CONDICIONES GENERALES DE COMPRA

Estas Condiciones Generales son suscritas entre BT Global ICT Business Spain S.L.U, empresa constituida en España con CIF número B- 88625496 y con domicilio social en C/ María Tubau, 3; 28050 Madrid ("BT") y el Proveedor cuyos datos se incluyen en el párrafo de la firma (cada uno individualmente es la "Parte" y juntos las "Partes"). Cada Parte acepta estas Condiciones Generales de Compra.

1. Objeto y ámbito de aplicación

1.1 Las presentes Condiciones Generales de Compra (en adelante "CGC") tienen por objeto establecer un marco jurídico general de derechos y obligaciones entre las partes, siendo de aplicación a todos los Pedidos otorgados, adjudicados y emitidos por BT para la entrega de bienes, la adquisición de servicios o las ejecuciones de obras.

1.2 La contratación de servicios por parte de BT podrá hacerse bien mediante la firma de un contrato o a través de un Pedido. En determinados supuestos se utilizarán estas dos formas simultáneamente, firmándose en primer lugar un contrato y con posterioridad se emitirán Pedidos sobre ese contrato.

1.3 Con independencia de que telefónicamente se lleve a cabo el anticipo de la solicitud de suministro de servicios o entrega de bienes, BT efectuará los Pedidos por escrito y los remitirá al Proveedor mediante fax, correo ordinario, correo certificado o correo electrónico. Todo Proveedor de BT deberá tener correo electrónico o número de fax, y haberlo comunicado previamente a BT.

1.4 Salvo derogaciones generales o particulares expresamente reflejadas en Anexos a las presentes CGC o lo dispuesto en el Pedido que, en su caso, ambas partes puedan suscribir, estas CGC son de aplicación exclusiva a las relaciones comerciales entre BT y el Proveedor, considerándose de rango superior a cualesquiera otras contrarias del Proveedor que las contradigan.

1.5 El Proveedor acepta que los trabajos o servicios realizados por el mismo en ejecución de Pedidos previamente a la aceptación de las presenten condiciones generales, se sujeten a las mismas, desde la fecha en que se realizaron y en su integridad.

1.6 Única y exclusivamente podrán modificar o completar las presentes CGC, las condiciones del Proveedor que hayan sido expresamente aceptadas por escrito por BT e incorporadas al presente documento como Anexo o Condiciones Particulares.

2. Condiciones de pago. Facturación

2.1 El pago de los servicios prestados por el Proveedor se llevará a cabo a los sesenta (60) días de la fecha de recepción de la factura, mediante transferencia bancaria en la cuenta designada por el Proveedor en el correspondiente Pedido.

2.2 La factura correctamente emitida deberá ser enviada conjuntamente en formato electrónico a facturas@BT.com y en papel a BT, Atención: Cuentas a pagar, C/ María Tubau, 3, 28050 Madrid

2.3 En las facturas deberá figurar el domicilio del Proveedor, el NIF, la fecha, el número del Pedido y la descripción de los servicios realizados, así como cualesquiera otras menciones exigidas por la normativa aplicable.

2.4 Las facturas que no cumplan lo establecido en los apartados anteriores serán devueltas al Proveedor, notificándose la fecha de devolución y la causa de la misma, sin que por ello BT incurra en mora en el pago.

2.5 Los precios contenidos en cada Pedido o en sus Anexos son cerrados y definitivos. En el supuesto de que el precio esté estipulado en una divisa extranjera, se pagará en esa divisa. No obstante, si las prestaciones fueran periódicas, BT sólo se hará cargo de las fluctuaciones respecto del tipo de cambio existente a la firma del Pedido que no excedan del 5% de dicho tipo de cambio, minorándose el precio en proporción al quebranto sufrido por BT.

2.6 El devengo del precio que BT deberá pagar al Proveedor de conformidad con lo establecido en esta condición, tendrá lugar el último día de cada mes para las mercancías entregadas en ese mes o para los servicios efectivamente prestados durante ese mes.

2.7 El Proveedor será responsable de cualquier diferencia en fletes, portes u otros gastos originados en la entrega de la mercancía objeto del Pedido, sin que quepa repercusión alguna de los mismos a BT, salvo pacto por escrito en contrario.

3. Cargos e Impuestos.

3.1 Todos los impuestos, tasas y cualquier otro tipo de exacción fiscal serán a cargo del Proveedor, ya sean directos o indirectos, excepto el IVA que será por cuenta de BT. En caso de aparición de nuevos impuestos, se pagarán por la parte a quién corresponda de acuerdo con lo que determine la ley.

3.2 Si a lo largo de la duración del Contrato ocurriesen cambios en el mercado que afecten a cualquiera de los servicios que el Proveedor presta al amparo del mismo, BT podrá requerir una revisión de los precios en caso de que se detecten importantes desviaciones de precios que produzcan a BT una pérdida significativa de competitividad.

3.3 Se entiende que existe pérdida significativa de competitividad, cuando BT presente una o más ofertas independientes (no se considerarán ofertas independientes aquellas en las que participe un mismo operador, parcial o totalmente, directamente), o información pública sobre precios, formuladas o elaboradas, por empresas con entidad y autorización para prestar los Servicios que cubran todos los servicios objeto del mismo y de las que resulte un precio total inferior al menos en un 5% por 100 al establecido en el Contrato.

3.4 Al objeto de verificar que las circunstancias anteriores se dan, y sólo para el caso de existir discrepancias a la hora de verificar el criterio de BT, cualquiera de las partes podrá someter la cuestión, a un auditor, bajo los siguientes principios:

a. El que solicite al auditor deberá pagarlo.

b. El auditor deberá ser persona de reconocido prestigio en el mercado.

c. El auditor emitirá dictamen a instancias de la parte solicitante en un plazo no superior a 30 días.

d. El auditor deberá dictaminar si las ofertas o la información presentadas, se refieren a la globalidad de los servicios contratados por BT y si los precios ofertados se encuentran entre los que correspondan a ese mercado en ese momento.

e. Las Partes se obligan a cumplir y actuar en consecuencia con el dictamen del auditor independiente. A cuyo efecto, en el plazo de quince días desde la comunicación escrita del

auditor a las partes dictaminando la conformidad de las ofertas con los criterios establecidos en la presente cláusula, si el Proveedor no igualara las ofertas presentadas, BT tendrá derecho a dar por vencido anticipadamente el Contrato mediante la mera comunicación por escrito al Proveedor, sin que éste tenga derecho a indemnización o cantidad alguna por tal concepto, poniendo de manifiesto dichas circunstancias con un preaviso de quince días de antelación.

3.5 El Proveedor será el único responsable de cualquier pagos, sanción, retención y pagos a cuenta que le sean imputables en relación con sus trabajadores, frente a empresas de seguros, Hacienda, Seguridad Social, Ministerio de Trabajo y similares; así como del cumplimiento de todas las contribuciones fiscales y de la Seguridad Social (empleador y empleado) y cualquier gravamen sobre ingresos (según corresponda) o los salarios de su personal (los cuales en ningún caso serán considerados como empleados de BT) o de sus posibles subcontratistas (como una empresa de servicios personales) y se compromete a trasladar estos compromisos a sus subcontratistas.

3.6 El Proveedor indemnizará a BT por cualquier reclamación de daños y perjuicios o de cualquier otro tipo, y/o por cualquier denuncia que pueda recibir solidaria, subsidiariamente o mediante el ejercicio de cualquier acción directa o indirecta, en relación con los empleados del Proveedor, incluyendo y sin que constituya limitación, pagos a la Seguridad Social, indemnizaciones por despido, cantidades pagadas en acuerdos extrajudiciales laborales o cualquier otro pago de cantidad, sanción, impuesto o por cualquier otro concepto que le pudiera ser requerido a BT, como consecuencia del incumplimiento por parte del Proveedor de las obligaciones establecidas en la presente cláusula o en la siguiente. A estos efectos, y sin perjuicio de la resolución del contrato en virtud de lo establecido en la cláusula 10.1.B) del presente contrato, BT podrá retener todos los pagos al Proveedor que por cualquier concepto se encuentren pendientes de pago en cuantía suficiente para cubrir dichas responsabilidades.

4. Entrega de productos y servicios.

4.1 El Proveedor se compromete a entregar los bienes y/o servicios contemplados en un Pedido en la fechas de entrega indicados en el mismo y en la dirección reflejada en éste. En el precio de los bienes y/o servicios se incluirán todos los gastos directa o indirectamente relacionados con los bienes, la mercancía o el servicio hasta ese punto de entrega. Las mercancías serán transportadas a riesgo y ventura del Proveedor. La transmisión del riesgo se efectuará a la aceptación de las mercancías o los servicios. Cada paquete en el que se envíe la mercancía, deberá indicar claramente la dirección de entrega, así como el número de Pedido.

4.2 La verificación y la recepción de las mercancías será efectuada después de la entrega. La recepción inicial por BT debe entenderse como una recepción provisional. El Proveedor no considerará por tanto el acuse de recibo de BT, o la firma de BT como la aceptación definitiva. La recepción definitiva (incluyendo los test de control de calidad o cualesquiera otras pruebas que BT lleve a cabo), en su caso, se efectuará en un plazo máximo de 30 días a contar desde la fecha de recepción provisional. La fecha de recepción definitiva será la que se tenga en cuenta a efectos del inicio del período de la garantía aplicable a la mercancía o los servicios.

4.3 La transmisión de la propiedad de las mercancías se producirá una vez estén entregadas y aceptadas definitivamente en el lugar de entrega mencionado en la condición 4.1 anterior.

5. Período de Garantía.

5.1 El Proveedor garantiza a BT que los materiales, equipos o servicios de cualquier naturaleza, suministrados bajo un Pedido están libres de defectos, son conformes a las especificaciones,

planos, muestras o descripciones establecidas que les sean aplicables, son adecuados para el fin al que se destinan, son nuevos y de primera calidad.

5.2 El Proveedor es responsable de los vicios aparentes u ocultos de todas las mercancías y los servicios entregados, incluyendo cualquier parte cuya fabricación o realización se haya encargado total o parcialmente a un tercero. El Proveedor indemnizará a BT de una manera plena contra todo daño, perjuicio y reclamación o acción de cualquier tipo que BT sufra sin que sea aplicable ningún tipo de exclusión o limitación de responsabilidad a este respecto.

5.3 El Proveedor garantiza los bienes entregados que sean objeto del Pedido o los servicios prestados bajo dicho Pedido por un período mínimo de veinticuatro (24) meses desde su aceptación definitiva por BT. BT podría proceder por sí misma o por medio de terceros a la realización de los trabajos necesarios para subsanar faltas o defectos, pudiendo deducir de los pagos pendientes los gastos que se deriven, si el Proveedor no lo hiciere diligentemente.

5.4 El Proveedor garantizará el Software por un periodo de 1 año, desde el momento en que BT lo comience a utilizar.

5.5 El Proveedor llevará a cabo todas las acciones necesarias para informar y mantener informado a BT sin demora, de todos los defectos de fabricación, reales o sospechados, de los que tenga conocimiento, de manera que se puedan evitar posibles daños y perjuicios.

5.6 Las piezas, materiales y servicios que aparezcan como defectuosos durante el periodo de garantía serán inmediatamente remplazados a cargo del Proveedor en condiciones idénticas a las iniciales. El Proveedor, no obstante, podrá recuperar las piezas y materiales defectuosos. Las piezas y materiales reemplazados tendrán el mismo periodo de garantía que las inicialmente suministradas, comenzando la garantía en el momento del reemplazo.

5.7 Sin perjuicio de cualquier otro derecho o acción que BT pueda ejercitar, el Proveedor se compromete a mantener indemne a BT y a indemnizarle por cualquier responsabilidad derivada de o relacionadas con cualquier demanda interpuesta en virtud de la normativa laboral o de seguridad social por Personal del Proveedor en relación con los Servicios o la terminación de este Contrato o cualquier pedido o por el cese en la prestación de los servicios (o parte de los mismos), incluyendo, entre otros, cualquier reclamación, demanda de relación laboral o derechos relacionados, o cualquier reclamación por discriminación de cualquier tipo.

6. Derecho de Auditoria.

6.1 El Proveedor garantizará que cualquier Subcontratista otorgue a BT (y a sus representantes) el derecho de acceso a cualquier sitio, registro, documento o información referida al personal, sistemas, instalaciones, equipos, software o cualquier otro dato que pudiese resultar relevante, del Proveedor o de su Subcontratista:

a. en cualquier momento durante el curso del Contrato y por un período posterior de 12 meses luego de su terminación o vencimiento; para auditar el cumplimiento por parte Proveedor de sus obligaciones contractuales, como así también de los cargos e impuestos cobrados a BT; y

b. en cualquier momento durante la vigencia del Contrato y por un período posterior 6 años a partir de su terminación o vencimiento, para cumplir con cualquier solicitud, requisito u obligación solicitada por cualquier Autoridad Administrativa o devengados de la Ley.

6.2 Cada Parte asumirá sus propios costos de participación en cualquiera de dichas auditorías.

7. Normativa y Políticas de Obligado Cumplimiento.

7.1 El Proveedor deberá cumplir todas las leyes y disposiciones aplicables tanto al Pedido desde su formalización, como al material, elementos y/o servicios que constituyen su objeto.

7.2 El Proveedor procurará y garantizará que el Personal de su Proveedor cumpla con todas las Leyes aplicables en el cumplimiento de las obligaciones del Proveedor en virtud del Contrato.

7.3 El Proveedor deberá, y procurará que todo su Personal, cumpla con las Política disponibles actualmente en la URL https://groupextranet.bt.com/selling2bt/articles/side/our_privacy_policy.html. BT comunicará los cambios de URL al Proveedor. Dicho cumplimiento se acomodará a los siguientes principios:

a. cuando en dichas políticas se indique que BT debe cumplir con alguna previsión u obligación, el Proveedor cumplirá y procurará que todo su Personal cumpla con dicha Política como hubiera sido adoptada por el propio Proveedor;

b. en caso de modificación de la Política de BT se le otorgará al Proveedor un período razonable a partir de la notificación (o cualquier otro período especificado en el Política) para que pueda cumplir con la Política modificada; y

c. no se considerará que el Proveedor infringe esta Cláusula 7 cuando pueda demostrar que su desempeño en relación con el Contrato cumple con sus propias políticas, siempre que dichas políticas no sean menos estrictas que las Políticas relevantes.

8. Seguridad del Personal del Proveedor.

8.1 Cuando se presta el Servicio en las propias instalaciones de BT, tanto el Proveedor como el personal bajo su dependencia asignado a la prestación de los Servicios, se comprometen a ajustarse a las normas internas de organización, seguridad y funcionamiento de las oficinas e instalaciones de BT. A tal efecto, BT tendrá informado en todo momento al Proveedor de las normas internas de organización, seguridad y funcionamiento aplicables en sus oficinas e instalaciones, quien, a su vez, se obliga a tener informado de las mismas en todo momento a su Personal.

8.2 Durante la vigencia del contrato, el Proveedor se compromete a cumplir la ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, y su normativa de desarrollo, en lo que respecta al Personal asignado a la prestación del Servicio. Con este motivo presentará una política preventiva adecuada a los riesgos del Personal asignado a la prestación del Servicio, que mantendrá actualizada durante la vigente del Contrato. Siempre que haga modificaciones deberá ponerlo en conocimiento de BT. El Proveedor se compromete igualmente a dar información y formación a sus empleados antes de que ocupen los puestos para los que son contratados. Las partes acuerdan coordinar sus políticas de salud y seguridad.

8.3 Durante la vigencia del presente contrato y para cumplir con lo dispuesto en la ley mencionada en el punto 8.2 anterior, el Proveedor se compromete, de forma previa a la firma del contrato, a acreditar documentalmente en la herramienta Web designada por BT a estos efectos:

a. Su política preventiva en función de los riesgos a los que se encuentren expuestos sus empleados. Esta política deberá incluir un sistema de vigilancia de la salud, de conformidad con lo dispuesto en el artículo 22 de la ley 31/ 1995 de Prevención de Riesgos Laborales y en el artículo 37.3 del R. D. 39/1997, Reglamento de los Servicio de Prevención.

b. La información y formación dada por escrito a los empleados del Proveedor que presten sus servicios en BT relativas a la existencia de los riesgos generales y del puesto, de su política preventiva y de la obligación de conocerla y cumplirla.

c. La mutua de accidentes de trabajo y enfermedad profesional a la que esté asociada el Proveedor y has cuando, debiendo informar del cambio de mutua si se produce durante la duración del contrato o Pedido.

d. Cualquier documentación preceptiva para el desempeño del Servicio objeto de este contrato.

e. Cualquier accidente que sufra uno de los trabajadores durante la prestación de los servicios objeto del Pedido o durante la entrega de cualquier bien.

8.4 Si los servicios prestados requieren de la presencia física de sus empleados en cualquiera de las instalaciones de BT o de sus clientes, en cumplimiento de la ley de Prevención de Riesgos Laborales, el Proveedor deberá:

a. acreditarse documentalmente en la herramienta Web designada por BT.

b. mantener la documentación que se requiere en la anterior herramienta actualizada en todo momento, incluyendo tanto la documentación de empresa, como la de los trabajadores que prestarán el Servicio así como cualquier documentación preceptiva para el desempeño del Servicio a prestar.

c. informar a BT a través del coordinador del servicio de cualquier accidente y/o enfermedad profesional que sufra uno de sus trabajadores durante la realización del Servicio y de registrar la información relativa a dicho accidente y/o enfermedad profesional, enviando la información por mail a servicio.de.prevencion@bt.com.

8.5 La solicitud de alta en la herramienta Web, se realizará a través del envío de un correo electrónico a servicio.de.prevencion@bt.com. Posteriormente se enviará un usuario y contraseña para poder acceder a ella, y para gestionar la documentación de empresa y trabajadores que se solicita.

8.6 Por su parte, BT se compromete a:

a. Informar a través de la herramienta Web al Proveedor de los riesgos laborales y de las medidas preventivas a adoptar, respecto de las tareas inherentes al Servicio.

b. Informar a través de la herramienta Web al Proveedor de los resultados de las evaluaciones de riesgos que se realicen y de los cambios que se produzcan en los riesgos y en las medidas preventivas para que pueda cumplir con sus obligaciones legales en materia de prevención de riesgos laborales.

c. Informar a través del coordinador designado de todo daño para la salud que sufra cualquier trabajador del Proveedor en el desarrollo del Servicio.

d. Garantizar a los trabajadores del Proveedor que presten sus servicios al amparo de este contrato el mismo nivel de protección en seguridad y salud que al resto de trabajadores.

8.7 Durante la vigencia de este contrato, ambas partes se comprometen a coordinar su política preventiva si fuese necesario y en los términos que especifique la legislación vigente en materia de prevención de riesgos laborales.

9. Fuerza Mayor.

9.1 "Evento de fuerza mayor" significa cualquier circunstancia surgida más allá del control razonable de una Parte que obstaculiza, retrasa o impide que esa Parte cumpla con cualquiera de sus obligaciones contractuales, incluyendo accidentes nucleares, incendios, inundaciones, tormentas, sequías, desastres naturales, ataques terroristas, conmoción civil o conflicto armado, pandemias o epidemias declaradas por las autoridades sanitarias competentes.. Para evitar dudas, la simple escasez de mano de obra, materiales, equipos o suministros (a menos que sea causada por eventos o circunstancias que sean eventos de fuerza mayor), huelgas, cierres patronales u otras disputas industriales que involucren a la fuerza laboral de la parte, no constituirá un Evento de Fuerza Mayor.

9.2 Si una Parte se ve impedida de cumplir con cualquiera de sus obligaciones por la ocurrencia de un Evento de Fuerza Mayor, esa Parte ("Parte Afectada") podrá, tan pronto como tenga conocimiento del Evento de Fuerza Mayor, reclamar la exención de responsabilidad con respecto a cualquier retraso en el cumplimiento o cualquier incumplimiento de dicha obligación en la medida en que el retraso o el incumplimiento se deban a un Evento de Fuerza Mayor, siempre y cuando la Parte afectada notifique prontamente a la otra Parte por escrito, en cualquier caso no más tarde de un (1) día, después de haber tenido conocimiento de que era probable que se produjera tal demora, la causa de la demora o del incumplimiento y la duración probable de la demora o del incumplimiento.

10. Resolución - Terminación – Anulación del Pedido.

10.1 Cualquiera de las partes podrá, en cualquier momento, poner fin al Pedido o Contrato, notificándolo por escrito a la otra, si:

a. cualquier suceso de fuerza mayor impidiera el cumplimiento de todo o una parte sustancial de las obligaciones de la otra parte con relación a tal Servicio por un periodo continuado de veinte (20) días desde la fecha en que tal obligación debiera haberse realizado; o

b. la otra parte incumpliera cualquier término o condición establecidos en el Pedido o en estas CGC.

10.2 BT tendrá el derecho a rescindir éste Contrato y/o cualquier Pedido que se lance con las mismas, total o parcialmente, sin necesidad de oponer causa justificada notificándolo por escrito a la otra parte con un preaviso de un (1) mes, debiendo pagar al Proveedor únicamente por los cargos ya generados que tuviera pendientes de pago a la fecha de su finalización anticipada.

10.3 En los supuestos de resolución parcial, se exigirán exclusivamente los derechos y obligaciones correspondientes a los servicios que se sigan prestando.

10.4 No obstante la resolución del Pedido, seguirán vigente las obligaciones de derechos de propiedad intelectual e industrial (condición 12) protección de datos personales (condición 13), y confidencialidad (condición 14).

10.5 En caso de incumplimiento de cualquiera de las presentes CGC, y en particular en caso de retraso en la entrega, BT podrá anular el Pedido, sin perjuicio de la reclamación de los daños y perjuicios ocasionados.

11. Cesión y subcontrataciones.

11.1 El Proveedor no cederá ni subcontratará el Pedido ni los servicios objeto del mismo o el contenido de las obligaciones dimanantes de estas CGC, total o parcialmente, sin el consentimiento previo por escrito de BT. Tal permiso, si se otorga, no liberará al Proveedor de ninguna obligación o responsabilidad que tenga de conformidad con el Pedido o estas CGC. El Proveedor posibilitará que BT tenga acceso razonable al subcontratista para obtener garantías adecuadas acerca de la realización y calidad del Servicio.

11.2 BT se reserva el derecho de ceder la totalidad o parte del Pedido a cualquier empresa, que o bien forme parte de su grupo de empresas o bien tenga similar solvencia económica previa notificación por escrito al Proveedor con al menos treinta (30) días de antelación a la fecha en que tal cesión vaya a ser efectiva.

12. Propiedad Intelectual.

12.1 Propiedad Intelectual e Industrial de BT:

a. La titularidad y todos los Derechos de Propiedad Intelectual o Industrial sobre las Mercancías de BT, materiales, software, manuales operativos y documentación asociada, suministrada o puesta a disposición del Proveedor o generada por parte del Proveedor de cualquier otra manera en conexión con estas CGC o con los contratos y Pedidos, permanecerá siendo plenamente propiedad de BT o del titular de los mismos. Nada en estas CGC se entenderá o interpretará como que BT concede al Proveedor ningún tipo de licencia o derecho sobre la propiedad intelectual o industrial de BT. Los derechos de Propiedad Intelectual sobre los trabajos desarrollados por el Proveedor al amparo de las presentes CGC y de los Pedidos o contratos suscritos en el Proveedor y BT serán propiedad de esta última. El Proveedor cede expresamente y en exclusiva a BT todos los derechos de explotación sobre dichos trabajos, incluyendo los derechos de reproducción, distribución, comunicación pública y transformación, para todo el mundo y por toda la duración de los derechos de propiedad intelectual. Esta cesión se entiende incluida en el precio pactado.

b. El Proveedor mantendrá cualquier software así como cualquier otro material que contenga Derechos de Propiedad Intelectual o Industrial de BT como confidencial y se asegurará de que no se copian, revelan o utilizan por tercero sin la previa autorización por escrito por BT. El Proveedor indemnizará a BT por todos los daños y perjuicios que pueda causarle por su incumplimiento de esta cláusula 12.1.

12.2 Propiedad Intelectual e Industrial sobre los productos y servicios de las CGC:

a. En caso de que las mercancías incluyan software, el Proveedor concede a BT una licencia irrevocable y no exclusiva, para todo el mundo, y con derecho a sublicenciar en caso de que BT venda o alquile la mercancía a un tercero, para el uso del software o la mercancía con la que se suministra y con este único fin.

b. El Proveedor garantiza a BT, y queda obligado a acreditar documentalmente ante ella, si fuere requerido, que dispone de las patentes, marcas o derechos de uso de marcas en su caso, licencias y demás derechos de propiedad intelectual e industrial del Software que pudiera aportar. El Proveedor exime a BT de toda responsabilidad por las infracciones de la propiedad intelectual y/o industrial en que aquél pudiera incurrir. Además el Proveedor se compromete a realizar, a su propio coste, cuantas acciones sean necesarias para mantener a BT indemne, incluyendo la defensa jurídica de BT frente a todas las reclamaciones y/o demandas que

pudiera recibir como consecuencia de las infracciones del proveedor, directa o indirectamente, de los derechos de propiedad intelectual e industrial de terceros.

13. Protección de Datos de Carácter Personal.

13.1 A los efectos de esta cláusula, los siguientes términos tendrán los siguientes significados

"BT" significará cualquier empresa del Grupo BT (según se recoge en el artículo 42 del Código de Comercio) que proporcione datos personales al Proveedor o de la cual el Proveedor adquiera Datos Personales en relación con el Contrato.

"**Normativa sobre Protección de Datos**" significa el Reglamento General de Protección de Datos de la Unión Europea 2016/679 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos como la Ley Orgánica 3/2018 de Protección de Datos y Garantías de Derechos Digitales, y cualquier enmienda o normativa posterior de desarrollo de la misma. Los términos que se empleen en esta cláusula y estén definido en dicha normativa tendrán el significado que allí se les atribuye.

13.2 Las Partes se obligan a cumplir en todo momento lo dispuesto en la Normativa sobre Protección de Datos en el desarrollo de su actividad y en la ejecución del presente Contrato y a trasladar y reflejar las estipulaciones y obligaciones de esta cláusula 13 en los contratos con sus subcontratistas y agentes, garantizando el cumplimiento de lo previsto en la misma.

13.3 Con el fin exclusivo de mantener y gestionar la relación contractual y para la correcta ejecución del Contrato, cada parte recibirá datos personales de la otra (fundamentalmente, datos de contacto comercial de empleados y, en su caso, de subcontratistas y agentes) obligándose a:

a. garantizar que cuentan en todo momento con la base jurídica o legitimación necesaria para el tratamiento de los Datos personales que facilite a la otra parte.

b. tratar los datos personales recibidos de la otra parte con la finalidad única de mantener y gestionar la relación contractual entre las partes, contactar con la otra parte a los efectos del presente Contrato, así como para la correcta ejecución de los derechos y obligaciones dimanantes del mismo.

c. informar a los interesados de los extremos y en la forma y plazos previstos en la cláusula 14 del GDPR.

d. en caso de que se produzca una violación de la seguridad de los datos personales, notificarlo a la otra parte en el momento en que tenga conocimiento de la misma indicando los aspectos relevantes que deba conocer y garantizando, en todo caso, que la otra parte pueda cumplir con las obligaciones que, en su caso, le correspondan de acuerdo con lo previsto en la normativa sobre Protección de Datos

13.4 El proveedor autoriza a BT a ceder los datos personales antes citados a las empresas de su grupo a los únicos fines de la gestión del Contrato y cumpliendo con sus normas corporativas vinculantes.

13.5 No entra dentro del objeto del presente Contrato que ninguna de las partes lleve a cabo ningún tipo de tratamiento de datos personales como encargado del tratamiento por cuenta de la otra parte. En caso de que se vaya a producir, por cualquier causa, tal tipo de tratamiento, ambas partes negociarán de buena fe un nuevo acuerdo que recoja los pactos necesarios para llevar a cabo dicho tratamiento de acuerdo con la normativa sobre Protección de Datos

e incluyendo como mínimo las medidas de seguridad de la condición 16. Así mismo, en el caso de que el Proveedor trate datos personales por cuenta de BT, está podrá requerir al Proveedor que complete un cuestionario con el objeto de conocer los datos personales que recaba y el tratamiento que de ellos realiza, de acuerdo con la Generic Standard GS 12 Data Privacy disponible en https://groupextranet.bt.com/selling2bt/articles/side/policies_portal.html.

13.6 Cualquier incumplimiento por parte del Proveedor de la presente Cláusula 13 o de la Legislación en materia de Protección de Datos se considerará un incumplimiento grave del presente Contrato.

14. Confidencialidad y publicidad.

14.1 El Proveedor se obliga expresamente a mantener como confidencial la información que BT le suministre como consecuencia de las relaciones comerciales que se establezcan entre las partes. Así, durante la vigencia de estas CGC, o de los Pedidos y una vez finalizados los mismos, cada una de las partes cuidará de que toda la documentación, información, datos técnicos, diseño, fabricación, instalación o explotación que hayan podido intercambiarse no llegue a conocimiento de competidores de cualquiera de las partes o de terceros que puedan perjudicar el posicionamiento de investigación industrial o comercial de BT.

14.2 Cada Parte mantendrá en la más estricta confidencialidad toda la Información confidencial que se le divulgue y:

a. solo divulgará información confidencial a aquellos empleados, agentes, compañías del grupo, funcionarios, directores, asesores, aseguradores, subcontratistas y proveedores, que necesiten conocerla para que dicha Parte cumpla con sus obligaciones o reciba un beneficio conforme al Contrato, y se compromete a que aquellos que reciban información confidencial conforme a ésta Cláusula 14.2.a) cumplan con las obligaciones establecidas en esta Cláusula 14.1 como si fuesen parte del Contrato;
b. solo divulgará información confidencial conforme lo exija la ley española, a los órganos administrativos y a los tribunales;
c. no utilizará la Información confidencial de ninguna otra manera que la estipulada en el Contrato.

14.3 La cláusula 14.2 no se aplicará a la información confidencial que:
a. se encontré a disposición del público a raíz de un hecho ajeno a un incumplimiento del Contrato;
b. con anterioridad al Contrato ya sea legalmente disponible para una Parte como no confidencial previo a su divulgación por la Parte propietaria de la información considerada como confidencial;
c. las Partes acuerdan por escrito que no es información confidencial; o

d. fuese conocida por la Parte receptora previo a su divulgación por la Parte reveladora.

14.4 A solicitud escrita de una Parte, la otra Parte le devolverá o destruirá, a su propio costo, cualquier Información confidencial recibida de la Parte solicitante dentro de un plazo razonable y confirmará su realización por escrito a solicitud de la parte solicitante.

14.5 Las Partes acuerdan que si cualquiera de ellas incumple esta Cláusula 14, además de compensación por daños y perjuicios, podrá solicitar una medida cautelar o el cumplimiento específico de las obligaciones requeridas por la Parte afectada por el incumplimiento.

15. Personal del Proveedor asignado a la prestación de servicios.

15.1 Para la prestación de los Servicios, el Proveedor utilizará su propio personal, el cual estará siempre bajo su dependencia, supervisión y control profesional, y sobre el que el Proveedor ejercerá la dirección, control, selección, formación, sustitución, aseguramiento, retribución, disciplina y cuantas otras facultades atribuye la legislación laboral al empresario o empleador. El Proveedor deberá proveer a sus empleados con el equipamiento, herramientas y materiales necesarios para que puedan desempeñar adecuadamente las tareas objeto de este Contrato.

15.2 La relación entre las partes tiene exclusivamente carácter mercantil, no existiendo vínculo laboral alguno entre BT y el personal del Proveedor que se encuentre prestando sus servicios en los locales de aquélla. Por tanto, el personal del Proveedor asignado a la prestación de los Servicios no podrá ser considerado ni de hecho ni de derecho, empleado de BT. En ningún momento podrá entenderse que la firma de este Contrato significa el establecimiento de relación laboral alguna entre BT o su cliente principal y el personal a cargo, directa o indirectamente del Proveedor. A este efecto serán obligaciones del Proveedor las siguientes:

a. Proveer los recursos humanos necesarios, tanto en calidad como en cantidad, para llevar a cabo todas sus obligaciones bajo lo dispuesto en el presente Contrato, realizando y gestionando el servicio bajo su control y coordinación, aplicando las normas y metodologías adecuadas y proporcionando a BT, periódicamente, información suficiente para facilitar la supervisión y toma de decisiones a lo largo de la realización del servicio, todo ello con independencia de que los trabajos objeto de este servicio se desarrollen en las instalaciones del Proveedor, de BT o de su cliente principal, según las necesidades del mismo.

b. Hacerse cargo de todas las obligaciones de carácter laboral –incluidas las correspondientes a seguridad y salud de los trabajadores–, de Seguridad Social en relación con sus trabajadores, así como de cualquier gasto o coste adicional incurrido por sus empleados en la prestación de los Servicios recogidos en el presente contrato, eximiendo, a este respecto, de toda responsabilidad a BT, fuera de lo establecido expresamente en el presente contrato. El incumplimiento de cualquier obligación del Proveedor con sus empleados podrá dar lugar a la resolución del presente Contrato.

c. La formación del Personal del Proveedor que preste sus servicios en las instalaciones de BT es una facultad y obligación de la competencia exclusiva del Proveedor, si bien ésta se ajustará a los estrictos requerimientos de las funciones que integran los servicios objeto de contrato, siendo impartida por el Proveedor de conformidad con el material y contenido acordado previamente con BT o con la Agencia de formación de esta última, en su caso. En el Precio del Servicio está incluido la formación del Personal.

d. El personal del Proveedor en las instalaciones de BT estará perfectamente identificado como trabajador de la primera compañía, debiendo portar algún tipo de signo distintivo que facilite su identificación. Así mismo, BT pondrá a disposición del personal del Proveedor que trabaje en las instalaciones de la primera un lugar que permita diferenciarlos claramente de los empleados de BT, añadiendo o incluyendo, si fuera necesario, a estos efectos, algún tipo de distintivo en el mobiliario o zona ocupada por el personal del Proveedor que coadyuve a esta finalidad.

e. En los supuestos en que el Personal preste el Servicio en las instalaciones del Proveedor, tanto el Proveedor como BT designarán cada una sus correspondientes Coordinadores o Supervisores de Servicio, que serán las personas de contacto y enlace entre ambas compañías a los efectos de la prestación del Servicio. Con carácter general, los responsables de BT o de su cliente principal en ningún caso podrán dar instrucciones de trabajo a los trabajadores del Proveedor, recurriendo para ello al responsable de proyecto con el fin de que éste sea el único que dé las instrucciones oportunas al personal de su proyecto.

f. El Proveedor designará entre el Personal asignado a la prestación de los Servicios un Supervisor o Coordinador que será la única persona de contacto y enlace con BT y sus empleados dentro de las instalaciones de esta última. Asimismo, BT designará, por su parte, un Supervisor o Coordinador, que será la única persona de BT que mantenga el contacto y enlace con el Proveedor dentro de las instalaciones de BT.

g. Se evitará que el Personal del Proveedor asignado a la prestación de los Servicios interactúe, a los efectos del presente contrato, tanto con BT como con los empleados de esta última. Cualquier comunicación y/o petición que tenga necesidad de realizar el Personal del Proveedor destacado en BT deberá canalizarse necesariamente a través del Supervisor o Coordinador del Proveedor, quien hará llegar debidamente las comunicaciones al Coordinador o Supervisor de BT.

h. Poner a disposición de BT, a requerimiento de ésta, los documentos que acrediten la vinculación de los trabajadores y el cumplimiento de sus obligaciones laborales, fiscales y en materia de Seguridad Social.

15.3 Se establecen las siguientes obligaciones a asumir por BT o por su cliente principal:

a. Abstenerse de aplicar o comunicar a los trabajadores cualquier medida que afecte a sus condiciones laborales.

b. Comunicar a los responsables del proyecto o servicio las cuestiones relativas a la prestación del mismo que afecten a las condiciones laborales de cara a que adopten las medidas oportunas, no acordándose medida o régimen alguno mientras no haya constancia de que ha sido comunicado a los trabajadores por su responsable jerárquico en la empresa.

15.4 Los Supervisores o Coordinadores del Proveedor realizarán revisiones periódicas del desempeño del Personal asignado a la prestación de los Servicios, tratando individualmente la consecución de objetivos, productividad y plan de carrera, diseñado por el Proveedor para cada uno de sus trabajadores.

15.5 El Proveedor se compromete a que el Personal destacado para la ejecución de los servicios contratados posea la cualificación y experiencia necesaria, garantizando en todo momento que los servicios a prestar en virtud de este contrato sean de calidad profesional, de acuerdo con los requisitos de pericia, destreza y conocimientos que generalmente cabe esperar en la prestación de los servicios objeto de este contrato entre compañías de servicios de buena reputación, comprometiéndose, asimismo, a que el Personal actúe, en el ejercicio de sus compromisos, obligaciones y trabajos, con la diligencia debida y conforme a las normas de urbanidad generalmente aceptadas y aceptables en el medio profesional en el que éste prestará sus servicios.

15.6 BT y el Proveedor realizarán controles de calidad sobre el desarrollo del Servicio, según la política y parámetros de calidad fijados previamente por BT y acordados por las Partes.

15.7 El Proveedor se compromete a prestar los servicios de conformidad con los parámetros establecidos y obligaciones asumidas en el presente contrato y Anexos, así como con aquellas instrucciones que pudiera establecer BT, siendo el Proveedor libre de emplear el Personal que considere conveniente en cada momento para la ejecución del presente contrato. Siempre que se produzca una variación en el Personal afecto al Servicio. El Proveedor planificará y ejecutará un redimensionamiento del servicio de forma que se garantice en todo momento el mismo nivel de calidad del servicio contratado.

15.8 Los responsables de BT y el Proveedor mantendrán reuniones periódicas, para tratar de la ejecución y desarrollo del Servicio, de conformidad con lo establecido en el presente Contrato y sus Anexos.

15.9 BT no será responsable por cualquier pérdida o daño que se pueda ocasionar a la propiedad del Proveedor o del Personal del Proveedor mientras se encuentren en un establecimiento de BT.

15.10 El Proveedor se compromete a mantener indemne a BT y a indemnizarle por cualquier responsabilidad derivada de o relacionadas con cualquier demanda interpuesta en virtud de la normativa laboral o de seguridad social por Personal del Proveedor en relación con los Servicios o la terminación de este Contrato o cualquier pedido o por el cese en la prestación de los servicios (o parte de los mismos), incluyendo, entre otros, cualquier reclamación, demanda de relación laboral o derechos relacionados, o cualquier reclamación por discriminación de cualquier tipo.

16. Medidas de seguridad adicionales aplicables al acceso/tratamiento de datos.

16.1 Este apartado contempla las obligaciones en materia de seguridad a cumplir por el Proveedor en la prestación de los servicios a BT, cuando el suministro implique el acceso a datos de BT o de terceros con lo que esta tiene relación, que o bien sean personales o no siéndolos sean confidenciales) de BT y son adicionales y complementarias a las recogidas en la condición sobre Protección de Datos.

16.2 Salvo que BT le solicite su entrega, el Proveedor procederá a eliminar los datos tratados o generados una vez finalice el contrato o el periodo legal en que los mismos deban ser conservados por el Proveedor por imperativo legal.

16.3 EL Proveedor asume la responsabilidad de hacer pública y divulgar entre todas las personas que intervengan directa o indirectamente en el tratamiento de los datos, las medidas de seguridad, normas y procedimientos que se adopten para garantizar la seguridad de los datos, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Asimismo, informará sobre el Deber de Secreto al que está obligado por Ley. El Proveedor asume así la responsabilidad de garantizar que todas aquellas personas que intervengan en el tratamiento de los datos durante la prestación del servicio conocen los objetivos y alcance de sus funciones, así como las obligaciones que se derivan, las normas que deben cumplir y las consecuencias de su incumplimiento.

16.4 Sistema de Registro de incidencias:

a. El Proveedor establecerá un sistema de Registro de Incidencias en el que se debe hacer constar:
   (i) Fecha y hora en el que se produjo la incidencia.
   (ii) Tipo de incidencia.
   (iii) Datos identificativos de la persona que realiza la notificación.
   (iv) Datos identificativos de la persona a quien se comunica la notificación.
   (v) Efectos que se deriven de la incidencia.
   (vi) Medida correctora aplicada.

b. Cualquier anomalía o mal funcionamiento que se produzca y que afecte o que pudiera llegar a afectar a la seguridad de los datos de carácter personal, será notificada inmediatamente a BT, debiendo indicar todos los puntos recogidos en el punto a) anterior.

c. El Proveedor adoptará las medidas preventivas y/o correctivas necesarias para garantizar la resolución del incidente y eliminar o minimizar los efectos sobre la seguridad de los datos y la probabilidad de que se repita la incidencia. BT será informada sobre las características de las medidas adoptadas y podrá desestimarlas si no se consideran adecuadas.

16.5 Acceso a los datos:

a. Sólo aquellas personas cuya intervención sea necesaria en alguna de las fases del tratamiento que configura el servicio tendrán acceso a los datos de carácter personal o confidencial, ficheros y recursos afectados. El Proveedor podrá solicitar de BT un listado completo de las personas con acceso a los recursos protegidos (cualquier parte componente del sistema de información).

b. El Proveedor mantendrá un mapa de usuarios que especifique qué usuarios tienen acceso a qué recursos protegidos y el tipo de acceso permitido. Los permisos de acceso se establecerán exclusivamente basándose en las necesidades derivadas de las funciones asignadas al usuario de manera que se garantice la restricción de acceso a los datos y recursos. BT podrá solicitar al Proveedor una descripción de las asignaciones que se realicen.

c. El Proveedor implantará mecanismos de autenticación de usuarios con acceso a los sistemas que permitan comprobar de forma segura la identidad del usuario con el fin de evitar suplantaciones de identidad y accesos no autorizados.

d. El Proveedor adoptará las medidas de seguridad necesarias que permitan garantizar que los procesos de autenticación son seguros. Se adoptarán normas de seguridad y control específicas para preservar la calidad de las contraseñas de usuario y controlar su asignación, distribución y almacenamiento de forma segura. BT podrá invalidar las medidas de seguridad adoptadas por el Proveedor si entiende que estas son insuficientes con respecto a la política de seguridad implantada en BT. El Proveedor deberá cambiar sus contraseñas con una periodicidad de al menos un año y en cualquier caso debería documentarse en el Documento de Seguridad.

e. El Proveedor implantará un mecanismo de control de acceso a los recursos que asegure la restricción de acceso de los usuarios exclusivamente a los recursos autorizados y con los permisos establecidos. Identificará a los responsables de la administración del control de acceso lógico y sólo las personas designadas podrán conceder, alterar o anular el acceso sobre los datos y recursos y siempre conforme a los criterios de seguridad establecidos por el Responsable del Tratamiento.

16.6 Soportes de datos y copias de seguridad

a. Todos los soportes que contenga datos de carácter personal (tanto los datos base como los resultantes de los procesos que conforman el tratamiento objeto del servicio contratado) estarán inventariados e identificados físicamente de manera que siempre pueda conocerse:

i. Su ubicación física.
ii. Su contenido.
iii. El grado de sensibilidad y confidencialidad de la información que contiene.

b. El intercambio de soportes que contengan datos de carácter personal entre el BT y el Proveedor se realizará adoptando las medidas de seguridad necesarias para proteger la integridad del soporte y de la información que contienen así como la confidencialidad de los datos, durante los traslados que se prevean. El Proveedor especificará en cada caso las condiciones en que se efectuará el traslado.

c. El Proveedor es responsable de controlar el que los soportes que se encuentran bajo su tutela no sean trasladados en ningún caso fuera de las instalaciones designadas para el tratamiento o almacenamiento de los mismos, sin el conocimiento y la autorización de BT. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, deberá ser autorizada siempre por el Responsable del Tratamiento.

d. El Proveedor establecerá procedimientos de actuación para la realización, siempre como mínimo con carácter semanal, de copias de respaldo. Igualmente, el Proveedor establecerá procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

e. El Proveedor se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.

17. Obligaciones en materia de corrupción.

17.1 En esta Condición "Filial" significa en relación con el Proveedor, (i) cualquier persona o entidad bajo su control; y (ii) cualquier persona o entidad que la controla y (iii) cualquier otra persona o entidad bajo el control de una persona o entidad supervisora según (ii).

17.2 El Proveedor se obliga a que:

a. asegurará que ella y sus Filiales participen únicamente en negocios legítimos y prácticas éticas y se atengan a y cumplan con todas las leyes aplicables, incluidas, pero no como limitación, las leyes anticorrupción de cualquier país en el que se ejecute el Contrato, en el Reino Unido y los Estados Unidos;

b. no dará, ofrecerá, acordará ni prometerá, y hará que sus Filiales no proporcionen, ni directa ni directamente, ningún dinero o cualquier otra cosa de valor a nadie ni buscará ni recibirá ningún dinero ni cualquier otra cosa de valor de nadie, como incentivo o recompensa por una acción favorable o indulgencia de cualquier acción o ejercicio de influencia. Esto es aplicable a cualquier obsequio, oferta, acuerdo o promesa de hacerlo a cualquier gobierno oficial, nacional o regional, a cualquier director o jefe de cualquier organismo corporativo o a cualquier otra persona;

c. ni él, ni sus Filiales, contratistas, ejecutivos, directores, empleados, accionistas (cuyas acciones no cotizan en bolsa), miembros o agentes son una "Persona expuesta políticamente". Esto se define como: una persona que en los últimos doce (12) meses ostentó una función pública importante en cualquier estado y los miembros de su familia y asociados cercanos. Una función pública importante incluye: jefes de estado, jefes de gobierno y ministros; miembros del parlamento; miembros de cuerpos judiciales de alto nivel; embajadores, encargados de negocios y oficiales militares de alta graduación; así como miembros de organismos administrativos, de dirección o supervisión de empresas de propiedad estatal;

d. toda la información que ha proporcionado el Proveedor a BT y a sus representantes en relación con sus obligaciones, según esta Condición, es actual, precisa y completa. Si existe algún cambio material de esta información, el Proveedor notificará a BT dichos cambios lo antes posible. BT puede finalizar el Contrato si no está de acuerdo con dichos cambios;

e. antes de contratar a un subagente para realizar los servicios en nombre de BT según el Contrato, el Proveedor obtendrá la aprobación por escrito de BT y procurará que cada uno de los subagentes acepten por escrito las disposiciones indicadas en esta Condición (mutatis mutandis);

f. a petición de BT, el PROVEEDOR proporcionará documentos e información a BT confirmando el cumplimiento del Proveedor y de sus Filiales con esta Condición y permitirá que BT (o sus agentes) revisen, en cualquier momento, los libros y registros de las Filiales, en relación con el trabajo realizado en nombre de BT;

g. si existen cambios en su propiedad, el Proveedor informará a BT de dichos cambios lo antes posible. BT puede finalizar el Contrato si BT no está de acuerdo con dichos cambios. En lo que respecta a las sociedades cotizadas en bolsa, este párrafo 2(g) sólo es aplicable si un nuevo propietario o grupo de propietarios adquiere el 5% o más del capital en acciones con derecho de voto del Proveedor; y

h. mantendrá una cuenta independiente de todas las cantidades recibidas por él según el Contrato y de todos los pagos realizados por él en relación con su función de proporcionar servicios a BT según el Contrato, mantendrá dicha cuenta con el nivel de detalles suficiente para que puedan verificarse las transacciones y el destino de cualquier pago a la satisfacción de BT y hará que dicha cuente esté disponible para BT o sus agentes, periódicamente, por solicitud, para dicha verificación.

17.3 Con independencia de cualquier disposición del Contrato que diga lo contrario, cuando se admita o se detecte que el Proveedor o cualquiera de sus Filiales hayan incumplido con el párrafo 2 de esta Condición o que cualquier manifestación o afirmación realizada por el Proveedor o cualquiera de sus Filiales en relación con esta Condición sea materialmente incorrecta:

a. BT tendrá la opción de finalizar el Contrato inmediatamente;
b. el Proveedor perderá el derecho a cualquier comisión adeudada por BT; y
c. el Proveedor indemnizará a BT por cualquier responsabilidad resultante.

17.4 Las disposiciones de los párrafos 2 y 3 de esta Condición sobrevivirán a la finalización o vencimiento del Contrato.

18. Ley, Jurisdicción y resolución de conflictos.

18.1 El Contrato entre BT y el Proveedor estará regulado por la Ley Española.

18.2 La nulidad y, por tanto, la inaplicabilidad de alguna de las cláusulas y/o anexos integrantes de las presentes CGC no motivarán la invalidez de las restantes, que permanecerán vigentes.

18.3 Compromiso de resolución extrajudicial de conflictos

18.3.1 Las Partes acuerdan resolver cualquier disputa o reclamación que surja o esté relacionada con este Acuerdo mediante negociación directa entre ellas, sin recurrir a los Tribunales, salvo que no se llegue a un acuerdo mediante dicha negociación.
18.3.2 Procedimiento de resolución de disputas.
18.3.2.1 El procedimiento de resolución de disputas se iniciará mediante notificación a la otra Parte, detallando la naturaleza y todos los pormenores de la disputa, junto a los documentos relacionados con la disputa que consideren pertinentes, y una propuesta de resolución.

18.3.2.2 Las Partes acuerdan negociar de buena fe y usar esfuerzos razonables para resolver la disputa dentro de los 14 días hábiles siguientes a la notificación. Durante este período, las Partes deben mantener confidencialidad respecto de todos los asuntos discutidos en la negociación, excepto en el acta de inicio y de conclusión del proceso de negociación.

18.3.2.3 Oferta Final: al vencerse el plazo de 14 días, ambas Partes presentarán una oferta para resolver la disputa. Si no se alcanza un acuerdo dentro de los 7 días hábiles siguientes a la presentación de las ofertas, se considerará concluido el proceso de negociación. La falta de acuerdo permitirá a cualquiera de las Partes presentar una demanda ante los tribunales.

18.3.3 Documentación acreditativa del intento de resolución. Las Partes firmarán un documento conjunto que registre la fecha de inicio de la negociación, los asuntos discutidos, las ofertas realizadas y la falta de acuerdo al concluir el proceso de negociación. Este documento servirá como prueba del intento de resolver la disputa. El acto inicial y el acto final del proceso de negociación no son confidenciales y pueden ser adjuntados a la demanda judicial para probar el intento de resolución extrajudicial del conflicto.

18.3.4 Excepciones. Nada en esta cláusula impedirá a cualquiera de las Partes:

18.3.4.1 Solicitar medidas cautelares u otro tipo de remedio inmediato cuando exista un riesgo inminente para la Parte, que no pueda resolverse adecuadamente mediante negociación.

18.3.4.2 Ejercer cualquier derecho o recurso legal disponible en caso de incumplimiento de los términos de este Acuerdo, después de intentar resolver el conflicto mediante negociación.

18.3.5 Suspensión de plazos de prescripción. Durante el proceso de negociación, se suspenderán los plazos de prescripción o caducidad para el ejercicio de cualquier acción legal, los cuales comenzarán a contarse nuevamente una vez que la negociación haya finalizado sin acuerdo o las Partes hayan comunicado por escrito la terminación del proceso. Las Partes tendrán 30 días hábiles desde la conclusión del proceso de negociación para presentar una demanda ante los tribunales.

18.4 Para cualquier conflicto o controversia no resuelta por el método anterior, ambas Partes acuerdan someterlo a los tribunales de Madrid capital.

19. Definiciones e interpretaciones.

19.1 Los siguientes términos tendrán el significado que se les asigna a continuación:

"Autoridad" significa cualquier autoridad reguladora, gubernamental y/o judicial o cualquier organización autorreguladora, bolsa de valores, asociación de valores u órgano administrativo encargado de hacer cumplir las Leyes Aplicables y/o Asuntos Regulatorios. Para evitar dudas, el término Autoridad incluye cualquier reemplazo o sucesor de una Autoridad;

"Cliente BT" significa un cliente BT existente o potencial;

"Bienes" significa los bienes (incluido cualquier firmware y software asociado) según lo establecido en el Contrato (pero excluye cualquier Software en la medida en que se licencia por separado);

"Cargos" significa el precio a abonar por BT al Proveedor por los bienes, software o servicios relevantes establecidos en el Contrato;

"**Condiciones Generales**" o "**Contrato**" significa este documento comprendido desde la Cláusula 1 a la 19 y sus Anexos;

"Defecto" significa (a) la probable falla de cualquiera de los Bienes o Software, para cumplir u operar de acuerdo con el Contrato; o (b) cuando la calidad de cualquiera de los Bienes o Software (incluido su desarrollo, rendimiento o rendimiento) (i) es tal que no son como se podía

razonable de esperar; (ii) no es satisfactorio para ningún propósito para el cual tales Bienes o Software generalmente se compran o usan; (iii) no cumple con los requisitos de BT; o (iv) no está de acuerdo con el Contrato, y **"defectuoso"** se interpretará en consecuencia;

"Derechos de propiedad intelectual" significa cualquier marca comercial, marca de servicio, nombre comercial y comercial, nombres de dominio de Internet, patentes, patentes menores, derechos de autor y derechos relacionados, derechos de bases de datos, derechos de diseño, derechos de topografía de semiconductores, derechos de uso y protección de información confidencial (incluidos conocimientos y secretos comerciales), o cualquier derecho de propiedad intelectual similar en cualquier parte del mundo, ya sea registrado o no, y todos los derechos similares o equivalentes que subsisten o subsistirán ahora o en el futuro en cualquier parte del mundo;

"Directiva" significa la Directiva 95/46/EU del Parlamento Europeo y del Consejo de 24 de Octubre de 1995;

"**Documentación**" significa las guías de instalación, de usuario y mantenimiento; publicidad y/u otra documentación relacionada con el uso, mantenimiento y/u operación de los Bienes, Software o Servicios;

"Entregable" hace referencia a aquellos materiales que deben ser preparados o creados por o en nombre del Proveedor, una Compañía del Grupo Proveedor o cualquier Subcontratista en el curso del cumplimiento de las obligaciones del Contrato;

"**GDPR**" significa Reglamento General de Protección de Datos (EU) 2016/679 y cualquier modificación o reemplazo de la misma (incluida cualquier ley o regulación nacional correspondiente o equivalente que transponga al GDPR);

"**Grupo BT**" significa *BT GLOBAL ICT BUSINESS SPAIN, S.L.U*, con domicilio social en la calle María Tubau, 3, 28050 Madrid (en adelante BT) y cualquier empresa o corporación dentro del Grupo BT;

"Información" significa toda aquella ya sea en forma tangible o de cualquier otra forma, incluidas, entre otras, especificaciones, informes, datos, notas, documentación, dibujos, software, salidas de computadora, diseños, diagramas de circuitos, modelos, patrones, muestras, invenciones, (si capaz de ser patentado o no) y conocimientos, y los medios (si los hay) sobre los que se proporciona dicha información;

"Información confidencial" se refiere a toda aquella información, que se transmite por una Parte o sus empleados, agentes, Compañías del grupo, funcionarios o asesores, a la otra Parte en virtud o en conexión con el Contrato; antes, durante o después de la fecha de dicho acuerdo, incluyendo: (a) los términos del Contrato; (b) todos los conocimientos técnicos o comerciales, derechos de propiedad intelectual, precios, especificaciones, informes, datos, notas, documentación, dibujos, programas informáticos, salidas informáticas, diseños, diagramas de circuitos, modelos, patrones, muestras, invenciones (si es posible de estar patentado o no), desarrollos, secretos comerciales, procesos o iniciativas de naturaleza confidencial; (c) cualquier información que deba considerarse razonablemente confidencial y relacionada con el negocio, asuntos, clientes, personal, clientes, proveedores, planes o estrategia de la Parte reveladora o sus Compañías del Grupo; (d) las operaciones, la información del producto, los diseños, los secretos comerciales o el software de la Parte reveladora o las Compañías del Grupo; y (e) cualquier Información divulgada por un Cliente de BT al Proveedor;

"Ley Aplicable" se refiere a las leyes, reglamentos, orientación reglamentaria, obligaciones, promulgaciones, deberes legales o reglas (incluidos los códigos industriales obligatorios y legalmente requeridos, los códigos de conducta vinculantes) aplicables al Contrato o el suministro de los Bienes, Software o Servicios, incluyendo (a) según sus modificatorias; y (b) cualquier legislación aplicable;

"**Legislación de Protección de Datos**" significa (i) el GDPR; (ii) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.; (iii) cualquier otra ley nacional de privacidad aplicable; (iv) cualquier ley modificatoria o de reemplazo; y (v) cualquier código de práctica emitido por una Autoridad de Supervisión;

“Medidas de seguridad mínimas que tienen que aplicar los proveedores” significa las medidas de seguridad del Anexo 1, también accesibles en Selling to BT que deben aplicar mínimamente los Proveedores o sus subcontratistas;
"**Personal del Proveedor**" significa cualquier persona contratada por el Proveedor o sus subcontratistas para el cumplimiento de las obligaciones devengadas del Contrato;
"Política" y **"Políticas"** son las políticas y estándares genéricos de BT y del Grupo BT accesibles en el Portal de Políticas (BT cada vez que modifica una política, notifica al Proveedor a través del Portal de Políticas);
"Portal de Políticas" significa el repositorio en línea de las Políticas accesible en https://groupextranet.bt.com/selling2bt/PoliciesPortal/index.html o cualquier otra URL que pueda ser notificada al Proveedor de vez en cuando;
“Proveedor”: significa la persona física o jurídica que conoce, consiente y acepta estas Condiciones Generales de Compra junto con los Pedidos o Anexos a las mismas que se puedan acordar;
"Responsable", "Datos personales", "Infractor de la seguridad de datos personales" "Encargado del tratamiento" tendrán los significados que se les atribuyen en la Directiva y / o en el GDPR;
"Servicios" significa cualquiera o todos los servicios establecidos en el Contrato, incluida la provisión de Materiales del Proveedor;

El Proveedor reconoce y acepta estas Condiciones Generales de Compra.

PROVEEDOR: _____
CIF: _____

Firmado en _____, el _____ de _____ de 202X

Apoderado: _____
Cargo: _____

ANEXO 1: POLÍTICA DE BT EN MATERIA DE SEGURIDAD

El Proveedor cumplirá (y se asegurará de que cualquier Subcontratista y Personal contratado cumpla) con la versión 5.3 de los Requisitos de Seguridad del Proveedor de BT disponibles en BT Supplier Security Requirements 5.3 o cualquier otro sitio web que notifique BT de forma puntual.

Inicialmente, el Proveedor atendiendo a los servicios suministrados a BT deberá observar las **Secciones XXXXX** del mencionado documento.

Otras secciones adicionales podrían llegar a ser aplicables si el alcance, método o lugar de trabajo cambia a lo largo del periodo. El alcance del trabajo debe revisarse periódicamente para detectar posibles cambios que afecten a la seguridad debiendo comunicarse los cambios significativos a BT.

Cualquier incumplimiento de esta Condición por parte del Proveedor será considerado un incumplimiento material del Contrato.

REQUISITOS DE SEGURIDAD DE LOS PROVEEDORES DE BT 5.3

Contenido

1. Introducción

1.1 Los clientes de BT tienen la expectativa de que BT y su cadena de suministro de Terceros prestan sus servicios utilizando estándares para los sistemas de gestión de la seguridad de la Información (ISMS). Sus ISMS deben cubrir infraestructura, redes, equipo y sistemas TI para proteger los servicios que se presten y la información de cliente BT/BT cubierta por estos servicios. Este documento establece los Requisitos de Seguridad de BT y es aplicable a todos aquellos Terceros que trabajen en o en nombre del Grupo BT, incluyendo Openreach, EE y PlusNet, y a los que referirá en adelante en el resto del documento como «BT». Usted recibirá asesoramiento sobre los conjuntos de controles de seguridad que corresponden al servicio que esté prestando a BT.

1.2 Estos Requisitos de Seguridad son adicionales y sin perjuicio de cualquier otra obligación de Terceros establecida en el Contrato. Están diseñados para garantizar que BT mantiene el control y la supervisión de su red y de los datos de usuario.

2. Requisitos de Acceso Limitado

2.1 Sin perjuicio de cualquier obligación de confidencialidad que pueda tener, si el Personal del Tercero tiene acceso a Información de BT, dicho Tercero deberá:

2.2 Asegurar que el Personal del Tercero no revele ni acceda a la Información de BT salvo que sea preciso para prestar el Servicio; y

2.3 Aplicar todos los sistemas y procesos, tanto técnicos como organizativos que puedan ser precisos para proteger la Información de BT (i) de la destrucción ilegítima o accidental y (ii) de las pérdidas, alteraciones, revelaciones no autorizadas o accesos a la Información de BT de acuerdo con las Buenas Prácticas de Seguridad de la Industria.

3. Seguridad de la Información General

3.1 Previa solicitud razonable, el Tercero deberá poner a disposición de BT copias de las certificaciones de seguridad y una declaración de cumplimiento pertinente para el Servicio con el fin de demostrar el cumplimiento de estos Requisitos de Seguridad.

3.2 Si se produjeran cambios significativos en los estándares de seguridad tecnológicos o industriales, los Servicios o la forma en la que se prestan, BT puede emitir una modificación del Contrato durante el período de vigencia del mismo si fuera preciso realizar un cambio en los conjuntos de controles de seguridad que correspondan. El Tercero deberá cumplir la modificación del Contrato acordada dentro de un plazo razonable teniendo en cuenta la naturaleza del cambio y el riesgo para BT.

3.3 El Tercero deberá revisar esta política de Requisitos de Seguridad cuando se produzcan cambios sustanciales en los Servicios o en la forma de prestarlos con el fin de garantizar que se sigan cumpliendo todos los controles de seguridad aplicables.

3.4 Si el Tercero subcontrata obligaciones en el Contrato, facilitará a BT una lista de los subcontratistas pertinentes y su ubicación, y deberá asegurarse de que todos los Contratos con los Subcontratistas en cuestión y los Subcontratistas de estos incluyan condiciones escritas que insten al Subcontratista a cumplir las secciones relevantes de estos Requisitos de Seguridad o los requisitos equivalentes de seguridad de Terceros, incluyendo derechos de auditoría para BT equivalentes a los de la sección 5.

3.5 Si se va a emplear a una cuarta parte para prestar el servicio y esta tiene que mantener o tratar Información de BT, el Tercero debe obtener la autorización de BT para compartir esa información. El Tercero debe mantener una relación contractual con dicha cuarta parte y garantizar que esa cuarta parte trabaje dentro de un marco de seguridad estándar del sector.

3.6 La Información de BT puede conservarse durante todo el tiempo necesario para cumplir el Contrato, tras el cual no debe retenerse más de dos años salvo que se haya acordado un período de conservación diferente entre BT y el Tercero, dentro de las limitaciones que marcan las leyes pertinentes.

3.7 Si los Servicios son dar apoyo directo a un contrato con el gobierno del Reino Unido, el Tercero deberá cumplir con la versión más reciente de Cyber Essentials Plus - https://www.cyberessentials.ncsc.gov.uk/

3.8 Cuando vaya a tratarse o almacenarse Información de BT en el extranjero, el Tercero deberá informar a BT de las ubicaciones geográficas y BT se reserva el derecho a rechazar las ubicaciones que sean consideradas de alto riesgo.

Gestión de la Información de BT

3.9 A no ser que la Parte Interesada de BT especifique lo contrario, toda la Información de BT está clasificada como «Confidencial». Cuando se trate de datos personales o datos personales sensibles, usted debe consultar al Equipo de Protección de Datos y Privacidad del Tercero por si fuesen necesarios controles adicionales.

Los controles de seguridad siguientes son «requisitos para la gestión verbal», cuyo alcance queda limitado a las comunicaciones verbales.

3.10 Si existe una necesidad de debatir, enseñar o intercambiar Información de BT mediante una plataforma de colaboración, por ejemplo, Teams

- Verificar que solo estén presentes los individuos que necesiten conocer la información.
- Si hay un Tercero o contratista externo implicado, debe haber firmado o bien un contrato con el Tercero, o un Acuerdo de Confidencialidad (NDA) antes de iniciar las conversaciones.
- El Tercero deberá verificar quién está en la conferencia antes de empezar.

3.11 Si existe la necesidad de hablar sobre cierta Información de BT con alguien en persona, por teléfono móvil o por teléfono fijo.

- Nadie que no tenga necesidad de conocer la información debe participar en las conversaciones, ni poder escucharlas.
- Si un Tercero o contratista externo implicado debe participar en la conversación, estos deben haber firmado bien un contrato con el Tercero, o tener un NDA antes de iniciar las conversaciones.
- No debe dejarse información confidencial o altamente confidencial en los servicios de buzones de voz.

Los controles de seguridad siguientes son «requisitos de gestión escrita» y su alcance cubre los materiales mantenidos en formato de papel. Esto incluye, sin limitarse a, cartas, actas, notas y circulares. Comprende además material electrónico impreso, como informes o documentos de trabajo una vez estén en formato de papel.

3.12 Si se van a almacenar copias en papel de Información de BT en instalaciones de Terceros, mientras no estén en uso deben guardarse en una sala segura con cerradura y restringirse el acceso exclusivamente a las personas que necesiten ver el material. Los documentos no deben dejarse desatendidos.

3.13 Si es necesario imprimir, fotocopiar o duplicar Información de BT, se aplicarán los controles de seguridad siguientes:

- Si va a imprimir o copiar el material, hágalo exclusivamente en las instalaciones del Tercero.
- No deben dejarse fotocopias ni impresiones desatendidas en un punto de impresión, deben recogerse en el momento de su creación.
- Cuando la impresora o fotocopiadora tenga una función de memoria mediante la que se pueda recordar y reimprimir el material copiado, se la debe reiniciarse la misma lo antes posible para borrar la memoria.

3.14 Si es necesario sacar copias de Información de BT de las instalaciones del Tercero:

- A menos que se haya acordado como parte del ámbito de trabajo, el Tercero debe obtener la autorización expresa de la parte interesada de BT.
- Si se aprueba, la información no debe ser identificable mientras permanezca en tránsito y debe mantenerse en una carpeta, bolsa o funda anonimizada o en blanco.
- El material nunca debe dejarse desatendido y debe permanecer bajo el control directo de la persona que transporte el material, especialmente en transporte público.

3.15 Cuando ya no sean necesarias, las copias en papel de Información de BT deben eliminarse de la manera siguiente:

- Las copias en papel no deben tirarse en papeleras de desechos generales.
- Si se utiliza una trituradora, debe tener un estándar mínimo de P4 DIN66399.
- Si no se dispone de ninguna de las trituradoras aprobadas, la información debe eliminarse en cubos de desechos confidencial.

En el caso de «información altamente Confidencial», además se aplica lo siguiente:

- La información solo debe ser eliminada en contenedores de desechos confidencial después de haberse triturado.
- En el caso de información que debe ser triturada in situ por el proveedor, se debe obtener un certificado de destrucción del proveedor.

Los controles de seguridad siguiente se aplican a la Información de BT en formato electrónico

3.16 Al almacenar Información de BT en un PC o Portátil de Terceros, se aplicarán los controles siguientes:

- Solo se permite en dispositivos con encriptado de disco duro, como Bitlocker.

- Todos los documentos deben encriptarse individualmente.
- Debe aplicarse la Gestión de Derechos de la Información (IRM) al documento.
- Si se incluye, la información debe conservar la etiqueta de clasificación de BT.

3.17 Al guardar un documento de BT en una ubicación interna de compartición de archivos para el almacenamiento, la colaboración y la compartición general de archivos, se aplicarán los controles de seguridad siguientes:

- La ubicación en la que vaya a guardarse el material debe disponer de permisos de acceso concedidos únicamente a aquellos que necesiten ver y utilizar el documento.
- Si se incluye, la información debe conservar la etiqueta de clasificación de BT.
- Todos los documentos deben encriptarse individualmente.
- Debe aplicarse la Gestión de Derechos de la Información (IRM) al documento.
- Si el servicio incluye el pago mediante tarjeta de pago, de acuerdo con los Estándares de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS), los datos no deben guardarse en ningún momento en sitios de almacenamiento de archivos.
- Si hacen falta cuentas de invitado para dar acceso a un Tercero o contratista externo implicado, deben haber firmado bien un contrato con un Tercero o tener un NDA antes de obtener acceso.

3.18 Si es necesario guardar Información de BT en soportes extraíbles de Terceros (como una unidad de memoria USB), se aplicarán los controles de seguridad siguientes:

- El dispositivo debe estar encriptado al mismo nivel que el disco duro.
- Si se perdiera o se sustrajera , el Tercero debe avisar del incidente de seguridad.
- Debe tener pruebas de la autorización previa por parte de la Parte Interesada de BT para transferir material «altamente confidencial» a soportes extraíbles.
- Si entra dentro del ámbito del servicio, el material de PCI o los datos personales no deberán almacenarse en soportes extraíbles.
- Los dispositivos destinados al soporte y el mantenimiento no deberán usarse para ninguna otra finalidad.

3.19 La Información de BT no deberá almacenarse en ordenadores, portátiles, soportes extraíbles ni dispositivos móviles personales.

3.20 La Información de BT no deberá ser enviada y reenviada desde la dirección de e-mail de trabajo de un Tercero a una cuenta de e-mail personal o externa a menos que sea propiedad de un Tercero o contratista externo que tenga un contrato firmado con un Tercero o que tenga un NDA y se utilice para prestar el servicio.

3.21 Para minimizar el riesgo del ataque y las oportunidades de que los atacantes manipulen el comportamiento humano mediante su interacción con navegadores web y sistemas de e-mail, implemente procesos para garantizar que solo estén permitidos navegadores web y clientes de correo totalmente autorizados, y desinstale o desactive cualquier aplicación adicional o complemento de cualquier navegador o cliente de correo no autorizado.

3.22 El Tercero deberá tener implementadas medidas de respaldo para recuperar la Información de BT en 3 días laborables en el supuesto de corrupción, pérdida o degradación.

3.23 Al eliminar datos/Información de BT, se deben mantener los registros completos de conservación y eliminación de datos que aporten pistas de auditoría, pruebas y rastreo. Esto debe incluir:

- Prueba de la destrucción y/o eliminación (incluida la fecha y el método empleado).
- Registros de auditoría del sistema para la eliminación.
- Certificados de eliminación de datos.
- Especificar quién se ha encargado de la eliminación (incluyendo a los colaboradores de la eliminación/Terceros o contratistas).
- Debe generarse un informe de destrucción y verificación para confirmar el éxito o fracaso de cualquier proceso de destrucción/eliminación. Es decir, del proceso de sobrescribir debe generarse un informe que detalle los segmentos que no se hayan podido borrar.

3.24 Cuando se desechen equipos que contengan datos/Información de BT, se deberá proporcionar un rastreo de auditoría para los siguientes tipos de equipo:

- Soportes extraíbles.
- Unidades de disco.
- Cintas de copia de seguridad.
- Componentes informáticos.

3.25 Deben existir registros completos que ofrezcan un rastreo de auditoría e incluyan como mínimo:

- El nombre de la aplicación o servicio que utilizó ese equipo.
- El tipo de equipo, como ordenador de sobremesa, portátil, servidor, cinta, rúter, etc.
- El número de discos duros que contiene el equipo (si procede).
- Identificación del equipo por su número de serie.
- Identificación de los componentes del equipo por su número de serie.
- Seguimiento completo de los activos para todos los equipos y componentes durante todo el ciclo de vida de eliminación de los mismos.
- Prueba de la destrucción y/o eliminación (incluida la fecha y el método empleado).
- Datos de quién se ha encargado de la eliminación (incluyendo colaboradores de la eliminación/Terceros / contratistas de eliminación de residuos).
- Debe emitirse un informe de la destrucción y verificación que confirme el éxito o el fracaso de cualquier proceso de reciclaje/saneamiento. Por ejemplo, de los procesos de sobrescribir se debe generar un informe detallado de las secciones que no se hayan podido borrar. Dichos informes deben incluir la capacidad, el fabricante, el modelo y el número de serie del soporte.

Funciones y responsabilidades

3.26 Todos los Terceros deben conocer y comprender los requisitos de estos controles de seguridad y garantizar que todas las personas involucradas en la prestación de un servicio a BT estén familiarizadas y cumplan los requisitos pertinentes de este estándar.

Gobernanza

3.27 El Tercero en cuestión debe contar con un marco de seguridad industrial para la gobernanza de la información y la ciberseguridad que esté consolidado y sea uniforme, con el fin de que cubra los siguientes componentes:

- Políticas y procedimientos de Información y Ciberseguridad adecuados aprobados y comunicados.
- Una estrategia de seguridad de la información.
- Requisitos legales y regulatorios correspondientes a la Información y la Ciberseguridad (incluyendo la privacidad) que sean entendidos y gestionados.
- Procesos de gobernanza y gestión de los riesgos que aborden los riesgos de la información y ciberseguridad.

3.28 El Tercero debe garantizar que se definan e implementen funciones y responsabilidades apropiadas para la Información y Ciberseguridad que incluyan:

- Un Responsable de Seguridad de la Información a tiempo completo (o equivalente), a nivel ejecutivo y que asuma la responsabilidad del programa de seguridad de la información.
- Un grupo de trabajo, comité u organismo equivalente de alto nivel que coordine la actividad de seguridad de la información en el Tercero, que esté presidido por un miembro ejecutivo y que se reúna de forma regular.
- Una función especializada en la seguridad de la información con funciones y responsabilidades adecuadas y definidas.

3.29 El Tercero debe asegurarse de que haya una responsabilidad personal por la información y los sistemas procurando que exista la responsabilidad apropiada de los entornos, información y sistemas empresariales críticos y que se asigne a personas capaces.

3.30 El Tercero debe garantizar que BT sea notificado (por escrito) lo antes posible, en caso de poder hacerlo legalmente si el Tercero es objeto de una fusión, adquisición o cualquier otro cambio de propiedad.

Gestión de incidentes

3.31 El Tercero debe contar con un marco de gestión de incidentes consolidado y uniforme para garantizar que estos se gestionen, se contengan y se mitiguen adecuadamente, y que incluya los siguientes componentes:

- Garantizar que el personal conozca sus funciones y el orden de las operaciones cuando se necesite una respuesta.
- Garantizar que los incidentes se comuniquen de acuerdo con los criterios establecidos.
- Garantizar que el impacto del incidente se comprenda.
- Garantizar que se ejecuten los procedimientos forenses cuando sean precisos internamente o a través de una función especializada.

- Garantizar que se integren las lecciones aprendidas de los incidentes en los casos de buenas prácticas.
- Garantizar que la información relacionada con un incidente que afecte a BT sea tratada como «Confidencial».

3.32 El Tercero tomará todas las medidas razonables para garantizar que se designe a las personas apropiadas y asuman la responsabilidad como Puntos de Contacto para asuntos de riesgos de seguridad, gestión de incidentes y gestión del cumplimiento. El Tercero deberá notificar a la Parte Interesada de BT, los datos de Contacto de esas personas y los posibles cambios que pueda haber.

3.33 El Tercero informará a BT por e-mail security@bt.com o por teléfono al (+44) 0800 321 999, en un plazo razonable desde que tenga conocimiento de cualquier incidente que afecte al servicio en BT o a la Información de BT y, en cualquier caso, no más tarde de veinticuatro (24) horas desde el momento en el que el Tercero tenga conocimiento del mismo.

3.34 Sin demoras injustificadas, el Tercero deberá tomar las medidas correctivas adecuadas y oportunas para mitigar los riesgos y los efectos relacionados con el incidente para reducir su gravedad y duración.

3.35 El Tercero presentará en los 30 días posteriores a un incidente un informe a la Parte Interesada de BT con respecto a cualquier incidente que afecte al servicio en BT o la Información de BT, que debería incluir, como mínimo:

fecha y hora, lugar, tipo de incidente, impacto, estado y resultado (incluyendo las recomendaciones de resolución o acciones emprendidas).

3.36 El Tercero deberá realizar un análisis de la causa de origen de todos los incidentes de seguridad. Los resultados de este análisis deben hacerse llegar al nivel de dirección adecuado dentro de la organización del Tercero.

Gestión del cambio

3.37 El Tercero debe garantizar que todos los cambios de IT sean aprobados, registrados y probados, incluyendo la recuperación en caso de cambios fallidos, antes de la implementación, para evitar perturbaciones en el servicio o violaciones de seguridad y que exista un procedimiento para realizar las actualizaciones de emergencia de manera controlada.

3.38 El Tercero deberá garantizar que los cambios se reflejen en los entornos tanto de producción como de recuperación.

3.39 El Tercero deberá garantizar que el mantenimiento y la reparación de los activos de la organización se realice y se registre con herramientas controladas y aprobadas.

3.40 El Tercero deberá garantizar que el mantenimiento remoto de los activos organizativos se apruebe, se registre y se realice de forma que se impida el acceso no autorizado.

Gestión de amenazas y ciberseguridad

3.41 El Tercero debe garantizar que exista un marco para la evaluación de las amenazas y los riesgos de Ciberseguridad implementado para que el perfil de riesgo de Ciberseguridad de

las operaciones, los activos, las instalaciones y los miembros de la organización sea comprendido y gestionado mediante:

- La evaluación de las vulnerabilidades de los activos.
- La identificación de las amenazas tanto internas como externas.
- La sensibilidad de la información/datos en cuestión.
- La evaluación de los posibles impactos empresariales.
- Se utilizan las amenazas, vulnerabilidades, probabilidades e impactos para determinar el riesgo.
- Garantizar que el marco de gestión de amenazas y Ciberseguridad se acuerda a un nivel adecuado en la organización.

3.42 El Tercero debe garantizar que todos los riesgos y amenazas identificados dentro de la evaluación de amenazas y Riesgos de Ciberseguridad se prioricen y se actúe como corresponda para mitigar los riesgos dentro de un calendario adecuado.

3.43 El Tercero debe notificar a la Parte Interesada de BT si no puede remediar o reducir determinadas áreas sustanciales de riesgo que podrían afectar al servicio prestado.

Gestión de identidades y control de acceso

3.44 El Tercero deberá contar con un marco consolidado y uniforme para garantizar que las identidades y las credenciales se gestionen de forma segura a través de personal autorizado:

- La concesión, reactivación, modificación y desactivación de los derechos de acceso basándose únicamente en aprobaciones documentadas y autorizadas.
- Garantizar que las cuentas durmientes estén deshabilitadas.
- Deshabilitar las cuentas del personal que ya no esté empleado en la empresa.
- Implementar procesos y herramientas para seguir, controlar, prevenir, corregir el uso, asignación y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.
- Se realicen revisiones de acceso periódicas para garantizar que ese acceso sea adecuado a su objetivo.
- Se exige que las cuentas de usuario se recertifiquen al menos anualmente y que las cuentas privilegiadas lo hagan trimestralmente.
- Garantizar que los secretos y credenciales permanentes (por ejemplo, el acceso mediante cuentas de acceso de emergencia de tipo «break-glass») estén protegidos dentro de un almacenamiento protegido mediante hardware y que solo estén a disposición de la(s) persona(s) responsable(s) en caso de emergencia.
- Garantizar que las credenciales no persistentes (por ejemplo, autenticación de nombre de usuario y contraseña) se almacenen en un servicio centralizado con un control de acceso adecuado basado en la función, que se deberá actualizar en función de cualquier cambio pertinente en las funciones y responsabilidades dentro de la organización.

3.45 El almacenamiento central para credenciales permanentes deberá estar protegido mediante hardware. Por ejemplo, en un host físico, podría encriptarse la unidad utilizando un Módulo de Plataforma Fiable (TPM). Cuando se utilice una máquina virtual (VM) para prestar un servicio de almacenamiento central, dicha VM y los datos que contenga también deberán encriptarse, además de utilizar un inicio seguro y estar configurados para garantizar que solo pueda ser puesta en marcha en el entorno adecuado. El Tercero debe garantizar que el acceso remoto se gestione de manera que tan solo las personas autorizadas puedan acceder de forma remota a los sistemas Terceros y que las conexiones sean seguras y eviten las fugas de datos, con un control adecuado como la autenticación multifactor (MFA).

La autenticación de doble factor debe lograrse con una ID de usuario, una contraseña y uno de los siguientes métodos:

- Generador de contraseñas de un solo uso: requiere un PIN/contraseña específica del usuario para visualizar la contraseña de un solo uso.
- Una tarjeta inteligente con un chip según la norma ISO 7816, y con el correspondiente lector y software de lectura de tarjetas. Las tarjetas inteligentes sin contacto no están permitidas.
- Autenticación basada en certificados emitidos de acuerdo con la política de certificados de Infosec del Tercero.

Para evitar dudas, si se proporciona el acceso privilegiado para el soporte a través de acceso remoto, debe realizarse mediante una conexión segura y utilizar autenticación de doble factor.

3.46 El Tercero debe garantizar que los permisos y autorizaciones de acceso para todos los sistemas (incluyendo las herramientas, aplicaciones, bases de datos, sistemas operativos, equipos, etc.) se gestionen incorporando los principios del mínimo privilegio y la separación de funciones.

3.47 El Tercero deberá comprobar que cada transacción pueda ser atribuida a una sola persona identificable y, si existen credenciales compartidas, debe haber controles adecuados de compensación (incluyendo procedimientos para acceso a cuentas de acceso de emergencia). Las credenciales compartidas para acceso privilegiado no están permitidas.

3.48 El Tercero debe garantizar que toda la autenticación se gestione de forma acorde al riesgo de la transacción, es decir, longitud y complejidad adecuadas de la contraseña, frecuencia de los cambios de contraseña, autenticación multifactorial, gestión segura de credenciales de contraseña y otros controles. El acceso privilegiado se realizará mediante cuentas protegidas con autenticación multifactor. Las cuentas de acceso de emergencia de tipo «break-glass» deben contar con credenciales seguras exclusivas para cada punto de acceso de equipo de la red.

3.49 Deben aplicarse los controles apropiados al gestionarse las autenticaciones fallidas, incluyendo notificaciones en pantalla, registro de fallos y bloqueo de usuarios.

3.50 Deben aplicarse procesos y controles para gestionar y autorizar las cuentas de servicio e invitados.

Protección y clasificación de los datos

3.51 El Tercero debe contar con un marco regulatorio o un sistema de clasificación, etiquetado y gestión de la información consolidado y uniforme (alineado con las Buenas Prácticas de la industria/requisitos de BT) y que contenga los siguientes componentes:

- Directrices de gestión de la información.
- Protección de la información de acuerdo con su nivel de clasificación asignado.
- Garantía de que todo el personal sabe que la Información de BT no deberá emplearse para ningún fin distinto al que se haya suministrado.

Prevención de la fuga de datos

3.52 El Tercero debe tener un marco operativo establecido y coherente que asegure la implementación de protección contra la fuga de datos inapropiada, garantizando que la protección incluya, entre otros, los siguientes vectores:

- E-mail, internet / pasarela web (incluyendo el almacenamiento en línea y correo web), USB, óptico y otros tipos de puertos / almacenamiento portátil, etc., informática móvil y BYOD, servicios de acceso remoto, mecanismos para compartir archivos y redes sociales.
- Los dispositivos no autorizados no deben conectarse a la red (ya sea a la red corporativa del vendedor o a los sistemas/red de BT) ni emplearse para acceder a información no pública.

PCI DSS

3.53 El Tercero debe contar con un marco de gestión de vulnerabilidades consolidado y uniforme que incluya los siguientes componentes:

- Políticas y procedimientos de procesos.
- Funciones y responsabilidades definidas.
- Herramientas apropiadas como sistemas de detección de intrusos y análisis de vulnerabilidades.

3.54 El marco de gestión de vulnerabilidades del Tercero debe garantizar que se comprueben de manera rutinaria los siguientes elementos para detectar posibles incidencias de ciberseguridad:

- Sistemas y activos clave.
- Conexiones no autorizadas.
- Programas/aplicaciones no autorizados.
- Actividad de red.

3.55 El marco de gestión de vulnerabilidades del Tercero debe garantizar que:

- Existan procesos para recibir, analizar y responder a las vulnerabilidades reveladas en la organización tanto de fuentes internas como externas (por ejemplo, pruebas internas, boletines o investigadores de seguridad).
- Solo se permitan herramientas, tecnologías y usuarios autorizados.

- Las vulnerabilidades identificadas se mitiguen o documenten como riesgos aceptados.

Registro y monitorización continua de la seguridad.

3.56 El Tercero debe garantizar que exista un marco de gestión de registros y auditoría consolidado y uniforme que garantice que los sistemas clave que incluyan aplicaciones se configuran para registrar eventos clave (incluyendo accesos privilegiados y actividad del personal) y dichos registros deberán conservarse durante un período mínimo de 13 meses. Los registros para el equipo de red con Funciones Críticas de Seguridad deben registrarse por completo y estar disponibles para ser auditados durante 13 meses.

Como mínimo, el Tercero debe garantizar que los registros traten los siguientes eventos:

- Arranque y apagado del sistema
- Autenticación con éxito o sin éxito
- Conexión y desconexión del sistema
- Creación, modificación y borrado en/de cuentas
- Cambio de credenciales
- Aumento de privilegios
- Bloqueo de cuentas
- Fijaciones y retiradas de hardware
- Alertas y mensajes de error de administración del sistema y de la red
- Cambios en la administración de eventos de seguridad, incluida la administración de grupos y los cambios en las políticas de seguridad
- Punto de inicio y fin del proceso registrado
- Eventos de activación o desactivación de registros
- Cambios en el tipo de eventos registrados tal y como exija el rastreo de auditoría (por ej., los parámetros de arranque y cualquier cambio en los mismos)
- Modificación de registros (o intento de modificación)
- Cualquier forma de acceso en el plano de administración de los sistemas que se usan en relación con una red o servicio público de comunicaciones electrónicas del Reino Unido

Como mínimo, el Tercero debe garantizar que se capturen los siguientes parámetros de registro para cada evento:

- Identidad del activo al que hace referencia el suceso
- Tipo de evento
- Fecha y hora del evento
- Una indicación del éxito/fracaso del evento
- ID de usuario de la cuenta
- Identificación de la fuente del evento, como la ubicación del usuario/sistema, direcciones IP del ID del terminal, ID del terminal u otro medio de identificación.

3.57 El marco de auditoría, registro y monitorización del Tercero debe incluir los siguientes componentes:

- Los registros de eventos generen alertas en tiempo real o casi real para identificar la actividad no autorizada.
- Los eventos y alertas se monitoricn de forma continua por una función independiente y se investiguen, clasifiquen y se les asigne un nivel de gravedad.
- Las alertas clasificadas generen procesos de Gestión de Incidentes de Seguridad que se basen en casos prácticos de supervisión protectora establecidos y en guías según los acuerdos de nivel de servicio y la gravedad.
- Los registros se traten como si se clasificaran como información «Confidencial» como mínimo y se protejan contra la manipulación, el acceso no autorizado y la pérdida.
- La actividad de registro y monitorización se sincronice con una fuente de tiempo NTP aprobada.
- Se establezcan procesos para identificar y configurar casos prácticos de supervisión protectora adicionales y registros de eventos, correlaciones y alertas asociados necesarios para tratar amenazas y riesgos significativos existentes o emergentes.

4. Seguridad del Personal del Tercero

4

4.1 El Tercero deberá garantizar que todo el Personal del Tercero haya firmado acuerdos de confidencialidad antes de comenzar a trabajar en los edificios o en los Sistemas de BT o de tener acceso a la Información de BT. El Tercero deberá conservar los acuerdos de confidencialidad y poner a disposición de BT las pruebas para su auditoría.

4.2 El Tercero tendrá que hacer frente a las violaciones cometidas por el propio Tercero y a los estándares y controles de seguridad aplicables de BT a través de procesos formales integrales de medidas disciplinarias que podrían incluir la exclusión del individuo de las siguientes actividades:

- Acceso a los Sistemas o la Información de BT; o
- Ejecución de cualquier trabajo vinculado a la prestación del Servicio.

Además, el Tercero debe asegurarse de haber implementado los procesos pertinentes para garantizar que todo el Personal del Tercero que haya sido excluido no tenga posteriormente acceso a los Sistemas o la Información de BT y que no se le permita trabajar en relación con la prestación del Servicio.

4.3 El Tercero, en la medida de lo permitido por la ley, deberá contar con un mecanismo confidencial para que el Personal del Tercero pueda denunciar de manera anónima si recibe instrucciones para actuar de manera incoherente o que incumpla estos Requisitos de Seguridad. Los informes pertinentes se notificarán a BT.

4.4 A criterio de BT, cuando el Personal del Tercero ya no esté asignado al Servicio, los activos físicos o la Información de BT que esté en su poder deberán o bien devolverse al equipo operativo de BT pertinente, o bien destruirse de manera segura según los controles de seguridad 3.22 y 3.23.

4.5 El Tercero debe contar con un marco regulatorio consolidado y uniforme sobre el uso aceptable de redes sociales personales y corporativas que incluya garantizar que el personal:

- no publique ningún contenido calumnioso, obsceno o abusivo relativo a la organización o a sus clientes
- no use los logotipos de la organización o los clientes sin permiso previo
- no exponga información de la organización o el cliente que no sea pública sin autorización previa
- no publique opiniones acerca de la organización o sus clientes que pueda interpretarse razonablemente como un comentario oficial de la organización o de sus clientes
- no revele ninguna Información de BT etiquetada como «General», «Confidencial» o «Altamente confidencial».

4.6 El Tercero debe garantizar que todo el personal del Tercero bajo su control siga un curso de formación obligatoria en seguridad de la información que incluya las buenas prácticas en Ciberseguridad y protección de datos personales en el plazo de un mes desde su incorporación y actualice sus conocimientos al menos una vez al año incluyendo si procede:

- Usuarios privilegiados
- Partes Interesadas del Tercero (como subcontratistas, clientes, socios)
- Altos ejecutivos
- Personal de ciberseguridad y seguridad física

4.7 El Tercero debe garantizar que exista una evaluación para verificar que el usuario comprende la formación y toma conciencia.

4.8 El Tercero debe asegurarse de que se lleve un registro actualizado en el que figure el Personal del Tercero que ha recibido la formación mencionada en el apartado 4.6 anterior, los contenidos correspondientes y, en su caso, la lista de evaluaciones realizadas.

5. Revisión de auditoría y seguridad

5.1 Sin perjuicio de cualquier otro derecho de auditoría que pueda tener BT, con el fin de evaluar el cumplimiento por parte del Tercero de los controles de seguridad de esta política de Requisitos de Seguridad, dicho Tercero suministrará a BT o a sus representantes el acceso y la asistencia que sean precisos y apropiados para poder realizar revisiones de seguridad basadas en documentos o auditorías in situ. Se deberá dar un aviso mínimo de 30 días laborales al Tercero antes de hacer una auditoría rutinaria in situ.

El alcance de la auditoría será la revisión de todos los aspectos de las políticas, procesos y sistemas del Tercero (siempre que este proteja la confidencialidad de la información que no esté relacionada con la prestación del Servicio a BT) y que sean relevantes para el Servicio prestado.

5.2 El Tercero trabajará con BT para implementar las recomendaciones acordadas y llevar adelante cualquier acción correctiva que se considere necesaria y que derive de una revisión de seguridad basada en documentos o una auditoría in situ dentro de los 30 días posteriores a la notificación por parte de BT de un incumplimiento grave, 90 días después a la notificación por parte de BT de un incumplimiento leve, o el período que se haya acordado entre las partes.

6. Derecho de Inspección

6.1 El Tercero debe permitir que BT realice una inspección del entorno de control en el que se desarrollan, fabrican o prestan los servicios para realizar pruebas y/o evaluaciones del cumplimiento en materia de seguridad como respuesta a una solicitud razonable (o inmediatamente después de un incidente).

6.2 El Tercero será el responsable de los costes de eliminar las debilidades de seguridad que identifique BT dentro de un calendario acordado por ambas Partes.

6.3 Si se produce un incidente grave, el Tercero deberá colaborar plenamente con BT en cualquier investigación en curso dirigida por BT, una autoridad regulatoria y/o cualquier fuerza o cuerpo de seguridad estatal, permitiendo el acceso y colaborando según se necesite para investigar el incidente. Es posible que BT tenga que solicitar la cuarentena del Tercero para la evaluación de las correspondientes instalaciones pertenecientes al Tercero que ayuden en la investigación, y el Tercero no deberá retrasar ni retener de forma injustificada dicha solicitud.

7. Certificaciones de seguridad

7.1 Los Sistemas del Tercero, el Servicio, los Servicios asociados, los procesos y las ubicaciones físicas deben cumplir y deberán seguir cumpliendo de manera continuada la norma ISO/IEC 27001 (o certificaciones que demuestren unos controles equivalentes, respaldados con el informe de un auditor independiente) y cualquier enmienda o actualización del estándar emitido. Este cumplimiento deberá ser garantizado mediante la debida certificación de ISMS del Tercero por parte de un Servicio de Acreditación Británico (UKAS) o un organismo certificador autorizado equivalente cuando el alcance y la declaración de aplicabilidad incluyan los servicios que se prestan en las ubicaciones donde se prestarán.

7.2 El Tercero deberá enviar un certificado válido al comienzo del Contrato y en el momento de las recertificaciones.

7.3 Si el alcance del certificado o la declaración de aplicabilidad cambia durante la vigencia del contrato hasta el punto de que deje de cubrir todos los servicios prestados en las ubicaciones desde donde se prestan, el Tercero deberá informar a BT en un período razonable. El Tercero deberá informar a BT en el plazo de 2 días laborales de cualquier incumplimiento importante identificado por el organismo certificador o el Tercero, y que suponga un riesgo para los servicios que están siendo prestados.

8. Seguridad física – Instalaciones de BT

8.1 El Tercero deberá cumplir todas las instrucciones pertinentes que se le faciliten con respecto al acceso a las instalaciones de BT y los sistemas de entrada al edificio. Todo el Personal del Tercero que trabaje en las instalaciones de BT deberá tener y mostrar de forma clara una tarjeta identificativa proporcionada por el Tercero o BT que deberá incluir una imagen fotográfica con una representación clara y fehaciente del empleado del Tercero.

8.2 BT también puede suministrar al personal del Tercero una tarjeta de acceso electrónica y/o una tarjeta de visitante de duración limitada que deberá utilizarse de acuerdo con las instrucciones de emisión y revocación locales.

8.3 El Tercero deberá notificar a BT en el plazo de 24 horas cuando una persona del Tercero ya no necesite acceso al edificio de BT y/o acceso a los sistemas de entrada de BT.

8.4 Solo los servidores aprobados de BT, los PC Webtop y los dispositivos finales de confianza de BT podrán conectarse directamente (en el puerto LAN o conexión inalámbrica) a los dominios de BT. El Tercero no deberá conectar ningún equipo que no haya sido aprobado por BT a ningún dominio de BT sin la autorización previa por escrito de BT.

8.5 Deberán cumplirse las políticas y las directrices de seguridad física para trabajar en las instalaciones de BT, que deberán incluir, entre otros, el acompañamiento al personal del Tercero y la adopción de prácticas de trabajo pertinentes dentro de áreas seguras.

8.6 Cuando el Tercero esté autorizado a proporcionar a su personal acceso no acompañado a áreas dentro de las instalaciones de BT, el firmante autorizado del Tercero y el personal del Tercero deberán cumplir el documento guía Acceso de los proveedores a las sedes de BT - Guía de seguridad obligatoria Venta a BT.

9. Seguridad física - Instalaciones de Terceros

9.1 El Tercero debe tener un proceso de acceso físico que incluya métodos y autorizaciones de acceso a las instalaciones de Terceros (sedes, edificios o áreas internas) donde se presten los servicios o donde se almacene o se procese Información de BT. El método de acceso deberá incluir uno o más de los siguientes:

- Una tarjeta de identificación del Tercero autorizado con una imagen fotográfica impresa en la misma que ofrezca una representación clara y fehaciente de la persona.
- Una tarjeta de acceso electrónico autorizado para acceder a las áreas pertinentes de las instalaciones.
- Acceso de seguridad por teclado, que debe disponer de procesos de autorización, difusión de cambios de código (que se hará mensualmente como mínimo) y cambios de código ad hoc.
- Reconocimiento biométrico.

9.2 El Tercero debe contar con procesos y procedimientos para controlar y monitorizar a los visitantes y otras personas externas, incluyendo al personal con acceso físico a áreas seguras o para fines de mantenimiento del control ambiental, mantenimiento de alarmas y servicio de limpieza.

9.3 Las áreas seguras en las instalaciones de Terceros utilizadas para prestar el servicio (por ej., salas de comunicaciones de redes) deben estar separadas de las áreas de acceso general y se protegerán mediante controles de entrada adecuados a los que solo se permitirá acceder a las personas autorizadas. El acceso a estas áreas debe ser auditado regularmente y debe hacerse una evaluación para renovar la autorización de derechos de acceso como mínimo una vez al año.

9.4 El Tercero deberá contar con sistemas de seguridad de CCTV en lugares donde se almacene o gestione Información de BT. Las grabaciones y grabadoras deben ubicarse en lugares seguros para evitar la manipulación, eliminación o visualización «fortuita» de las correspondientes pantallas de CCTV y el acceso a las grabaciones debe someterse a control y limitarse tan solo a las personas autorizadas. Las grabaciones de los CCTV deben guardarse durante un período mínimo de 20 días.

9.5 El Tercero debe haber implementado las medidas adecuadas que garanticen la seguridad física con respecto a lo siguiente:

- Medidas de prevención de incendios, incluyendo entre otras, alarmas, y equipos de detección y extinción.
- Se deben tener en cuenta las condiciones climáticas como temperatura, humedad y electricidad estática y la correspondiente gestión, monitorización y respuesta a condiciones extremas (como apagado automático, alarmas).
- Equipos de control, incluyendo entre otros, aire acondicionado y detección de agua.
- Prevención de daños por agua, localización de depósitos de agua, tuberías, etc. dentro de las instalaciones.

9.6 El Tercero debe garantizar que el acceso físico a las áreas que guardan Información de BT se haga a través de tarjetas inteligentes o de proximidad (o sistemas de seguridad equivalentes, o mejores) y el Tercero deberá llevar a cabo comprobaciones mensuales para garantizar que solo las personas competentes dispongan de dicho acceso.

9.7 El Tercero debe asegurarse de conocer la prohibición de fotografiar y/o capturar imágenes con Información de BT. Si existe una necesidad empresarial de capturar esas imágenes, deberá obtenerse la confirmación por escrito de la Parte Interesada de BT.

10. Suministro de entorno de alojamiento para los equipos de BT

10.1 Si el Tercero dispone de un área de acceso seguro en sus instalaciones para el alojamiento de los equipos de BT o de los clientes de BT, deberá:

- Entregar a BT un plano de planta del espacio asignado en el área segura de las instalaciones.
- Garantizar que los armarios de BT y de los clientes de BT en las instalaciones se mantengan cerrados con llave y que solo pueda acceder el personal autorizado por BT, los representantes aprobados por BT y el personal competente del Tercero.
- Implementar un proceso seguro de gestión de claves.

10.2 BT proporcionará al Tercero:

- Un registro de los activos físicos de BT y/o de los clientes de BT presentes en las instalaciones del Tercero.
- Datos de los empleados, subcontratistas y agentes de BT que necesiten acceder a las instalaciones del Tercero de forma continua.

11. Desarrollo de software seguro

11.1 El Tercero debe garantizar que los entornos productivos y no productivos estén debidamente controlados asegurándose que se tomen las siguientes medidas:

- Segregación de los entornos productivos y no productivos con separación de deberes.
- No deben utilizarse datos activos en las pruebas salvo que se haya acordado previamente con los responsables de los datos y existan unos controles acordes al entorno de producción.
- Segregación de funciones entre el Desarrollo productivo y no productivo.

11.2 El Tercero debe contar con un marco de Desarrollo de sistemas consolidado y uniforme para evitar las vulnerabilidades de seguridad y las brechas de Ciberseguridad que contenga los siguientes componentes:

- Sistemas desarrollados de acuerdo con las mejores prácticas de desarrollo seguro (como OWASP).
- Código almacenado de forma segura y sometido a Controles de Calidad.
- Código adecuadamente protegido frente a las modificaciones no autorizadas una vez que las pruebas se hayan aprobado y se haya lanzado a producción.

12. Custodia

12.1 Si se precisa un Contrato de Custodia (contrato de depósito de garantía) para proteger a todas las partes, tanto los bienes propios como los de Terceros (es decir, Propiedad Intelectual/código Fuente, etc.), el Tercero deberá contar con un marco regulatorio consolidado y uniforme que incluya los siguientes aspectos:

- Ejecución de un Contrato de Custodia con un agente independiente, neutral y reconocido.
- Entrega y actualización continua del código fuente y otros materiales al agente de custodia para garantizar que la información necesaria esté actualizada.
- Almacenamiento seguro del código fuente y el resto del material hasta que se cumplan las condiciones de publicación.
- Condiciones de publicación apropiadas.
- Actualizaciones continuas, los correspondientes pagos y las revisiones del Contrato de Custodia.

13. Acceso a los Sistemas de BT

13.1 El Tercero deberá cumplir todas las instrucciones pertinentes que se le faciliten con respecto al acceso y el uso de los Sistemas de BT.

13.2 El Tercero deberá notificar a BT en el plazo de 24 horas cuando una persona del Tercero ya no necesite acceso.

13.3 El Tercero garantizará que la identificación de usuario, contraseñas, PIN, tokens y el acceso a los recursos de conferencias correspondan a un empleado del Tercero individual y no se compartan. Los detalles se deben guardar en forma segura y separada del dispositivo utilizado para acceder. Si una contraseña la conoce otra persona, debe cambiarse inmediatamente.

Conectividad entre Sistemas

13.4 La vinculación entre dominios con los Sistemas de BT no está permitida salvo que esté específicamente aprobada y autorizada por BT.

13.5 El Tercero debe hacer todo lo posible para garantizar que no entre malware en los Sistemas de BT (tales expresiones que generalmente se conocen en el sector informático).

13.6 Si existe conectividad entre los Sistemas de BT y los de un Tercero, esta se realizará a través de enlaces seguros con protección de datos por encriptación de acuerdo con los controles de criptografía establecidos en 14.9, 14.10, 14.11, 14.12 y 14.13.

13.7 Además, el Tercero asegurará que los sistemas y la infraestructura utilizados se integren en una red lógica específica. Esta red solo debe constar de los sistemas dedicados a la prestación de un servicio seguro de tratamiento de datos del cliente.

14. Sistemas de Terceros que alojan Información de BT

14.1 El Tercero debe garantizar que se apliquen a los sistemas/activos/Redes/aplicaciones los últimos parches de seguridad asegurando que:

- El Tercero despliegue parches tan pronto como sea razonablemente posible y haga todo lo posible por desplegar dentro de los siguientes plazos tras la publicación del parche:

	Explotados activamente en estado salvaje	**EPSS elevado** Vulnerabilidad CVSS: >8,0 (elevada + crítica) EPSS: >= 70 % (Vector de ataque a la red - ver sección de definiciones)	**Menor EPSS** Vulnerabilidad CVSS: >8,0 (elevada + crítica) EPSS: <70 % (Vector de ataque a la red - ver sección de definiciones)	**Otros** (no son vectores de ataque a la red)
Interfaz con exposición externa	7 días	14 días	30 días	90 días
Interfaz con exposición interna	7 días	14 días	30 días	90 días/BAU

- El Tercero usa parches obtenidos de distribuidores directos de sistemas y parches patentados que estén (i) firmados digitalmente o (ii) verificados usando un hash de distribuidor (no deben utilizarse hashes MD5) para el paquete de actualización de forma que el parche pueda identificarse que procede de una comunidad de soporte reconocida dedicada a software de código abierto.
- El Tercero prueba todos los parches en los sistemas que representan con exactitud la configuración de los sistemas de producción objetivo antes de desplegar el parche en los sistemas de producción, y comprueba el correcto funcionamiento del servicio al que se aplica el parche tras cualquier acción de parcheado.
- Monitoree a todos los proveedores pertinentes y resto de fuentes de información correspondientes a alertas de vulnerabilidad.
- Si un sistema no puede parchearse, se deben aplicar medidas correctivas apropiadas.
- El Tercero facilitará parches de seguridad críticos con independencia de futuras versiones, con el fin de maximizar la velocidad a la que es posible implementar el parche.

14.2 El Tercero debe garantizar que, al menos una vez al año, se encargará de realizar una prueba de penetración/evaluación de la seguridad informática aprobada por seguridad de BT de carácter independiente sobre su infraestructura y las aplicaciones informáticas empleadas para prestar servicios que incluya sitios de Recuperación ante desastres para identificar vulnerabilidades que podrían aprovecharse para filtrar datos/servicios y prevenir cualquier

infracción de seguridad a través de ciberataques. El Tercero debe permitir a BT, previa solicitud razonable, acceder a los informes de las pruebas de penetración correspondientes a los servicios que se estén prestando.

14.3 El Tercero debe asegurarse de que el acceso a los puertos de diagnóstico y de gestión, así como a las herramientas de diagnóstico estén bajo controles seguros.

14.4 El Tercero debe asegurarse de que el acceso a las herramientas de auditoría esté limitado al personal relevante del proveedor y su uso esté monitorizado.

14.5 El Tercero debe asegurarse de que los servidores que se usan para prestar los servicios no se instalen en redes no fiables (redes fuera del perímetro de seguridad del Tercero, que estén fuera de su control administrativo, como en el caso de Internet) sin los controles de seguridad apropiados.

Gestión de activos

14.6 El Tercero debe mantener un inventario de activos de información fiable y actualizado con todos los activos tecnológicos que tengan el potencial de almacenar o procesar información, de modo que solo se permita el acceso a los dispositivos autorizados, y se localicen los dispositivos no autorizados y no administrados, evitando así que logren el acceso. Este inventario incluirá todos los activos de hardware, estén o no conectados a la red de la organización. Si procede, en el inventario se incluirá cualquier equipo de BT que se encuentre en las instalaciones de Terceros.

14.7 El Tercero debe garantizar que el inventario de activos de información tiene inventariados o catalogados los siguientes componentes:

- Dispositivos y sistemas físicos, plataformas y aplicaciones de software y sistemas de información externos.
- Los recursos se prioricen (por ejemplo, hardware, dispositivos, datos, tiempo y software) de acuerdo con su clasificación, criticalidad y valor empresarial.
- Flujos de datos Organizativos y de Comunicación, incluyendo flujos de Terceros/externos.
- Procesos manuales que gestionen datos de BT o de Clientes de BT.

14.8 El Tercero deberá mantener un inventario de activos de software preciso y actualizado de todos los programas de software de la red, para que solamente se instale y pueda ejecutarse software autorizado, y se localice el software no autorizado y no administrado, y evitar su instalación o ejecución.

Criptografía

14.9 El Tercero deberá asegurarse de que la Información de BT clasificada como Confidencial o con mayor grado de confidencialidad está adecuadamente encriptada (en tránsito y en reposo). El cifrado se realiceíntegramente con algoritmos criptográficos y cifrados modernos y seguros que utilicen mecanismos robustos de protección de la integridad y que cumplan los estándares de la industria para la negociación segura de protocolos y claves y la gestión de claves. Las siguientes opciones TLS no están permitidas para datos en tránsito: TLS v1.0, TLS

v1.1 y SSL (en cualquier versión). Las siguientes opciones SSH (SFTP) no están permitidas: SSH v1. Las siguientes opciones IPSec no están permitidas: IKE versión 1.

14.10 Las claves criptográficas deben alcanzar o superar las siguientes longitudes mínimas:

- Las claves simétricas (como AES) deben tener una longitud de al menos 256 bits.
- Las claves asimétricas (como RSA) deben tener una longitud de al menos 3072 bits.
- Las claves de curva elíptica deben tener una longitud de al menos 384 bits.

14.11 Si el NIST anuncia que un algoritmo criptográfico ya no es seguro, no deberá utilizarse en nuevas implementaciones. Los proyectos existentes deben revisar el uso continuo de algoritmos criptográficos obsoletos y proporcionar un plan de migración para abandonarlos en favor de una alternativa más segura.

14.12 En el caso de la encriptación simétrica, no se permiten los siguientes algoritmos: 3DES-168 (salvo que sea obligado por una norma internacional), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed y ARIA.

14.13 Deben utilizarse hashes con sal para proteger los datos almacenados, como las contraseñas. El hashing también puede emplearse para anonimizar datos antes de tratarlos, por ejemplo, MSISDN o pagos. Los siguientes algoritmos de hashing no están permitidos: MD2, MD4, MD5 y SHA-1.

Configuración de sistemas

14.14 El Tercero debe contar con un marco regulatorio consolidado y uniforme para garantizar que los sistemas estén correctamente configurados, incluyendo los siguientes componentes:

- Sistemas y dispositivos de red configurados para funcionar de acuerdo con los principios de seguridad (por ejemplo, concepto de funcionalidad mínima y software no autorizado).
- Garantizar que los dispositivos tienen la hora correcta y coincidan.
- Sistemas libres de cualquier forma de software malicioso.
- Comprobaciones apropiadas y monitorización para garantizar que se mantiene la integridad de los sistemas/dispositivos.

Protección contra malware

14.15 El Tercero debe garantizar que se aplique la última protección Antimalware a todos los activos de TI para evitar la interrupción del servicio o impedir violaciones de seguridad y garantizar que se implementen los procedimientos de concienciación del usuario apropiados.

El antimalware debe incluir la detección (entre otros) de ransomware, código móvil no autorizado, virus, troyanos, software registrador de claves, programas espía, gusanos, troyanos, etc.

Mitigación de las denegaciones de servicio

14.16 El Tercero deberá garantizar que los sistemas clave estén protegidos de los ataques de denegación de servicio (DoS) y los ataques distribuidos de denegación de servicio (DDoS).

15. Terceros que alojan Información de BT

15.1 Además de los controles de la Sección 14, en los Sistemas del Tercero que contengan Información de BT, cuando el Tercero aloje Información de BT en un centro de datos o nube, las instalaciones deberán contar con una certificación ISO/IEC 27001 válida para la gestión de la seguridad (o certificaciones que avalen controles equivalentes respaldados por un informe de un auditor independiente).

16. Seguridad de la red – Red propia de BT

Si el Tercero va a instalar equipos, configurar, mantener, gestionar, reparar o monitorizar la red propia de BT, se aplicarán los controles siguientes:

16.1 Cuando se le solicite, el Tercero proporcionará a BT los nombres, direcciones y otros datos similares que BT exija razonablemente de cualquier empleado del Personal del Tercero que:

- participe directamente de forma puntual en la implementación, mantenimiento y/o administración del o de los Servicio(s) antes de su contratación respectiva.
- contacte con BT en relación con las vulnerabilidades identificadas en el/los Servicio(s) de BT y/o Terceros.

16.2 En relación con sus actividades de soporte en el Reino Unido, el Tercero deberá contar con un equipo de seguridad experimentado con al menos una persona de nacionalidad británica que deberá servir de enlace con el Contacto de seguridad de BT y el equipo deberá asistir a las reuniones que puntualmente decida mantener el Contacto de seguridad de BT.

16.3 El Tercero proporcionará a BT un programa (actualizado según se precise puntualmente) de todos los componentes activos incluidos en el/los Servicio(s) y sus fuentes respectivas.

16.4 El Tercero se asegurará de que la instalación de nuevos sistemas, equipos o software en la red propia de BT use la versión de software y el parche más reciente.

16.5 El Tercero se asegurará de que todos los registros relevantes para la seguridad estén habilitados en todos los equipos de la red que instale el Tercero y se envíen a los sistemas de registro de red de BT.

16.6 El Tercero deberá proporcionar información a BT de manera oportuna (es decir, lo antes posible para permitir la corrección antes de su divulgación pública) en relación con cualquier vulnerabilidad en el/los Servicio(s) y cumplir (a expensas del Tercero) con cualquier requisito razonable relacionado con las vulnerabilidades que puedan ser notificados por BT.

16.7 El Tercero se asegurará de que todos los componentes relacionados con la seguridad incluidos en el/los Servicio(s), como los identificados por o para BT ocasionalmente, sean evaluados externamente a coste del Tercero a satisfacción razonable de BT.

16.8 El Tercero deberá proporcionar a BT rápidamente, y en cualquier caso en un plazo de 7 Días Laborables, todos los detalles de cualquier peculiaridad y/o funcionalidad en el/los Servicio(s) o que esté planificada en la hoja de ruta del o de los Servicio(s) que puntualmente:

- conozca el Tercero; o
- BT crea de forma razonable y, por tanto, informe al Tercero de que están diseñadas para, o podrían usarse para, la interceptación legal o cualquier otra interceptación del tráfico de telecomunicaciones. En esos detalles se deberá incluir toda la información que sea

razonablemente necesaria para que BT conozca en profundidad la naturaleza, la composición y la envergadura de tales funciones y/o funcionalidades.

16.9 El Tercero no deberá usar ninguna herramienta de monitorización de redes que pueda visualizar la información de las aplicaciones.

16.10 El personal del Tercero que cree, desarrolle y/o dé soporte a la red de BT deberá superar una comprobación previa al empleo L2 como mínimo. Algunos roles identificados por BT requerirán controles preempleo L3.

16.11 El Tercero permitirá a BT la instalación de software de seguridad según las especificaciones de BT en cualquier infraestructura virtual del Tercero (incluyendo, sin limitarse a, contenedores y máquinas virtuales) o la de un sistema operativo instalado por Tercero que se ejecute en Redes de BT.

16.12 El Tercero debe garantizar que se apliquen a los sistemas/activos/Redes/aplicaciones los últimos parches de seguridad asegurando que:

- El Tercero despliegue parches tan pronto como sea razonablemente posible y haga todo lo posible por desplegar dentro de los siguientes plazos tras la publicación del parche:

	Explotados activamente en estado salvaje	**EPSS elevado** Vulnerabilidad CVSS: >8,0 (elevada + crítica) EPSS: >= 70 % (Vector de ataque a la red - ver sección de definiciones)	**Menor EPSS** Vulnerabilidad CVSS: >8,0 (elevada + crítica) EPSS: <70 % (Vector de ataque a la red - ver sección de definiciones)	**Otros** (no son vectores de ataque a la red)
Interfaz con exposición externa	7 días	14 días	30 días	90 días
Interfaz con exposición interna	7 días	14 días	30 días	90 días/BAU

- El Tercero usa parches obtenidos de distribuidores directos de sistemas y parches patentados que estén (i) firmados digitalmente o (ii) verificados usando un hash de distribuidor (no deben utilizarse hashes MD5) para el paquete de actualización de forma que el parche pueda identificarse que procede de una comunidad de soporte reconocida dedicada a software de código abierto.
- El Tercero prueba todos los parches en los sistemas que representan con exactitud la configuración de los sistemas de producción objetivo antes de desplegar el parche en los sistemas de producción, y comprueba el correcto funcionamiento del servicio al que se aplica el parche tras cualquier acción de parcheado.
- Monitoree a todos los proveedores pertinentes y resto de fuentes de información correspondientes a alertas de vulnerabilidad.
- Si un sistema no puede parchearse, se deben aplicar medidas correctivas apropiadas.
- El Tercero facilitará parches de seguridad críticos con independencia de futuras versiones, con el fin de maximizar la velocidad a la que es posible implementar el parche.

Cuando el Tercero entregue o ponga a disposición bienes, servicios o instalaciones para que se utilicen en relación con una producto ICT o servicio ICT, incluyendo el servicio público de comunicaciones electrónicas del Reino Unido, se aplicarán los siguientes controles de seguridad.

16.13 Cuando el Tercero esté dando soporte a más de un operador, deberán implementarse controles para evitar que un operador o su red pueda afectar negativamente a cualquier otro operador o su red.

16.14 Cuando el Tercero esté ejerciendo una función administrativa para más de un operador, se aplicarán los controles siguientes:

- Implementar una separación lógica dentro de la red del Tercero para separar datos y redes de clientes.
- Implementar una separación entre los entornos de gestión del Tercero usados para distintas redes de operadores.
- Implementar y hacer cumplir las funciones de seguridad en la demarcación entre la red del Tercero y la red del operador.
- Implementar controles técnicos para limitar el potencial de que los usuarios o los sistemas puedan impactar negativamente a más de un operador.
- Implementar Estaciones de Trabajo de Acceso Privilegiado física y lógicamente independientes para cada operador.
- Implementar dominios administrativos y cuentas independientes para cada operador.

16.15 Al proporcionar un equipo de red, los Terceros deben facilitar a BT una «declaración de seguridad» que detalle la producción del equipo seguro y el modo en que se garantiza la seguridad del equipo durante toda la vida útil del mismo. Esta declaración de seguridad cubrirá los requisitos de la Evaluación de Seguridad del Proveedor y deberá aprobarse a un nivel adecuado de antigüedad acordado con BT.

16.16 Cuando el Tercero suministre el equipo de red, se aplicarán los controles siguientes:

- El Tercero garantiza que adherirá a un estándar no inferior al especificado en la «declaración de seguridad» publicada.
- El Tercero proporcionará una guía actualizada que describa la implementación segura del equipo.
- El Tercero ofrecerá soporte para todo el equipo y todos los subcomponentes de software y hardware durante toda la duración del contrato.
- El Tercero facilitará información sobre todos los principales componentes y dependencias de Terceros, incluyendo, pero sin limitarse al producto y a la versión, a los componentes de código abierto, al nivel de soporte y al periodo.
- El Tercero solucionará cualquier problema de seguridad descubierto en sus productos que suponga un riesgo de seguridad para un servicio o red de BT dentro de un plazo razonable a partir de la notificación del mismo, y mientras tanto ofrecerá actualizaciones periódicas sobre el progreso. El plazo anteriormente mencionado se negociará entre BT y el Tercero

de modo razonable por ambas partes. Esto incluirá todos los productos afectados por la vulnerabilidad, y no solo el producto por el que se reportó la vulnerabilidad.

- El Tercero eliminará o cambiará las contraseñas predeterminadas y las cuentas preprogramadas o codificadas o se asegurará de que el equipo de red esté configurado para permitir a BT hacerlo.
- Siempre que sea posible, el Tercero deshabilitará los protocolos de administración sin cifrar y, cuando no sea posible, identificarán la presencia de estos protocolos a BT para que se pueda mitigar su uso.

16.17 Si el Tercero ha obtenido certificaciones o evaluaciones de seguridad reconocidas internacionalmente para el equipo (por ejemplo, Common Criteria o NESAS), debe compartir con BT todas las conclusiones que validen dicha evaluación o certificación.

16.18 Cuando la propia red del Tercero tenga el potencial de afectar las Redes de BT en UK, el Tercero deberá, según recomendación de BT, superar el mismo nivel de pruebas que BT pone en práctica en las Redes de BT en UK, debiendo además solucionar cualquier vulnerabilidad identificada según haya sido acordado por ambas partes.

16.19 El Tercero autoriza a BT a compartir según convenga información sobre problemas de seguridad cuando sea necesario para la seguridad de la red.

16.20 La infraestructura y los sistemas utilizados para mantener las redes de BT en UK deben estar ubicados en el Reino Unido.

16.21 Cuando el Tercero lleve a cabo las Funciones de Supervisión de la Red de BT en UK, el equipo utilizado para esta función deberá estar tanto ubicado dentro del Reino Unido como ser operado por el personal con sede en el Reino Unido.

16.22 Cuando el Tercero sea responsable de los registros de seguridad de la red y los registros de auditoría, ambos deberán almacenarse dentro del Reino Unido y protegerse según la legislación británica.

16.23 Cuando el Tercero opera como Tercero Administrador, BT se reserva el derecho a determinar los permisos de las cuentas que utiliza el Tercero para acceder a su red y a exigir todos los registros relacionados con la seguridad de la red del Tercero, en la medida en que estos registros estén relacionados con el acceso a la red de BT. El Tercero monitorizará y auditará las actividades de su personal cuando acceda a la red de BT.

17. Seguridad de redes de Terceros

17.1 El Tercero debe asegurarse de que se establezca y se mantenga la integridad de la red garantizando el adecuado control de los siguientes componentes y notificando a BT en los casos en los que esto no sea técnicamente posible:

- Las conexiones externas con la red estén documentadas, dirigidas a través de un cortafuegos y verificadas y aprobadas antes de que se establezcan las conexiones para impedir violaciones de la seguridad de los datos.
- La red esté debidamente diseñada usando principios de «defensa en profundidad» para garantizar que las infracciones de ciberseguridad se minimicen garantizando la existencia de controles apropiados que eviten cualquier ataque intencionado como la «segmentación de redes».

- El diseño e implementación de la red se revise al menos anualmente.
- Todo el acceso inalámbrico a las redes estará supeditado a protocolos de autorización, autenticación, segmentación y encriptación para evitar violaciones de seguridad.
- Uso de comunicaciones seguras entre dispositivos y estaciones de gestión.
- Uso de comunicaciones seguras entre dispositivos; incluyendo la encriptación de todos los accesos de administrador sin consola.
- Uso de un diseño sólido de arquitectura, dividido en capas y zonas y equipado con un sistema eficaz de gestión de identidades y configuración del sistema operativo que debe estar adecuadamente protegido y documentado.
- Mediante la desactivación (cuando se pueda) de servicios, aplicaciones y puertos que no se usen.
- Mediante la desactivación o eliminación de cuentas de invitados.
- No autorizando relaciones de confianza entre servidores.
- Uso del principio de seguridad de buenas prácticas de «privilegio mínimo» para realizar una función.
- Garantizando la implementación de medidas apropiadas para la detección de intrusión y/o protección.
- Donde proceda, monitorización de la integridad de los archivos para detectar cualquier adición, modificación o eliminación de datos o archivos de sistema críticos.
- Cambiar todas las contraseñas por defecto y suministradas por los proveedores antes de que los componentes de red operen.
- Deshabilitar los protocolos de administración sin cifrar siempre que sea técnicamente posible.

17.2 La red del Tercero deberá cumplir todos los requisitos legales y regulatorios; y

- Hacer todo lo posible para evitar que personas no autorizadas (por ej., hackers) accedan a la red o redes del Tercero.
- Hacer todo lo posible para reducir el riesgo de mal uso de la red o redes del Tercero por parte de las personas autorizadas con acceso.
- Hacer todo lo posible para detectar las Violaciones a la Seguridad y garantizar una rápida rectificación de cualquier brecha de datos personales, de la identificación de las personas que obtuvieron acceso y de la determinación de cómo lo obtuvieron.

17.3 Cuando el Tercero entregue o ponga a disposición bienes, servicios o instalaciones para que se utilicen en relación con un producto ICT o servicio ICT, incluyendo el servicio público de comunicaciones electrónicas del Reino Unido, se aplicarán los siguientes controles de seguridad adicionales:

- Los sistemas orientados al exterior, excluyendo el Equipo en las Instalaciones del Cliente (CPE), se sometan a pruebas de seguridad cada dos años o cuando se produzca un cambio significativo.

- Los conjuntos de datos sensibles y las Funciones Sensibles o Críticas no se alojen en equipos situados en el Borde expuesto de la red.
- Si no está protegido criptográficamente, deberá implementarse una separación física y lógica entre el Borde expuesto y las Funciones Sensibles o Críticas.
- Deberá implementarse una separación de seguridad mediante Funciones de Cumplimiento de Seguridad entre el Borde expuesto y las Funciones Sensibles o Críticas.

18. Seguridad de la Nube

18.1 El Tercero debe estar certificado al menos con la última versión de la norma ISO27017 o contar con un marco consolidado y uniforme para garantizar que todo el uso de tecnología en la Nube y los datos no públicos almacenados en la nube estén aprobados y se sometan a controles apropiados equivalentes a la última versión de la Cloud Security Alliance, Cloud Controls Matrix (CCM).

18.2 Los acuerdos en materia de servicios (internos o externalizados) de infraestructuras y redes deberán documentar con claridad las responsabilidades compartidas, los controles de seguridad, la capacidad y los niveles de servicio así como los requisitos empresariales o del cliente.

18.3 El Tercero deberá implementar medidas de seguridad en todos los aspectos del servicio prestado, de forma que se proteja la confidencialidad, disponibilidad, calidad e integridad minimizando las oportunidades de que las personas no autorizadas (por ej., otros clientes de la nube) accedan a la Información de BT y a los servicios utilizados por BT.

18.4 Hasta el punto en que el Tercero aporte aplicaciones o servicios alojados a BT, ya sean de tenencia única o múltiple, incluyendo software como servicio (SaaS), plataforma como servicio (PaaS), infraestructura como servicio (IaaS) y ofertas similares, para recopilar, transmitir, almacenar o tratar de cualquier otro modo Datos Confidenciales, el Tercero deberá proporcionar a BT la capacidad de:

- aislar lógicamente dichos Datos Confidenciales de los datos del resto de clientes del Tercero.
- restringir, registrar y monitorizar el acceso a dichos Datos Confidenciales en cualquier momento, incluyendo el acceso por parte del personal del Tercero
- crear, habilitar, deshabilitar y eliminar la clave superior de encriptación (conocida como Clave Gestionada por el Cliente) utilizada para encriptar y desencriptar las claves subsiguientes, incluyendo la clave de encriptación de datos inferior.
- restringir, registrar y monitorizar el acceso a la Clave Gestionada por el Cliente en cualquier momento; ninguna clave posterior de encriptación, clave de encriptación en una jerarquía de clave inferior a la Clave Gestionada por el Cliente, deberá almacenarse en el mismo sistema que los Datos Confidenciales, a menos que esté encriptada por la Clave Gestionada por el Cliente, lo que también se conoce como estar «envuelta» por la Clave Gestionada por el Cliente.

19. Tarjetas SIM

19.1 Cuando el Tercero suministre Tarjetas SIM, se aplicarán los controles siguientes:

- En el caso de las tarjetas SIM de perfil fijo, el Tercero garantizará que los datos SIM sensibles estén adecuadamente protegidos por el fabricante de la tarjeta SIM.
- En el caso de las tarjetas SIM de perfil fijo, el Tercero garantizará que la integridad, la confidencialidad y la disponibilidad de los datos sensibles de la tarjeta SIM compartidos con el fabricante de la tarjeta SIM estén protegidas en cada paso de su ciclo de vida.

20. Información clasificada como OFICIAL o de nivel superior por el Gobierno de Reino Unido (HMG)

20.1 Los Requisitos de Seguridad adicionales que se recogen en el Anexo 1 a los presentes Requisitos de Seguridad se aplicarán a todos los Terceros que almacenen, traten o transmitan información clasificada como OFICIAL de acuerdo con el Programa de clasificación de seguridad del Gobierno de Su Majestad en vigor en cada momento.

21. Términos definidos e interpretación

21.1 Salvo que se defina lo contrario posteriormente, las palabras y expresiones utilizadas en estos Requisitos de Seguridad tendrán el mismo significado que en el Contrato:

«**Acceso»** y **«Accedido»** significa el tratamiento, gestión o almacenamiento de la Información de BT por uno o más de los siguientes métodos:

a. por interconexión con los Sistemas de BT;

b. en papel o formato no electrónico;

c. Información de BT en los Sistemas del Proveedor; o

d. por medios móviles

y/o acceso a las instalaciones de BT para la provisión de suministros, excluyendo el suministro de hardware y la asistencia a reuniones.

«Información de BT» significa toda la Información relativa a BT o un Cliente de BT suministrada al Proveedor y toda la Información tratada o gestionada por el Proveedor en nombre de BT o un Cliente de BT con arreglo al Contrato.

«Parte Interesada de BT» significa el representante de BT que tenga la propiedad del ámbito del trabajo que el Tercero esté acometiendo.

«Sistemas de BT » significa los Servicios y componentes del Servicio, productos, redes, servidores, procesos, sistema basado en papel o sistemas informáticos (en su totalidad o en parte) propiedad de BT y/u operados por BT u otros sistemas que puedan estar alojados en instalaciones de BT.

«Redes de BT en UK» significa cualquier red pública de comunicaciones electrónicas operada por BT en UK, según se define en la sección 32 de la Ley de Comunicaciones de 2003.

«BYOD» significa «traiga su propio dispositivo».

«Contrato» significa el Contrato suscrito por las Partes para el suministro de bienes, software o Servicios que menciona los presentes Requisitos de Seguridad.

«Equipo en las instalaciones del cliente» significa equipo suministrado al cliente y gestionado por el proveedor que se use, o se pretenda usar, como parte de la red o servicio. Esto excluye los dispositivos electrónicos de consumo como teléfonos móviles y tabletas, pero incluye dispositivos como cortafuegos en el borde, equipo SD-WAN o kit de acceso inalámbrico fijos. **“”**

«Cyber Essentials Plus» significa el programa respaldado por el gobierno del Reino Unido para ayudar a las organizaciones a protegerse de ataques informáticos comunes.

«Ciberseguridad» significa el modo en que los particulares y las organizaciones reducen el riesgo de ciberataques. La función principal de la ciberseguridad es proteger contra robo y daños los dispositivos que todos utilizamos (smartphones, portátiles, tabletas y ordenadores) y los servicios a los que accedemos, tanto en internet como en el trabajo.

"EPSS" significa el Sistema de Puntuación de Predicción de Explotación.

«Contrato de custodia» significa el acuerdo de depósito de código fuente suscrito con arreglo al Contrato para utilizar, copiar, mantener y modificar dicho código fuente para los fines empresariales de BT (incluyendo el derecho a compilar ese código fuente).

«Borde expuesto» significa el equipo que bien está en las instalaciones del cliente, accesible mediante equipo del cliente/usuario o bien es físicamente vulnerable. El equipo físicamente vulnerable incluye equipo en armarios externos o conectado a mobiliario urbano. El Borde expuesto incluye CPE, equipo de estación de base, equipo OLT y equipo MSAN/DSLAM.

«Buenas Prácticas de Seguridad de la Industria» significa, en relación con cualquier acción y circunstancia, la aplicación de las prácticas, políticas, estándares y herramientas de seguridad que podrían esperarse de forma razonable y general de una persona cualificada y experimentada comprometida en el mismo tipo de actividad bajo las mismas circunstancias o similares.

«Producto TIC», un elemento o grupo de elementos de una red o de un sistema de información.

«Servicio TIC», un servicio consistente total o principalmente en la transmisión, el almacenamiento, la recuperación o el tratamiento de información por medio de redes y sistemas de información.

«NDA» significa un acuerdo de confidencialidad, un contrato vinculante entre dos o más partes que evita la comunicación de información sensible a otras personas.

"NESAS" significa el Esquema de Garantía de Seguridad de Equipos de Red de GSM Association.

«Activo de Red» significa un producto que forma parte de una colección de componentes interconectados que constituyen una red, como ordenadores, routers, hubs o controladores de telecomunicaciones.

«Vector de Ataque a la Red» significa que el componente vulnerable está vinculado a la pila de red y el conjunto de posibles atacantes va más allá de las demás opciones que se enumeran a continuación, incluyendo todo Internet. Este tipo de vulnerabilidad suele denominarse «explotable de manera remota» y puede considerarse como un ataque explotable a nivel de protocolo a uno o más saltos de la red de distancia (por ejemplo, mediante uno o más routers). Un ejemplo de un un ataque de red sería que un atacante provoque una denegación de servicio (DoS) al enviar un paquete TCP diseñado especialmente mediante una red de área extensa (por ejemplo, CVE 2004 0230).

«Función de Supervisión de Red» se refiere a los componentes de la Red de BT en UK que supervisan y controlan las Funciones Críticas de Seguridad, lo que los hace de importancia vital para la seguridad general de la red. Son esenciales para que BT pueda entender la red, proteger la red o recuperar la red.

«Seguridad de la Red» significa la seguridad de los nodos y las rutas de comunicaciones interconectadas que conectan lógicamente todas las tecnologías del usuario final y los sistemas de gestión asociados.

«NIST» significa Instituto Nacional de Estándares y Tecnología, una unidad del Departamento de Comercio estadounidense. Antes conocido como Oficina Nacional de Estándares, el NIST fomenta y mantiene los estándares de medición. También cuenta con programas activos para promover y ayudar a la industria y a la ciencia a desarrollar y aplicar estos estándares.

«Declaración de información oficial sensible» significa la declaración escrita que debe aportar el Proveedor con respecto a los roles identificados por el Proveedor que tengan Acceso a información clasificada como «Oficial sensible» o con mayores privilegios respecto de las infraestructuras en las que se almacenen, traten o transmitan información clasificada como «Oficial sensible», de la que se adjunta una plantilla en el Anexo 1.

«Estación de trabajo de acceso privilegiado (PAW)» se refiere a las estaciones de trabajo que permiten el Acceso Privilegiado.

«Función Crítica de Seguridad» significa cualquier función de la Red o el Servicio de BT cuya operación es probable que tenga un efecto material sobre el correcto funcionamiento de toda la red o el servicio, o una parte material de los mismos.

«Requisitos de Seguridad» significa este documento tal y como se actualice de forma puntual.

«SIM» significa un token o componente de hardware único, y su correspondiente software, utilizado para autenticar el acceso del suscriptor a la red. En el sentido utilizado en este documento, SIM abarca las UICC/eUICC de hardware, las aplicaciones SIM/USIM/ISIM, las funcionalidades eSIM y RSP y cualquier subprograma SIM.

«Subcontratista» significa un Subcontratista del Proveedor que desarrolle o participe en la provisión de Suministros o que emplee o contrate a personas para participar en la provisión de Suministros.

«Servicio» significa la totalidad de los «**Bienes**», «**Software**» o «**Servicios**» que se definen en el Contrato.

«Transacción» se refiere a datos/información transaccional capturados de transacciones, es decir, datos generados por diversas aplicaciones durante la ejecución o el soporte de procesos diarios de negocio.

«Módulo de Plataforma Fiable» significa la tecnología diseñada para ofrecer funciones relacionadas con la seguridad y basadas en hardware. Un chip de TPM es un criptoprocesador seguro que está diseñado para realizar operaciones criptográficas. El chip incluye diversos mecanismos de seguridad física para lograr que sea resistente a la manipulación, por lo que el software malicioso es incapaz de alterar las funciones de seguridad del TPM. Las funciones de TPM más comunes se usan para las mediciones de la integridad del sistema y para la creación y el uso de claves. Durante el proceso de inicio de un sistema, el código de inicio que se carga (incluido el firmware y los componentes del sistema operativo) puede medirse y registrarse en el TPM. Las mediciones de integridad pueden usarse como prueba de cómo se inició un sistema y para asegurarse de que se usó una clave basada en TPM solo cuando se usó el software correcto para iniciar el sistema.

«Tercero» significa un Proveedor de BT.

«Tercero Administrador» es un proveedor de servicios gestionados, proveedor de funciones de grupo o soporte externo para equipos de proveedores de terceros (por ejemplo, función de soporte de tercera línea)

«**Personal del Tercero**» significa cualquier persona que el Proveedor o sus Subcontratistas contraten para la ejecución de las obligaciones del Proveedor de acuerdo al Contrato.

«Red de Tercero» significa la Red de cualquier proveedor.

«Sistemas de Terceros» significa cualquier ordenador, aplicación o sistemas de red propiedad del Proveedor que se use para acceder, almacenar o tratar Información de BT o que participe en la provisión de Suministros.

Interpretación

21.2 Cualquier palabra que siga a los términos «incluido/a(s)», «incluyendo», «en particular», «por ejemplo» o expresiones similares se deberá interpretar en sentido ilustrativo y no limitará el sentido de las palabras, descripciones, definiciones, frases o términos que los preceden.

21.3 Siempre que un derecho u obligación de una de las Partes se exprese como un derecho u obligación que esta «**puede**» ejercer o ejecutar, la opción de ejercerlo o ejecutarlo quedará a la entera discreción de esa Parte.

21.4 Si se incluye un hipervínculo («**URL**»), dicha referencia se aplicará al recurso online accesible a través de la citada URL u otra URL de sustitución tal y como se haya notificado a la Parte correspondiente de forma puntual.

Versión	Descripción	Autor	Fecha
5.0	Ley de (Seguridad en las) Telecomunicaciones 2021 (TSA) Legislación y adopción de CIS por parte de BT	Jemma Turner	25/10/22
5.1	Modificación a 14.9 TLS	Jemma Turner	17/04/23
5.2	Modificación de diversas cláusulas para incorporar TSA y las vulnerabilidades	Jemma Turner	30/11/23
5.3	Ampliación para fines de cumplimiento NIS2	Jemma Turner	06/05/25

ANEXO 1 – Requisitos de Seguridad Adicionales

Si el Tercero debe Acceder, almacenar, tratar o transmitir información clasificada como OFICIAL o superior, el Tercero deberá cumplir los presentes Requisitos de Seguridad de BT junto con los requisitos que se recogen en este Anexo 1. En todos los casos, el control del máximo nivel sustituirá a los requisitos documentados en otros puntos de estos Requisitos de Seguridad.

1. EMPLEADOS

1.1 Todo el Personal del tercero que tenga Acceso a información clasificada como OFICIAL o superior, o con privilegios elevados a infraestructuras que almacenen, traten o transmitan información clasificada como OFICIAL o superior:

1.1.1 como mínimo deberá someterse al cribado preempleo de acuerdo con el Estándar de Seguridad Básico para el personal (BPSS);

1.1.2 deberá firmar una declaración de acuerdo con la Ley de Secretos Oficiales; y

1.1.3. se le deberá impedir el acceso a la información o a los sistemas, a no ser que posea las autorizaciones de seguridad necesarias que se especifican en el contrato relevante.

2. FORMACIÓN EN SEGURIDAD

2.1. El Tercero exigirá formación en seguridad en la contratación y al menos una vez al año para todos los empleados que tengan acceso a información clasificada como OFICIAL o superior, o con privilegios elevados a infraestructuras que almacenen, traten o transmitan información clasificada como OFICIAL o superior. Esta formación tratará los requisitos de gestión para la información de acuerdo con los requisitos del Programa de clasificación de seguridad del Gobierno de Su Majestad, tal y como se detalla en la Guía de BT para la protección de la información del HMG para Terceros, que BT deberá entregar al Tercero.

2.2. El Tercero actualizará las descripciones laborales de los puestos de trabajo de todos los empleados que tengan acceso a información clasificada como OFICIAL o superior, o con privilegios elevados a infraestructuras que almacenen, traten o transmitan información clasificada como OFICIAL o superior, para exigir la participación en la formación que se describe en el apartado 2.1 anterior. El Tercero deberá mantener un registro de la formación que deberá poner a disposición de BT previa solicitud.

3. CONTROL DE ACCESO

3.1. Si un empleado abandona la empresa o cambia de puesto, sus derechos de Acceso deberán revocarse desde los correspondientes sistemas del Tercero en el plazo de 1 Día Laborable.

3.2. Si a los empleados del Tercero, incluyendo Contratistas, empleados temporales y trabajadores de agencia, se les han otorgado privilegios mayores para la infraestructura de BT, el Tercero deberá enviar una notificación escrita a BT en el plazo de 1 Día Laborable desde el momento en que ya no precisen Acceder a los Sistemas de BT (por ej., si un empleado deja la empresa o cambia de puesto).

3.3. Si los empleados del Tercero, incluyendo Contratistas, empleados temporales y trabajadores de agencia, tienen tarjetas de Acceso permanente a las instalaciones de BT, el Tercero deberá enviar una notificación escrita a BT en el plazo de 1 Día Laborable desde el momento en que ya no tengan que Acceder a las instalaciones de BT (por ej., si un empleado deja la empresa o cambia de puesto).

4. VALORACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS

4.1. El Tercero implementará procedimientos adicionales de gestión de la información para cumplir con los requisitos de gestión de acuerdo con las exigencias del Programa de clasificación de seguridad del Gobierno de Reino Unido y actualizaciones posteriores periódicamente.

5. RESPUESTA A INCIDENTES Y NOTIFICACIÓN - ACUERDOS DE NIVEL DE SERVICIO

5.1. El Tercero será informado de los acuerdos específicos en materia de servicios que sustenten el proceso de respuesta a los incidentes. Estos pueden sustituir a cualquier otro acuerdo anterior establecido en estos Requisitos de Seguridad.

6. AUDITORÍA, PRUEBAS Y MONITORIZACIÓN

6.1. El Tercero implementará monitorización de seguridad 24/7 cuando BT así lo especifique para la infraestructura del Tercero que admite el procesamiento, almacenamiento o transmisión de información clasificada como OFICIAL o superior.

7. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES

7.1. El Tercero elaborará un plan de continuidad del negocio y de recuperación de desastres de acuerdo con la norma BS ISO 22301 en el plazo de 30 días desde la firma del Contrato.

8. LOCALIZACIÓN

8.1. Salvo que BT especifique otra cosa, el Servicio deberá estar físicamente localizado dentro de las fronteras físicas del Reino Unido o, si fuera aplicable, del Espacio Económico Europeo (EEE). Cualquier soporte y/o administración remota del Servicio por parte del Proveedor desde una ubicación en el extranjero solo se llevará a cabo de conformidad con el proceso de aprobación que se establece en el contrato aplicable entre BT y el departamento gubernamental correspondiente.

9. REQUISITOS ADICIONALES PARA INFORMACIÓN OFICIAL SENSIBLE O SUPERIOR

9.1 Todos los puestos identificados por el Tercero como el de Acceso a información clasificada de «OFICIAL SENSIBLE» o superior, o con privilegios elevados a infraestructuras que almacenen, traten o transmitan información clasificada como OFICIAL SENSIBLE o superior deberán documentarse en la Declaración de información OFICIAL SENSIBLE y entregar a BT la Declaración de información OFICIAL SENSIBLE cubierta antes de firmar el Contrato.

9.2 Cuando el Proveedor necesite acceder, almacenar, tratar o transmitir información clasificada como Información Oficial Sensible del HMG o superior, el Proveedor realizará una Evaluación de Riesgos de Seguridad del Personal en todos los puestos identificados en la Declaración de información OFICIAL SENSIBLE del párrafo 2, de conformidad con los requisitos estipulados en el documento «National Protective Security Authority (NPSA) Personnel Security Risk assessment - A guide» (4ª Edición - junio de 2013 o posterior).

ANEXO 1, DOCUMENTO 1 – MODELO DE DECLARACIÓN DE INFORMACIÓN OFICIAL SENSIBLE

1. Sistemas/Servicios en cuestión

Enumere los sistemas y servicios a prestar como soporte del cliente del Gobierno de Reino Unido.

Sistema	Servicio

2. Puestos del Tercero que requieren un nivel de autorización de seguridad.

Puesto	Nivel de autorización de seguridad exigido
* por ejemplo, DBA	SC

3. PCI DSS

Sistema	Tipo de Evaluación de vulnerabilidad	Frecuencia

4. Auditoría, Pruebas y Monitorización

Sistemas a monitorizar 24/7 según indicaciones de BT

ANEXO 2

No aplica

ANEXO 3, Reglamento de aplicación NIS 2 - Código de buenas prácticas para la conversión de los requisitos contractuales de seguridad

Las referencias que figuran a continuación se refieren a las disposiciones del anexo del Reglamento de Ejecución de la Comisión por el que se establecen disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas de gestión de riesgos en materia de ciberseguridad («Reglamento de Ejecución NIS 2»).

Reglamento de aplicación NIS2	Requerimiento	Cláusula de Requisitos de Seguridad de BT
5.1.4	Basándose en la política de seguridad de la cadena de suministro y teniendo en cuenta los resultados de la evaluación de riesgos realizada de conformidad con el punto 2.1. del presente anexo, las entidades pertinentes garantizarán que sus contratos con los proveedores y prestadores de servicios especifiquen, en su caso mediante acuerdos de nivel de servicio, lo siguiente	Ver abajo
5.1.4.a	requisitos de ciberseguridad para los proveedores o prestadores de servicios, incluidos los requisitos relativos a la seguridad en la adquisición de servicios de TIC o productos de TIC establecidos en el punto 6.1. 6.1 requiere: (a) requisitos de seguridad aplicables a los servicios de TIC o productos de TIC que se adquieran; (b) requisitos relativos a las actualizaciones de seguridad a lo largo de toda la vida útil de los servicios de TIC o productos de TIC, o a su sustitución una vez finalizado el período de asistencia; (c) información que describa los componentes de hardware y software utilizados en los servicios de TIC o productos de TIC (d) información que describa las funciones de ciberseguridad implementadas en los servicios de TIC o productos de TIC y la configuración necesaria para su funcionamiento seguro (e) garantía de que los servicios de TIC o los productos de TIC cumplen los requisitos de seguridad con arreglo a la letra a) (f) métodos adecuados para validar que los servicios de TIC o productos de TIC suministrados cumplen los requisitos de seguridad establecidos, así como documentación de los resultados de la validación.	5, 16.15, 16.16
5.1.4.b	los requisitos en materia de cualificación y formación, y en su caso de certificación, exigidos a los empleados de los proveedores o prestadores de servicios	4.6, 7

5.1.4.c	requisitos relativos a la verificación de los antecedentes de los empleados de los proveedores y prestadores de servicios	16.10, Supplier Agreement and Policies Portal Selling to BT
5.1.4.d	obligación de los proveedores y prestadores de servicios de notificar, sin demora injustificada, a las entidades pertinentes los incidentes que supongan un riesgo para la seguridad de la red y los sistemas de información de dichas entidades	3.33
5.1.4.e	disposiciones sobre los plazos de reparación	3.39, 14.1, 16.12
5.1.4.f	el derecho a auditar o a recibir informes de auditoría	5
5.1.4.g	obligación de los proveedores y prestadores de servicios de gestionar las vulnerabilidades que supongan un riesgo para la seguridad de la red y los sistemas de información de las entidades pertinentes	14.1, 16.12
5.1.4.h	requisitos relativos a la subcontratación y, cuando las entidades pertinentes permitan la subcontratación, requisitos de ciberseguridad para los subcontratistas de conformidad con los requisitos de ciberseguridad mencionados en el punto (a)	3.4
5.1.4.i	obligaciones de los proveedores y prestadores de servicios a la terminación del contrato, como la recuperación y eliminación de la información obtenida por los proveedores y prestadores de servicios en el ejercicio de sus funciones	3.23, 3.24

ANEXO 2: MEDIDAS DE CIBERSEGURIDAD DEL GRUPO SANTANDER

El Proveedor cumplirá (y se asegurará de que cualquier Subcontratista y Personal contratado cumpla) con esta cláusula de ciberseguridad siempre y cuando se adquieran por BT servicios y productos para el Grupo Santander.

Cualquier incumplimiento de esta Condición por parte del Proveedor será considerado un incumplimiento material del Contrato.

Este compromiso sobrevivirá al Contrato.

CLÁUSULA DE CIBERSEGURIDAD

DEFINICIONES

A los solos efectos de esta cláusula, los términos definidos a continuación tendrán el significado que se indica y todos los demás términos definidos que aparezcan en esta Cláusula tendrán el significado establecido en el Contrato:

- "**Activo de Información**" significará un compendio de información, ya sea tangible o intangible, que merece protección.
- "**Escaneo de Vulnerabilidades**" significará una técnica utilizada para probar los en busca de vulnerabilidades publicadas en repositorios públicos que permite probar la seguridad mediante técnicas automatizadas en una red a través del análisis de puertos abiertos y servicios en ejecución en un componente individual del sistema o red.
- "**FIPS**" significará el estándar federal de tratamiento de la información que determina los requisitos de seguridad que debe cumplir un módulo criptográfico.
- "**Incidencia relacionada con las TIC**" significará un suceso único o una serie de sucesos vinculados que comprometen la seguridad de la red y de los sistemas de información, y tienen un impacto adverso en la disponibilidad, autenticidad, integridad o confidencialidad de la información, o en los servicios prestados por la entidad financiera.
- "**Información del Cliente**" significará información proporcionada por el Cliente o en su nombre, de conformidad con el Contrato para la prestación de los Servicios o el desarrollo del Proyecto, incluida (sin limitación), la Información Confidencial.
- "**Mínimo Privilegio Requerido**" significará el principio de mínimo privilegio, que establece que los usuarios y los programas sólo deben tener los privilegios necesarios para completar sus tareas.
- "**NIST**" significará, en sus siglas en inglés, el Instituto Nacional de Normas y Tecnología de EEUU.
- "**OWASP**" significará, en sus siglas en inglés, el proyecto abierto de seguridad de aplicaciones web.
- "**PCI DSS**" significará, en sus siglas en inglés, el estándar de seguridad de datos de la Industria de tarjetas de pago aprobado por el Consejo sobre Normas de Seguridad de la PCI actualmente en vigor.
- "**Pruebas de Penetración Dirigidas a Amenazas**" significará el marco que imita las tácticas, técnicas y procedimientos de los actores de amenazas de la vida real percibidos como una amenaza cibernética genuina, que ofrece una prueba controlada, a medida, dirigida por inteligencia (Red Team) de los sistemas críticos de producción en vivo de la entidad.
- "**Red Team**" significará un ejercicio dirigido no informado para emular las capacidades de ataque o explotación de un adversario potencial con respecto a un grupo de activos con el fin de determinar la capacidad del atacante para superar las defensas perimetrales y comprometer los sistemas internos.
- "**Red y Sistema de Información**" significará (a) una red de comunicaciones electrónicas en el sentido del artículo 2, letra a), de la Directiva 2002/21/CE; (b) todo dispositivo o grupo de dispositivos interconectados o relacionados entre

sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales; o (c) los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los puntos (a) y (b) para su funcionamiento, utilización, protección y mantenimiento.

- "**Riesgo de las Tecnologías de la Información y la Comunicación**" significará cualquier circunstancia que pueda detectarse razonablemente en relación con el uso de la Red y los Sistemas de Información, incluido un mal funcionamiento, sobrecarga de capacidad, fallo, interrupción, deterioro, uso indebido, pérdida u otro tipo de evento, malicioso o no, que, si se materializa, puede comprometer la seguridad de la Red y de los Sistemas de Información, de cualquier herramienta o proceso dependiente de tecnología, de la operación y ejecución de procesos, o de la prestación de servicios, poniendo así en peligro la integridad o disponibilidad de datos, software o cualquier otro componente de los servicios e infraestructuras TIC o causando una violación de la confidencialidad, un daño a la infraestructura física de las TIC u otros efectos adversos.
- "**Separación de Funciones**" significará el principio por el que ningún usuario debe tener privilegios suficientes para hacer un mal uso del sistema por su cuenta.
- "**Sistema de Gestión de Identidades y Accesos**" significará el sistema que aborda la necesidad organizativa de una solución sistémica que gestione el acceso y la autenticación del usuario en aplicaciones, bases de datos o redes externas e internas.
- "**Sistema de Gestión de Seguridad de la Información**" significará las políticas, los procedimientos, las directrices y los recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información y su Red y Sistemas de Información. Se trata de un enfoque sistemático de la gestión de la información para que siga siendo segura, mediante la aplicación de un proceso de gestión de riesgos, tal como se define en la norma ISO/IEC 27001.
- "**SOC 2 de Tipo 2**" significará el informe sobre la descripción de la administración del sistema de una organización de servicios y la idoneidad del diseño y la eficacia operativa de los controles.
- "**Test de Penetración**" significará un tipo de evaluación específica llevada a cabo en sistemas de información o componentes individuales del sistema que pretende simular las acciones de los adversarios que realizan ciberataques hostiles sobre activos concretos con el objetivo de proporcionar un análisis pormenorizado de las vulnerabilidades del activo que podría aprovechar el atacante.
- "**Vulnerabilidad**" significará una debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado por una amenaza.

MEDIDAS DE CIBERSEGURIDAD

El Proveedor deberá desarrollar, implementar y mantener un Sistema de Gestión de la Seguridad de la Información y distribuir dentro de su Organización un conjunto de procedimientos y políticas que cumplan, como mínimo, con los siguientes requisitos:

1. <u>General</u>

1.1. El Proveedor se asegurará de que esté implementado un Sistema de Gestión de la Seguridad de la Información eficaz que se ajuste a la legislación aplicable y a las normas de seguridad internacionales más estrictas, como la norma ISO/IEC 27001 y el Marco de Ciberseguridad del NIST, o cualquier otra que pueda resultar aplicable. Como parte del Sistema de Gestión de Seguridad de la Información, el Proveedor deberá aplicar una política de seguridad de la Red y Sistemas de Información que tenga en cuenta los principios de seguridad integral, gestión de Riesgos de las Tecnologías de la Información y de las Comunicaciones, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y Separación de Funciones. El Sistema de Gestión de Seguridad de la Información incluirá, como mínimo: análisis y gestión de Riesgos de las Tecnologías de la Información y de las Comuniaciones, gestión de Riesgos de las Tecnologías de la Información y de las Comunicaciones de terceros y del Proveedor, catálogo de medidas (de seguridad, organizativas, tecnológicas y físicas), gestión y profesionalización del personal, contratación de productos o servicios de seguridad, detección y gestión de incidencias, planes de recuperación y aseguramiento de

la continuidad del negocio, mejora continua, interconexión de Red y Sistemas de Información y registro de actividad de los usuarios.

El Proveedor deberá reflejar y especificar todas las regulaciones aplicables, estándares industriales (incluido, pero no limitado a PCI DSS) y requerimientos legales en el Sistema de Gestión de Seguridad de la Información.

El Proveedor deberá revisar exhaustivamente todos estos aspectos de forma periódica, al menos una vez al año, así como, tras la ocurrencia de incidencias relevantes relacionada con las TIC o conclusiones derivadas de pruebas o auditorias de procesos relevantes. El Proveedor se compromete a subsanar de manera diligente cualquier deficiencia identificada y a mejorar de manera continua sus Sistemas de Gestión de Seguridad de la Información.

1.2. El Proveedor deberá informar al Cliente de cualquier cambio en su Sistema de Gestión de Seguridad de la Información y/o en su Red y Sistema de Información, incluyendo, pero no limitándose, a sistemas, medidas de seguridad, procesos o procedimientos que puedan afectar, reducir o limitar el nivel de seguridad o los derechos y obligaciones de la presente Cláusula, y proporcionará al Cliente un informe ejecutivo analizando las implicaciones de seguridad de la información de dicho cambio, al menos dentro de los treinta (30) días anteriores a la implementación efectiva de dicho cambio. El Cliente podrá rescindir automáticamente el presente Contrato sin incurrir en penalización o coste alguno (salvo el pago de los honorarios pendientes por los Servicios ya prestados) si el Cliente determina que el cambio podría alterar la eficacia de las medidas de seguridad acordadas en virtud de la presente Cláusula o podría representar un Riesgo para las Tecnologías de la Información y/o las Comunicaciones para los Activos de Información y los Sistemas de Red e Información del Cliente.

1.3. El Proveedor designará a la siguiente persona como enlace de seguridad de la información para trabajar con el equipo de Ciberseguridad del Cliente con el fin de revisar y coordinar todos los asuntos, preocupaciones o dudas que se planeen en relación con los requisitos, normas y prácticas de Información del Cliente y requisitos Ciberseguridad:

Sr/Sra.: _____
C/ _____
Email: _____
Teléfono: _____

1.4. El Proveedor deberá notificar sin demora al Cliente:

a) En caso de que se produzca algún cambio en los datos indicados anteriormente o en relación con otros asuntos de seguridad que no estén relacionados con incidentes de ciberseguridad: cybergrc.risk.continuity@gruposantander.com.
b) Cualquier notificación relativa a incidencias de ciberseguridad deberá notificarse a la siguiente dirección de correo electrónico: cybersecurityincidents@gruposantander.com.

1.5. El Proveedor prestará sin coste adicional, una colaboración y asistencia plenas al Cliente para permitir que este cumpla con sus obligaciones reglamentarias incluidas las relativas a seguridad de los datos, auditoría, cualquier posible notificación de una incidencia de ciberseguridad, cualquier solicitud o queja recibida de una autoridad relacionada con la Información del Cliente o cualquier otra solicitud, notificación o investigación por parte de las autoridades.

1.6. En ningún caso la implementación de las medidas de ciberseguridad señaladas en esta Cláusula podrán constituir una justificación para la disminución de los niveles establecidos en los acuerdos de nivel de servicio (SLA) acordados con el Proveedor.

1.7. Si aún no lo ha hecho, el Proveedor contratará una póliza de seguro con cobertura de ciberseguridad para los daños causados por una Incidencia de Seguridad a la Información del Cliente, a la Red y los Sistemas de Información del cliente o de terceros.

1.8. Para evitar dudas, en caso de conflicto y/o incoherencia entre las medidas de esta Cláusula de Ciberseguridad y las medidas contenidas en otras partes del Contrato (incluidas, en particular, las aplicables a datos personales o subcontratación), las disposiciones que impongan las obligaciones más estrictas serán las que prevalezcan.

2. Gestión de identidades y control de acceso

2.1. El Proveedor implementará y documentará las politicas, procedimientos y mecanismos adecuados de gestión de identidades y control de acceso de los usuarios autorizados para garantizar la confidencialidad, integridad y disponibilidad de la identificación y autenticación únicas de los usuarios y de los sistemas a los que acceden (incluidos los accesos remotos y de emergencia) a la Información del Cliente y a la Red y los Sistemas de Información del Cliente, para habilitar la asignación de los derechos de acceso de usuario, con arreglo a lo siguiente. Para ello, el Proveedor debe identificar, autenticar y autorizar las responsabilidades de los usuarios para el acceso a la Información del Cliente y a la Red y los Sistemas de Información del Cliente, así como identificar e implementar controles esenciales a estos efectos, incluyendo controles y herramientas encaminados a prevenir accesos no autorizados, mantenimiento de registro de todas las asignaciones de identificación y un proceso de gestión del ciclo de vida. El proveedor se asegurará de que los derechos de acceso se proporcionen sobre la base de los principios del "Mínimo Privilegio Requerido" y la "Separación de Funciones". El cumplimiento de estas políticas y procedimientos debe ser objeto de un seguimiento continuo y de revisiones periódicas, al menos anualmente.

2.2. Como mínimo, el Proveedor implementará los controles adecuados para garantizar lo siguiente:

a) Todas las Redes y Sistemas de Información deberán estar integrados en un Sistema de Gestión de Identidades y Acceso.
b) La asignación de una identidad única, correspondiente a una cuenta de acceso única a cada miembro del personal con acceso a la Red y a los Sistemas de Información y la implantación (evitando cuentas genéricas no asignadas a una lista de usuarios específicos) de controles y herramientas sobre restricciones de acceso a la Red y a los Sistemas de Información para evitar accesos no autorizados.
c) Se utilizan cuentas dedicadas para la realización de tareas administrativas en los Sistemas de Red e Información.
d) Los derechos de acceso deben ser proporcionados, retirados o modificados cuando corresponda y de acuerdo con los flujos de aprobación previamente establecidos. El Proveedor implementará los procedimientos adecuados para tramitar los derechos de acceso de nuevas incorporaciones, movimientos internos y bajas.
e) Los derechos de acceso deben certificarse y revisarse periódicamente para garantizar que los usuarios mantienen los derechos estrictamente necesarios, al menos cada seis meses.

2.3. El Proveedor sólo podrá aplicar requisitos mínimos diferentes en materia de gestión de identidades y control de acceso cuando así lo acuerden expresamente las Partes.

2.4. Además de las medidas de seguridad descritas en la presente cláusula de Ciberseguridad, cuando el Proveedor almacene y/o gestione Información y/o Redes y Sistemas de Información del Cliente, el Proveedor deberá implementar y aplicar, para cada acceso del Cliente, MFA y cualquier otro control de acceso y configuración que pueda ser solicitado por el Cliente.

3. Separación de la información y almacenamiento

3.1. El Proveedor implementará y mantendrá medidas y procedimientos de seguridad apropiados para garantizar que la Información del Cliente pueda tratarse por separado, incluidos, entre otros, los siguientes: (a) no se utilizarán datos de producción para pruebas de desarrollo sin el consentimiento expreso previo del Cliente, que se reserva el derecho a solicitar controles adicionales en tales casos; (b) el desarrollo de una nueva aplicación o software se mantendrá separado del entorno de producción; (c) la Información del Cliente se mantendrá separada de la información de otros clientes y de la propia información del Proveedor.

3.2. El Proveedor asegurará el aislamiento lógico del almacenamiento de la Información del Cliente de la de otros clientes así como el despliegue de todas las medidas técnicas necesarias para asegurar la separación de la Información del Cliente.

4. Ciclo de vida del desarrollo seguro de Software

4.1. En caso de que el Proyecto o Servicio conlleve un desarrollo de software, el Proveedor se asegurará de que el software desarrollado por el Proveedor que forme parte del Servicio o Proyecto, o que pueda proporcionar acceso a la Información y/o la Red y los Sistemas de Información del Cliente, se desarrolle utilizando prácticas de codificación segura como OWASP o equivalente. Dicho software se someterá a pruebas de seguridad durante el proceso de desarrollo para detectar vulnerabilidades. Todas las vulnerabilidades detectadas se subsanarán antes del despliegue. El Proveedor deberá contar con una auditoría independiente de terceros o una certificación (SOC 2 Tipo 2 o equivalente) que cubra el procedimiento de desarrollo de software y la gestión de Vulnerabilidades, garantizando que el producto o servicio no tiene ninguna Vulnerabilidad crítica. El Proveedor entregará al Cliente una copia del informe o de la certificación.

4.2. El Proveedor supervisará el uso de cualquier biblioteca de terceros con licencia (incluidas las de código abierto) y la existencia de cualquier versión o actualización, manteniendo informado al Cliente en todo momento. En caso de activos o componentes comerciales adquiridos y utilizados en el funcionamiento de los Servicios, el Proveedor también hará un seguimiento del uso de bibliotecas de terceros, incluidas las de código abierto, manteniendo informado al Cliente en todo momento.

5. Transferencia de información y Prevención de Pérdida de Datos

5.1. El Proveedor se asegurará de que las transferencias electrónicas de Información del Cliente a través de una red pública o no segura se realicen de forma segura utilizando métodos de cifrado estándar del sector adecuados, como FIPS o NIST. El Proveedor contará con controles técnicos adecuados para evitar la transferencia no autorizada de Información del Cliente a dispositivos informáticos portátiles.

5.2. En el caso de que el Proveedor utilice sus propios ordenadores, estaciones de trabajo o cualquier otro dispositivo tecnológico para la prestación del servicio, deberá contar con medidas, políticas y procedimientos de Prevencion de Pérdida de Datos (DLP) efectivos diseñados para evitar la transferencia no autorizada de Información del Cliente. Estas medidas deberán incluir, como mínimo:

a) DLP en el correo electrónico para bloquear el envío de Información del Cliente fuera de la organización.
b) DLP para impedir la navegación en páginas potencialmente dañinas, o que faciliten el robo de datos (filesharing) u otros repositorios de datos no autorizados.
c) DLP en ordenadores que deshabilite los accesos de escritura a discos extraíbles.

5.3. Asimismo, si el servicio está basado en un sistema o aplicación del Proveedor, se restringirá el acceso a dicho sistema o aplicación de forma que sus empleados únicamente puedan acceder desde dispositivos gestionados por la empresa que implementen, como mínimo, las medidas acordadas en esta cláusula. Cuando se requiera acceso remoto a los sistemas se utilizarán siempre conexiones que apliquen cifrado de información (por ejemplo, mediante VPN o protocolos de comunicación cifrada), así como medidas de seguridad similares a las existentes en el caso del acceso a través de ordenadores corporativos.

6. Antimalware

6.1. El Proveedor deberá instalar protección antivirus y/o antimalware en sus Redes y Sistemas de Información aplicando la versión vigente en cada momento, que se actualizará periódicamente de acuerdo con las recomendaciones del fabricante.

7. Identificación y pruebas de Vulnerabilidad

7.1. El Proveedor realizará los siguientes ejercicios y entregará los informes al Cliente, incluida la confirmación de que se han corregido las Vulnerabilidades o, en su caso, de que existe un plan para corregirlas:

- Escaneos de Vulnerabilidades, al menos, una vez a la semana en sistema de producción activos
- Test de Penetración y ejercicios de Red Team sobre activos expuestos a internet relacionados con los sistemas de producción activos del Servicio o el Proyecto, realizados por un experto independiente debidamente cualificado, al menos una vez al año y adicionalmente siempre que se produzcan cambios relevantes en la infraestructura, procesos y procedimientos de la Red y los Sistemas de Información, así como cuando los cambios realizados se deban a Incidentes de Seguridad o por cambios significativos de aplicaciones críticas expuestas a internet.
- pruebas avanzadas al menos cada tres (3) años, o cuando lo solicite la autoridad competente del Cliente, mediante Pruebas de Penetración Dirigidas a Amenazas a través de un experto independiente debidamente cualificado.

7.2. El Proveedor notificará inmediatamente y, en cualquier caso, en un plazo de 24 horas cualquier Vulnerabilidad crítica[1] para la que exista un parche o esté disponible públicamente el vehículo para explotarla ("exploits") en sistemas de producción activos.

7.3. Además, el Cliente, mediante un tercero cualificado designado por él y acordado con el Proveedor (consentimiento que no se denegará injustificadamente), estará facultado para realizar Escaneos de Vulnerabilidades, Test de Penetración y ejercicios de Red Team en los activos del Proveedor orientados a Internet y/o en la Red y los Sistemas de Información únicamente con respecto a los productos y servicios dedicados del Cliente o del Proveedor. En este sentido, el Cliente, a mediante un tercero cualificado designado por él, notificará al Proveedor con una antelación razonable la realización de estas actividades y establecerán en coordinación con el Proveedor el calendario de actuación, a fin de que estos ejercicios tengan el menor impacto posible en las actividades del Proveedor. Dado que la planificación será acordada entre las Partes y el conrol del Proveedor sobre el ejercicio, ni el Cliente ni el tercero cualificado que este designe asumirán responsabilidad u obligación alguna por los daños que el Proveedor pueda sufrir derivados de la realización de estas actividades.

7.4. El Proveedor se encargará de los planes de corrección de Vulnerabilidades de todos los activos bajo su responsabilidad, teniendo en cuenta la criticidad y la exposición de acuerdo con los siguientes requisitos:

- La corrección de la Vulnerabilidad debe hacerse directamente resolviendo la Vulnerabilidad o bien desarrollando o aplicando controles suficientes para mitigar el riesgo de las Tecnologías de la Información y las Comunicaciones.
- Las Vulnerabilidades Altas y Críticas deben ser corregidas en un plazo máximo de treinta (30) días, y las Medias en un plazo máximo de noventa (90) días[2].

7.5. El Proveedor implementará y mantendrá las medidas y procedimientos de seguridad adecuados para garantizar la actualización y parcheado periódicos de todo el hardware y software informático incluyéndose la realización de tests previos a su instalación en entornos de producción para eliminar las vulnerabilidades y suprimir los fallos que podrían propiciar Incidentes de ciberseguridad. La publicación de nuevos parches de seguridad debe ser comprobada semanalmente.

7.6. Además, el Proveedor debe asegurarse de que todos los activos tecnológicos (software y hardware) asociados al Servicio o Proyecto tienen un contrato en vigor con el fabricante o, en su defecto, un contrato de soporte ampliado que incluya la publicación de los parches de seguridad necesarios. En caso de que esto no sea posible, el Proveedor garantizará la migración del activo antes de la fecha de finalización del soporte del software o de las vulnerabilidades.

8. Subcontratistas y terceros

8.1. En caso de que el Cliente haya autorizado a un Subcontratista para el Servicio o Proyecto según lo establecido en el Contrato, el Proveedor deberá: (a) identificar las medidas de seguridad del Subcontratista y describir el tratamiento previsto que este llevará a cabo para que el Cliente pueda evaluar cualquier potencial Riesgo de Tecnologías de la Información y las Comunicaciones e (b) imponer condiciones contractuales legalmente vinculantes al Subcontratista que repliquen las contenidas en este Contrato.

[1] Criticidad basada en una puntuación del Sistema Común de Puntuación de Vulnerabilidades CVSS (CVSS) > 7

[2] Según el CVSS

8.2. El Proveedor evaluará periódicamente a sus subcontratistas y a cualquier otro tercero designado por él mediante auditorías, resultados de pruebas u otras formas de evaluación para validar y garantizar que dichos terceros tengan la capacidad de cumplir los requisitos de seguridad establecidos en esta Cláusula. Las auditorías, resultados de pruebas u otras formas de evaluación realizadas por le Proveedor con respecto a sus Subcontratistas se facilitarán al Cliente anualmente. Sin perjuicio de lo anterior, el Cliente se reserva el derecho de solicitar estos resultados en cualquier momento para el cumplimiento de sus obligaciones legales, reglamentarias y contractuales en materia de ciberseguridad. Estos derechos se extenderán a cualesquiera autoridades competentes y/o de resolución.

8.3. El Proveedor reconoce y acepta que seguirá siendo responsable ante el Cliente en caso de incumplimiento de las condiciones de esta Cláusula por parte de un Subcontratista o cualquier otro tercero designado por él y que asumirá plena responsabilidad ante el Cliente por el desempeño efectivo de las obligaciones correspondientes de cualquier subcontratista que participe en la prestación de los Servicios tanto si este es designado directamente por el Proveedor o indirectamente a través de una cadena de subcontratación.

9. Gestión y notificación de infomes de Incidencias

9.1. El Proveedor desarrollará, documentará e implementará un proceso de gestión de incidencias que incluirá la identificación, calificación, cuantificación, clasificación y escalado de las Incidencias de Ciberseguridad, así como su gestión, notificación y resolución. Dicho procedimiento de gestión de Incidencias de Ciberseguridad deberá ajustarse a la normativa aplicable y remitirse al Cliente para su evaluación. El Proveedor probará exhaustivamente todos los aspectos del proceso de gestión de Incidencias de Ciberseguridad de forma periódica, pero con una frecuencia no inferior a una vez cada doce (12) meses. El Proveedor se compromete a subsanar sin demora cualquier deficiencia en el proceso de gestión de Incidencias de Ciberseguridad que se descubra en dichas pruebas.

9.2. El Proveedor deberá notificar al Cliente de inmediato y, en cualquier caso, en un plazo máximo de cuatro (4) horas después de tener conocimiento de cualquier Incidencia de Ciberseguridad. La obligación de notificar se extenderá a cualquier circunstancia que haga sospechar de la existencia de un Incidente, sin que sea necesario que este se haya materializado o que haya producido un efecto adverso real. La notificación se enviará a la siguiente dirección de correo electrónico cybersecurityincidents@gruposantander.com.

9.3. Sin coste adicional, el Proveedor deberá proporcionar lo antes posible al Cliente, entre otros, (i) una descripción detallada de las categorías de Incidencias relacionadas con las TIC y su impacto en el Proveedor; fecha y hora de detección; información sobre el origen; Información del Cliente, y/o Red y Sistemas de Información afectados; información sobre si el incidente es recurrente o está relacionado con uno anterior; una indicación de si ha habido un impacto o impacto potencial en otras instituciones financieras y Proveedores terceros, (ii) las medidas de mitigación aplicadas para revertir la situación, y (iii) copia de todos los informes internos y forenses como, por ejemplo, informes forenses preliminares, informes de auditoría o informes de cualquier otra naturaleza que se elaboren, los cuales deberán contener, como mínimo, un inventario de indicadores de compromiso y hechos confirmados, así como los logs y cualquier otra información y cooperación que el Cliente pueda solicitar razonablemente en relación con la Incidencia relacoinada con las TIC. Si existen artefactos maliciosos que permitan elaborar perfiles de la amenaza (pruebas, muestras, scripts, etc.), estos se compartirán con el Cliente. El Proveedor tomará las medidas necesarias para investigar inmediatamente la Incidencia relacionada con las TIC e identificar, prevenir y mitigar sus efectos, manteniendo informado al Cliente en todo momento. A discreción razonable del Cliente, el Proveedor concederá al Cliente acceso a sus instalaciones. Además, el Proveedor proporcionará un informe emitido por un tercero independiente que describa las medidas adoptadas para la resolución y mitigación del correspondiente Incidente relacionado con las TIC, confirme su aplicación, y que el incidente ha sido resuelto y no supone un riesgo para la Información del Cliente y/o su Red y Sistemas de Información.

9.4. El Proveedor notificará al Cliente, de forma totalmente anonimizada, cualquier Incidente de Ciberseguridad relevante o crítico en la que el Proveedor esté directamente involucrado y afecte a una entidad de similares características al Cliente.

9.5. El Proveedor no podrá poner a disposición de ningún tercero ninguna comunicación o comunicado de prensa relativo a una Incidencia de Ciberseguridad que afecte al Cliente sin su aprobación por escrito, a no ser que así se exija legalmente.

9.6. El Cliente comunicará las Incidencias de Ciberseguridad a las autoridades competentes (notificaciones iniciales, intermedias y finales), así como, en su caso, a las personas físicas afectadas de acuerdo a la normativa aplicable. Sin perjuicio de lo anterior, el Proveedor colaborará con el Cliente en la elaboración y gestión de dichas notificaciones. En este sentido, ambas partes gestionarán la Incidencia de Ciberseguridad de manera coordinada cuando se requiera notificación a un tercero.

10. Confidencialidad, contratación y formación

10.1. El Proveedor se asegurará de que todos los empleados y contratistas que tengan acceso a la Información o las Redes y Sistemas de Información del Cliente: (i) tengan una obligación de confidencialidad, al menos, tan estricta como las impuestas al Proveedor en virtud del Contrato; (ii) estén adecuadamente cualificados y se mantengan al día de todas las obligaciones de seguridad pertinentes, dispongan de las habilidades técnicas correspondientes y reciban formación en ciberseguridad, como mínimo, anualmente; (iii) estén sujetos a normativa que requiera la aportación de antecedentes de acuerdo a la misma; y (iv) el Proveedor se asegurará de que todos los empleados, incluidos los contratistas y el personal temporal, reciban una formación de concienciación adecuada sobre las políticas y los procedimientos pertinentes, así como sobre las amenazas más recientes que puedan afectar a su función laboral.

11. Eliminación de la información

11.1. Siempre de acuerdo con lo dispuesto en las secciones de protección de datos del Contrato y las secciones relativas al plan de continuidad de negocio, el Proveedor se asegurará de que cualquier información que tenga, ya sea original, reproducida o derivada de la Información del Cliente, con independencia del soporte en el que esté, sea destruida físicamente cuando ya no sea necesaria, en cualquier caso a más tardar treinta (30) días después de la finalización de los servicios aplicables o siete (7) días después de la solicitud del Cliente, de conformidad con la norma NIST de destrucción de discos duros SP 800-88[3] o una norma internacional equivalente. Los registros y certificados de destrucción deberán conservarse y ponerse a disposición del Cliente.

12. Detección y supervisión

12.1. El Proveedor establecerá e implementará políticas y procedimientos para detectar actividades anómalas que puedan afectar a la seguridad de la información y responderá adecuadamente a los eventos de ciberseguridad. Como parte de esta supervisión continua, el Proveedor debe implementar capacidades adecuadas y eficaces para detectar intrusiones, así como eventos que afecten a la confidencialidad, integridad y disponibilidad de la Información del Cliente o de los Activos de Información en los que se encuentra. El Proveedor mantendrá soluciones suficientes para detectar y supervisar eventos con respecto a la actividad del usuario o del sistema.

12.2. Todos los Activos de Informaicón y Redes y Sistemas de Información que gestionen o traten Información del Cliente deben registrar todos los intentos reales o intentados de acceso, así como las violaciones de acceso a la Información Confidencial y a los sistemas que contienen la Información Confidencial, incluidas las adiciones, supresiones, alteraciones y copias de la Información Confidencial durante al menos cinco (5) años, sin perjuicio de los periodos mínimos de conservación establecidos por la normativa aplicable, y facilitarán informes al Cliente previa solicitud.

12.3. Las actividades de los servicios y usuarios que afectan a la Información del Cliente podrán ser monitorizadas por el Centro de Seguridad de las Operaciones (SOC) del Cliente. Para ello, a la solicitud del Cliente, el Proveedor pondrá a disposición del Cliente los registros de seguridad de las aplicaciones donde se procese la Información del Cliente.

13. Protección y segmentación de la Red y los Sistemas de Información

[3] Directrices para la higienización de soportes (NIST SP 800-88)

13.1. El Proveedor aplicará, como mínimo, las sisguientes medidas para proteger la Red y los Sistemas de Información:

a) Segmengación de Red para aislar las partes que compartan niveles similares de importancia y establecer mecanismos de control del tráfico para restringir transferencias entre segmentos; la comunicación entre áreas con diferentes niveles críticos deberá estar segmentada (por ejemplo, mediante firewalls).
b) Red separada y dedicada para la administración de los activos TIC.
c) Identificación e implementación de controles de acceso a la red para prevenir y detectar conexiones a la red por parte de cualquier dispositivo o sistema no autorizado, o cualquier punto final que no cumpla con los requisitos de seguridad aquí contenidos.
d) Diseño de redes de acuerdo con los requisitos de seguridad y teniendo en cuenta las prácticas más avanzadas para garantizar la confidencialidad, integridad y disponibilidad de la red.
e) Aseguramiento del tráfico de red entre las redes internas e Internet y otras conexiones externas.
f) Identificación de funciones, responsabilidades y pasos para la definición, implementación, aprobación, cambio y revisión de reglas de cortafuegos y filtros de conexión. El Proveedor verificará la adecuación de las reglas de cortafuegos y filtros de conexión existentes al menos cada seis meses.
g) Realización de revisiones de la arquitectura de red y del diseño de seguridad de la red al menos una vez al año para identificar posibles Vulnerabilidades. Implantación de una línea de base de configuración segura de todos los componentes de la red y endurecimiento de la red y de los dispositivos de red.
h) Procedimiento para limitar, bloquear y finalizar las sesiones remotas y del sistema tras un período predefinido de inactividad.
i) Medidas para aislar temporalmente, cuando sea necesario, las subredes y los componentes y dispositivos de red.

13.2. El Proveedor dispondrá de navegación web y correo electrónico seguros, así como de controles de acceso a redes (NAC). En los casos en que el Servicio o Proyecto esté conectado a Internet, el Proveedor debe utilizar arquitecturas resistentes para soportar ataques de denegación de servicio.

14. Evaluación de Riesgos de Tecnologías de la Información y las Comunicaciones

14.1. El Proveedor llevará a cabo, como mínimo una vez al año y siempre que se produzcan cambios relevantes en la infraestructura de las Redes y los sistemas de Información, análisis y evaluaciones de impacto del riesgo de las Tecnologías de la Información y las Comunicaciones con el fin de: (a) identificar amenazas razonablemente previsibles que podrían resultar en el tratamiento no autorizado de la Información del Cliente; (b) evaluar la probabilidad de que estas amenazas ocurran y el potentcial daño que podrían causar, teniendo en cuenta la naturaleza y clasificación de la Información del Cliente, con particular atención a la Información Confidencial; y (c) evaluar la suficiencia de las medidas, políticas y procedimientos de seguridad para proteger la Información del Cliente y las Redes y los Sistemas de Información.
14.2. Las evaluaciones de riesgo y planes de tratamiento deben considerar las implicaciones de Ciberseguridad y los estándares sectoriales y requisitos legales aplicables. El Proveedor implementará los controles apropiados para gestionar los riesgos identificados y presentará al Cliente evidencia del rendimiento de los análisis de riesgo, las evaluaciones de impacto y los planes de tratamiento.

15. Cifrado

15.1. El Proveedor se asegurará de que la Información del Cliente (cuando esté en forma eléctronica) sea cifrada en cualquier Red y Sistema de Información mediante la implementación de controles que incluyan, como mínimo, los siguientes elementos:

a) reglas para el cifrado de datos en reposo y en tránsito;

b) reglas para el cifrado de datos en uso. Cuando el cifrado de los datos en uso no sea posible, el Proveedor procesará los datos en uso en un entorno separado y protegido o tomará medidas equivalentes que garanticen la confidencialidad, integridad, autenticidad y disponibilidad de los datos;
c) reglas para el cifrado de las conexiones de red internas y del tráfico con partes externas;
d) disposiciones para la gestión de claves criptográficas que establezcan el uso correcto, la protección y el ciclo de vida de las claves criptográficas;
e) el uso de algoritmos criptográficos que no hayan sido declarados vulnerables u obsoloetos por normas de seguridad internacionales como FIPS o NIST.

15.2. El Proveedor debe permitir la gestión de claves de cifrado a través de la infraestructura del Cliente (BYOK, siglas del inglés "Bring Your Own Key") para que el Cliente tenga control absoluto sobre las claves de cifrado. Si la gestión está delegada en el Proveedor, este debe utilizar elementos diseñados al efecto tales como Módulos de Seguridad de Hardware (HSM) o cualquier otro mecanismo que ofrezca garantías similares.

16. Gestión de Activos de Información y diagrama de flujo de datos

16.1. El Proveedor debe mantener (a) un registro actualizado de los activos informáticos utilizados para la prestación de los Servicios (hardware, software y red), gestionados de acuerdo con su importancia en relación a la necesidad de de negocio y la estrategia de riesgos de la organización; y (b) un diagrama de flujo de datos que incluya la Información del Cliente. Tanto el registro de activos como el diagrama de flujo de datos pueden ser solicitados por el Cliente ocasionalmente.

17. Certificaciones

17.1. El Proveedor deberá entregar una copia de las certificaciones disponibles y vigentes en cada momento. Como mínimo, aquellas certificaciones que se hayan presentado o alegado ante el Cliente durante el proceso de homologación deberán estar vigentes durante la vigencia del Servicio asociado. Adicionalmente, si bajo la consideración del Cliente desde una perspectiva de gestión de riesgos, es necesario, el Cliente se reserva el derecho de solicitar la ampliación del alcance de la certificación para cubrir los servicios.

18. Mejores conficiones

18.1. El Proveedor declara y garantiza que todas las medidas de ciberseguridad adoptadas en virtud del presente Contrato son equivalentes o mejores que las condiciones ofrecidas por el Proveedor a cualquiera de sus clientes existentes para servicios similares. En caso de que el Proveedor celebre un contrato con otro cliente por el que proporcione términos más favorables de los aquí acordados, el Proveedor informará al Cliente lo antes posible y deberá celebrar un acuerdo por escrito para proporcionar dichas condiciones al Cliente.

19. Subsistencia de las restantes estipulaciones

19.1. Salvo lo dispuesto en el presente Anexo, éste no anula ni modifica las restantes estipulaciones del Contrato o de sus Anexos, que permanecerán en pleno vigor y efecto y se limitarán a ser modificadas por el presente Anexo de conformidad con lo dispuesto en el mismo. En caso de contradicción entre los términos del presente Anexo y los del Contrato, prevalecerán las disposiciones del presente Anexo.
19.2. Y, en fe de lo cual, las Partes firman el presente documento, por duplicado, quedando un ejemplar en poder de cada una de ellas y a un solo efecto, en el lugar y fecha indicados en el encabezamiento.