que considere.

2.19.4.2. El Proveedor se compromete a colaborar con Prosegur para dar efecto a sus obligaciones, y en concreto (i) a colaborar en la obtención de los registros e inscripciones relativas a los Derechos de Propiedad Intelectual e Industrial de Prosegur (ii) a informar inmediatamente a Prosegur de cualquier resultado obtenido en el marco de la relación contractual con Prosegur, facilitando toda la documentación y otros soportes necesarios para garantizar la titularidad de Prosegur sobre los Desarrollos Ad Hoc para Prosegur.

2.19.4.3. El Proveedor reconoce que la retribución pactada en favor del Proveedor satisface asimismo las obligaciones y compromisos asumidos por su parte en esta cláusula, renunciando a reclamar por los mismos.

2.19.5 Software.

2.19.5.1. En el hipotético caso de que el Proveedor licencie Software Estándar (aquél desarrollado de manera genérica para un mismo uso por multitud de personas) a Prosegur para la ejecución de este acuerdo, dicha licencia será exclusiva, irrevocable, sublicenciable de uso (incluido en favor del Grupo Prosegur), de ámbito mundial y por el plazo máximo de vigencia de tales derechos.

2.19.5.2. El Proveedor garantiza que no utilizará software de código abierto (bajo una licencia de código abierto) para la ejecución de este acuerdo sin el consentimiento previo y por escrito de Prosegur. Para ello informará a Prosegur de los términos y condiciones de la licencia aplicable, confirmará que el programa de ordenador en su conjunto no pueda ser considerado como software de código abierto, y que su uso no restringe el uso de los servicios, productos, Entregables y Desarrollos Ad Hoc para Prosegur. En caso de uso autorizado, el Proveedor se compromete y garantiza el cumplimiento de los términos y condiciones de la licencia aplicable.

2.20. Confidencialidad de la información y documentos

2.20.1. Se considerará información confidencial la información protegida frente al acceso de personas no autorizadas y en concreto:

a) Toda la información (escrita o verbal) y materiales, de cualquier tipo o naturaleza mostrada o facilitada (ya sea con anterioridad o posterioridad a la fecha del Pedido / Contrato por Prosegur o sus administradores, empleados, representantes, filiales o por sus asesores, abogados, auditores o Proveedores externos, o tratada en el marco de las actividades objeto del Pedido / Contrato y toda la información a la que el Proveedor/Contratista acceda o conozca durante la ejecución de los servicios objeto del Pedido / Contrato y, en todo caso, cualquier dato relativo o asociado a persona física determinada o determinable, ya se trate de información o materiales relativos a Prosegur o a terceros (ya se trate, sin que ello tenga carácter limitativo, de información o datos relativos a clientes, proveedores, empleados o cualquier otro tercero que mantenga relación de cualquier tipo con Prosegur o cualquiera de las sociedades o entidades del Grupo Prosegur);

b) El contenido del servicio, la existencia de previas conversaciones y negociaciones entre Prosegur y el Proveedor/Contratista, la existencia de cualquier oferta de bienes, obras y/o servicios, de cualquier documento de aceptación de cualquier oferta de bienes, obras y /o servicios, o de cualquier otro acuerdo, contrato o documento relativo o encaminado a la prestación de bienes, obras y

/o servicios por parte del Proveedor/Contratista a Prosegur , así como el contenido de tales conversaciones, negociaciones, oferta de bienes, obras y/o servicios, carta, contrato, acuerdos, contratos o documentos.

c) a título enunciativo no limitativo comprende el modo de operar del Grupo Prosegur, secretos comerciales, secretos empresariales, ideas, planes de negocio, planes de expansión, marketing o información de ventas, nuevas oportunidades de negocio, proyectos de desarrollo, derechos de propiedad intelectual e industrial, cualquier información científica o técnica, invención, diseño, proceso, procedimiento, fórmula, mejora, tecnología o método; cualesquiera conceptos, muestras, informes, datos, know-how, trabajos en curso, diseños, dibujos, fotografías, herramientas de desarrollo, especificaciones, programas de ordenador, código fuente, código objeto, organigramas y bases de datos, independientemente de que la información conste por escrito, o en otro formato documental, oral, visual, electrónico o formato legible por máquina, muestras, modelos o de otro tipo. Las Partes acuerdan por la presente que no se requiere que la Información Confidencial sea novedosa, tenga carácter único, sea patentable, pueda protegerse mediante derechos de autor o sea un secreto comercial a fin de que la misma pueda catalogarse de Información Confidencial y, por lo tanto, pueda ser protegida.

En lo sucesivo, cualquiera de las informaciones referidas en los apartados a), b) y c) se referirá como la “Información Confidencial”.

2.20.2. Obligación de confidencialidad:

a) La Información Confidencial será tratada confidencialmente por el Proveedor/Contratista y no será revelada, de forma total ni parcial, ni directa ni indirectamente (a través de sus empleados, colaboradores tanto externos como internos, subcontratistas, auditores u otras entidades vinculadas) a terceros, bajo ningún concepto, salvo previo consentimiento escrito de Prosegur. En particular, el Proveedor/Contratista se compromete a adoptar las medidas necesarias para evitar que terceros no autorizados puedan acceder a la Información Confidencial y a limitar el acceso a la misma a los empleados autorizados que precisen disponer de ella para la realización de los bienes, obras y/o servicios, trasladándoles idéntica obligación de confidencialidad.

b) El Proveedor/Contratista, garantiza que la Información Confidencial no será utilizada ni explotada, en su propio beneficio o en beneficio de tercero, para usos o finalidades distintas de la prestación de los bienes, obras y/o servicios.

c) El Proveedor/Contratista, se compromete a no realizar copias, ni difundir, ni comunicar, ni prestar ni, de otra forma, reproducir, revelar o divulgar la Información Confidencial a ningún tercero, así como a no publicarla ni de cualquier otro modo, bien directamente, bien a través de terceras personas o empresas, ponerla a disposición de terceros, sin el previo consentimiento por escrito de Prosegur.

d) El Proveedor/Contratista se compromete a que toda la Información Confidencial a la que tenga acceso permanecerá en las instalaciones de Prosegur, sin que pueda ser trasladada a un lugar diferente, salvo previo consentimiento escrito de Prosegur.

e) Las obligaciones establecidas para el Proveedor/Contratista en el Pedido / Contrato serán también de obligado cumplimiento para sus empleados, colaboradores, tanto externos como internos, subcontratistas, abogados y auditores por lo que el Proveedor/Contratista responderá frente al Prosegur si tales obligaciones son incumplidas por tales empleados, colaboradores, subcontratistas, abogados y auditores. El Proveedor/Contratista se compromete a obtener de sus colaboradores externos o subcontratistas autorizados por Prosegur un compromiso por escrito en idénticos términos

a los estipulados en la presente cláusula con respecto a la Información Confidencial que estuviera en poder de los mismos.

2.20.3. Excepciones a la obligación de confidencialidad. Auditorías:

a) La obligación de confidencialidad no será aplicable y, por tanto, no se considerará Información Confidencial la información que sea o resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por el Proveedor/Contratista; que haya sido publicada con anterioridad a la fecha del Pedido / Contrato; que obre ya en legítimo poder del Proveedor/Contratista y no esté sujeta a un acuerdo de confidencialidad entre las partes, siempre que este hecho sea puesto de manifiesto a la otra parte con anterioridad al momento de la revelación; que sea recibida a través de terceros sin restricciones y sin que implique incumplimiento de obligación legal o contractual alguna del tercero; o que sea independientemente desarrollada por el Proveedor/Contratista para fines distintos a los bienes, obras y/o servicios a prestar a Prosegur y que haya sido desarrollada sin uso o asistencia de Información Confidencial.

b) No estará sujeta a la obligación de confidencialidad aquí prevista la revelación de Información Confidencial que responda al cumplimiento de una orden de naturaleza judicial o administrativa, y siempre que el Proveedor/Contratista que hubiera recibido la orden correspondiente informe previamente por escrito a Prosegur acerca de la obligación de proceder a dicha revelación.

c) Prosegur queda autorizado a fiscalizar el desarrollo de los bienes, obras y/o servicios encargados en orden a su adecuación a las instrucciones emitidas y normativa existente aplicable, pudiendo solicitar al Proveedor/Contratista para ello cuanta información estime pertinente, acceder a la ubicación física en el que se desarrollen los servicios y realizar, directamente o a través de terceros, cuantas auditorias y comprobaciones estime de interés.

2.20.4. Devolución de la Información Confidencial: A la finalización de la obra o la entrega de bienes y/o de la prestación del servicio objeto del Pedido / Contrato, o antes de esa fecha si así fuese solicitado por Prosegur y no fuere necesario para el Proveedor/Contratista disponer de ellos para prestar los servicios a Prosegur, el Proveedor/Contratista, deberá restituir al Prosegur cualquier Información Confidencial que se halle en posesión del Proveedor/Contratista.

2.20.5. Propiedad de la Información Confidencial: No se reconoce en favor del Proveedor/Contratista ningún derecho o título de propiedad o cualquier otro derecho sobre la Información Confidencial, excepto por los derechos de uso estipulados en el Pedido / Contrato y con las limitaciones indicadas en el mismo.

2.20.6. Duración: La duración de las obligaciones de confidencialidad presente será indefinida, manteniéndose en vigor con posterioridad a la finalización por cualquier causa, de la relación entre Prosegur y el Proveedor/Contratista.

2.20.7. Incumplimiento: El Proveedor/Contratista, se responsabiliza y deberá indemnizar a Prosegur por todos los daños y perjuicios ocasionados como consecuencia del incumplimiento de cualquiera de las obligaciones de confidencialidad establecidas.

2.20.8 En todo caso, la prestación de los servicios objeto de toda oferta de servicios por el Proveedor, o a través de subcontratistas autorizados por el Cliente, no obstaculizará las facultades de inspección del Banco de España y/u otros organismos regulativos de la actividad del Cliente. El Proveedor se compromete a permitir el acceso directo y sin restricciones del Banco de España y otros organismos regulativos a la información del Cliente en poder del Proveedor o de sus subcontratistas autorizados por el Cliente, a los efectos de que el Banco de España u otros organismos regulativos puedan realizar

en los locales del Proveedor o de sus subcontratistas las comprobaciones pertinentes en relación con dicha información, incluyendo la verificación de la idoneidad de los sistemas y aplicaciones utilizados. El Proveedor se compromete a obtener de sus subcontratistas autorizados por el Cliente un compromiso por escrito en idénticos términos a los estipulados en la presente estipulación con respecto a la información en poder de los mismos, el acceso a sus locales y la verificación de la idoneidad de los sistemas y aplicaciones utilizados.

6.21. Protección de datos personales

6.21.1. Para el supuesto de que el Proveedor tenga que acceder a datos de carácter personal que resulten de titularidad de Prosegur será necesario suscribir el contrato de Encargado de Tratamiento previsto en el Anexo III.

6.21.2. En todo caso, el Proveedor que tenga que tener acceso a datos de carácter personal titularidad de Prosegur (en adelante, los "Datos") estará sujeto al cumplimiento del régimen legal previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE -Reglamento general de protección de datos- (en adelante, "RGPD"), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)..

Con carácter general, en cumplimiento de lo dispuesto en la normativa de protección de datos que resulta de aplicación, el Proveedor que tenga acceso a datos de carácter personal expresamente manifiesta y se obliga a:

a. Utilizar y tratar los Datos con el único y exclusivo objeto de cumplir con el presente Contrato y siguiendo en todo caso las instrucciones recibidas de Prosegur. El Proveedor expresamente se abstendrá de dar a los Datos cualquier uso distinto al acordado y, en especial, se abstendrá de alterarlos, utilizarlos para su propio interés empresarial o comunicarlos o permitir el acceso de terceros a los mismos, ni siquiera para su conservación.

b. Observar la máxima confidencialidad y reserva respecto de los datos de carácter personal que le sean facilitados por Prosegur con respecto al desarrollo del objeto del presente Contrato, comprometiéndose a no desvelar a tercera persona alguna estos datos, así como cualquier otra información que se le hubiera facilitado respecto a Prosegur.

c. Devolver a Prosegur, una vez concluida la prestación de servicios objeto del presente Contrato, todos los documentos y archivos en los que se hallen reflejados todos o alguno de los Datos, cualquiera que sea su soporte o formato, así como las copias de los mismos.

d. Restringir el acceso y el uso de los Datos a aquellos de sus empleados, agentes y colaboradores que sea absolutamente imprescindible que tengan acceso y conocimiento de los mismos para el desarrollo del objeto del presente Contrato, obligándose a imponer a los mismos las obligaciones de confidencialidad y de prohibición de uso respecto de los Datos, en los mismos términos que se prevén en el presente Contrato, comprometiéndose a responder de cualquier incumplimiento de las referidas obligaciones por parte de cualesquiera de sus empleados, agentes y colaboradores anteriormente citados.

e. Adoptar, implantar y exigir las medidas de seguridad de índole técnica y organizativas necesarias, que garanticen una seguridad adecuada de los datos personales, incluida la

protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»), así como ir actualizando las medidas de seguridad conforme a las exigencias legalmente sobrevenidas durante la duración del presente Contrato y cualesquiera otras que sean objeto de notificación fehaciente por parte de Prosegur.

Concretamente, de conformidad con el artículo 32 del RGPD el Proveedor implementará las medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo, atendiendo al nivel de sensibilidad de los datos y actividades de tratamiento realizadas, entre las que se destacan, con carácter enunciativo que no limitativo, las siguientes:

- la seudonimización y el cifrado de datos personales, en su caso;
- 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;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

f. El Proveedor no podrá subcontratar ninguna de las prestaciones que formen parte del objeto de este Contrato que comporten el tratamiento de datos personales, salvo previa autorización expresa y otorgada por escrito por parte de Prosegur.

   Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito a Prosegur, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

   En caso de autorización, el subcontratista, que también tendrá la condición de encargado del tratamiento, estará obligado igualmente a cumplir las obligaciones establecidas en este Contrato para el Proveedor y las instrucciones que dicte Prosegur. 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…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

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

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

h. En caso de que se produzcan violaciones de la seguridad de los Datos Personales, el Proveedor deberá notificar las mismas sin dilación indebida, y en cualquier caso antes del plazo máximo de veinticuatro (24) horas y a través de cualquier dirección de contacto, física o electrónica,

proporcionada por Prosegur durante el desarrollo de la relación contractual entre las partes, junto con toda la información relevante para la documentación y comunicación de la incidencia.

6.21.3. Mantener indemne a Prosegur frente a cualquier reclamación que pueda ser interpuesta contra Prosegur ante la Autoridad de Control correspondiente, que tenga por causa el incumplimiento del Proveedor y/o de sus subcontratistas de lo dispuesto en el presente acuerdo y en la legislación vigente en materia de protección de datos personales, y acepta pagar el importe al que, en concepto de sanción, multa, indemnización, daños, perjuicios e intereses pueda ser condenado Prosegur, incluyendo honorarios de abogados, con motivo del citado incumplimiento.

6.22. Seguridad en tecnologías de la Información

El Proveedor se obliga a tener un sistema operativo en soporte, con las últimas actualizaciones de seguridad, al menos las de los últimos tres meses. Asimismo, garantiza que tiene instalados antivirus actualizados al día de la fecha con actualización automática habilitada.

El Proveedor no se conectará desde una máquina no propiedad de Prosegur para realizar tareas de administración sobre servidores de Prosegur.

En caso de incumplimiento de estas obligaciones, Prosegur queda excluida, con toda la extensión que permite el ordenamiento jurídico aplicable, de toda responsabilidad por los daños y perjuicios de cualquier naturaleza, directos e indirectos, entre otros, lucro cesante o pérdida de clientela, beneficios o de explotación, que puedan deberse de una vulneración de la seguridad de los equipos/sistemas informáticos o redes de comunicación del Proveedor, incluyendo situaciones de fuga de información o adulteración de la información, intervención o intromisión ilegal de los sistemas, de comunicación y/o software por malware (virus, troyanos, gusanos) y demás rutinas de programación perjudiciales de terceros, sin que la presente enumeración sea limitativa de otras formas que puedan alterar y/o afectar los sistemas informáticos o de comunicación de Prosegur.

El Proveedor responderá sin límite alguno por los daños y perjuicios de cualquier naturaleza, directos e indirectos, entre otros, lucro cesante o pérdida de clientela, beneficios o de explotación, por cualquier interrupción, disrupción o caída del servicio prestado a Prosegur, causada por actos u omisiones de terceros derivados del incumplimiento de dichas obligaciones.

En caso de que el Proveedor identifique una vulneración de la seguridad de sus sistemas, deberá informarlo al responsable del proyecto de Prosegur, por cualquier medio que deje constancia y dentro del plazo de 24 horas desde que tenga conocimiento de la misma. El cumplimiento de esta obligación no exime al Proveedor de responsabilidad por el incumplimiento de las obligaciones anteriores.

El Proveedor debe cumplir lo previsto en el Anexo V Uso de Recursos Informáticos y Sistemas, así como firmar el anexo "*DECLARACIÓN DEL USUARIO SOBRE EL USO DE LOS RECURSOS INFORMÁTICOS Y SISTEMAS",* que forma parte de esta.

Todo Proveedor que requiera acceso a las tecnologías de la Información de Grupo Prosegur, preste servicios/productos tecnológicos y/o digitales, así como servicios no tecnológicos que tienen la capacidad de acceso a las tecnologías de la información y/o información del Grupo, debe cumplir lo previsto en el Anexo IV. En caso de que el proveedor preste servicios que no requieran de acceso a las tecnologías de la Información de Grupo Prosegur, le aplicarán aquellos epígrafes del anexo que permitan evaluar el riesgo del proveedor en relación a Prosegur.

2.22.1 Auditoría

Seguridad de la Información se reserva el derecho de realizar auditorías técnicas y revisar el estado de cumplimiento del proveedor para con el Esquema de Control establecido por este.

Respecto a las auditorías técnicas, los costes y gastos asociados a la intervención de Prosegur correrán por su cuenta. En caso de detectar vulnerabilidades, el Proveedor se hará cargo de remediarlas, acorde a los procedimientos de gestión de vulnerabilidades técnicas del Grupo Prosegur y según los siguientes tiempos de resolución:

- Crítica: 10 días.
- Alta: 20 días.
- Medias: 90 días.
- Bajas: 180 días.

En caso de no cumplir los plazos, se aplicará una penalización del 5% sobre la facturación total anual, que se compensará en las futuras facturas asociadas al servicio.

6.23. Solución de divergencias y litigios

6.23.1. La legislación aplicable al Pedido / Contrato será la del lugar de su cumplimiento. Se entenderá por lugar de cumplimiento aquél en el que, según el Pedido / Contrato, deban ser entregados los bienes o ejecutada la obra y/o prestados los servicios.

6.23.2. En ausencia de pacto, los bienes se entenderán entregados y las obras y/o servicios ejecutados en el lugar donde tenga su domicilio social a efectos legales la correspondiente sociedad del Grupo Prosegur que firme el correspondiente Pedido/Contrato.

6.23.3. Para cualquier divergencia que pudiera surgir respecto de la interpretación, ejecución o cumplimiento del Pedido / Contrato, las partes se someterán expresamente a la competencia de los Tribunales ordinarios de la ciudad donde se encuentre el domicilio social de la empresa de Grupo Prosegur que firme o el correspondiente Pedido / Contrato.

6.24. Archivos

6.24.1. El Proveedor/Contratista mantendrá al día un registro completo del bien suministrado y/u obras y/o servicios realizados bajo el Pedido / Contrato, así como todas las transacciones relacionadas con el mismo. El Proveedor/Contratista mantendrá la totalidad de dichos registros por un período de tres años como mínimo después de la finalización del Pedido / Contrato. Dichos registros estarán disponibles para su posible auditoria por parte de Prosegur. La auditoría, si fuera el caso, no se aplicará a las Patentes del Proveedor/Contratista ni a cualquier información adicional con relación a ellas.

6.24.2. Prosegur, con el objetivo de aumentar la exigencia sobre sus proveedores en materia sostenible, se reserva el derecho de revisión de las políticas medioambientales, laborales y de gobierno corporativo de sus principales proveedores.

7. ANEXOS

7.1. Documentos Asociados:

Código	Nombre
DS-GLO-EF-COM-02	Anexo I: Listado de límites exigibles en los seguros según productos o servicios
MD-GLO-EF-COM-02	Anexo II: Modelo de aval bancario fiel cumplimiento y garantía de bienes, obras y/o servicios
MD-GLO-LEG-07	Anexo III: Contrato de Encargado de Tratamiento
	Anexo IV: Requerimientos de Riesgo Tecnológico, Ciberseguridad y Continuidad de Negocio
	Anexo V: Uso de Recursos Informáticos y Sistemas de Prosegur

7.2. ANEXO I: LISTADO DE LÍMITES DS-GLO-EF-COM-02

IMPORTES EXIGIBLES EN LOS SEGUROS SEGÚN PRODUCTOS O SERVICIOS (POR SINIESTRO)

ACTIVIDAD	PYME	MULTINACIONAL
TODOS		
Seguros de Accidentes:	Mínimo legal	Mínimo legal
Seguro de Responsabilidad Civil explotación actividad trabajos prestados	3.000.000 €	6.000.000 €
Responsabilidad Civil producto, retirada de producto, post-trabajos, unión y mezcla, contaminación y polución	3.000.000 €	6.000.000 €
Seguros Responsabilidad Civil Patronal	300.000 €	600.000 €
Responsabilidad Civil de automóviles, maquinaria autoporpulsada, aeronaves, embarcaciones:	Mínimo legal	Mínimo legal
Seguros adaptados al lugar de prestación		
CONSTRUCCION		
Seguro de Construcción/Edificación y Montaje:	Presupuesto obra	Presupuesto obra
Responsabilidad Civil producto, retirada de producto, post-trabajos, unión y mezcla, contaminación y polución	3.000.000 €	6.000.000 €
Responsabilidad Civil Maquinaria Industrial:	3.000.000 €	6.000.000 €
Daños propios equipos de construcción; alquilados o propiedad del Contratista:	Valor de reposición	Valor de reposición
Seguro decenal:	Mínimo legal	Mínimo legal
SERVICIOS PROFESIONALES		
Responsabilidad Civil Profesional actividad profesional prestada	3.000.000 €	6.000.000 €
Ciber riesgos y protección de datos	3.000.000 €	6.000.000 €
SERVICIOS PROFESIONALES TECNOLOGICOS		
Responsabilidad Civil Profesional Tech PI	3.000.000 €	6.000.000 €
Ciber riesgos y protección de datos	3.000.000 €	6.000.000 €
TECNOLOGIA		
Responsabilidad Civil Profesional Tech PI	3.000.000 €	6.000.000 €
Responsabilidad Civil producto, retirada de producto, post-trabajos, unión y mezcla, contaminación y polución	3.000.000 €	6.000.000 €
Ciber riesgos y protección de datos	3.000.000 €	6.000.000 €
TRANSPORTE DE LAS MERCANCIAS COMPRADAS		
Cobertura del transporte puerta a puerta	Valor transportado	Valor transportado
Transporte carga y descarga		
ALMACENAMIENTO DE STOCKS EN ALMACENES PROVEEDOR		
Cobertura todo riesgo almacén	Valor transportado	Valor transportado
GARANTIA DE PRODUCTO Y SERVICIO		
Garantía del producto	Mínimo legal	Mínimo legal
Retirada de producto		
Garantía rotura de stock		
Responsabilidad frente a clientes		
Lucro cesante / perdida de actividad		

7.3. ANEXO II. MODELO DE AVAL MD-GLO-EF-COM-02

La entidad [•] (en adelante, el "BANCO"), provista de C.I.F. [•] con domicilio en [•], y en su nombre y representación Don [•] y Don [•] con poderes suficientes para obligarle en este acto según resulta de la escritura de apoderamiento otorgada por el Notario de [•], Don [•], en fecha [•] de [•] de [•], con el número [•] de protocolo

AVALA

De forma incondicional, irrevocable y solidaria, con renuncia expresa a los beneficios de división, excusión y orden, hasta los límites que se indican y en las condiciones más abajo expresadas a [ ] (en adelante el [PROVEEDOR]), con domicilio social en [ ] y con NIF [ ], para garantizar el pago por parte de la PROVEEDOR a PROSEGUR COMPAÑÍA DE SEGURIDAD, S.A. (en adelante, "PROSEGUR") de cuantas obligaciones han sido asumidas por el PROVEEDOR en el contrato de [ ] de fecha [ ] (en adelante, el "CONTRATO") en virtud del cual el PROVEEDOR [ ] a PROSEGUR (en adelante los [BIENES] [OBRAS] [SERVICIOS]) y especialmente para responder del pago de cualesquiera pérdidas, reclamaciones por daños y perjuicios, reclamaciones, causas de acción, responsabilidades, sanciones, penalizaciones, costas y, o gastos cuantificados y determinados de cualquier naturaleza en los que incurra el PROVEEDOR frente a PROSEGUR o las que le sean imputadas a esta última, por responsabilidad del PROVEEDOR ahora o en el futuro, como consecuencia de cualquier declaración engañosa o inexacta, incumplimiento, contingencia y, o, reclamación de terceros derivada de la ejecución del CONTRATO.

PRIMERO. - EJECUCIÓN. Este aval bancario se hará efectivo, en una o varias ocasiones, a primer requerimiento de pago por PROSEGUR, en una o varias veces, hasta el límite máximo de […] ([…]) EUROS, contra el requerimiento realizado por PROSEGUR, al que se adjunte copia del requerimiento de pago que la PROSEGUR haya remitido al PROVEEDOR y manifestación de haber transcurrido diez (10) días hábiles desde el envío de dicha notificación del requerimiento de pago, sin que el PROVEEDOR haya satisfecho su importe.

El BANCO se compromete a efectuar el pago de la cantidad requerida hasta los importes máximos (individuales y conjuntos) anteriormente previstos, en el plazo improrrogable de tres (3) días desde la recepción de tal comunicación, y en la cuenta que a tales efectos le indique PROSEGUR.

SEGUNDO. - RENUNCIA A EXCEPCIONES. El presente Aval es irrevocable y se otorga con carácter abstracto y a primera demanda, el BANCO no podrá oponer o alegar contra PROSEGUR ningún tipo de excepción y, en particular, las excepciones personales que el PROVEEDOR pudiese acreditar contra PROSEGUR. De este modo, una vez presentando el requerimiento descrito en el apartado anterior, el BANCO en modo alguno podrá cuestionar a PROSEGUR la validez de la reclamación al BANCO.

TERCERO. - PLAZO DE VALIDEZ. Este aval entrará en vigor a la fecha de hoy y tendrá validez durante […] ([…]) años a contar desde el día de hoy. Llegada dicha fecha, si el BANCO no ha recibido comunicación fehaciente alguna de pago de cantidad realizada por el PROVEEDOR, caducará y quedará extinguido automáticamente.

CUARTO. - CESIÓN. PROSEGUR podrá ceder el presente aval a cualquier tercero. Para que dicha cesión sea válida frente al BANCO, bastará con que la misma sea comunicada al BANCO por PROSEGUR. En este caso todas las referencias a PROSEGUR contenidas en el presente aval se entenderán realizadas con relación al cesionario del presente aval.

QUINTO.-. - GASTOS. Cualesquiera costes y gastos relativos al presente aval bancario serán pagados y soportados exclusivamente por el PROVEEDOR.

El presente aval ha sido inscrito en esta misma fecha en el Registro Especial de Avales con el número [•].

[*INTERVENIDO POR NOTARIO PÚBLICO*]

7.4. ANEXO III. CONTRATO DE ENCARGO DE TRATAMIENTO

REUNIDOS

De una parte, PROSEGUR (en adelante, el "Responsable del tratamiento"), y de otra parte, el Proveedor (en adelante el "Encargado del tratamiento"), que serán referidas conjuntamente como las "**Partes**" e, individualmente, cada una de ellas como la "**Parte**"

EXPONEN

I. Que, como consecuencia de la prestación de los servicios detallados en el Contrato de compra o suministro, el Encargado del Tratamiento puede acceder a datos de carácter personal que se encuentran bajo la responsabilidad, custodia y protección de **PROSEGUR**; teniendo a estos efectos el Proveedor la condición legal de Encargado del tratamiento con respecto a los mismos.

II. Que, en consecuencia y dando pleno cumplimiento a lo establecido en la normativa nacional y comunitaria que resulta de aplicación, las Partes desean recoger en el presente Acuerdo las condiciones del tratamiento de los datos por parte del Proveedor, de conformidad con lo previsto en la legislación española.

III. Que, sin perjuicio de lo anterior, las Partes desean cumplir asimismo con las exigencias que, en relación con la regulación de la relación de Encargado del tratamiento, establece el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y, a tal efecto, suscriben las siguientes

CLÁUSULAS

Primera - Tratamiento de datos personales

La prestación de servicios podría implicar el acceso por parte del Encargado del tratamiento a información confidencial y datos de carácter personal responsabilidad de PROSEGUR. En este sentido, el Proveedor tendrá la consideración de Encargado del tratamiento, y su tratamiento de los datos de carácter personal responsabilidad de PROSEGUR consistirá única y exclusivamente en acceder y, en su caso, almacenar los datos personales estrictamente necesarios para prestar los servicios referidos en el Contrato de compra o suministro.

Segunda - Confidencialidad y deber de secreto

Salvo que las Partes acuerden lo contrario, las mismas y el resto de las sociedades pertenecientes a su grupo o que tengan vinculación con la misma, mantendrán absoluto secreto en relación con este acuerdo, su negocio y la información y la documentación referente a la otra Parte que haya llegado a su conocimiento como consecuencia del cumplimiento del acuerdo. Asimismo, el Encargado del tratamiento se compromete de forma específica a tratar como confidencial toda aquella información responsabilidad del Responsable o terceros a la que pueda tener acceso, con motivo de la prestación de sus servicios y se compromete a que dichos datos permanezcan secretos.

A estos efectos, el Encargado del tratamiento se compromete a tomar, respecto de sus empleados o colaboradores, las medidas necesarias para que resulten informados de la necesidad del cumplimiento de las obligaciones que le incumben como Encargado del tratamiento y que, en

consecuencia, deben respetar, así como a garantizar que los datos personales que conozca en virtud del presente acuerdo permanecen secretos incluso después de finalizado el presente acuerdo por cualquier causa. Para ello, el Encargado del tratamiento realizará todas las advertencias (mediante formación, mensajes de concienciación, etc.) y suscribirá los documentos que sean necesarios con sus empleados o colaboradores, con el fin de asegurar el cumplimiento de tales obligaciones. Éstos deberán estar informados de forma comprensible de la existencia del presente acuerdo, de las normas de seguridad que afectan al desarrollo de sus funciones, las consecuencias en caso de incumplimiento y el carácter confidencial de la información y del deber de secreto de los datos personales, subsistiendo la obligación de confidencialidad y secreto aún finalizada la relación con el Encargado del tratamiento.

Dicha obligación de información a los empleados y colaboradores del Encargado deberá llevarse a cabo de modo tal que permita la documentación y puesta a disposición de PROSEGUR del cumplimiento de aquella obligación.

Adicionalmente, la información y documentación confidencial no podrá ser utilizada para fin distinto al cumplimiento del objeto del acuerdo, salvo que dicha información sea de general conocimiento y excepto por lo que se refiere a la información requerida en virtud de Ley o cualquier otra regulación aplicable y obligatoria.

Una vez finalizado el presente acuerdo, la obligación de confidencialidad y deber de secreto prevista en esta cláusula se mantendrá de forma indefinida incluso hasta después de cesar en su relación con el Responsable del tratamiento, cualquiera que fuera la causa.

En caso de detectarse cualquier tipo de actuación indebida por cualquier persona que desempeñe funciones profesionales para el Encargado del tratamiento (acceso a información que no corresponde a sus funciones, uso indebido de usuarios y contraseñas, un usuario con más autorizaciones de las necesarias o cualquier otra), será responsabilidad y obligación expresa del Encargado del tratamiento la comunicación inmediata a PROSEGUR junto con informe detallado de los hechos.

Tercera- Instrucciones del Responsable del tratamiento

El Encargado del tratamiento se compromete a tratar los datos personales a los que tenga acceso únicamente conforme a las instrucciones por escrito que, a tal efecto, le indique el Responsable del tratamiento; siempre siguiendo, cuando menos, con la misma política de protección de datos personales y con la política de medidas de seguridad para su resguardo que aquellas empleadas para tal efecto por PROSEGUR. Este compromiso se extenderá asimismo con respecto a las transferencias internacionales de datos de carácter personal a un tercer país o una organización internacional.

En consecuencia, los datos que se conozcan u obtengan en virtud de este acuerdo:

- no podrán ser utilizados para ninguna otra finalidad distinta de la ejecución del mismo, tendrán carácter confidencial y no serán publicados o puestos en conocimiento de terceras partes sin la autorización previa y por escrito del Responsable del tratamiento. En ningún caso tratará los datos para fines propios.
- no serán comunicados a terceros sin la previa autorización por escrito de PROSEGUR. En este sentido, el Encargado del tratamiento, por escrito y de manera previa a que PROSEGUR autorice la comunicación, identificará la entidad o entidades a que vaya a comunicar los datos, qué datos

o categoría de datos personales van a ser objeto de la comunicación y las medidas de seguridad a aplicar para proceder a la misma.

En este sentido, el Encargado del tratamiento se compromete a informar inmediatamente al Responsable del tratamiento en el caso en que una instrucción dirigida por este pudiera infringir las disposiciones que resultasen aplicables en materia de protección de datos recogidas en el ordenamiento comunitario o de los Estados miembros.

En el caso de que el Encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del presente acuerdo, será considerado también Responsable del tratamiento, respondiendo personalmente de las infracciones en que hubiera incurrido, así como de los daños y perjuicios que puede causar en este caso a PROSEGUR.

Cuarta - Subcontratación de los servicios

El Encargado del Tratamiento no podrá subcontratar ninguna de las prestaciones que formen parte del objeto del Contrato que comporten el tratamiento de datos personales, salvo previa autorización expresa y otorgada por escrito por parte de Prosegur.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito a Prosegur, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

En caso de autorización, el subcontratista, que también tendrá la condición de encargado del tratamiento, estará obligado igualmente a cumplir las obligaciones establecidas en el presente Contrato de Encargo de Tratamiento y las instrucciones que dicte Prosegur. Corresponde al Encargado del Tratamiento 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…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

En el caso de incumplimiento por parte del sub-encargado, el Encargado del Tratamiento inicial seguirá siendo plenamente responsable ante Prosegur en lo referente al cumplimiento de las obligaciones.

Quinta - Medidas de seguridad

El Encargado del tratamiento se compromete a cumplir las medidas de seguridad, de carácter organizativo y técnico, que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo que pudiera derivarse del tratamiento, con el fin de garantizar la seguridad e integridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, los costes de aplicación, la naturaleza de los datos almacenados, el alcance del tratamiento, así como los riesgos a que estén expuestos y el impacto que esto pudiera tener sobre los derechos y libertades de las personas físicas, ya provengan de la acción humana o del medio físico o natural, dando así cumplimiento a lo exigido por la normativa vigente.

El Encargado del tratamiento estará sujeto a unas medidas de seguridad que serán adecuadas para la protección de los datos personales y demás información que deberá llevarse a cabo por el Encargado del tratamiento y de acuerdo con el resultado de la evaluación de riesgos realizada por

PROSEGUR habida cuenta del estado de la tecnología, los costes de aplicación, la naturaleza de los datos almacenados, el alcance y los fines del tratamiento y los riesgos a que estén expuestos. En este sentido, el Encargado del tratamiento deberá proporcionar a PROSEGUR la información necesaria en aquellos casos en que el análisis de riesgo realizado por aquélla o por el Encargado del tratamiento determine que el tratamiento entraña un riesgo elevado.

Como consecuencia, el Encargado del tratamiento deberá aplicar sobre los datos personales objeto de las operaciones de tratamiento, como mínimo, las especificadas en el APÉNDICE I del presente Contrato.

Sexta - Notificación de brechas de seguridad

El Encargado del tratamiento tendrá la obligación de garantizar la implantación de los requisitos de seguridad establecidos en este acuerdo y de comunicar a PROSEGUR cualquier incidente que afecte a la información, documentación y datos personales responsabilidad de PROSEGUR, ya sea directa o indirectamente.

Cuando el Encargado del tratamiento o cualquier persona involucrada en los servicios detectara una incidencia que produjera robo, perdida o daño alguno de la información, que una persona hubiera accedido a la misma sin autorización, o que la información hubiera sido utilizada de forma inapropiada, el Encargado del tratamiento deberá comunicarse inmediatamente con PROSEGUR informando de los detalles de la incidencia y en cualquier caso antes del plazo de veinticuatro (24) horas, a través de correo electrónico dpo@prosegur.com, acompañando toda la información relevante para la documentación y comunicación de la incidencia, y como mínimo, la siguiente información (siempre que se disponga de ella):

1. 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.
2. 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.
3. Descripción de las posibles consecuencias.
4. Descripción de las medidas adoptadas o propuestas para remediar la brecha de seguridad de los datos personales incluyendo, en su caso, las medidas para mitigar los posibles efectos negativos.

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

Será responsabilidad del Encargado del tratamiento acometer las acciones de contención y resolución del incidente que sean necesarias.

PROSEGUR, realizará un seguimiento periódico del estado de la resolución del incidente, comprometiéndose el Encargado del tratamiento a responder con los informes que le sean solicitados.

Séptima - Registro de las categorías de tratamientos

El Encargado del tratamiento, en aquellos casos en los que así viniera determinado por el Reglamento General de Protección de Datos y el resto de legislación aplicable en la materia, deberá

llevar, por escrito, un registro de todas las categorías de tratamientos efectuados cuenta de PROSEGUR que refleje:

1. Los datos de contacto tanto de PROSEGUR como del Encargado del tratamiento, así como, en su caso, los de sus representantes y delegados de protección de datos.
2. Las categorías de tratamientos realizados en nombre de PROSEGUR.
3. En su caso, las posibles transferencias internacionales de datos que se pudieran producir en el seno del tratamiento concreto.
4. Una descripción general de las medidas de índole técnica y organizativa que aplique.

Octava - Transferencias Internacionales

Con carácter general el Encargado del Tratamiento no podrá realizar transferencias internacionales de los datos responsabilidad del Responsable del Tratamiento fuera del Espacio Económico Europeo, salvo que exista autorización previa de éste, por escrito.

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

En el caso de que el Responsable del Tratamiento autorice las mencionadas transferencias internacionales de datos y los datos se vayan a transferir a un país que no cuente con un nivel adecuado de protección o equivalente, se deberán firmar las cláusulas contractuales tipo que la Comisión Europea ha establecido al efecto. En este sentido, el Encargado del Tratamiento deberá facilitar dichos trámites al Responsable del Tratamiento, de manera previa a la realización de la transferencia internacional de datos.

Novena - Derechos de los interesados

El Encargado asistirá al responsable, mediante la aplicación de aquellas medidas técnicas y organizativas que resulten apropiadas, y de conformidad con la naturaleza de los datos tratados, en relación con las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados y, en particular, sus derechos de acceso, rectificación, supresión (“derecho al olvido”), oposición al tratamiento de sus datos, solicitud de la portabilidad de sus datos de carácter personal, limitación del tratamiento, así como a la facultad de no ser objeto de una decisión individual automatizada, incluyendo la elaboración de perfiles.

En el caso de que las personas afectadas ejerzan los derechos mencionados en el apartado anterior ante el Encargado del tratamiento, ésta debe comunicarlo por correo electrónico a la dirección protecciondedatos@prosegur.com. La comunicación deberá hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con cualquier otra información que pueda ser relevante para resolver la solicitud.

Décima - Devolución o destrucción de los datos

Una vez cumplida la prestación contractual, el Encargado se compromete a devolver a Prosegur los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el Encargado del tratamiento.

Asimismo, el Encargado del tratamiento deberá garantizar que al finalizar la relación contractual con cualquier persona con la que desempeñe una función profesional:

- la persona devuelve y no conserva de ninguna forma la información y medios de PROSEGUR.
- confirmar lo anterior de forma manuscrita o bien mediante cualquier medio similar que permita el marco legal vigente.
- la cancelación inmediata de las autorizaciones a los procesos de información.

No obstante, lo anterior, el Encargado del tratamiento puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de los servicios.

Décimo primera – Auditoría

PROSEGUR, en cumplimiento de su capacidad de control, podrá realizar por su cuenta revisiones que verifiquen el cumplimiento de las políticas y medidas de seguridad exigidas en este acuerdo para la protección de información y datos personales. Las revisiones podrán ser en los sistemas de información e instalaciones de tratamiento de datos del Encargado del tratamiento o bien a través de la recopilación de información que corrobore el cumplimiento por parte del Encargado del tratamiento.

En cualquier caso, el Encargado del tratamiento deberá mantener a disposición de PROSEGUR, la documentación (en soporte físico o electrónico) que acredite el cumplimiento de sus obligaciones conforme al acuerdo.

Asimismo, el Encargado del tratamiento deberá acreditar que ha realizado los correspondientes análisis de riesgos y, si PROSEGUR así se lo indica, las evaluaciones de impacto sobre la protección de datos pertinentes.

A fin de facilitar o incluso evitar la revisión por parte de PROSEGUR, el Encargado del tratamiento podrá aportar las oportunas certificaciones cuyos ámbitos de aplicación incluyan los servicios y personal ofrecidos por esta a PROSEGUR. Si el Encargado del tratamiento decidiera aportar las mencionadas certificaciones, deberá asimismo aportar la documentación pertinente, certificación, ámbito de aplicación así como presentar los informes de las auditorías a las que de acuerdo a la certificación se encuentra sometida. En caso de que PROSEGUR encontrase incumplimientos de seguridad incompatibles con la prestación del servicio, según el análisis de riesgos realizado por éste, dependiendo de la gravedad de los mismos, podrá requerir al Encargado del tratamiento la resolución inmediata de los problemas detectados mediante la elaboración de un plan detallado de acciones correctivas.

Todo lo anterior, sin perjuicio de la posibilidad de realizar cualesquiera otras auditorías o revisiones a efectos de verificar de otras obligaciones presentes en este acuerdo.

Décimo segunda - Deber de diligencia

El Encargado del tratamiento se compromete a facilitar al Responsable del tratamiento toda aquella información que resulte necesaria para demostrar el cumplimiento de sus obligaciones, e informará al Responsable del tratamiento en relación con su adhesión a un código de conducta aprobado, o su adscripción a cualquier mecanismo de certificación que pueda garantizar el cumplimiento de sus obligaciones en relación con el tratamiento de datos de carácter personal.

Las personas que desempeñan funciones profesionales para el Encargado del tratamiento deben ser conscientes de la importancia de la información de PROSEGUR, tratar la misma de forma segura y estar formados y cualificados en todas y cada una de las fases de proceso de la información, para todas y cada una de las funciones que desempeñen. Estos deberán observar toda la diligencia

posible y medidas adecuadas para proteger el proceso de la información en cumplimiento de su deber de buena fe a la que están obligados contractualmente.

Décimo tercera - Deber de Información

Los datos personales de los contactos del Encargado del tratamiento serán, a su vez, tratados por PROSEGUR, con domicilio social en calle Pajaritos, 24, Madrid, en calidad de Responsable de tratamiento, con la finalidad de gestionar la relación mantenida con este en su condición de prestador de servicios y con base en la ejecución de prestación de servicios, pudiendo aquel ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad y a no ser objeto de decisiones individualizadas automatizadas, enviando un correo electrónico a la dirección de correo protecciondedatos@prosegur.com, adjuntando copia de su DNI o documento acreditativo equivalente. El interesado también tendrá derecho a presentar una reclamación en materia de protección de datos ante la Agencia Española de Protección de Datos. Prosegur los tratará mientras dure la relación contractual, momento en el que serán bloqueados durante los plazos de prescripción de las acciones legales aplicables.

Décimo cuarta – Inteligencia Artificial

En el supuesto de que la prestación de los servicios implique el uso de soluciones de Inteligencia Artificial por parte del Encargado del tratamiento, garantizará que la solución de Inteligencia Artificial cumpla con los principios y requerimientos detallados en el **APENDICE II** del presente Contrato.

Asimismo, el Encargado del Tratamiento garantiza el cumplimiento de los requerimientos exigidos por la normativa vigente que resulte de aplicación al caso concreto.

A este respecto, el Encargado del Tratamiento implementará las medidas necesarias para garantizar y evidenciar el cumplimiento de las obligaciones establecidas en el párrafo anterior.

PROSEGUR, en cumplimiento de su capacidad de control, podrá realizar revisiones que verifiquen el cumplimiento de las políticas y medidas exigidas en este acuerdo para la implementación de soluciones de Inteligencia Artificial. El Encargado del Tratamiento se compromete a participar en el proceso de evaluación y a implantar aquellas medidas que solicite PROSEGUR para el cumplimiento de su Política de Inteligencia Artificial Responsable.

Décimo quinta - Indemnidad

El Encargado del tratamiento se obliga a mantener indemne a Prosegur frente a cualquier reclamación que pueda ser interpuesta contra Prosegur ante la Autoridad de Control correspondiente, que tenga por causa el incumplimiento del Encargado del Tratamiento y/o de sus subcontratistas de lo dispuesto en el presente acuerdo y en la legislación vigente en materia de protección de datos personales, y acepta pagar el importe al que, en concepto de sanción, multa, indemnización, daños, perjuicios e intereses pueda ser condenado Prosegur, incluyendo honorarios de abogados, con motivo del citado incumplimiento.

Décimo sexta - Jurisdicción

El presente acuerdo se regirá e interpretará con arreglo a las leyes de España con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a la jurisdicción exclusiva de los Juzgados y Tribunales de la ciudad de Madrid.

APÉNDICE I. MEDIDAS DE SEGURIDAD

De conformidad con los artículos 28 y de 29 de GDPR, esta sección hace referencia a las medidas de seguridad que el Encargado del tratamiento debe adoptar para garantizar el nivel de seguridad apropiado al riesgo.

El Encargado del Tratamiento debe implementar las siguientes medidas técnicas y organizativas de seguridad, con vistas a garantizar la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daños.

1. Medidas organizativas

El Encargado del Tratamiento estará obligado al cumplimiento de las medidas en relación con el personal al que se dará acceso a los datos personales:

I. Medidas organizativas genéricas

1. El Encargado del Tratamiento deberá garantizar la existencia y publicación de una política de Seguridad de la Información y de Protección de Datos para asegurar que el Encargado del tratamiento ha implementado las medidas necesarias para garantizar un nivel de seguridad adecuado al riesgo, y la protección de los datos personales se lleva a cabo de acuerdo con la legislación vigente de aplicación.

2. El Encargado del Tratamiento deberá garantizar la existencia de una estructura (departamento asignado/rol) encargada de la seguridad de la información y de la protección de datos personales (datos internos y datos externos de otros clientes).

3. Inventariar los recursos informáticos (servidores, ordenadores, aplicaciones de software, copias de seguridad) que contienen datos personales.

II. Adhesión y cumplimiento de las Políticas Corporativas de PROSEGUR

1. El Encargado del Tratamiento se adhiere a la Política de Seguridad de la Información de PROSEGUR (NG/GLO/GR/04), al documento sobre Requisitos de Seguridad de la Información para proyectos de nuevas tecnologías (NE/GLO/GR/SI/12), y a la Política General de Protección de Datos (NG-GLO-LEG-12 - 3P), a la versión más reciente de los mismos. En este sentido, serán de aplicación las disposiciones de los citados documentos y todas las medidas de seguridad definidas o a las que se haga referencia en los mismos.

III. Medidas genéricas relativas al personal

1. El Encargado del Tratamiento debe elaborar y aplicar una Política de Seguridad de la Información que se ajuste a las mejores prácticas de seguridad y que incluya las obligaciones relativas al personal.

2. El Encargado del Tratamiento debe garantizar que el personal asignado al servicio tenga las habilidades y capacidades adecuadas para desempeñar sus funciones.

3. El Encargado del Tratamiento deberá garantizar la elaboración de un programa de formación y sensibilización para los proveedores, empleados Y terceros de la organización que traten datos personales. Todos los usuarios que acceden a los datos personales deben haber recibido una formación adecuada al respecto para las funciones a realizar.

4. Los contratos de trabajo deben incorporar cláusulas específicas de adhesión a las políticas de seguridad y privacidad de la organización y deben ser firmados por los nuevos

empleados antes de que se les conceda el derecho a acceder a los activos, recursos o instalaciones para el tratamiento de datos personales.

IV. Deber de confidencialidad y secreto

1. Con el fin de impedir el acceso de personal no autorizado a los datos personales, el Encargado del Tratamiento debe garantizar la adopción de medidas para evitar que los datos personales sean expuestos a terceros (pantallas electrónicas desatendidas, documentos impresos dejados en zonas de acceso público, medios que contengan datos personales, etc.). Esta consideración incluye las pantallas utilizadas para ver las imágenes del sistema de videovigilancia, si las hubiere. El personal bloqueará la pantalla o finalizará la sesión activa cada vez que abandone su escritorio o estación de trabajo.
2. EL Encargado del Tratamiento debe garantizar que los documentos impresos y los medios electrónicos se almacenarán en un lugar seguro (gabinetes o estanterías de acceso restringido) las 24 horas del día y bajo custodia cuando estén fuera de sus dispositivos de almacenamiento o salas de archivo correspondientes.
3. Los documentos impresos (papel) o electrónicos (CD, pen drive, discos duros, etc.) que contengan datos personales no podrán ser descartados a menos que se pueda garantizar su destrucción para que la información que contienen sea irrecuperable.
4. Los datos personales o cualquier otro tipo de información personal no podrán ser revelados a terceros, con especial cuidado para no revelar datos personales protegidos en conversaciones telefónicas, correos electrónicos, etc.
5. El deber de confidencialidad y secreto persiste incluso después de la terminación de la relación laboral o de la prestación de servicios.

V. Derecho de los interesados

1. El Encargado del Tratamiento debe disponer de un protocolo de actuación para atender a los interesados que ejerzan sus derechos, a fin de garantizar una respuesta rápida y eficaz en el ejercicio de los mismos.
2. El Encargado del Tratamiento debe tramitar las solicitudes para ejercer los derechos de protección de datos, incluidos, entre otros, el acceso, la rectificación y la supresión.
3. El Encargado del Tratamiento debe informar al Responsable del Tratamiento de dichas solicitudes y asistir al Responsable del Tratamiento en la atención de las mismas.

VI. Violaciones de la seguridad de los datos personales

1. El Encargado del Tratamiento debe disponer de un procedimiento para gestionar y notificar eventos (incidentes, vulnerabilidades, problemas, etc.) en virtud del cual los eventos deben gestionarse adecuadamente y comunicarse al Responsable del Tratamiento.
2. En caso de violación de los datos personales, como el robo o el acceso no autorizado a los datos personales, se informará inmediatamente al Responsable del Tratamiento de los datos de la violación, incluyendo toda la información necesaria para aclarar los hechos y acontecimientos que hayan podido dar lugar al acceso no autorizado a los datos personales. Asimismo, se prestará asistencia al Responsable del Tratamiento para que notifique a la Autoridad de Control y, en su caso, a los interesados afectados, la violación de los datos personales, teniendo en cuenta la información disponible por parte del Encargado del Tratamiento.

3. El Encargado del Tratamiento debe mantener un registro de todas las tareas de mantenimiento y/o soporte de los sistemas del Responsable del Tratamiento.

2. Medidas Técnicas.

I. Medidas relacionadas con el control del acceso físico y ambiental

1. Las instalaciones deberán disponer de medidas de seguridad perimetrales (muros, vallas, puertas de acceso, barreras, videovigilancia, mecanismos de autenticación de acceso en las instalaciones, recepción de visitantes, etc.) para proteger los sistemas de información y los datos personales contra el acceso físico no autorizado y la manipulación.
2. Los accesos a las salas y oficinas en las que se traten datos personales deberán disponer de medidas técnicas y organizativas de protección contra el acceso no autorizado (control electrónico de acceso, videovigilancia, ventanas equipadas con un sistema de detección de roturas o alteraciones, procedimiento de solicitud de acceso a la sala u oficina, identificación personal, sistema de alarma de detección de intrusos).
3. Debe ser necesaria una autorización previa para sacar de las instalaciones los dispositivos de soporte de almacenamiento (discos duros, dispositivos extraíbles, cintas de copia de seguridad) que contengan datos personales.
4. Las entradas y salidas de las zonas de seguridad de las instalaciones deberán estar restringidas y supervisadas mediante mecanismos de control de acceso y videovigilancia para garantizar que sólo el personal autorizado pueda acceder a dichas zonas.
5. El Encargado del Tratamiento deberá garantizar la aplicación de medidas técnicas y organizativas para proteger los datos contra amenazas inmediatas tales como fugas de agua, incendios en el centro de tratamiento de datos, cortes de energía, vandalismo, etc.

II. Medidas relativas al control de acceso lógico

1. El Encargado del Tratamiento deberá definir, documentar y establecer un proceso normalizado de gestión de cuentas para el acceso a los sistemas de información que tratan datos personales [solicitud de autorización, creación, edición y supresión].
2. El acceso a los datos personales o a los sistemas de tratamiento de datos personales sólo se concede a los usuarios que disponen de las autorizaciones correspondientes (según el proceso establecido).
3. El Encargado del Tratamiento debe documentar e implementar un proceso para asegurar que las cuentas de acceso al sistema se cambien en consecuencia después de cambios organizacionales (por ejemplo, cambios funcionales, bajas, despidos, etc.).
4. El Encargado del Tratamiento debe garantizar que cada cuenta de usuario tiene un ID único asignado e inequívoco.
5. Los cambios realizados en las cuentas de los usuarios deben ser trazables (creación, edición, cancelación) y se debe mantener un registro de los mismos (por ejemplo, en documentos o registros en sistemas de información).
6. El Encargado del Tratamiento deberá garantizar la revocación de las autorizaciones de los usuarios inmediatamente después de la finalización de la relación contractual (incluida la subcontratación).
7. Las cuentas de acceso privilegiado para los sistemas de tratamiento de datos personales deben estar restringidas exclusivamente al personal autorizado y limitadas en número.

8. Las cuentas privilegiadas sólo deben concederse al personal técnicamente cualificado que haya recibido previamente un curso específico de formación y sensibilización para la gestión y utilización de cuentas privilegiadas.
9. Los usuarios que necesiten llevar a cabo actividades privilegiadas con datos personales deben tener dos cuentas en el sistema: una cuenta estándar para llevar a cabo tareas y operaciones rutinarias, y una cuenta privilegiada para llevar a cabo tareas que requieran permisos privilegiados.
10. Las contraseñas estándar de las cuentas de usuario deben cumplir los siguientes requisitos de complejidad y seguridad:
    - Deben ser almacenados de forma cifrada en los sistemas de información.
    - Las contraseñas no deben mostrarse durante el proceso de ingreso de la contraseña por parte del usuario.
    - La contraseña debe cambiarse de forma obligatoria tras el ingreso de la contraseña inicial de acceso al sistema.
    - La validez máxima de la contraseña debe ser de noventa (90) días. El sistema deberá forzar el cambio obligatorio de la contraseña transcurrido el plazo de validez máxima.
    - La longitud mínima de la contraseña debe ser de ocho (8) caracteres (incluyendo 2 números o caracteres especiales).
    - El histórico de contraseñas debe ser, como mínimo, de tres (3).
    - El número de intentos fallidos consecutivos a la hora de introducir la contraseña antes de que la cuenta se bloquee debe ser, como máximo, de tres (3).
    - La cuenta deberá desbloquearse de forma automática trascurridos, como mínimo, 15 minutos en el caso de haber introducido la contraseña errónea de forma reiterada.
    - Se deberá de impedir la introducción de contraseñas triviales o fáciles de adivinar.
11. El control del acceso a los datos y a los sistemas de información que tratan datos personales debe basarse en un concepto de roles y permisos formalmente documentados.
12. La asignación de autorizaciones/papeles debe ser válida sólo por un tiempo limitado y hacerse teniendo en cuenta los principios segregación de funciones (SoD) y principio del mínimo privilegio.
13. Los roles y autorizaciones concedidas a los sistemas de información utilizados para el tratamiento de datos personales deberán estar registradas.
14. Las autorizaciones concedidas deben revisarse periódicamente (al menos una vez al año) para garantizar su cumplimiento y validez.
15. Debe existir una política clara de control y difusión periódica entre los empleados, que forme parte de las actividades de concienciación y sensibilización que lleva a cabo la organización.
16. Los ordenadores y puestos de trabajo del Encargado del Tratamiento con acceso a los sistemas de información que procesan datos personales deben disponer de un salvapantallas protegido por contraseña que se active automáticamente tras un período de inactividad no superior a quince (15) minutos.

17. Los empleados y terceros que utilicen las computadoras y estaciones de trabajo del Encargado del Tratamiento deben estar obligados a bloquear sus pantallas de visualización cuando abandonen sus escritorios o estaciones de trabajo.

III. Medidas relativas al control de transferencia, almacenamiento y portabilidad

1. Todas las transferencias electrónicas de datos personales deben estar cifradas, cuando corresponda.
2. Los datos personales tratados de forma automatizada deberán almacenarse de forma cifrada, cuando corresponda.
3. Debe formalizarse y conservarse un registro de las transmisiones de datos personales a través de un soporte físico [por ejemplo, memorias extraíbles, cintas de backup, cds, discos duros, etc.].
4. La administración remota de los sistemas de información que procesan datos personales debe realizarse a través de un canal de comunicación seguro (SSH, IPSec, TLS /SSL, VPN, etc.).
5. El Encargado del Tratamiento incorporará medidas técnicas en los sistemas de información para evitar la posibilidad de una exportación no autorizada de datos personales (por ejemplo, la restricción de las características funcionales para descargar, imprimir y almacenar datos en los sistemas de información que procesan datos personales).
6. El soporte físico utilizado para la transmisión de los datos personales debe estar cifrado.
7. Antes de eliminar los soportes informáticos (USB, discos duros, etc.) que procesan datos personales sensibles, estos soportes deben ser borrados de forma segura (lo que hace que los datos sean irrecuperables).

IV. Control de gestión de incidentes de seguridad

1. Los ordenadores y los periféricos (por ejemplo, plataformas de correo electrónico, sistemas de acceso a Internet) tendrán una aplicación para detectar y protegerse contra software malicioso (por ejemplo, virus, troyanos, etc.), que debe actualizarse periódicamente.
2. El Encargado del Tratamiento debe disponer de un procedimiento de gestión de eventos de seguridad que establezca los criterios para clasificar, priorizar y escalar los incidentes de seguridad.
3. El Encargado del Tratamiento debe evaluar periódicamente la disponibilidad de actualizaciones de seguridad para los sistemas de TI y sus componentes (incluidos clientes, componentes de red, servidores, etc.) que procesan datos personales. Las actualizaciones de seguridad se instalan regularmente a través de un proceso formal.
4. Los sistemas de información que procesan datos personales deben ser analizados regularmente para detectar vulnerabilidades conocidas. Las vulnerabilidades detectadas deben clasificarse en función de su criticidad e impacto en la seguridad, y corregirse en consecuencia.
5. El Encargado del Tratamiento debe contar con un equipo de respuesta a eventos de seguridad para responder a los eventos de seguridad y contribuir a la coordinación de la resolución de los eventos de seguridad.

V. Control de resiliencia operacional

1. El Encargado del Tratamiento debe definir, documentar e implementar planes de continuidad de TI que abarquen los sistemas y componentes críticos de TI.
2. El Encargado del Tratamiento debe tener herramientas para detectar y prevenir intrusiones y ciberataques (por ejemplo, cortafuegos, IPS, IDS, herramientas para detectar y prevenir ataques dirigidos, etc.).
3. El Encargado del Tratamiento debe tener herramientas o servicios para detectar y limitar el impacto de los ataques de denegación de servicio (por ejemplo, DoS, DDoS, etc.).
4. El Encargado del Tratamiento debe ejecutar regularmente simulaciones de ataques informáticos (por ejemplo, pruebas de intrusión/penetración). Las desviaciones detectadas se deben evaluar y corregir regularmente de acuerdo con un procedimiento definido.
5. Los componentes y dispositivos que procesan datos personales deben protegerse mediante la aplicación de las medidas técnicas y organizativas correspondientes contra las catástrofes causadas por elementos naturales (por ejemplo, incendios, inundaciones, tornados, etc.).
6. Las redes de telecomunicaciones del Encargado del Tratamiento deben segmentarse mediante la implementación de cortafuegos para poder limitar su impacto en caso de un evento de seguridad.
7. Existe una política de copias de seguridad para los datos procesados por los sistemas informáticos. La política debe establecer el alcance de los sistemas de TI, la frecuencia de las copias de seguridad, el período de almacenamiento, la ubicación física de las copias y las medidas de seguridad para salvaguardar la confidencialidad y la integridad (por ejemplo, el cifrado). La política también considera los requisitos reglamentarios y legales.
8. Se deben realizar copias de seguridad periódicas de los sistemas informáticos (incluidos los datos de configuración del sistema) que procesan los datos personales de acuerdo con la política establecida.

VI. Control de desarrollo y operaciones de aplicaciones TI

1. El Encargado del Tratamiento debe incluir la seguridad como un elemento integrado en su ciclo de vida de desarrollo de software mediante la adopción de normas reconocidas internacionalmente para el desarrollo de aplicaciones seguras. El Encargado del Tratamiento debe identificar e implementar los requisitos legales y de seguridad durante las primeras etapas de desarrollo.
2. Se debe mantener un registro para los usuarios y administradores en la medida en que las actividades estén relacionadas con el acceso a la aplicación (inicio de sesión, cierre de la sesión, intentos exitosos/fallidos, etc.). El registro permite la identificación de al menos quién llevó a cabo la acción, cuándo se llevó a cabo y el tipo (por ejemplo, inicio de sesión, intento de acceso, etc.).
3. Los datos de registro deben almacenarse de forma segura y el acceso a los mismos debe estar restringido al personal autorizado. Los registros que deben almacenarse teniendo en cuenta su contenido y/o requisitos legales deben ser eliminados después de cumplir con su propósito.

4. El Encargado del Tratamiento realizará pruebas (estáticas / dinámicas) sobre el código fuente que él o un tercero esté desarrollando antes de desplegarlo en el entorno de producción.

5. Los entornos que no son de producción (por ejemplo, desarrollo, pruebas, consolidación) deben estar completamente separados del entorno de producción.

VII. Control de aseguramiento y cumplimiento

1. El Encargado del Tratamiento deberá realizar periódicamente (al menos una vez al año) y de forma independiente revisiones de seguridad de los sistemas informáticos que tratan datos personales con el fin de garantizar el cumplimiento y la eficacia de los controles técnicos, organizativos y legales establecidos. Se debe llevar un registro de las pruebas (y de los resultados de las mismas). Las desviaciones son evaluadas, priorizadas y corregidas.

2. Realizar simulaciones y pruebas periódicas de los planes de continuidad del servicio de TI establecidos (al menos una vez al año). Se debe llevar un registro de las pruebas (y de los resultados de las mismas). Las desviaciones se evaluarán, priorizarán y corregirán.

3. El Encargado del Tratamiento deberá realizar revisiones periódicas (al menos una vez al año) sobre la seguridad de los controles de seguridad física y ambiental implementados para garantizar su eficacia. Se debe llevar un registro de las pruebas (y de los resultados de las mismas). Las desviaciones son evaluadas, priorizadas y corregidas.

4. El Encargado del Tratamiento debe realizar pruebas periódicas de las copias de seguridad realizadas y de los procedimientos de restauración definidos para garantizar la integridad y disponibilidad de las copias. Se debe llevar un registro de las pruebas (y de los resultados de las mismas). Las desviaciones deben ser evaluadas, priorizadas y corregidas.

5. El Encargado del Tratamiento debe revisar periódica e independientemente sus procesos de gestión de la seguridad de la información. El alcance de las revisiones debe incluir al menos controles que puedan afectar a la seguridad de los datos personales del procesador de datos.

6. El Encargado del Tratamiento debe disponer de procesos, procedimientos operativos e instrucciones para garantizar el cumplimiento de los requisitos legales y reglamentarios, y de la normativa aplicable a la naturaleza del servicio.

APÉNDICE II.- INTELIGENCIA ARTIFICIAL RESPONSABLE

La solución de inteligencia Artificial propuesta por parte del PROVEEDOR debe cumplir con los siguientes principios:

Respeto a la autonomía humana

Se debe garantizar el respecto a la libertad y autonomía de los seres humanos. El sistema de IA propuesto deberá haber sido diseñado de forma que se vean favorecidas las aptitudes cognitivas, sociales y culturales de las personas; debiendo garantizarse la supervisión y el control humanos sobre los procesos de trabajo del sistema de IA propuesto.

Principio de prevención del daño

Se debe garantizar que el sistema de IA no provocará daños ni perjudicará de cualquier otro modo a los seres humanos, protegiendo la dignidad humana, así como la integridad física y mental.

El sistema y el entorno de IA son seguros y robustos desde un punto de vista técnico y, en ningún caso se destinará a usos malintencionados.

Asimismo, se debe prestar especial atención a los posibles efectos adversos que pudiera provocar un sistema de IA, estableciendo medidas concretas para su mitigación, al objeto de prevenir posibles daños.

Principio de equidad

Se debe garantizar que el desarrollo, despliegue y utilización del sistema de IA es equitativo, comprometiéndose a garantizar una distribución justa e igualitaria de los beneficios y costes, y asegurar que las personas y grupos no sufran sesgos injustos, discriminación ni estigmatización.

El PROVEEDOR procurará evitar que se produzcan sesgos injustos, pudiendo establecer medidas concretas con el fin de aumentar la equidad social a través de la utilización de sistemas de IA.

Asimismo, el uso del sistema de IA propuesto respetará el principio de equidad, entendida como la capacidad de ofrecer la posibilidad de oponerse a las decisiones adoptadas por el sistema de IA, así como trasladar su oposición a las personas que los manejan, y proporcionalidad entre medios y fines, por lo que estudiará cuidadosamente cómo alcanzar un equilibrio entre los diferentes intereses y objetivos contrapuestos.

Principio de explicabilidad

Se debe la explicabilidad del sistema de IA propuesto, para ello, todos los procesos que impliquen un desarrollo de IA son transparentes, comunicándose de manera clara y concisa las capacidades y la finalidad del sistema de IA a las partes implicadas.

Requerimientos para soluciones de IA Responsable

A continuación, se exponen los principales requerimientos que debe garantizar la solución del sistema de IA para ser un IA Responsable, los cuales se deben evaluar y abordar continuamente a lo largo de todo el ciclo de vida de los sistemas de IA:

Acción y supervisión humana

Los sistemas de IA deberán respaldar la autonomía y toma de decisiones de las personas, apoyando la acción humana y promoviendo los derechos fundamentales, además de permitir la supervisión humana.

El PROVEEDOR garantizará, en la medida de lo posible, un mínimo de intervención humana en la toma de decisiones automatizadas de los sistemas de IA, con la principal finalidad de preservar la adopción de decisiones éticas, no discriminatorias y garantistas de los derechos y libertades de las personas cuya información se procesa.

Solidez técnica y seguridad

La solidez técnica requiere que el sistema de IA se desarrolle con un enfoque preventivo en relación con los riesgos, de modo que se comporten siempre según lo esperado y minimicen los daños

involuntarios e imprevistos, evitando asimismo causar daños inaceptables, debiendo garantizarla integridad física y mental de los seres humanos.

En este sentido, el PROVEEDOR observará que el sistema de IA es robusto y cumple con las medidas de seguridad adecuadas permitiendo garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y procesada en ellos.

A tal fin, realizará rigurosas pruebas y evaluaciones de seguridad para garantizar que el sistema de IA responde de manera adecuada ante incidentes de seguridad que puedan provocar la destrucción, pérdida, alteración accidental o ilícita, o la comunicación o acceso no autorizado a la referida información

Gestión de la privacidad y de los datos

El sistema de IA observará la prevención del daño a la privacidad, lo cual implica una adecuada gestión de los datos, que abarque la calidad e integridad de los mismos. En consecuencia, el sistema de IA, su protocolo de acceso y su capacidad para procesar datos deberá ser desarrollados sin vulnerar la privacidad.

En caso de que la solución de Inteligencia artificial proporcionada por el PROVEEDOR trate datos personales, el PROVEEDOR, como responsable del sistema de IA, implementará medidas de seguridad de carácter legal, organizativo y técnico que resulten adecuadas, para garantizar la protección de las libertades y derechos fundamentales de los interesados que pudieran verse afectados, en riguroso cumplimiento del Reglamento General de Protección de Datos, REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 (en adelante, RGPD) y de la normativa local que resulte de aplicación. Asimismo, garantiza que exclusivamente sean objeto de tratamiento los datos que resulten estrictamente necesarios para cada uno de los fines pretendidos, limitando asimismo su conservación al periodo de tiempo.

Transparencia

Para que un sistema de IA sea transparente debe disponer de (i) trazabilidad: que las decisiones del sistema de IA queden registradas con la finalidad de poder identificar los motivos de una decisión errónea por parte del sistema, lo cual ayuda a prevenir futuros errores, (ii) explicabilidad: que las decisiones que adopte un sistema de IA sean comprensibles para los seres humanos y estos tengan la posibilidad de rastrearlas y (ii) comunicación: que las personas tengan conocimiento de que están interactuando con un sistema de IA, debiendo identificarse el sistema de IA como tal, así como que, cuando sea necesario, se ofrezca al usuario la posibilidad de decidir si prefiere interactuar con un sistema de IA o con otra persona, con el fin de garantizar el cumplimiento de los derechos fundamentales.

Diversidad, no discriminación y equidad

Para que un sistema IA Responsable sea fiable, es preciso que el mismo garantice la inclusión, diversidad, igualdad de acceso, mediante procesos de diseño exclusivo, así como la igualdad de trato a lo largo de todo el su ciclo de vida.

Adicionalmente, en el desarrollo interno y/o adquisición de soluciones de IA, el PROVEEDOR garantizará, en todo caso, la igualdad y la no discriminación de las personas que pudieran verse afectadas en su utilización, y en particular la ejercida por razón de raza, color, orígenes étnicos o sociales, sexo, orientación sexual, edad, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo.

Bienestar ambiental y social

El PROVEEDOR fomentará la sostenibilidad y la responsabilidad ecológica a través de los sistemas de IA, e impulsará la investigación de soluciones de Inteligencia Artificial para hacer frente a temas como el Desarrollo Sostenible.

Rendición de cuentas

El PROVEEDOR implementará mecanismos que permitan garantizar la responsabilidad y rendición de cuentas sobre el sistema de IA y sus resultados, tanto antes de su implantación como después de esta.

En este sentido, el PROVEEDOR se responsabilizará de las acciones y decisiones adoptadas por un sistema de IA, especialmente a medida que se progresa hacia sistemas más autónomos y capaces de tomar decisiones automatizadas y, en especial, cuando dichas decisiones tengan efectos jurídicos en el interesado.

7.5. ANEXO IV: Requerimientos de Riesgo Tecnológico, Ciberseguridad y Continuidad de Negocio

1. CONSIDERACIONES PREVIAS

El Proveedor utilizará los recursos de información y/o datos propiedad de GRUPO PROSEGUR únicamente, en el marco del desarrollo de la prestación de servicios encomendada y con la finalidad previamente establecida.

1.1. Obligación de guardar reserva

Todo el personal del Proveedor que, con motivo de la prestación del Servicio, o por cualquier otra circunstancia, sea conocedor de información relacionada con GRUPO PROSEGUR, tendrá la obligación de guardar secreto o reserva sobre la misma y no podrá comunicarla a terceros en ningún momento, ya sea antes, durante o con posterioridad a la prestación del Servicio sin la autorización previa y expresa de GRUPO PROSEGUR.

El Proveedor y su personal, solo podrá utilizar la información para el fin previsto en el objeto del Contrato suscrito, respondiendo ante GRUPO PROSEGUR de los daños y perjuicios que del incumplimiento pudieran derivarse para GRUPO PROSEGUR.

En el caso en que el Proveedor subcontrate, será responsable de que se respeten y cumplan los mismos criterios de confidencialidad y normas sobre la información relacionada con GRUPO PROSEGUR, descritas en las cláusulas de este anexo.

El Proveedor, así como el personal de este involucrado en proveer el servicio a GRUPO PROSEGUR, evitará que se tome cualquier acción o incurrir en omisión que pudiera resultar en la divulgación no autorizada o mal uso de los Activos de Información implicados en el desarrollo del servicio.

1.2. Confidencialidad de la Información

El Proveedor debe, con carácter general, tratar como información sensible la información de GRUPO PROSEGUR y tomar las medidas adecuadas a tal clasificación.

El tratamiento de la información debe permitir su trazabilidad, entendiendo como tal la capacidad de conocer qué personas y cuándo han accedido y tratado la información de GRUPO PROSEGUR.

Se entenderá como tratamiento cualquier operación realizada con la información, como son, aunque no exclusivamente, su lectura, escritura, modificación, copia, transmisión, grabación o archivado mediante medios manuales o con aplicaciones informáticas.

2. CUMPLIMIENTO DE LA LEGISLACIÓN

El Proveedor debe cumplir con todas las leyes vigentes que le afecten en su ámbito de aplicación, en materia de seguridad de la información y privacidad, así como las regulaciones asociadas a la industria a la que el Cliente presta la actividad, los requisitos normativos, reglamentarios y estatutarios.

3. MARCO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN

El Proveedor debe establecer un marco normativo de seguridad en las tecnologías de la información que garantice la correcta implantación de las medidas de seguridad indicadas en este anexo y que esté alineado con los criterios de GRUPO PROSEGUR en relación con la seguridad aplicable sobre la información manejada.

El Proveedor debe actualizar, de manera periódica, dicho marco normativo de seguridad, de acuerdo con las modificaciones del servicio y con las nuevas leyes, normativas o estándares de referencia internacional y por países que puedan surgir en materia de seguridad tecnológica y protección de la información, como el Cyber Security Framework de NIST, las normas ISO 27000 y 22301 y/u otras de naturaleza similar.

Este marco normativo debe contener como mínimo, documentación relativa a:

- Gestión de usuarios.
- Control de acceso y gestión de *logs* de actividad.
- Gestión del personal.
- Formación y concienciación.
- Gestión de incidencias e incidentes.
- Gestión de la continuidad del servicio.
- Gestión de las operaciones.
- Procedimientos de tratamiento y destrucción de la información.
- Gestión del cambio.
- Desarrollo software y nuevas adquisiciones de sistemas. (Si fuera de aplicación)
- Política de contraseñas.
- Procedimientos de divulgación y almacenamiento de la información.
- Modelo de relación y reporte con GRUPO PROSEGUR.
- Programa de auditoría del servicio y mejora continua del mismo.

Cada uno de los procedimientos indicados pueden solicitarse por GRUPO PROSEGUR para comprobar y verificar que se da cumplimiento a los requisitos mínimos y garantías acordadas con el proveedor.

El Proveedor debe comunicar a sus empleados encargados de prestar servicio a GRUPO PROSEGUR, el marco normativo, velando por la aceptación por su parte.

3.1. Gestión del riesgo

El Proveedor se compromete a llevar a cabo periódicamente, un análisis de riesgos que le permita determinar las medidas técnicas, procedimentales y organizativas más apropiadas para garantizar y poder demostrar que el tratamiento de la información se lleva a cabo de una forma responsable y segura, respetando las medidas de seguridad, y garantizando la privacidad y el cumplimiento de los derechos legales de los interesados.

Estas medidas, deberán adoptar un enfoque preventivo en lugar de correctivo y ser revisadas de forma periódica para garantizar que se mantienen actualizadas.

El Proveedor, de forma periódica y adicionalmente, cuando se produzcan cambios relevantes en el entorno tecnológico; debe realizar un proceso actualización del análisis de riesgos, contemplando la

valoración de aquellos aspectos específicos involucrados en el Servicio prestado a GRUPO PROSEGUR.

El Proveedor debe contar con un Plan de Tratamiento de Riesgos para gestionar aquellos que afecten a los servicios que presta a GRUPO PROSEGUR.

Dicho plan, deberá supervisar, evaluar y reportar la efectividad de las acciones definidas para el tratamiento de los riesgos.

3.2. Esquema de control

El Proveedor se compromete a cumplir con todas aquellas políticas, normas y procedimientos de seguridad del GRUPO PROSEGUR que se consideren aplicables por las actividades que se realicen y que se pongan a disposición del Proveedor una vez se comiencen a prestar los servicios contratados.

El Proveedor acepta y se obliga a cumplir el esquema de control aplicable al servicio prestado, según la clasificación resultante de la evaluación realizada por GRUPO PROSEGUR y cuyo resultado será puesto a disposición del Proveedor.

El Proveedor debe establecer los controles de seguridad adecuados con la finalidad de reducir el riesgo de acceso y modificación no autorizados a la información relevante contenida en los sistemas, (aplicaciones, sistemas operativos y bases de datos), que soporten la prestación del servicio y evitar la pérdida, sustracción, indisponibilidad y tratamiento no autorizado de los activos de información de GRUPO PROSEGUR.

Los requerimientos de seguridad indicados deberán ser aplicados por el Proveedor.

Si el Proveedor subcontratase, a su vez, a un tercero, será responsable de que los requerimientos indicados de seguridad se apliquen y cumplan también por este tercero.

Deberá reportar y evidenciar dicho cumplimento a GRUPO PROSEGUR en caso de ser requerido.

Si el Servicio trata información sujeta a certificaciones de seguridad, el Proveedor deberá presentar a GRUPO PROSEGUR y a su requerimiento, las certificaciones correspondientes.

GRUPO PROSEGUR se reserva la facultad de modificar en cualquier momento los requerimientos de seguridad contenidos en este contrato y en sus anexos, comunicándolo al Proveedor, con indicación de las fechas para su entrada en vigor.

4. ORGANIZACIÓN DE LA SEGURIDAD

4.1. Identificación de responsabilidades

El Proveedor debe contar con Responsables de Riesgo Tecnológico y Seguridad de la Información formalmente designados, con el fin de que estos velen por el cumplimiento de las políticas de seguridad y proporcionen el seguimiento de los controles implantados, con el fin de asegurar la integridad, confidencialidad y disponibilidad, autenticidad y trazabilidad de los datos y sistemas, así como garantizar el cumplimiento de toda la normativa que les sea de aplicación.

El Responsable de Riesgo Tecnológico y Seguridad debe realizar el control y la coordinación de las medidas de seguridad aplicadas por el Proveedor, así como realizar y reportar a GRUPO PROSEGUR los resultados de dichas revisiones.

El Proveedor debe designar un Coordinador encargado de la gestión de los aspectos de seguridad con GRUPO PROSEGUR. Este Coordinador deberá asistir al Comité de Coordinación integrado por el Proveedor y GRUPO PROSEGUR, en caso de que éste sea convocado por GRUPO PROSEGUR, con el fin de realizar un seguimiento oportuno del servicio y definir los planes de acción necesarios para garantizar el correcto desempeño de los servicios contratados.

El Proveedor debe comunicar la existencia e identificar a las personas que ostenten las responsabilidades o cargos de Security Officer (CISO) y del Incident Manager, (IM), si tuvieran la necesidad u obligación de contar con ellos en el desempeño de las funciones anteriores y con el fin de establecer las comunicaciones que fuesen oportunas.

El Proveedor debe comunicar a través de los canales establecidos con GRUPO PROSEGUR, cualquier cambio que se produzca respecto de la designación inicial de responsables para el servicio. Dicha comunicación deberá efectuarse en un plazo máximo de 24 horas.

4.2. Planes de formación y concienciación

El Proveedor implementará planes de formación y concienciación en materia de seguridad de la información, que incluyan a todos los empleados que prestan servicio a GRUPO PROSEGUR.

El Proveedor debe desarrollar de manera explícita un plan de concienciación relativo a la importancia de la seguridad de la información, la protección de datos de carácter personal y la necesidad de garantizar el correcto tratamiento y la confidencialidad de la información sobre los mismos.

El Proveedor debe implementar de manera explícita, un plan de formación relativo a la importancia del desarrollo seguro de código en caso de ser aplicable a la prestación de servicio contratado.

4.3. Notificación

El Proveedor debe notificar a GRUPO PROSEGUR cualquier incidencia relevante que incumpla cualquier aspecto relativo a la seguridad de la información y recogido en los contratos y/o acuerdos de servicio vigentes con GRUPO PROSEGUR en un plazo máximo de 24 horas.

El Proveedor debe notificar a GRUPO PROSEGUR cualquier cambio en la prestación del servicio, y que afecte a la forma de prestarlo, (cambio en el proceso) a los sistemas utilizados para dar el servicio, (cambio en la infraestructura), o al personal involucrado en un plazo máximo de 24 horas.

5. MEDIDAS TECNOLÓGICAS

5.1. Clasificación y gestión de activos

El Proveedor debe contar con un inventario de activos de información (CMDB), en el que se identifique el tipo de información contenida en cada uno de ellos, la propiedad del activo, la custodia y el grado de sensibilidad de la información manejada.

El Proveedor debe establecer un proceso de Clasificación de la información y de categorización de los activos, asignándoles un nivel de seguridad en relación con los riesgos inherentes y la criticidad de los sistemas e información que soportan.

El Proveedor debe mantener y actualizar este inventario periódicamente, ante cualquier cambio que afecte a los activos que forman parte de la prestación del servicio.

La identificación de los soportes de información se realizará con un sistema de etiquetado solo comprensible para los usuarios autorizados.

El Proveedor debe cifrar los datos en la distribución de soportes y en dispositivos portátiles, evitando el tratamiento en aquellos que, por configuración o tecnología, no permitan dicho cifrado. Deberá adoptar dichas medidas de cifrado de forma proporcional a los riesgos afectos, sobre todo para aquellos entornos más desprotegidos.

El Proveedor debe contar con un Procedimiento de Gestión, Acceso, Almacenamiento, Tratamiento, Distribución y Eliminación de Soportes que garantice el cumplimiento de las medidas de seguridad exigidas por el GRUPO PROSEGUR.

En particular, el Proveedor debe garantizar la custodia segura, el acceso únicamente por personal autorizado, el traslado y la manipulación segura de los mismos, un registro de

entrada y salida que permita una trazabilidad completa de todos los movimientos; así como la eliminación completa de información previo al desechado del soporte.

5.2. Control de acceso

El Proveedor debe establecer los controles suficientes y necesarios para asegurar que el acceso físico y lógico a los sistemas que contienen, transmiten o tratan información relevante, se controlan de acuerdo con los requisitos establecidos por GRUPO PROSEGUR en el marco indicado en este anexo.

El Proveedor, a la hora de conceder un nivel de acceso a la información, aplicaciones y sistemas implicados en este servicio, debe realizarlo mediante un sistema de gestión de identidades, basado en roles y funciones y teniendo en cuenta el principio de "menor privilegio", asegurando que se concede el nivel de acceso mínimo necesario para cada uno de sus empleados o terceros implicados en el servicio prestado a GRUPO PROSEGUR.

El Proveedor debe establecer una segregación de funciones adecuada, que defina las medidas suficientes y necesarias para asegurar que los derechos de acceso, (roles y perfiles) para cada usuario del servicio, se asignan de acuerdo con las necesidades funcionales de cada uno de sus usuarios y que estas necesidades funcionales, no ponen en peligro o comprometen la seguridad, integridad y disponibilidad de los activos de información que forman parte del servicio externalizado.

El Proveedor debe realizar revisiones periódicas sobre los permisos y los controles de acceso configurados en los sistemas involucrados en el servicio y GRUPO PROSEGUR podrá acceder a los resultados de dichas revisiones, así como solicitar la implantación de medidas correctivas en caso de encontrar deficiencias.

5.2.1. Controlar acceso a aplicaciones y sistemas

- El Proveedor debe definir una Norma de Control de Acceso y de Gestión de Contraseñas de acuerdo con los requisitos del Servicio y de Seguridad de la Información establecidos por GRUPO PROSEGUR.

- El Proveedor debe implantar los mecanismos necesarios para evitar la existencia de usuarios genéricos, salvo en aquellos casos que sean expresamente requeridos por las tecnologías o sistemas empleados para el desarrollo del servicio.

    - Esta tipología de usuarios debe ser informada, aprobada y validada previamente por GRUPO PROSEGUR.

- El Proveedor debe implantar los mecanismos necesarios que permitan identificar de manera inequívoca a sus usuarios con acceso a los sistemas soporte del servicio prestado a GRUPO PROSEGUR.

- El Proveedor debe garantizar que no se comparten códigos ni contraseñas de usuario entre los mismos.

- El Proveedor debe registrar los datos de cada intento de acceso, incluyendo al menos la información relativa al usuario, fecha y hora, fichero accedido, tipo de acceso y si la operación ha sido autorizada o denegada. Si el acceso es correcto y ha sido autorizado, se guardará el registro accedido en sus estados anterior y posterior al acceso.

- El Proveedor debe realizar una verificación periódica del control de accesos, reflejando los datos de los intentos de acceso válidos o no.

    - Estos registros deben conservarse durante el plazo mínimo de 2 años para la búsqueda de evidencias ante la ocurrencia de o eventos, incidencias, o incidentes de seguridad.

- El Responsable de Seguridad del Proveedor debe tener control directo sobre el acceso a los mecanismos de control del registro de accesos.

- El Proveedor debe implantar los mecanismos necesarios que permitan mantener un registro operativo y actualizado de usuarios, sistemas o aplicaciones implicados en el servicio.

    - Dicho registro debe reflejar todos los cambios en el mapeo: altas, bajas y posibles modificaciones en los activos indicados anteriormente.

- El Proveedor debe asegurar que los usuarios afectos a la prestación del servicio que experimentan una ausencia o aquellas cuentas que se detecten como inactivas por más de sesenta, (60), días sean suspendidas, bloqueadas y posteriormente deshabilitadas en plazos razonables.

- El Proveedor debe asegurar que a los usuarios implicados en la prestación del servicio que se les modifiquen sus responsabilidades laborales pasen por un proceso de revisión y actualización de sus perfiles y niveles de acceso, acorde a sus nuevas necesidades y que garantice la aplicación del principio de “mínimo acceso y capacidad requerida”.

- El Proveedor debe implantar los mecanismos necesarios que permitan restringir el acceso a Internet o a cualquier tipo de conexión que posibilite la fuga de información de los datos del GRUPO PROSEGUR y que trate en virtud de este clausulado.

- El Proveedor debe establecer los controles suficientes y necesarios para asegurar que el acceso lógico a los sistemas que almacenan procesos o transmiten información relevante, se controla de acuerdo con los requisitos establecidos por GRUPO PROSEGUR.

    - Las bajas de cualquier usuario del Proveedor o de cualesquiera terceros subcontratados por este, gestores o participantes de la prestación del servicio a GRUPO PROSEGUR, deberán tramitarse en un plazo máximo de 24 h.

- El Proveedor debe establecer un mecanismo que limite el número de intentos reiterados de acceso no autorizado. El Proveedor debe asegurarse de que los empleados que tengan que utilizar conexiones remotas para la prestación del servicio, cumplan las directrices de las directrices de Acceso Remoto de GRUPO PROSEGUR que se facilitarán una vez se den comienzo las actividades correspondientes y contratadas. Es responsabilidad del proveedor verificar que se cumplen los siguientes aspectos:

    - Todos los accesos remotos deben informarse y ser autorizados por parte del Grupo Prosegur.

    - Las credenciales deben tener un identificador único asociado a un usuario y deben ser intransferibles.

    - En el caso de que un empleado comparta sus credenciales o comparta su sesión abierta con otros usuarios:

        1. Se considerará y reportará por parte del proveedor, como un incidente de seguridad.

        2. El usuario será dado de baja inmediatamente de los sistemas del grupo Prosegur.

        3. El empleado, y por ende el proveedor, será responsable directo de los daños ocasionados, las acciones, (u omisiones) realizadas por el usuario, pudiendo recaer sobre el mismo las sanciones estipuladas para este tipo de incidentes, así como aquella impuestas por terceros y derivadas de este incumplimiento

- El Proveedor debe establecer mecanismos que permitan identificar los accesos realizados para aquellos ítems de información con acceso concedido a múltiples usuarios.

- El Proveedor debe garantizar la realización de revisiones periódicas sobre los controles y permisos de acceso configurados en los sistemas afectos al Servicio.

- El Proveedor debe establecer las medidas adecuadas asegurar que accesos remotos al entorno tecnológico están debidamente controlados y monitorizados.

- El Proveedor debe asegurar que la información relacionada al Servicio prestado no es transmitida a terceros sin la previa autorización de GRUPO PROSEGUR y cumpliendo con todos los requisitos legales.

5.2.2. **Controles de acceso a instalaciones y CPDs**

El Proveedor debe asegurar el control del acceso a las salas donde se ubican los activos implicados en el servicio prestado a GRUPO PROSEGUR, con las salvaguardas administrativas, lógicas y físicas apropiadas, incluyendo en función de la criticidad de los sistemas, pero no limitado, las siguientes medidas:

- Bloqueo de las puertas de acceso.
- Control de acceso a las oficinas y centros de procesamiento de datos del Proveedor.
- Existencia de personal de seguridad física.
- Medidas de videovigilancia

El Proveedor debe garantizar que los intentos de acceso no autorizados se detecten, impidan y se informen de manera inmediata a GRUPO PROSEGUR.

Todos los puntos de entrada y salida deben estar asegurados, registrados y monitorizados para asegurar que sólo el personal autorizado accede a las instalaciones.

En caso de que el Proveedor utilice tarjetas de identificación o medidas similares para sus empleados que forman parte del servicio prestado a GRUPO PROSEGUR, debe existir un proceso documentado, junto con los procedimientos de apoyo, para asegurar que las credenciales perdidas y las fichas queden inhabilitadas inmediatamente después de la notificación de la pérdida.

El Proveedor debe contar con procedimientos y mecanismos suficientes para asegurar que, si un empleado que forma parte del servicio prestado a GRUPO PROSEGUR finaliza su relación laboral con el proveedor, las credenciales de identificación sean inmediatamente revocadas.

El Proveedor debe asegurar que todos los activos de información de GRUPO PROSEGUR que forman parte del servicio externalizado, y en su posesión, estén físicamente asegurados en un área de acceso controlado o en un contenedor de almacenamiento seguro.

El Proveedor debe informar a GRUPO PROSEGUR ante cualquier movimiento o eliminación de cualquier sistema o activo de información, el cual no podrá llevarse a cabo sin el consentimiento por escrito de GRUPO PROSEGUR.

5.2.3. **Controles de entorno físico y medioambiental**

El Proveedor será responsable de la implantación de medidas de seguridad física para la protección de los sistemas de información ubicados en sus instalaciones ante accesos no autorizados y daños físicos.

Entre los controles físicos y ambientales deben tratarse:

- Medidas de protección ante incendios
- Medidas de protección ante inundaciones
- Controles del suministro eléctrico
- Otros controles que sean aplicables según la legislación y normativa vigente.

El Proveedor debe mantener actualizada la base de datos de personal con acceso autorizado y se debe controlar de acuerdo con los requisitos establecidos por GRUPO PROSEGUR.

5.2.4. **Autorización y autenticación**

El Proveedor debe implantar las medidas de seguridad necesarias y suficientes para asegurar que el acceso de administradores a sistemas de información se realiza empleando canales cifrados y autenticación fuerte.

En caso de que el Servicio requiera atender a clientes, el Proveedor debe implantar las medidas de seguridad necesarias y suficientes para asegurar que la autenticación de dichos clientes se realiza mediante mecanismos de doble factor, al menos para la ejecución de operaciones o consulta de información confidencial.

El Proveedor debe garantizar el almacenamiento cifrado de las contraseñas en los sistemas de tratamiento de la información.

El Proveedor debe implantar los mecanismos necesarios para evitar que los usuarios sean administradores locales de sus puestos, salvo requerimiento explícito y validación por parte de GRUPO PROSEGUR.

5.3. Cifrado

El Proveedor debe utilizar algoritmos de cifrado estándar con una longitud de clave basada en prácticas y estándares reconocidos internacionalmente para proteger la confidencialidad e integridad de los datos sensibles de GRUPO PROSEGUR.

El Proveedor debe proteger las claves de cifrado con mecanismos de seguridad apropiados y durante todo su ciclo de vida, desde su generación, pasando por su almacenamiento, distribución, renovación, archivo y terminando en su eliminación.

El Proveedor proporcionará a GRUPO PROSEGUR aquella documentación relativa a la gestión de las claves de cifrado para verificar que se cumplen los requisitos mínimos de seguridad para las claves criptográficas. En el caso de que sea necesario el acceso a los sistemas de Grupo Prosegur, se facilitará en el momento en que se inicie la actividad las normas y procedimientos que el Proveedor y su personal necesite conocer respecto a la gestión y uso de las claves de cifrado.

El Proveedor debe velar porque los dispositivos que traten datos críticos o sensibles sean cifrados. Especialmente aquellos dispositivos removibles, extraíbles o móviles como, por ejemplo: Portátiles, Discos Externos, Dispositivos de almacenamiento USB, etc.

El Proveedor debe garantizar el almacenamiento cifrado de las contraseñas en los sistemas de tratamiento de la información.

La pérdida de confidencialidad o compromiso de cualquier clave criptográfica que afecte a los sistemas de GRUPO PROSEGUR supone un incidente de seguridad, por lo que debe ser comunicada sin dilación para poner en marcha los mecanismos de respuesta oportunos.

5.4. Gestión de infraestructura y seguridad perimetral

El Proveedor informará a GRUPO PROSEGUR sobre la infraestructura tecnológica desplegada para darle Servicio, con el nivel de detalle requerido por GRUPO PROSEGUR para permitir realizar las tareas de supervisión/ monitorización que se establezcan.

El Proveedor debe desarrollar una infraestructura tecnológica para la prestación del servicio, de modo que se facilite la migración modular a otra ubicación o se posibilite una migración tecnología.

El Proveedor no debe conectar ni hardware, ni software ajeno al GRUPO PROSEGUR con la red de interna de GRUPO PROSEGUR sin:

- Realizar una evaluación del riesgo con el alcance necesario, incluyendo la identificación de los controles existentes y compensatorios basados en los requisitos dentro de este Anexo;
- Verificar la aplicación de los controles identificados en la evaluación de riesgos;
- La aprobación por escrito por parte del Responsable de Seguridad, (CISO) del GRUPO PROSEGUR.

El Proveedor debe proteger o desactivar los puertos de red desatendidos cuando no estén en uso. Si los requisitos de negocio justifican la necesidad de tenerlos habilitados, los puertos de la red pueden permanecer activos siempre que la dirección del Proveedor haya revisado la necesidad del negocio y haya una aprobación documentada. Ejemplos de tal necesidad incluirían puertos de red en salas de conferencias, áreas de trabajo compartidas, etc.

5.4.1. **Segregación de entornos. (En caso de aplicación)**

El entorno de producción del Proveedor debe estar segregado física y/o lógicamente del resto de entornos no productivos, de modo que exista control en el intercambio de información versiones, datos, etc., entre ellos.

La red de usuarios del Proveedor debe estar segregada de la red de sistemas centrales, permitiéndose únicamente la conectividad mínima necesaria para el acceso de los usuarios a los sistemas que necesiten para realizar sus funciones.

En todo caso, debe concretarse una segmentación en los entornos de operación, desarrollo y pruebas para reducir los riesgos de acceso no autorizados o de ejecución de cambios, así como que no se produzca impacto en los sistemas de producción en caso de incidencia.

5.4.2. **Seguridad de servidores. (En caso de aplicación)**

El Proveedor debe disponer de documentación o guías de bastionado de servidores, gestión de parches, versiones y vulnerabilidades que garantice la seguridad de los sistemas y la disponibilidad de estos.

El software instalado en los servidores debe ser sólo el indispensable para la correcta prestación del servicio y contar con una protección antivirus actualizada.

Los servidores deben estar plataformados de acuerdo con buenas prácticas reconocidas y solo tendrán activos los servicios necesarios para la operación del servicio.

Los servidores necesarios para la prestación del servicio deberán estar segmentados lógicamente, por ejemplo, dedicándose una VLAN dedicada para el servicio prestado a GRUPO PROSEGUR.

Se debe garantizar la protección de los datos y asegurar que estos no son visibles excepto para GRUPO PROSEGUR.

Los datos, ya sean residentes en bases de datos o sistemas de ficheros, solo estarán accesibles desde las aplicaciones que los procesen, y nunca deberán estar accesibles de manera pública desde redes externas.

El Servidor de base de datos deberá instanciarse en un sistema distinto al de ejecución de la aplicación, habilitando únicamente la comunicación con el servidor donde se aloje la aplicación; es decir, no deberá ser directamente accesible desde Internet.

Los servidores se encontrarán adecuadamente cerrados/precintados, al objeto de que cualquier manipulación pueda ser detectada visualmente.

5.4.3. **Seguridad perimetral**

El servidor que aloje la aplicación debe estar protegido de accesos de terceros mediante un Firewall.

En caso de que existan aplicaciones expuestas a Internet, el acceso a las mismas debe estar apantallado por un dispositivo que funcione como proxy inverso, ubicado en una DMZ protegida por una doble barrera de Firewall. No debe existir exposición de aplicaciones o servicios de forma directa a internet, a no ser que GRUPO PROSEGUR lo autorice expresamente.

El Proveedor debe garantizar que, en caso de integración de un nuevo software en dispositivos con permisos de conectividad con los sistemas de información de GRUPO PROSEGUR, dicho proceso esté precedido por una evaluación de riesgos y de que se incorporan al mismo procedimientos formales de control de cambios para determinar y proteger el impacto en la red de GRUPO PROSEGUR.

5.4.4. **Redes inalámbricas**

El Proveedor debe configurar los puntos de acceso a la red inalámbrica para garantizar que sólo los dispositivos autorizados puedan establecer una conexión con la red en la que se visualicen, alojen, almacenen, procesen, transmitan, impriman, respalden o se destruya información del GRUPO PROSEGUR.

Además, las conexiones establecidas deben utilizar las mejores prácticas de la industria para el cifrado y dotarse de las salvaguardias más apropiadas para proteger el acceso y uso no autorizado de dichas conexiones.

5.4.5. **Seguridad en Endpoints**

El Proveedor debe garantizar que los usuarios que presten servicio a GRUPO PROSEGUR, no sean administradores de su equipo, y por lo tanto, no puedan instalar o modificar software y sus configuraciones; ni hardware adicional.

El Proveedor debe implementar una solución de protección de endpoints que incluya, al menos:

- Aplicaciones antimalware como parte de las configuraciones seguras comunes para los sistemas, equipos y componentes y que estas detecten y actualicen las vulnerabilidades, no permitiendo su modificación o desconexión por parte de los usuarios y ejecutando escaneos con frecuencia.

- Cortafuegos personales dotados de reglas que restrinjan los puertos y servicios que se determinen; que proporcionen control contra la ejecución de programas maliciosos, permitan el control de dispositivos extraíbles y USBs; y que proporcionen capacidades de auditoría y registro de la actividad del usuario y la capacidad y estado del equipo.

- La implantación de herramientas IDS/IPS para identificar y detener actividades sospechosas, monitorizando el tráfico de red y los dispositivos que se conectan a ella.

- La implantación de restricciones adecuadas para evitar la ejecución de código malicioso en los equipos.

6. GESTIÓN DEL PERSONAL

El Proveedor debe implementar un proceso de gestión de recursos humanos para mantener registro y control, contratar, retener y despedir a los empleados, contratistas y otro personal subcontratado y afecto a la actividad que proporcione al GRUPO PROSEGUR.

El Proveedor debe comprometerse a implementar en el mismo, criterios de selección adecuados para los puestos afectos a la operativa de los sistemas de Grupo Prosegur.

El Proveedor debe asegurar que la gestión de los recursos humanos esta alineada con la gestión de los riesgos del servicio que presta a GRUPO PROSEGUR, y velar por que los procesos de alta, modificación y baja de los empleados se realizan en tiempos aceptables de forma que se garantice la seguridad de la información y los sistemas afectos al servicio.

El Proveedor debe asegurar que su personal y/o subcontratas con acceso a los sistemas, activos e información del Grupo Prosegur, conoce y cumple las políticas, normas y procedimientos que el GRUPO PROSEGUR facilite una vez se formalice el contrato y se inicien los servicios, especialmente en lo que se refiere a sus deberes y obligaciones en cuanto al uso de los sistemas, redes y otros recursos del Grupo Prosegur, así como las consecuencias y sanciones de su incumplimiento.

Adicionalmente, el Proveedor debe asegurar que sus empleados y terceros subcontratados, no llevarán a cabo, excepto con autorización previa y por escrito de GRUPO PROSEGUR, cualquiera de las siguientes actividades:

- La instalación de software o dispositivos en el entorno PROSEGUR que no han sido previamente aprobados.

- La carga de datos obscenos, ofensivos o inapropiados o de software que genere cualquier tipo de incumplimiento en el entorno Prosegur.

- El uso del entorno PROSEGUR para interceptar, analizar o realizar cualquier otro tipo de monitorización de tráfico de las redes PROSEGUR o de terceros sin petición conocimiento y autorización previa de Grupo Prosegur.

El Proveedor debe asegurar la correcta formación y concienciación de sus empleados en materia de ciberseguridad y privacidad de la información, disponiendo de Planes de Formación y Concienciación del personal, que deberán estar cogestionados por el equipo de gestión de riesgos y RRHH.

El GRUPO PROSEGUR podrá solicitar acceso y revisar el contenido de dichos Planes de Formación y Concienciación para verificar su adecuación a las necesidades del servicio contratado.

El Proveedor debe asegurarse de que se proporciona formación específica para usuarios con privilegios y funciones de seguridad, para garantizar que estos comprendan sus roles y responsabilidades exclusivas.

El Proveedor debe asegurarse de que todos los requisitos anteriores se aplican y verifican para el personal subcontratado.

7. GESTIÓN DE LAS OPERACIONES

El Proveedor debe establecer los controles de seguridad adecuados para asegurar que las operaciones llevadas a cabo sobre las aplicaciones y sistemas involucrados en el servicio son autorizadas y programadas de acuerdo con los requisitos acordados entre GRUPO PROSEGUR y el Proveedor.

En particular, el Proveedor debe definir procedimientos de gestión de las operaciones corrientes que realice para GRUPO PROSEGUR, incluyendo, pero no limitando, para la realización de copias de seguridad, los procedimientos para la recuperación de los sistemas y para la gestión de incidentes de continuidad de negocio.

El Proveedor debe implementar controles suficientes que garanticen que todos los elementos con los que prestará el Servicio se administran y explotan de forma segura.

Estos controles y la revisión de estos y sus informes de resultados y mejoras deben estar disponibles para GRUPO PROSEGUR, en caso de que lo solicite.

Los controles indicados en el punto anterior deben incluir como mínimo:

- Políticas implantadas de gestión usuarios/contraseñas de los operadores y administradores de sistemas o productos, incluyendo expresamente gestores de bases de datos.
- Acceso a los sistemas mediante herramientas que protejan la confidencialidad de las contraseñas de los administradores, por ejemplo, SSH en UNIX.
- Protección de los sistemas servidores frente a accesos no autorizados.
- El Servicio deberá proveer de mecanismos de autenticación multi-factor.

El Proveedor debe incluir en su Política de Contraseñas al menos los siguientes aspectos:

- Un procedimiento de distribución de contraseñas que garantice que éstas son conocidas únicamente por el usuario.
- Un procedimiento para controlar la caducidad de contraseñas y el almacenamiento ininteligible de las mismas.
- Robustez adecuada, de acuerdo con las siguientes reglas, en la medida que sea posible: a) mínimo de ocho (8) caracteres de longitud, b) tener mayúsculas, c) minúsculas, d) números y e) caracteres especiales, (por ejemplo: !, $, @).
- Caducidad de la contraseña (recomendable 60 días y no más de 90), con un procedimiento de cambio que no provoque una interrupción del servicio.

- Obligatoriedad de almacenamiento cifrado de las contraseñas de los sistemas y aplicativos que forman parte de la externalización.

7.1. Configuración de los sistemas

El Proveedor debe asegurar que existen procesos de gestión de la configuración y bastionado de los sistemas que cumplen los estándares internacionales y que permiten aplicar los requisitos de seguridad establecidos por el GRUPO PROSEGUR para los sistemas afectos a la prestación indicada en el contrato.

La gestión de la configuración debe encontrarse centralizada para todos los sistemas operativos, aplicaciones, servidores y otras tecnologías que requieran configuración.

El Proveedor debe mantener un registro con las configuraciones históricas por si fuese necesario para la resolución de problemas o bien para la investigación forense de incidentes.

Los cambios de configuración no autorizados que se detecten y que afecten a activos de GRUPO PROSEGUR se deben tratar como incidentes de seguridad y se deben comunicar al Grupo Prosegur.

El Proveedor debe instalar en los sistemas utilizados para prestar el servicio a GRUPO PROSEGUR, una protección antivirus que debe mantenerse operativa y actualizada en todo momento.

El Proveedor debe implementar controles para restringir los dispositivos de salida tales como USB, unidad lectora/grabadora de CD/DVD u otros, que permitan la extracción de datos de este.

7.2. Mantenimiento de sistemas. (En caso de aplicación)

El Proveedor debe implementar un proceso de monitorización de vulnerabilidades de la infraestructura tecnológica del Servicio, identificando y tratando oportunamente las vulnerabilidades que se detecten y sin exponer la información de GRUPO PROSEGUR a dichos riesgos.

Adicionalmente, deberá realizar periódicamente una evaluación de seguridad de la red interna y perimetral, bien con recursos propios o bien por parte de un tercero independiente.

El GRUPO PROSEGUR deberá tener acceso a dichos informes, así como la potestad de proponer medidas que subsanen las deficiencias encontradas en un plazo acordado entre las partes y razonables.

El Proveedor deberá proponer proactivamente la instalación de actualizaciones y parches de seguridad. Dichas actualizaciones y parcheados serán comunicadas y autorizadas previamente por GRUPO PROSEGUR.

Adicionalmente, GRUPO PROSEGUR podrá solicitar la instalación de actualizaciones y parches si lo considerara necesario.

En todo caso, el despliegue de parches deberá probarse en entornos previos, para evitar posibles impactos sobre el Servicio.

Con independencia del software base que dé soporte a la plataforma y de sus versiones, (sistemas operativos, base de datos, servidor web, etc.), debe existir una política de vigilancia y monitorización de alertas de seguridad, así como de actualización de los parches de seguridad publicados por los fabricantes de toda la infraestructura correspondiente y afecta al servicio.

Los tiempos de actuación no deberán superar las 24 horas en casos de fallos de seguridad clasificados por el fabricante de carácter grave/alto.

El Proveedor debe establecer los controles de seguridad adecuados en relación con los cambios que pudieran ser necesario realizar sobre las aplicaciones, o sistemas involucrados en el Servicio.

Estos controles deben cubrir como mínimo las solicitudes de cambios, los análisis de impacto, las autorizaciones, la realización de pruebas, las aprobaciones del usuario final y garantizar una separación adecuada de los entornos previos respecto del entorno de producción.

La ejecución de cualquier cambio en los sistemas de información asociados al Servicio debe ser revisada y aprobada previamente por GRUPO PROSEGUR y realizarse garantizando la integridad, confidencialidad y disponibilidad de la información y del Servicio.

El Proveedor debe establecer los mecanismos necesarios para realizar una administración y operación de los dispositivos de seguridad, siempre que GRUPO PROSEGUR haga una delegación expresa de tales funciones.

7.3. Ficheros temporales

El Proveedor, en caso de utilizar ficheros temporales o auxiliares para la prestación del servicio, debe proteger estos ficheros con las mismas medidas de seguridad utilizadas para los ficheros principales, y debe borrarlos, eliminarlos o destruirlos de forma segura una vez que hayan dejado de ser necesarios para los fines que motivaron su creación garantizando que no se permita su recuperación posterior.

Los responsables de los sistemas de información, designados a tal efecto, deberán verificar periódicamente la posible existencia de ficheros temporales creados automáticamente como consecuencia del mal funcionamiento de los sistemas.

7.4. Servicio compartido

El Proveedor debe implementar las medidas suficientes para garantizar la seguridad de la infraestructura tecnológica en caso de que se encuentre compartida con otros clientes del Proveedor. La infraestructura tecnológica del Servicio deberá poseer canales de comunicación cifrados entre otros servicios que ofrezca el Proveedor y las conexiones del personal responsable de la administración de la infraestructura. Por ejemplo; SSH, VPN con IPSEC, etc.

El almacenamiento de datos del Servicio prestado a GRUPO PROSEGUR deberá estar aislados lógicamente de otros repositorios de almacenamiento ajenos. El Servicio del Proveedor deberá tener la capacidad de cifrar información almacenada, mediante algoritmos fuertes de cifrado, en caso de ser requerido.

8. GESTIÓN DE INCIDENTES

El Proveedor debe tener establecidas una serie de medidas específicas y procedimientos donde se detallen las acciones a llevar a cabo para una correcta gestión (detección, resolución y comunicación a GRUPO PROSEGUR) sobre los incidentes de Seguridad, Contingencia Tecnológica y Continuidad de Negocio que sucedan durante la prestación del servicio y que puedan afectar al mismo o al GRUPO

PROSEGUR En cuyo caso deberán informar oportunamente de la ocurrencia de los mismos y del modo y plazo de resolución.

Este procedimiento deberá ser de pleno conocimiento por parte del todo el personal que preste servicio a GRUPO PROSEGUR.

En relación con la gestión de incidentes, el Proveedor debe contar, al menos, con procedimientos y mecanismos automatizados y de gestión que cubran la:

- Prevención.
- Detección.
- Análisis.
- Contención.
- Mitigación.
- Recuperación.
- Monitorización.

El Proveedor debe adoptar las medidas adecuadas para que en el menor tiempo posible se subsane la anomalía generadora del incidente.

El Proveedor debe registrar para cada incidencia ocurrida, recopilando y cumplimentando al menos, los siguientes conceptos: tipo de incidencia, descripción, momento en que se ha producido o detectado, persona que la notifica, persona a la que se comunica, efectos derivados, medidas correctoras aplicadas, procedimientos realizados de recuperación de datos, persona que los ejecuta, datos restaurados y grabados manualmente.

El Proveedor debe autorizar la ejecución de los procedimientos de recuperación de datos (en caso de ser necesario) según los planes de Recuperación de que disponga.

El Proveedor debe prestar el apoyo requerido a GRUPO PROSEGUR en el caso de que éste decida iniciar una evaluación independiente de seguridad o investigación de incidentes.

El Proveedor debe definir un medio de comunicación seguro para comunicar situaciones inusuales, incidentes o de cualquier otra índole relacionada a la confidencialidad de la información de GRUPO PROSEGUR sin dilación no justificada.

El Proveedor debe informar inmediatamente a GRUPO PROSEGUR en el caso de que se detecte o se tenga una sospecha de un incidente de seguridad remitiendo un informe preliminar que incluya la información básica y disponible relacionada con el incidente como por ejemplo, los procesos, activos e información afectada, las medidas que se han tomado y su resolución. GRUPO PROSEGUR puede realizar seguimientos sobre estos incidentes para identificar posibles situaciones en las que se deban acometer medidas concretas.

El Proveedor debe acordar con GRUPO PROSEGUR los criterios para la notificación de un incidente de seguridad, en los casos de fuga de información, disrupción del servicio, ataques que afecten a la reputación de GRUPO PROSEGUR y cualquier otro caso que sea acordado.

La falta de notificación de una incidencia crítica de la que se haya tenido conocimiento podrá ser considerada como falta muy grave contra la seguridad de los tratamientos y operaciones contratadas, pudiendo constituir quebranto de la buena fe contractual.

El Proveedor debe mantener un registro de incidentes de seguridad, al menos de los sistemas y activos que afectan a GRUPO PROSEGUR, conteniendo los incidentes producidos, el impacto, las fechas y tiempos de detección y solución del incidente, las personas que se han encargado de su gestión y las soluciones y medidas ejecutadas para resolverlo.

GRUPO PROSEGUR, puede solicitar el registro de incidencias que afecten a los sistemas y activos afectos al servicio y/o de su propiedad, cuando así se requiera, o bien solicitar un informe del seguimiento de eventos, incidencias e incidentes reportados y el Proveedor debe ponerlo a su disposición en un periodo razonable.

9. COMUNICACIONES

El Proveedor debe establecer todos los mecanismos necesarios para que las comunicaciones a través de redes públicas o redes inalámbricas de comunicaciones electrónicas estén cifradas.

En caso de aplicación, la conexión del CPD del Proveedor con los sistemas de GRUPO PROSEGUR solo se podrá llevar a cabo estableciendo las medidas de control que determine GRUPO PROSEGUR, tras un análisis detallado de las necesidades.

Las comunicaciones con el CPD de GRUPO PROSEGUR deben estar redundadas.

El Proveedor debe poner a disposición de GRUPO PROSEGUR, un mapa completo de la red de la prestadora del Servicio en el que se identifiquen todos los elementos de comunicaciones que intervengan, así como los elementos de seguridad.

El Proveedor debe contar con, al menos, las siguientes medidas de seguridad perimetral: Firewall, Sistemas de Detección y Prevención de Intrusos, (IDS/IDPS), Zona Desmilitarizada, (DMZ), Redes Privadas Virtuales, (VPN) y Proxy.

9.1. Seguridad en el uso del correo electrónico (En caso de aplicación)

Cuando el Proveedor realice envíos de correos en nombre de GRUPO PROSEGUR o con información que hace referencia a éste, debe cumplir las siguientes medidas:

- Las direcciones web, (URL) incluidas en los correos electrónicos y los contenidos de estos deben ser supervisados y aprobados previamente por el departamento de Seguridad de la Información de GRUPO PROSEGUR.

- El departamento de Seguridad de la Información de GRUPO PROSEGUR debe conocer los datos de GRUPO PROSEGUR que se van a incluir en los correos. Éstos no deben ser confidenciales ni secretos y este departamento determinará si deben ser asegurados y de qué modo.

- Seguridad de la Información de GRUPO PROSEGUR debe recibir:

    - El aviso previo del envío de los correos electrónicos.
    - Una breve explicación del contenido del correo electrónico.
    - Un ejemplo del correo electrónico/SMS que recibirán los clientes.
    - Conocer el buzón origen del envío del correo electrónico que recibirán los clientes.

- Deben quedar rastros y evidencias (logs) suficientes de cuándo y a quién se envían los correos desde el servidor de correos utilizado para el envío, tanto si se realiza en la infraestructura de GRUPO PROSEGUR como en la del Proveedor.

- En los registros de actividad (logs) debe quedar registrada la fecha y hora de envío, cuenta origen con la que se envía el correo y destinatarios del correo.

- Los correos deben incluir los avisos/recomendaciones acordadas con el departamento de Prevención Tecnológica del Fraude.

- Los correos deberán ser emitidos con un dominio registrado a nombre de GRUPO PROSEGUR.

- El Proveedor del Servicio, deberá arbitrar mecanismos de control sobre las listas negras de SPAM para controlar que los dominios de GRUPO PROSEGUR no aparezcan marcados como tal.

- Los correos enviados a clientes deben pasar los controles necesarios para estar libres de virus y para ello deberán explorarse con las herramientas de antivirus existentes en GRUPO PROSEGUR o, en caso de externalizarse, con las herramientas equivalentes y que operen en el Proveedor del Servicio.

10. GESTIÓN DE LA CAPACIDAD, DIMENSIONAMIENTO, ADQUISICION, OPERACIÓN Y MANTENIMIENTO DE SISTEMAS

El Proveedor debe gestionar la capacidad y recursos que afecten al servicio prestado estableciendo procesos de gestión de la plataforma, que contemplen la administración dinámica de los recursos en función de las en las necesidades y las obligaciones contractuales.

La adquisición de nuevos sistemas, equipos, componentes o software debe gestionarse teniendo en cuenta:

- Los riesgos asociados a cada actividad, servicio y sistemas.
- Deben ajustarse a los requisitos y arquitectura de seguridad establecidas para el servicio
- Las necesidades técnicas de los recursos.
- Los esfuerzos y medios económicos necesarios para su implantación.

El Proveedor debe establecer los controles de seguridad adecuados en relación con la adquisición y desarrollo de nuevas aplicaciones y/o nuevos sistemas, y en relación con los cambios que pudiera ser necesario realizar sobre las aplicaciones o sistemas involucrados en la externalización, durante la prestación del servicio.

Estos controles deben cubrir como mínimo, las autorizaciones, la realización de pruebas, las aprobaciones del usuario final y la existencia de entornos previos segregados respecto del entorno de producción.

10.1. **Uso y desarrollo de Software para la prestación del servicio. (En caso de aplicación)**

El Proveedor debe utilizar únicamente software licenciado, probado y autorizado por GRUPO PROSEGUR y el Proveedor, para el desarrollo del servicio externalizado.

Todos aquellos desarrollos que se realicen con el objeto de prestar servicios a GRUPO PROSEGUR serán autorizados por GRUPO PROSEGUR, debiendo el Proveedor:

- Abstenerse de almacenar datos de GRUPO PROSEGUR sin que GRUPO PROSEGUR lo conozca, autorice y/o audite.
- Realizar una revisión de seguridad del código fuente para cualquier software que no haya sido desarrollado por GRUPO PROSEGUR, de manera previa a su puesta en producción de acuerdo con los principios y buenas prácticas de desarrollo seguro.
- poner a disposición de GRUPO PROSEGUR todos aquellos desarrollos software hechos a medida, incluyendo código fuente, código objeto, manuales y cualquier otra información relevante para su administración y operación.
- Estar en disposición de realizar una evaluación del entorno de control, realizar pruebas de hacking ético o cualquier otra evaluación de seguridad con carácter previo a la puesta en producción de cualquier versión del sistema y en el momento que GRUPO PROSEGUR lo así lo requiera.
- Garantizar que los entornos diferentes a producción no contengan datos reales y que tengan implementados los mismos controles que el entorno productivo.
- Asegurar que los desarrollos realizados para la prestación de los Servicios a GRUPO PROSEGUR y las herramientas utilizadas para ello, cumplen con las leyes de propiedad intelectual y no vulneran ninguna legislación, normativa, contrato, derecho, interés legítimo o propiedad de terceros.
- Establecer los controles de seguridad adecuados en relación con la adquisición o desarrollo de nuevas aplicaciones o sistemas durante la prestación del Servicio. Estos controles deben cubrir como mínimo la realización de un análisis de viabilidad, verificación de autorizaciones, realización de pruebas, contar con las aprobaciones del usuario final y garantizar una separación adecuada de los entornos previos respecto del entorno de producción.
- Seguir las mejores prácticas de desarrollo de software seguro de acuerdo con los requerimientos del estándar, evitando la introducción de vulnerabilidades conocidas, en caso de que se desarrolle software.
- Situar los equipos de desarrollo del Proveedor dedicados a la prestación del servicio, en segmentos de red y entornos dedicados exclusivamente al desarrollo de aplicaciones, sin acceso a ambientes de producción ni a datos reales de GRUPO PROSEGUR.
- Establecer controles de seguridad adecuados en relación con la validación de integridad de los desarrollos en los entornos de producción.

11. REVISIONES DE CUMPLIMIENTO

11.1. Revisiones realizadas por GRUPO PROSEGUR

El Proveedor aceptará la realización de revisiones de cumplimiento de lo establecido en este anexo por parte de GRUPO PROSEGUR, o terceros designados por el Grupo, con carácter:

- Ordinario, como parte de la evaluación de la prestación del Servicio.
- Extraordinario, y siempre que se detecten eventos, incidencias o incidentes calificables de relevantes; o en caso de producirse alguna ampliación, modificación o reducción sustancial de los servicios o darse circunstancias que lleven a GRUPO PROSEGUR a considerar oportuno el realizarlas.

GRUPO PROSEGUR realizará estas revisiones con el alcance, seguimiento y periodicidad que se estime oportuno.

El Proveedor debe prestar cuanta colaboración sea necesaria para dar adecuado cumplimiento a los requerimientos de las revisiones que pudiera formularle GRUPO PROSEGUR o los terceros designados por GRUPO PROSEGUR y entregar a estos, cuanta documentación y/o evidencias le sean solicitadas a efectos de esta revisión.

Adicionalmente, GRUPO PROSEGUR puede ejercer el control sobre los riesgos tecnológicos asociados al Servicio, siendo el Proveedor responsable de proporcionar la siguiente información cuando le sea requerida:

- Revisión de informes de auditoría y/o certificaciones, por ejemplo, pero no limitadas a:
    - Informes de auditoría interna /control interno que les sean de aplicación en objeto o alcance.
    - Informes emitidos por terceros independientes. (SOC 2 tipo 2, ISAE 3402, SSAE 16, etc.).
    - Certificaciones de seguridad y continuidad de negocio. (ISO 27001, 22301 etc.).
    - Certificaciones de calidad del Servicio. (ISO 9001, ISO 2000, etc.).

Adicionalmente a los informes mencionados, GRUPO PROSEGUR deberá tener la capacidad e independencia para desarrollar un plan de evaluación de controles de riesgo tecnológico y ejecutarlo de acuerdo con los plazos, alcances y procedimientos que se acuerden con el Proveedor.

Este plan puede incluir, a modo de ejemplo, pero no limitativo, aspectos como los que se indican:

- Supervisión periódica de indicadores de seguridad del Servicio:
    - Los indicadores a supervisar acordados previamente a la firma del contrato y deberán revisarse periódicamente.
    - Acceso a cuadros de mando o consolas por parte de GRUPO PROSEGUR, que le permitan la monitorización continúa del riesgo tecnológico.
- Reporte de eventos relevantes por parte del Proveedor:
    - Eventos, incidencias o incidentes de seguridad.

  - Pruebas de recuperación ante desastres, contingencia tecnológica o de continuidad de negocio, totales o parciales.

- Información sobre la infraestructura tecnológica que da soporte a GRUPO PROSEGUR (en caso de que el Proveedor utilice infraestructura propia para la prestación del Servicio):
  - Arquitectura de red.
  - Arquitectura de seguridad perimetral.
  - Servidores y bases de datos.
  - Protocolos de red y comunicaciones.
  - Cualquier otro aspecto necesario para que GRUPO PROSEGUR pueda ejercer adecuadamente las funciones de control sobre el servicio o actividad prestada.
- Información de la monitorización realizada sobre los sistemas que prestan servicio a GRUPO PROSEGUR, así como el modelo de relación establecido para la comunicación de esta información cuando se considere necesario.

El Proveedor debe solventar las debilidades de control identificadas por GRUPO PROSEGUR en las revisiones realizadas, siguiendo los planes de acción acordados.

12. CONTROL INTERNO DEL PROVEEDOR

El Proveedor debe disponer de una función de control interno que velará por el cumplimiento con todos los controles requeridos por GRUPO PROSEGUR.

El Proveedor debe describir y colocar a disposición de GRUPO PROSEGUR, cuando así lo solicite, los procedimientos y controles que articulará internamente para asegurar que los requisitos enunciados se cumplen.

El Proveedor debe realizar todas aquellas auditorías legalmente exigibles, tanto de manera interna como externa, sobre aquellos sistemas involucrados en el servicio prestado a GRUPO PROSEGUR, dejando a disposición de GRUPO PROSEGUR los informes de auditoría generados.

El Proveedor debe realizar revisiones de seguridad sobre sus sistemas cuando se realicen cambios sustanciales en los sistemas de información, dejando a disposición de GRUPO PROSEGUR el informe de dicha revisión, y propondrá medidas correctoras.

12.1. Controles coordinados con GRUPO PROSEGUR

GRUPO PROSEGUR y el Proveedor acordarán los procedimientos para que todo incidente de seguridad sea comunicado diligentemente a GRUPO PROSEGUR. Se definirán protocolos de comunicación específicos para casos en los que se requiera una actuación inmediata por parte de GRUPO PROSEGUR para mitigar el impacto de incidentes de seguridad.

GRUPO PROSEGUR podrá verificar en cualquier momento el cumplimiento de los requisitos técnicos, tanto mediante visitas a las instalaciones del Proveedor, como haciendo uso de medios seguros de acceso remoto a los sistemas involucrados que se pactarán con el Proveedor.

Aquellos aspectos que se observen en estas revisiones y que GRUPO PROSEGUR considere una violación de los acuerdos establecidos o que puedan poner en riesgo los sistemas de GRUPO PROSEGUR serán notificadas al Proveedor, al que se dará un plazo razonable para su resolución.

13. DEVOLUCION DEL SERVICIO

GRUPO PROSEGUR y el Proveedor deben definir y acordar procedimientos de devolución del servicio de manera que se garantice un almacenamiento seguro de los soportes y en su caso, destrucción segura de la información utilizada por el Proveedor durante la prestación del Servicio.

14. DESTRUCCION DE LA INFORMACION

El Proveedor debe garantizar que se utilizan mecanismos de eliminación segura de información. Estos incluirán los casos de reciclaje de soportes y de final de Servicio.

Si la destrucción de la información la lleva a cabo un tercero, se debe comunicar a GRUPO PROSEGUR y disponer de un certificado de destrucción segura.

El Proveedor debe cumplir, en aquellos aspectos que sean de aplicación al servicio externalizado con las directrices proporcionadas en los estándares y prácticas internacionales aplicables.

Para los registros que cumplan con los requisitos legales de retención deben establecerse períodos de retención, y mantenerse adecuadamente, por el Proveedor. Además, GRUPO PROSEGUR puede proporcionar requisitos específicos de retención que el Proveedor aplicará, incluyendo, pero no limitado a, retención para litigio, propósitos legales o regulatorios.

El Proveedor debe asegurar que la destrucción de los sistemas y activos de GRUPO PROSEGUR que forman parte del servicio, se lleva a cabo de conformidad con el programa de gestión de registros del Proveedor.

Antes de que una estación de trabajo o un servidor sea reutilizado, desmantelado o devuelto al Proveedor de arrendamiento financiero, deben completarse las tareas de destrucción segura de la información que contengan, para que esta no pueda ser accedida o utilizada por terceros de forma no autorizada.

El Proveedor debe tener en cuenta y compensar el impacto de la eliminación en el medio ambiente.

15. MONITORIZACION

El Proveedor debe poner a disposición de GRUPO PROSEGUR cuando este así lo solicite, los procedimientos y controles que implementará para monitorizar y alertar sobre posibles violaciones de la seguridad de los sistemas.

El Proveedor debe implantar los mecanismos necesarios que permitan realizar un seguimiento sobre el software instalado en los equipos que prestan servicio a GRUPO PROSEGUR, de manera que

solamente pueda ser instalado el software imprescindible para la adecuada prestación del servicio, tanto si los sistemas son propiedad del usuario como si son propiedad de GRUPO PROSEGUR.

15.1. Custodia y explotación de los logs de seguridad.

En cuanto a los eventos que generen logs, se especificará por parte de GRUPO PROSEGUR el formato y contenido de los registros y el periodo de custodia. Si se solicita, estos logs deben estar disponibles en tiempo real, bien mediante acceso directo al sistema del Proveedor o mediante su recepción en repositorios internos de GRUPO PROSEGUR. Además, se deberá verificar que se genera trazabilidad en el resto de los sistemas involucrados indirectamente en el servicio o que hayan sido previamente analizados por GRUPO PROSEGUR.

El Proveedor debe generar logs, (acceso, autenticación, administración y actividad), como mínimo, de los siguientes eventos:

- Comunicaciones.
- Envío de ficheros, (sistemas involucrados en la transmisión, tanto en origen como en destino, y sistemas intermedios de almacenamiento temporal).
- Aplicaciones web.
- Sistemas de virtualización, (arquitectura cliente-servidor).
- Backend (servidores y aplicativos)

16. COPIAS DE RESPALDO Y RECUPERACION. (En caso de aplicación)

El Proveedor debe establecer y aplicar una política de realización de copias de respaldo que incluya los procedimientos de securización de las mismas y los procedimientos de prueba y recuperación de la información.

El Proveedor implementará controles para asegurar la correcta manipulación y transporte de los medios de almacenamiento de las copias de seguridad, asignando responsables, controles de accesos físicos y lógicos, cadena de custodia e inventarios periódicos, asegurando la confidencialidad de la información contenida.

El Proveedor debe implementar controles en su política de copias de respaldo que garanticen la recuperación de los datos en su estado original

El Proveedor debe establecer procedimientos para la realización, como mínimo, semanalmente de copias de respaldo, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

El Proveedor debe realizar copias de respaldo de sus sistemas de forma periódica que cumpla con lo establecido en los Tiempos Objetivos de Recuperación y el Punto Objetivo de Recuperación que deben estar incluidos en el Plan de Continuidad de Negocio y Recuperación ante desastre y que hayan sido acordados con GRUPO PROSEGUR.

El Proveedor debe localizar tanto los procedimientos de copias de respaldo y recuperación de datos como las mismas copias en un lugar diferente de aquel en el que se encuentren los sistemas de información.

El Proveedor debe almacenar como máximo una, (1) copia de seguridad completa e incrementales de los seis, (6) días posteriores en sus propias instalaciones, todas las copias que no estén en este margen, deben ser externalizadas.

La generación de copias o la reproducción de los documentos solo se podrá realizar bajo el control del personal indicado en el Documento de Seguridad, debiendo ser destruidas las copias desechadas de manera que sea inaccesible su información.

17. CONTINUIDAD DE NEGOCIO

El Proveedor dispondrá de un Plan de Continuidad de Negocio, así como de Planes Específicos de Recuperación ante Desastres TI, que le permitan recuperar el Servicio prestado a GRUPO PROSEGUR a un nivel preestablecido.

Los mismos, deberán estar formalmente documentados y serán probados anualmente o ante eventos, incidentes o cambios relevantes en el servicio, los aspectos normativos, la infraestructura, las personas o cualquiera de los activos afectos al servicio, pudiendo GRUPO PROSEGUR, acceder a la documentación y evidencias soporte necesarias para proceder a la verificación de estos con el fin de validar que se garantiza la disponibilidad del servicio prestado a GRUPO PROSEGUR.

Así mismo, el Proveedor debe formar parte de las pruebas que GRUPO PROSEGUR le solicite como parte de la Sistemática de Gestión de la Continuidad de Negocio del GRUPO PROSEGUR.

El Proveedor debe garantizar que todo el personal asignado a las labores de continuidad de negocio cuente con la suficiente experiencia, competencia y capacidad para desempeñar las funciones requeridas.

El Proveedor debe proporcionar de forma regular actualizaciones de la situación de la continuidad del servicio que presta a GRUPO PROSEGUR, en conformidad con las instrucciones que se le dispongan.

Si se diera una interrupción ante un evento de seguridad, el Proveedor asume la responsabilidad de reanudar los servicios prestados en los plazos y niveles de servicio que GRUPO PROSEGUR le marque en función de la criticidad de los sistemas afectados.

El Proveedor se considera responsable de la reanudación de los servicios en los plazos acordados y su no cumplimiento de forma injustificada puede acarrear consecuencias contractuales y sancionadoras.

Para los sistemas con mayor criticidad, puede requerirse que se reanuden las actividades en un plazo de 4 horas.

El Proveedor estará obligado a permitir que GRUPO PROSEGUR realice auditorías de su Plan de Continuidad de Negocio, (BCP) y del Plan de Recuperación ante Desastres, (DRP), que den servicio a los Activos de Información implicados en el servicio contratado.

18. GESTIÓN DE PROVEEDORES

El Proveedor debe garantizar que existen mecanismos de gestión de terceros subcontratados, cuando los servicios que proporcionen dependan de otros proveedores.

El Proveedor debe asegurar que su equipo de gestión de riesgos puede ejecutar operaciones coordinadas de respuesta a incidentes que incluya a proveedores de servicios externos que puedan afectar directa o indirectamente a las actividades, procesos y activos del Grupo Prosegur.

El Proveedor debe disponer de un proceso de selección y evaluación de proveedores en el que se evalúen los riesgos de la cadena de suministro. Los proveedores deben ser identificados, evaluados y priorizados como otros activos de la organización formando parte de los análisis de riesgos y de su tratamiento.

El Proveedor debe garantizar que en la firma de sus contratos de adquisición con terceros se identifican acuerdos de confidencialidad y acuerdos de nivel de servicio con los requisitos mínimos de seguridad, así como, otros contratos que reflejan las necesidades de la organización para proteger los sistemas y los datos del Grupo Prosegur. Estos contratos se deben revisar periódicamente y supervisar su cumplimiento.

El Proveedor debe asegurarse que tanto los terceros proveedores y subcontratas, como aquellos usuarios que tengan acceso a cualesquiera datos personales y otra información del Grupo Prosegur, con motivo del cumplimiento de su prestación laboral para la entidad, se comprometen y obligan a desarrollar sus funciones observando la máxima diligencia y especial buena fe en la custodia y tratamiento de estos.

El GRUPO PROSEGUR puede solicitar al Proveedor información o informes sobre las medidas y requisitos adoptados con un determinado proveedor.

El Proveedor será responsable frente a GRUPO PROSEGUR del incumplimiento por parte de las empresas subcontratadas involucradas en el servicio prestado o servicios prestados a GRUPO PROSEGUR en el caso de que las hubiese, de los requerimientos de descritos en este anexo.

El Proveedor debe determinar que se realiza una supervisión y auditorías periódicas de la prestación de servicios de terceros para verificar el cumplimiento de los acuerdos contractuales establecidos y concretamente de los requisitos establecidos en este documento.

El Proveedor debe garantizar especialmente el control de los cambios en los servicios por parte de los proveedores, teniendo en cuenta la importancia de la información, los sistemas y los procesos comerciales que están dentro del alcance del tercero.

El incumplimiento de cualquiera de las obligaciones contenidas en este anexo tanto de manera directa por parte del proveedor, como de manera indirecta por parte de las empresas subcontratadas por el mismo puede constituir una causa de resolución del contrato o tener otro tipo de consecuencias contractuales.

ANEXO V - USO DE RECURSOS INFORMÁTICOS Y SISTEMAS DE PROSEGUR

Medidas de Protección

En el caso de equipamiento informático suministrado por el Grupo Prosegur, el usuario debe cumplir con las medidas de protección que se indican a continuación:

Los equipos informáticos se deben utilizar únicamente para fines profesionales.

Queda prohibido el uso de aplicaciones y servicios web basados en servicios de streaming de audio o video, compra y venta de productos, redes sociales, noticias, deportes y en general, sitios no relacionados con la labor profesional.

Los usuarios deben guardar la información y los archivos que traten en el desempeño de sus funciones en las plataformas cloud de almacenamiento habilitadas y autorizadas por la organización (p.e onedrive) evitando guardarlos en los equipos de manera local.

Los usuarios se deben responsabilizar de que el equipamiento que le ha sido asignado no sea usado por terceras personas ajenas o no autorizadas para ello.

No se debe divulgar información sensible a terceros no autorizados, siendo especialmente cuidadosos con la información comunicada telefónicamente y en internet.

Los usuarios deben facilitar al personal técnico autorizado por Grupo Prosegur el acceso a sus equipos para realizar las labores de reparación, instalación o mantenimiento que pudieran darse.

Los usuarios deben proceder a la devolución de los recursos informáticos y/o de comunicaciones que le hubieran sido asignados por Grupo Prosegur, cuando cese su actividad en la organización.

De igual forma, cuando los medios informáticos o de comunicaciones proporcionados por el Grupo Prosegur estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados debe devolverlos inmediatamente a su unidad informática cuando finalice su vinculación con dicho puesto o función.

El usuario debe seguir las indicaciones e instrucciones para minimizar los riesgos derivados de las amenazas provocadas por malware prestando especial atención al uso de dispositivos extraíbles, correo electrónico, y software descargado de internet o desde fuentes desconocidas y/o ilegales.

Los sistemas en los que se detecte un uso inadecuado, o en los que no se cumplan los requisitos mínimos de seguridad, pueden ser bloqueados o suspendidos temporalmente por el Grupo Prosegur, restableciéndose el servicio cuando la causa de la amenaza o degradación desaparezca.

El usuario no debe vulnerar de ninguna forma los permisos de su cuenta, especialmente para instalar aplicaciones no relacionadas con sus funciones profesionales. En el caso de que el usuario precise la instalación de una aplicación específica para llevar a cabo sus funciones, debe realizar dicha petición a la Dirección de Tecnologías de la Información (en adelante DTI) a través del Service Portal.

No está permitido configurar en el dispositivo cuentas personales de servicios no definidos por Grupo Prosegur.

Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte de: páginas o contenidos ilegales inadecuados o que atenten contra la moral y las buenas costumbres; de los formatos de imágenes, sonidos o video; de virus y códigos maliciosos; en general, de todo tipo de programas y/o plug-in sin la expresa autorización de Grupo Prosegur.

El usuario es responsable de velar que los equipos que le han sido asignados se mantienen actualizados y con los correspondientes parches de seguridad.

Grupo Prosegur tiene la potestad de monitorizar la actividad en los equipos informáticos para verificar el buen uso que se hace de ellos, así como para prevenir y detectar incidentes de seguridad.

Queda prohibido el uso de dispositivos de almacenamiento extraíbles sin autorización previa.

Los puertos USB están desactivados por defecto, en caso de necesitarse su utilización, se debe solicitar al área de Seguridad de la Información y DTI, los cuales deben valorar la justificación de dicha solicitud.

En caso de autorizarse, el usuario es responsable de las acciones ejecutadas con la información extraídas o introducida en los recursos informáticos de Grupo Prosegur.

Los soportes de almacenamiento que se dispongan están destinados a un uso únicamente profesional.

La pérdida o sustracción de dichos soportes debe tratarse como un incidente de seguridad y ser notificada sin dilación.

Los soportes que vayan a ser reutilizados deben pasar previamente un proceso de borrado seguro en conformidad con las normas de Grupo Prosegur.

Los soportes que no vayan a reutilizarse deben ser destruidos por métodos seguros en conformidad con las normas de Grupo Prosegur

Devolución de equipos, dispositivos y soportes

En el caso de:

• Finalización del servicio para el cual se han destinado
• Finalización de la relación contractual del usuario con Grupo Prosegur.
• Obsolescencia de los equipos, dispositivos y/o soportes
• Averías en los equipos, dispositivos y/o soportes

Debe procederse a su devolución, enviando el dispositivo al área local correspondiente de microinformática a través de las vías dispuestas para ello con una solicitud indicando los motivos de la devolución:

En caso de finalización del proyecto: Se debe abrir una petición de servicio no catalogado en el Service Portal indicando, al menos, alguno los siguientes datos:

o Número de serie
o Hostname del equipo
o O útimo usuario que lo usó: EJ: ES00605432.

Una vez abierto el ticket, deben esperarse las instrucciones del departamento de Microinformática local para la devolución y recogida del equipo. En este supuesto, la reutilización del equipo del usuario que causa baja para entregarlo a la nueva incorporación debe validarse también por DTI por motivos de seguridad.

En caso de obsolescencia o avería: Debe abrirse un ticket en el Service Portal y seguir las instrucciones de devolución del equipo que indique el departamento de Microinformática local.

En cualquier caso, los equipos NO deben quedar en dependencias departamentales del negocio sin controles de seguridad física y lógica y tampoco deben usarse tras estar desconectados de la red durante un largo período de tiempo, ya que con ello se pone en peligro la seguridad en la compañía por posibles vulnerabilidades en los mismos.

Escritorio limpio y puesto de trabajo despejado

Es obligación de los usuarios llevar a cabo las siguientes medidas:

• Mantener el puesto de trabajo limpio y ordenado, sin más material encima de la mesa que el requerido para la actividad que se realiza en cada momento.

• En el momento que se finalice una tarea o función, el material debe retirarse a una zona segura en lugar cerrado, para ello, Grupo Prosegur puede asignar armarios y cajoneras con llave.

• Resguardar bajo llave la documentación y dispositivos de almacenamiento con información confidencial durante las ausencias prolongadas y al finalizar la jornada.

• No deben dejarse las llaves puestas en las cajoneras o armarios donde se guarda información confidencial.

• Debe tenerse precaución con la información que se muestra en las pantallas de los equipos siempre que se encuentre cerca de personal no autorizado para visualizar dicha información.

• Debe evitarse trabajar con información en papel. Las contraseñas y otra información de interés no deben encontrarse a la vista anotadas en papel o post-its.

• Comprobar que la documentación de apoyo a reuniones, presentaciones y demás eventos celebrados en las salas dispuestas a estos efectos, no permanece en ellas tras la finalización de los mismos.

• Imprimir siempre con la opción “Impresión protegida” activada, siendo necesario introducir una contraseña para que se lleve a cabo.

• En todas aquellas impresoras que dispongan de mecanismos de impresión segura con contraseña, el empleado debe asegurarse siempre de cerrar la sesión.

• Retirar inmediatamente de las impresoras, fotocopiadoras y faxes la información sensible asegurándose de que no queda documentación alguna en la bandeja de salida ni en la cola de impresión.

• Destruir todos los documentos desechados de manera que la información sensible no pueda ser legible o fácilmente recuperable. A estos efectos utilizar las destructoras de papel o contenedores dispuestos para tal fin.

• No deben dejarse desatendidos y a la vista tarjetas criptográficas que puedan ocasionar que personas no autorizadas accedan a la información y recursos de Grupo Prosegur.

Bloqueo del puesto de trabajo y las sesiones

Los usuarios de los sistemas tienen el deber de:

• Activar el protector de pantalla y el bloqueo del equipo cuando se deje desatendido el puesto de trabajo.

• Bloquear los equipos durante cualquier ausencia Utilizar los dispositivos que protegen físicamente los equipos portátiles, como los candados, siempre que se disponga de ellos.

• Comprobar que los equipos quedan apagados al finalizar la jornada laboral.

• Las imágenes que se visualicen tras el bloqueo de pantalla no deben poder incluir o revelar información confidencial.

• Cuando se vaya a dejar desatendido en ausencias prolongadas el puesto de trabajo, deben cerrarse las sesiones de aplicaciones y del sistema siempre que no se requiera su funcionamiento continuo por su funcionalidad.

• No modificar la configuración establecida para el bloqueo automático del equipo o el cierre automático de sesión mediante ningún método sin autorización previa.

Acceso a los sistemas de información

Credenciales de acceso

Los Usuarios son responsables de la custodia de las credenciales de acceso, certificados electrónicos de identificación y firma, así como el software u otros medios que les hayan sido asignados (por ejemplo, tarjetas criptográficas, tokens), para el acceso autorizado a los recursos y sistemas de Grupo Prosegur.

Los autenticadores son únicos para cada persona, intransferibles e independientes del recurso informático desde el que se realiza el acceso.

Utilización de Contraseñas

• Las contraseñas deben ser difíciles de adivinar.

• No deben utilizarse:
o Palabras de diccionario, jerga o dialecto.
o Palabras referentes al contexto de la organización o de las funciones de los usuarios.
o Palabras que contengan información personal como fecha de nacimiento, nombres de familiares, personas del entorno, números de teléfono, etc.…

• Los usuarios tienen la responsabilidad de la custodia y uso de las contraseñas.

• Las contraseñas deben conocerse solamente por el usuario que las utiliza. No deben comunicarse a ningún tercero, ni siquiera de la organización. Todas las contraseñas deben ser tratadas como información confidencial y de uso exclusivo por el usuario asignado. No se deben revelar las contraseñas por teléfono, incluso aunque le hablen en nombre de la DTI o de un superior jerárquico.

• No se deben transmitir las contraseñas mediante mensajes de correo electrónico ni a través de otro medio de comunicación electrónica.

• No se debe escribir ni reflejar la contraseña en un papel o documento donde quede constancia de esta. Tampoco se deben guardar en documentos de texto o notas dentro del propio ordenador o dispositivos móviles.

• Está prohibido utilizar las contraseñas usadas para las cuentas de recursos y servicios de Grupo Prosegur en aquellas cuentas que sean ajenas a la empresa y viceversa.

• El usuario tiene la obligación de cambiar las contraseñas cuando el sistema le notifique la necesidad del cambio con antelación a su expiración.

• Se debe cambiar inmediatamente la contraseña si se tiene algún indicio de que ésta ha sido vulnerada y notificarlo según el proceso establecido de comunicación de incidencias a la dirección seguridad.informacion@prosegur.com

• Queda prohibido el uso de mecanismos para recordar las contraseñas. Si se quiere hacer uso de herramientas como pueden ser los gestores de contraseñas, se necesita su previa homologación y validación por parte de Seguridad de la Información y DTI.

• No se debe comunicar la contraseña a nadie al encontrarse de vacaciones o periodos de ausencia prolongada.

• Si el usuario necesita cambiar la contraseña y el sistema ya no se lo permite o se ha suspendido la cuenta, debe comunicarlo como una incidencia al CAU a través del Service Portal y un administrador la restaurará verificando la identidad de forma previa.

Acceso Remoto

El acceso mediante VPN permite a los usuarios que se encuentran fuera de las instalaciones propias de Grupo Prosegur acceder a los recursos de información y de red estableciendo una conexión cifrada vía Internet.

En conformidad con lo anterior se establecen las siguientes directrices:

• El acceso remoto es concedido en base a las necesidades de las funciones que desempeñe cada usuario y en cualquier momento podrá ser retirado si se considera oportuno.

• El acceso remoto es concedido de forma previa por Grupo Prosegur a aquellos usuarios asignados o que justifiquen la necesidad de trabajar mediante esta vía.

• Queda prohibida la utilización de herramientas de acceso remoto distintas a las aprobadas por Grupo Prosegur.

• Los usuarios son responsables de resguardar sus credenciales de acceso remoto, evitar su difusión y garantizar su privacidad.

El usuario que hace uso de medidas para el acceso remoto debe velar por la seguridad física donde hará uso del acceso, como puede ser el domicilio, instalaciones de terceros, lugares de acceso público, etc.

• Los usuarios son los únicos responsables de las acciones realizadas sobre los recursos accedidos durante la sesión VPN.

• El acceso VPN a la red y a los recursos asociados tiene una finalidad puramente profesional, cualquier otro uso que se haga del mismo es considerado como indebido y la responsabilidad recae plenamente sobre el usuario.

• Los usuarios con acceso remoto que realicen tareas de soporte técnico, administración de equipos o desarrollo, no deben excederse en el uso de sus privilegios.

• El personal colaborador y terceros autorizados en el uso de la conexión remota tienen un acceso acotado para el desarrollo de sus funciones.

• Queda prohibido revelar a terceros o externalizar el contenido de cualquier información, secreta, confidencial o interna, de Grupo Prosegur accedida utilizando el servicio VPN.

• No están permitidas las conexiones paralelas cuando se está conectado vía acceso remoto.

• En la sesión de acceso remoto se permite el acceso a internet únicamente mediante el proxy de Grupo Prosegur.

• Queda prohibido que los usuarios se conecten a redes WI-FI públicas para la conexión a Internet necesaria para el acceso remoto. Aunque el flujo de información a través de la VPN se realiza de forma cifrada, este tipo de redes no cuentan con los mecanismos suficientes para garantizar la confidencialidad en la navegación web.

• El usuario debe cerrar las sesiones remotas con VPN cuando vayan a dejar de utilizarse para la función realizada o vaya a ausentarse de su lugar de trabajo.

• Grupo Prosegur puede monitorizar los accesos mediante conexión remota para prevenir ataques y detectar usos indebidos.

Acceso y Uso de Internet

• Debe realizarse un uso estrictamente profesional de Internet. Queda prohibido realizar usos con fines personales o recreativos.

• El acceso a Internet es concedido según las necesidades de las funciones que desempeñe cada empleado, y en cualquier momento puede ser retirado si Grupo Prosegur lo considerase oportuno.

• Los usuarios se comprometen a realizar un buen uso de Internet y son responsables de las sesiones iniciadas en Internet desde cualquier dispositivo.

• Está prohibido almacenar, revelar a terceros o externalizar el contenido de cualquier información propiedad de Grupo Prosegur, a través de cualquier medio en internet de acceso público o privado sin el consentimiento expreso de la compañía. Grupo Prosegur puede filtrar el contenido al que se puede acceder a través de Internet. Si un usuario justifica la necesidad del acceso a una dirección determinada, debe solicitarlo a través de su responsable para que éste lo solicite a la Dirección de TI (en adelante DTI).

• Grupo Prosegur puede monitorizar la actividad de los usuarios en Internet, así como registrar los accesos realizados.

• No deben visitarse páginas no fiables o sospechosas de contener contenido malicioso.

• En ningún caso está permitido modificar la configuración de los navegadores (opciones de internet) de los equipos ni la activación de servidores o puertos sin la autorización de DTI.

• Se prohíbe expresamente la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplan el código ético de Grupo Prosegur.

• Bajo ningún concepto se permite el uso y descarga de archivos P2P o similares.

• Antes de utilizar una información obtenida de Internet, los usuarios deben comprobar en qué medida se halla sujeta a los derechos derivados de la Propiedad Intelectual o Industrial, y/o pudiera vulnerar la normativa de aplicación en materia de protección de datos personales.

• Cuando se realicen intercambios de información o transacciones se debe acceder a las páginas web escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Cuando la página web se encuentre autenticada mediante certificado digital, el usuario debe verificar su autenticidad.

• Se debe comprobar la seguridad de la conexión asegurándose de su cifrado entre otras verificando que se utiliza el Protocolo HTTPS en la comunicación.

• El usuario debe borrar de forma periódica la información almacenada en los navegadores: cookies, historial, contraseñas…, etc.

• Se prohíbe la instalación de complementos y plug-ins no autorizados previamente por Grupo Prosegur.

• Queda prohibido el uso de herramientas de cualquier modalidad en la nube no autorizadas previamente por Grupo Prosegur, como por ejemplo para almacenar o compartir información.

• Queda vedado el uso de acceso a internet para participar en debates en tiempo real (canales de chat/IRC) ya sea mediante páginas web que brinden el servicio como de aplicaciones instaladas en los equipos (como MS Messenger, TOM, Yahoo, ICQ o similares).

• No se encuentra permitido la utilización de cualquier otro medio de acceso a Internet (por ejemplo, módems) que no hayan sido autorizados por el área de DTI.

• Se prohíbe el uso de Internet para propósitos que puedan influir negativamente en la imagen de Grupo Prosegur, de sus representantes o los terceros con los que mantiene relación.

Uso del Correo Electrónico

El correo electrónico es una herramienta que Grupo Prosegur habilita para aquellas comunicaciones requeridas como consecuencia del desarrollo de la actividad propia de la empresa con otras entidades o con otros usuarios. Se establecen las siguientes directrices en lo referente al uso del correo electrónico:

• El acceso y uso de estos servicios por parte de los usuarios, así como los privilegios asociados a dicho acceso, deben limitarse a los establecidos por sus obligaciones profesionales.

• Todas las cuentas de correo electrónico que existen en el servicio de correo son propiedad de Grupo Prosegur.

• Los usuarios deben únicamente utilizar las herramientas y programas de correo electrónico suministrados, instalados y configurados por el Grupo Prosegur.

• En el caso de personal externo, el uso de direcciones externas debe ser aprobado previamente por Grupo Prosegur.

• La cuenta de correo electrónico es personal e intransferible.

• Los usuarios son los únicos responsables de todas las actividades realizadas desde sus cuentas de correo electrónico.

• Los usuarios son responsables de resguardar sus credenciales de acceso al correo.

• La forma y contenidos de los correos enviados por el usuario deben estar alineados con el código de conducta de Grupo Prosegur, y en ningún caso se deben enviar correos ofensivos, amenazantes o de mal gusto.

• Cuando exista la necesidad de enviar correos a más de un destinatario se debe utilizar el campo “Con Copia Oculta (CCO)” para mantener la privacidad de los correos electrónicos de los destinatarios.

• El buzón de correo electrónico tiene una capacidad limitada. Cuando se alcance la cuota asignada, el sistema informa de esta situación al usuario, quien debe liberar espacio eliminando aquellos correos que no sean necesarios para el desempeño de sus funciones.

• El usuario debe vaciar la papelera de reciclaje diariamente, ya que los correos que contiene se incluyen dentro de la cuota asignada a cada buzón.

• El usuario debe mantener ordenados y clasificados todos sus buzones y carpetas. Los correos inservibles deben ser eliminados de forma definitiva.

• Los archivos adjuntos de elevado tamaño de bytes se deben comprimir antes de ser enviados.

• Se debe revisar la barra de direcciones antes de enviar un mensaje y responder únicamente a quien corresponda.

• En la medida de lo posible, en lugar de compartir documentos por correo electrónico, se debe indicar un enlace al recurso.

• Cuando se envíe información crítica o sensible, el mensaje debe ir cifrado. Si se conecta vía web, al finalizar la actividad se debe cerrar sesión.

• El correo electrónico es uno de los medios principales de entrada de programas maliciosos en ordenadores y sistemas. Por ello se establecen las siguientes normas:

o Nunca se debe pulsar en enlaces de correo o abrir archivos adjuntos a menos que se verifique la autenticidad y fiabilidad del correo y del contenido.
o No se debe responder a correo no solicitado o de origen desconocido, sobre todo si estos contuvieran ficheros adjuntos. Este tipo de mensajes deben ser eliminados inmediatamente.
o Los correos que incluyan archivos adjuntos con extensiones no permitidas (.exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta) o con extensiones aceptables que enmascaren las no permitidas, deben ser eliminados inmediatamente. En ningún caso se debe abrir correos que contengan este tipo de archivos adjuntos.
o Queda prohíbo el registro en servicios y páginas de internet con las cuentas de correo profesionales excepto en servicios autorizados.
o Cuando se reenvie o responda un correo, se debe eliminar toda la información irrelevante, tal como direcciones, firmas, cabeceras, etc.
o Debe desactivarse la vista previa para la bandeja de entrada.

• Todas las cuentas de correo genéricas y listas de distribución tienen un responsable asociado que debe cumplir las siguientes normas:
o Hacer uso del buzón o lista de distribución exclusivamente para el fin por el cual fue creado (atención a clientes, respuesta a peticiones, etc.).
o Se recomienda incluir una firma corporativa cuando se envían correos desde este tipo de cuentas.
o Autorizar de forma responsable el acceso y uso de estas cuentas.
o Proteger la reputación e imagen de Grupo Prosegur manteniendo un tono cordial en sus respuestas.
o Verificar al menos 2 veces al año que las personas que han sido autorizadas siguen siendo válidas.

• Cualquier hecho sospechoso se debe notificar al área Corporativa de Seguridad de la Información para tomar las acciones necesarias. Grupo Prosegur ha establecido un botón en las aplicaciones de correo “Reportar correo electrónico” para facilitar esta tarea.
• Grupo Prosegur puede monitorizar las cuentas de correo que pone a servicio de sus empleados, sin notificación previa, a fin de velar por el correcto uso y aprovechamiento de este recurso, así como detectar posibles incidentes de seguridad.

Usos Prohibidos

• Utilizar el correo electrónico con fines comerciales ajenos a la compañía. Participar en la propagación de “cartas en cadena”, esquemas piramidales, etc.

• Crear listas de distribución sin el consentimiento de DTI.

• Distribuir de forma masiva mensajes con contenidos inapropiados que atenten con el buen funcionamiento de los servicios en Internet.

• Enviar o reenviar mensajes con contenido difamatorio, ofensivo u obsceno.

• Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.

• Enviar correos SPAM de cualquier índole (Se consideran correos SPAM aquellos no relacionados con los procesos de trabajo).

• No se permite enviar archivos adjuntos con extensión .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta debido a que este tipo de archivos permiten enmascarar virus y éstos suelen ser utilizados para su propagación.

• La difusión de contenido ilegal; como por ejemplo amenazas, código malicioso, apología del terrorismo, pornografía infantil, software ilegal, o de cualquier otra naturaleza delictiva.

Almacenamiento Compartido

Los recursos de almacenamiento compartido son espacios dedicados para contener y compartir los documentos y archivos desarrollados como resultado de la actividad profesional entre los miembros de un grupo de trabajo.

Todos los usuarios con acceso a recursos de almacenamiento compartido deben cumplir las normas establecidas a continuación:

• El acceso y uso a los recursos de almacenamiento compartido por parte de los usuarios, así como los privilegios asociados a dicho acceso, deben limitarse a los necesarios para realizar sus funciones (cumpliendo el precepto “necesidad de conocer”).

• En ningún caso se permite el almacenamiento de información personal en los recursos de almacenamiento compartido.

• Queda prohibido el almacenamiento de ficheros ejecutables o instalables (.exe) en los recursos de almacenamiento compartido sin el control de DTI.

• No está permitida la solicitud de un recurso de almacenamiento compartido para el uso exclusivo de una persona.

• El respaldo y recuperación de la información contenida en los recursos de almacenamiento compartido es tarea exclusiva de DTI.

• Todos los recursos de almacenamiento compartido tienen un responsable asignado que es la persona en la que se delega la autorización de acceso al mismo. Este responsable debe revisar como mínimo cada 6 meses los permisos de acceso a dicho recurso de almacenamiento compartido. El uso del espacio asignado en el recurso de almacenamiento es responsabilidad de todas las personas autorizadas.

• En el caso de que se requiera mantener información histórica, DTI puede proporcionar un medio de almacenamiento alternativo y que garantice el archivo de la información.

• Para el almacenamiento de datos de carácter personal en los recursos de almacenamiento compartido se deben desplegar las medidas técnicas y de controles necesarios que garanticen el cumplimiento de la legislación aplicable en esta materia.

Uso de certificados y firma electrónica

• Es posible que, como parte de las actividades en Grupo Prosegur, el usuario utilice certificados y firma electrónica. El usuario debe:
o Conocer y cumplir las condiciones de utilización de los certificados previstas en la normativa de Grupo Prosegur, así como las limitaciones de su uso según la legislación aplicable.
o Actuar con diligencia respecto de la custodia y conservación de los datos de firma o certificado o cualquier otra información sensible como claves, códigos de solicitud del certificado, contraseñas, etc. incluyendo los soportes de los certificados o los equipos en los que se encuentren.
o NO debe revelar bajo ningún concepto los datos mencionados.
o Solicitar la revocación del certificado en caso de sospecha de pérdida de la confidencialidad, divulgación o uso no autorizado de los datos notificando a Seguridad de la Información por los métodos establecidos.

• En cualquier caso, el usuario se hace responsable del uso que pueda dar a dichos certificados y de su custodia segura, en caso contrario, podría dar lugar a la activación del proceso sancionador aplicable.

Gestión de Incidentes de Seguridad

Cuando un usuario detecte cualquier tipo de anomalía o incidencia de seguridad que pueda comprometer la seguridad, el buen uso y/o funcionamiento de los recursos informáticos o de los sistemas de información a los que tenga acceso, así como de la información y de los datos personales contenidos en los mismos, está obligado a informar al Área de Seguridad de la Información inmediatamente para que se tomen las medidas necesarias documentando la notificación con las pruebas y documentos de que se disponga.

• Se debe notificar a través de las siguientes vías:
o Por correo electrónico al departamento de Seguridad de la Información:
seguridad.informacion@prosegur.com

• El usuario está obligado a cooperar con Grupo Prosegur en la investigación y mitigación del incidente y si fuera necesario a tal fin debe entregar el recurso informático afectado o, en su caso, debe permitir el acceso al mismo de manera remota para que el personal técnico del Grupo Prosegur realice las comprobaciones pertinentes y verifique si puede seguir usando el recurso con seguridad.

DECLARACIÓN DEL USUARIO SOBRE EL USO DE LOS RECURSOS INFORMÁTICOS Y SISTEMAS DE PROSEGUR

El usuario declara:

• Que es responsabilidad del usuario proteger y utilizar los recursos y las herramientas asignadas de manera responsable y siempre teniendo presente los objetivos profesionales fijados.

• Que es responsabilidad del usuario hacer un buen uso de los recursos y dispositivos propiedad de Grupo Prosegur, utilizándolos para las funciones para las que se han asignado, respetando su integridad y utilizándose solo por la persona asignada como responsable de los mismos.

• Que es responsabilidad del usuario leer, entender y actuar en conformidad con todas las demás normas y documentos de Seguridad de la Información, así como cualquier otra que se le disponga desde la Dirección General de Grupo Prosegur.

• Que el usuario debe poner en conocimiento del Área Corporativa de Seguridad de la Información cualquier incidente, anomalía o sospecha, desde el punto de vista de seguridad de la información, que consideren relevante y que pudiera afectar a Grupo Prosegur.

• Que la información almacenada en los dispositivos y equipos es propiedad de Grupo Prosegur, y está sujeta a auditoría. Los equipos deben de ser de vueltos a Grupo Prosegur a petición de este en cualquier momento.

• Que, en el desarrollo de sus funciones, cuando el usuario gestione recursos de un Cliente, puede estar sujeto, asimismo, a la Política de Seguridad y las normas de seguridad que hubiera aprobado el Cliente si este así lo exige, sin perjuicio de la obligación de seguir cumpliendo con lo dispuesto en las normas de Grupo Prosegur.

• Que el incumplimiento de las normas y las directrices anteriores da lugar a las medidas legales a las que Grupo Prosegur pueda acogerse para la preservación de sus derechos en función de la legislación y los convenios que sean aplicables.

DECLARO HABER LEÍDO LA PRESENTE Y TENER CONOCIMIENTO ACERCA DE LAS NORMAS DE USO DE LOS RECURSOS INFORMÁTICOS DE PROSEGUR AQUÍ ESTABLECIDAS. _____, _____ de _____ de _____

Nombre

Documento de Identidad

Firma