Índice

1. Introducción y ámbito de aplicación

1.1 Este documento presenta los requisitos básicos de seguridad de BT aplicables al ámbito de trabajo que aborda un proveedor. Hay 3 niveles de requisitos.

El primer nivel, descrito en la sección 2, comunica a los proveedores que estén realizando un trabajo que disponen de información limitada de BT y que pueden tener limitado el acceso a los sistemas administrativos y redes de BT. A los proveedores que se encuadren en esta categoría no se les exigirá cumplir ningún otro requisito que aparezca en este documento.

El segundo nivel, descrito en las secciones 3 a 6, es obligatorio para todos los demás tipos de trabajo.

Para el tercer nivel, dependiendo del ámbito de trabajo, puede ser aplicable uno o más requisitos de los descritos en las secciones 7 a 18. Su representante de adquisiciones de BT le aconsejará al respecto.

Algunos de los requisitos pueden hacer referencia a un Anexo de los que figuran a continuación que proporciona información adicional. :

Anexo 1: Clasificación de la información
Anexo 2: Formación obligatoria
Anexo 3: Envío de problemas/consultas a un contacto de seguridad de BT
Anexo 4: Acceso a sitios y edificios de BT para organizaciones ajenas a BT (Reino Unido solamente)
Anexo 5: Requisitos de seguridad de alojamiento externo

1.2 Estos Requisitos de seguridad son adicionales y no afectan a cualesquiera otras obligaciones del proveedor en el contrato (incluyendo, entre otras, las obligaciones que aparecen en las condiciones tituladas "Confidencialidad", "Protección de datos personales" y las comprobaciones previas al empleo (PEC)).

2. Seguridad de la información con acceso limitado

El cumplimiento de la sección 2 es el único requisito aplicable si el proveedor está realizando un trabajo que tenga el acceso limitado a la información de BT y que pueda tener también el acceso limitado a los sistemas administrativos de BT (por ejemplo iSupplier) y a las redes de BT (estos tipos de trabajo incluyen, entre otros, los artículos de oficina, la gestión de instalaciones del edificio, los estudios de campo, los sistemas de cupones y productos con descuentos para empleados, los proveedores de contenidos de televisión y los titulares de derechos de BT.)

Sin perjuicio de las obligaciones de confidencialidad que pueda haber, en las que el proveedor o el personal contratado tengan acceso a información de BT o de clientes de BT (incluidos datos personales) relacionada con BT o con clientes de BT, el proveedor deberá:
(a) garantizar que el personal contratado no directamente empleado en el trabajo de BT no divulgue ni pueda acceder a dicha información (incluidos datos personales) y
(b) mantener (y asegurarse de que todo el personal contratado pertinente mantenga) dicha información (incluidos datos personales) segura y confidencial (incluyendo, entre otros, la creación de los sistemas y procedimientos que sean necesarios para proteger la seguridad de toda la información que pertenezca a BT o que BT controle en la medida en que esté en posesión o bajo el control del proveedor de acuerdo con las prácticas recomendables del sector y la implementación rigurosa de todos estos sistemas y procesos).

Las secciones 3 a 6 inclusive son aplicables a todos los compromisos de proveedores con BT (a excepción de aquellos proveedores de suministros con acceso limitado)

3. Seguridad general de la información

3.1 El proveedor notificará inmediatamente a BT los datos del contacto de seguridad del proveedor y cualquier cambio que se produzca en los mismos.

3.2 Al inicio del contrato, el proveedor notificará por escrito al contacto de seguridad de BT, utilizando el anexo 3, las ubicaciones geográficas en las que se prestan los principales servicios, dónde se encuentra el personal contratado pertinente o dónde se procesa o guarda la información de BT. Durante el contrato, el proveedor también deberá notificar cualquier propuesta de cambio de ubicación geográfica al contacto de seguridad de BT mediante el Anexo 3, de forma que BT pueda volver a evaluar cualquier riesgo para BT o para la información de los clientes de BT.

3.3 El proveedor deberá garantizar que todos los contratos con subcontratistas relevantes incluyan los términos escritos que exigen que el subcontratista cumpla los Requisitos de seguridad para proveedores de BT en la medida en que sean aplicables. Estos términos deben acordarse entre el proveedor y su subcontratista antes de que el subcontratista o cualquier miembro de su personal pueda acceder a los sistemas y a la información de BT.

3.4 El proveedor no utilizará información de BT para otro propósito que no sea el propósito para el que BT proporcionó dicha información al proveedor y solo en la medida necesaria para que el proveedor ejecute el contrato. El proveedor deberá tratar o usar la información de BT de una manera coherente con los requisitos del Anexo 1 de estos Requisitos de seguridad y de conformidad con la legislación aplicable.

3.5 El proveedor notificará al contacto de seguridad de BT, utilizando el Anexo 3, si el proveedor va a ser objeto de una fusión, adquisición o sufrirá cambios en la propiedad, de forma que podamos volver a evaluar cualquier riesgo para BT, para la información de BT o de sus clientes.

3.6 El proveedor deberá revisar estos Requisitos de seguridad, como mínimo una vez al año o cuando haya cambios en los suministros o en la forma en que estos se ofrecen, para asegurarse de que se estén cumpliendo todos los requisitos de seguridad aplicables.

3.7 El proveedor deberá gestionar de forma segura cualquier activo físico de BT y/o artículos de BT asignados al proveedor por BT.

- Los activos físicos y artículos de BT se almacenarán de forma segura cuando no se utilicen. Los ejemplos incluyen, entre otros, dispositivos de acceso remoto, ordenadores portátiles, equipos de red, servidores y documentación de BT.
- Los activos físicos de BT no deben sacarse fuera de las instalaciones de trabajo sin autorización previa.

3.8 El proveedor deberá contar, en lo que respecta a la entrega de los suministros, con los procedimientos formales de gestión de incidentes de seguridad con responsabilidades definidas. Cualquier información sobre cualquier incidente de seguridad se considerará "Confidencial". El proveedor informará al contacto de seguridad de BT, mediante el Anexo 3, en un plazo de tiempo razonable tras la toma de conciencia de cualquier incidente:

i) relacionado con pérdidas materiales, corrupción, daños o mal uso de la información de BT, activos físicos y artículos de BT o acceso indebido o no autorizado a los sistemas o a la información de BT o incumplimiento de cualquiera de las obligaciones del proveedor en virtud de estos Requisitos de seguridad; o

ii) relacionado con la imposibilidad de entregar los suministros de conformidad con el contrato.

iii) cualquier acción que incumpla los requisitos de este documento de seguridad).

Tras una razonable solicitud, el proveedor deberá proporcionar a BT lo antes posible un informe escrito con un plan corrector que incluya un calendario y las medidas que deban tomarse para evitar la repetición del incidente.

3.9 El proveedor deberá garantizar que los riesgos identificados de confidencialidad, integridad o disponibilidad de la información de BT en los procesos o sistemas del proveedor, se traten de inmediato.

3.10 BT podrá llevar a cabo evaluaciones de riesgo en cualquier parte pertinente del servicio, (lo que puede incluir subcontratistas relevantes para el servicio) con el fin de identificar riesgos adicionales para BT derivados de la entrega de los suministros, según sea aplicable. BT puede entonces estipular contramedidas adicionales para abordar cualquier riesgo. Todos los gastos asociados a la implementación de las contramedidas serán acordados por ambas partes.

3.11 El proveedor deberá contar con políticas y procesos de seguridad y mantener la documentación (las copias estarán disponibles en inglés) para demostrar el cumplimiento de estos Requisitos de seguridad y proporcionar a BT acceso a las pruebas de acuerdo con la sección 7 que figura más adelante.

3.12 El proveedor deberá garantizar la existencia de procedimientos y controles que protejan la transferencia de información de BT mediante el uso de mensajes de correo electrónico, de voz, fax y vídeo. (Por ejemplo, cuando en llamadas grupales se garantiza que todos los participantes están autorizados para discutir información de BT). Para obtener más información sobre el manejo de la información de BT, vea el Anexo 1.

3.13 El proveedor habrá implementado los procedimientos para hacer frente a las amenazas de seguridad dirigidas o centradas en BT o en contra de un tercero que trabaje en nombre de BT con el fin de proteger adecuadamente la información de BT.

3.14 El proveedor se asegurará de que las actividades laborales remotas y desde casa relacionadas con la información y los sistemas de BT estén sujetas a los controles de

seguridad adecuados dentro de la organización del proveedor, incluyendo, entre otras, el acceso remoto de usuarios sometidos a una autenticación de gran intensidad.

3.15 A la terminación o vencimiento del contrato, el proveedor deberá destruir de forma segura, según el Anexo 1 de estos Requisitos de seguridad (y procurar que todo el personal contratado y los subcontratistas lo hagan), cualquier información de BT conservada o controlada por el proveedor o sus subcontratistas, salvo que BT especifique otra cosa o esta información sea requerida en virtud de obligaciones legales o normativas. La información archivada debe separarse de las actividades diarias del negocio.

3.16 El proveedor debe conservar la información de BT durante el tiempo que sea necesario para prestar el servicio pero no más de dos años, a no ser que BT haya especificado un período de conservación distinto o dicha información sea necesaria para cumplir requisitos legales o normativos.

3.17 El proveedor se asegurará de contar con la disponibilidad, calidad, integridad y adecuada capacidad para ofrecer el rendimiento requerido del sistema o para entregar los suministros sin interrupciones garantizando:

- Un plan de reserva
- La protección, si procede, de los datos críticos del sistema
- El plan B se pone en marcha donde haya un requisito acordado
- El sistema o servicio es recuperable después de un gran fallo o desastre
- El plan se practica por lo menos una vez al año
- Las copias de seguridad de la información y el software, en su caso, se recogerán y probarán regularmente de acuerdo con una política consensuada de copias de seguridad para garantizar la restauración de los datos sin alteraciones.

4. Seguridad del personal contratado

4.1 El personal pertinente que preste servicios por contrata o personal contratado no dispondrá de acceso hasta que haya completado la formación en seguridad de BT, tal como se detalla en el Anexo 2 de estos Requisitos de seguridad. La formación en seguridad de la información de BT puede sustituirse por la propia formación equivalente en seguridad de la información de los proveedores, siempre que esta haya sido aprobada por parte de la seguridad de BT. Por consiguiente, la formación obligatoria debe actualizarse como se detalla en el Anexo 2. El proveedor deberá mantener los registros de la formación, que estarán disponibles para la auditoría de BT.

4.2 El proveedor se asegurará de que todo el personal contratado firme el acuerdo de confidencialidad para proveedores antes de empezar a trabajar en edificios de BT o con sistemas de BT o de tener acceso a información de BT. Estos acuerdos de confidencialidad debe conservarlos el proveedor y tenerlos disponibles para su revisión por BT en caso de auditoría.

4.3 El proveedor se encargará de las políticas y procedimientos sobre infracciones de seguridad a través de procesos formales que incluyan las medidas disciplinarias que correspondan.

4.4 El proveedor deberá mantener un servicio de atención telefónica confidencial para todo su personal, en la medida permitida por la ley, para que lo utilice el personal contratado si son instruidos para actuar de manera incoherente, infringiendo estos Requisitos de seguridad. Los informes relevantes se notificarán al contacto de seguridad de BT mediante el Anexo 3.

4.5 Cuando al personal contratado ya no se le asigne a los suministros, el proveedor se asegurará de revocar el acceso a la información de BT y de devolver o destruir cualquier activo, artículo o información de BT en posesión del personal contratado al equipo operativo correspondiente de BT, de conformidad con el Anexo 1 de estos Requisitos de seguridad. Cuando proceda, el proveedor implementará un procedimiento controlado de salida que incluya la solicitud por escrito al equipo operativo de BT de eliminar los accesos e identidad en BT. Hay que recordar al personal contratado que el acuerdo de confidencialidad firmado todavía está en vigor y que la información de BT adquirida por razones del trabajo en los suministros no debe divulgarse.

4.6 Como parte de la concesión de acceso, el proveedor deberá mantener y suministrar registros de todo el personal contratado que necesite acceso o esté proporcionando suministros de BT, incluyendo nombre, lugar de trabajo, dirección de correo electrónico de empresa, número de teléfono directo y extensión (si procede) de la empresa y/o número de móvil, fecha de solicitud del número de identificación de usuario (UIN) (si tienen uno), fecha en que fueron asignados al proyecto de BT , fecha en que terminaron la formación obligatoria, fecha en que abandonaron el proyecto de BT y una declaración de comprobación previa al empleo. El contacto de seguridad del proveedor deberá en todo momento garantizar que solo el personal contratado pertinente esté autorizado.

5. Auditoría y revisión de seguridad

5.1 El proveedor deberá permitir (y asegurarse de que todo el personal contratado lo permita) -en lo que respecta a los suministros y siempre que el proveedor mantenga la confidencialidad de la información relativa a sus otros clientes- tras una razonable solicitud de BT o de sus representantes autorizados, el acceso al proveedor y a cualquier subcontratista pertinente a las instalaciones, sistemas y registros que contengan información de BT y de clientes de BT (incluidos datos personales) en la medida en que sea razonablemente necesario para evaluar el cumplimiento de estos Requisitos de seguridad por parte del proveedor.

Esto puede incluir la evaluación de todos los elementos de los controles físicos y lógicos y la validación de los sistemas del proveedor que conserven información de BT. El proveedor deberá facilitar esta evaluación permitiendo que BT recopile, conserve y analice la información relacionada con la entrega de los suministros, si procede, para identificar posibles riesgos de seguridad, proporcionar los mencionados informes a BT y asistir a las reuniones que BT pueda solicitar de forma razonable.

Si BT lo solicita, el proveedor participará en una comprobación remota de estado en línea para fijar el cumplimiento básico de seguridad en las cláusulas de estos Requisitos de seguridad.

6. Investigación

6.1 Si BT tiene razones para sospechar que se ha producido una infracción por parte del proveedor o cualquier subcontratista de las disposiciones de estos Requisitos de seguridad que afecten a sistemas o a información de BT, BT informará al contacto de seguridad del proveedor. El proveedor cooperará plenamente con BT en cualquier investigación subsiguiente llevada a cabo por BT o por cualquier organismo de orden público, lo que puede suponer acceder a la información de BT en las instalaciones del proveedor, facilitando un aviso razonable al proveedor.

Durante la investigación, el proveedor cooperará con BT, proporcionando la ayuda razonable y las facilidades necesarias para investigar la infracción. BT puede exigir que el proveedor se ponga en cuarentena para la evaluación de cualquier activo tangible o intangible perteneciente al proveedor para facilitar la investigación y el proveedor no deberá retener o retrasar la solicitud injustificadamente.

En las secciones 7 a 18 de las cláusulas, la descripción de cada sección especifica a qué tipo de suministros se aplican las cláusulas.

7. Política y requisitos genéricos de seguridad

Se exige el cumplimiento de las cláusulas de la sección 7 si el proveedor tiene acceso a "información sensible" (según el término definido), o está prestando servicios de desarrollo, instalación, mantenimiento, soporte de funciones de red o servicios profesionales de TI.

7.1 El proveedor tendrá el certificado ISO27001 o cumplirá los requisitos de seguridad de la certificación ISO27001 o las políticas de seguridad alineadas con ISO27001 y/o trabajará para lograr la ISO27001 en un plazo acordado con BT.

7.2 Si lo obtiene, BT puede actualizar de vez en cuando las políticas relacionadas con la seguridad, las directrices, los requisitos de seguridad y otros requisitos. BT incorporará actualizaciones relevantes dentro de una versión actualizada de estos Requisitos de seguridad mediante la solicitud de un cambio de contrato, que BT deberá notificar por escrito al proveedor. Todos los gastos asociados a la implementación de los nuevos requisitos de seguridad deberán acordarse entre ambas partes.

7.3 El proveedor deberá poner a disposición de BT copias de las certificaciones de seguridad y la declaración de aplicabilidad correspondientes a los servicios prestados para apoyar la evidencia de cumplimiento de este calendario.

8. Seguridad física: instalaciones de BT

Se exige el cumplimiento de las cláusulas de la sección 8 si el proveedor está proporcionando suministros en instalaciones de BT.

8.1 Todo el personal contratado que trabaje en instalaciones de BT deberá estar en posesión de una tarjeta de identificación suministrada por el proveedor autorizado o por BT. Esta tarjeta se utilizará como medio de verificación de la identidad en las instalaciones de BT en todo momento e incluirá una imagen fotográfica nítida que se parezca realmente al

miembro del personal contratado. Al personal contratado también se le podrá facilitar una tarjeta electrónica de acceso y/o una tarjeta de visitante de duración limitada que se empleará de acuerdo con las instrucciones locales de emisión.

8.2 Solo se permite la conexión directa (en el puerto LAN o conexión inalámbrica) con los dominios de BT a los servidores de integración continua de BT aprobados, a los PC webtop de BT y a los dispositivos finales de confianza. El proveedor no conectará (y, si procede, se asegurará de que ningún miembro del personal contratado lo haga) ningún equipo no aprobado por BT a ningún dominio de BT sin la autorización previa por escrito del contacto de seguridad de BT (utilizando el Anexo 3). El contacto de seguridad de BT deberá presentar la autorización por escrito al iniciar el proceso de concesión de la política de seguridad en BT.

8.3 No se sacará información de BT de sus instalaciones ni se sacará ni instalará equipo ni software en sus instalaciones sin la autorización previa de BT.

8.4 La protección física y las directrices para trabajar en instalaciones de BT deben ser obedecidas, como por ejemplo, la obligación de ir acompañado cuando se accede a zonas seguras. Además, las órdenes o instrucciones que BT comunique al representante del proveedor se considerarán comunicadas al proveedor.

8.5 En los casos en que el proveedor esté autorizado a proporcionar a su personal contratado acceso sin alojamiento a zonas dentro de la propiedad de BT, el signatario autorizado ajeno a BT y el personal contratado deberán obedecer las instrucciones de orientación facilitadas por BT. Además, el signatario autorizado ajeno a BT y el personal contratado pasarán como mínimo las comprobaciones previas al empleo de nivel L2.

9. Seguridad física: instalaciones del proveedor

Se exige el cumplimiento de las cláusulas de la sección 9 si el proveedor está proporcionando suministros desde instalaciones ajenas a BT e incluye a todo el personal contratado y subcontratistas más los empleados, subcontratistas y agentes del proveedor.

9.1 El acceso a instalaciones ajenas a BT (sitios, edificios o zonas internas) donde se proporcionen suministros, o donde se almacene o procese la información de BT, se realizará a través de un proveedor autorizado provisto de tarjeta de identificación. Esta tarjeta se utilizará como medio de verificación de la identidad en las instalaciones que corresponda en todo momento e incluirá una imagen fotográfica nítida que se parezca realmente a la persona. Los individuos también pueden estar provistos de una tarjeta electrónica de acceso autorizado, específica para acceder a las instalaciones correspondientes o un acceso de seguridad mediante teclado con los procesos para controlar la autorización, difusión y modificación del código regular / código ad-hoc.

9.2 El proveedor deberá garantizar que el acceso a los sitios, edificios o zonas internas donde se lleven a cabo los suministros, o donde se almacene o procese la información de BT, deberá ser autorizado y adherirse a los procesos y procedimientos de seguridad, incluyendo a los subcontratistas con acceso físico a estas zonas (por ejemplo, para mantenimiento del control ambiental o empresas de alarma).

9.3 Si lo solicita la empresa BT o el propietario del proyecto de BT, el proveedor garantizará que el personal contratado pertinente se segregue de manera segura del resto del personal del proveedor.

9.4 Las zonas seguras en las instalaciones del proveedor (por ejemplo, salas de comunicaciones de red), estarán separadas y protegidas por adecuados controles de entrada para garantizar que solo se permita el acceso a estas zonas seguras a personal contratado autorizado. El acceso a estas zonas por parte de cualquier personal contratado debe auditarse regularmente mientras que la renovación de la autorización de los derechos de acceso a estas zonas debe llevarse a cabo, como mínimo, una vez al año.

9.5 El proveedor utilizará sistemas de seguridad de CCTV y su medio de registro asociado bien en respuesta a incidentes de seguridad, como una herramienta de vigilancia de seguridad o un elemento de disuasión bien como una ayuda para la posible detención de individuos capturados en el acto de cometer un delito. En los casos en que se graben las imágenes de CCTV (ya sea en una cinta o de forma digital), estas deben conservarse al menos 20 días. Este plazo podrá prorrogarse, sin embargo, en las siguientes situaciones:
i) Si las pruebas de vídeo de CCTV tienen que conservarse por un incidente o una investigación criminal.
ii) Si se especifica como requisito necesario para respetar la legislación.

Todas las cintas de vídeo de CCTV utilizadas para la grabación de imágenes de la cámara deben almacenarse en un armario cerrado con llave; dicha llave debe guardarse y controlarse de forma segura. El acceso al armario deberá restringirse con exclusividad al personal autorizado.
Todos los grabadores de vídeo de CCTV o vídeo digital deben ubicarse discretamente para impedir el acceso no autorizado y la posibilidad de visionar de forma 'casual' las pantallas de CCTV asociadas.

9.6 El proveedor deberá inspeccionar de forma regular la zona que rodea sus instalaciones y se utiliza para productos y/o servicios, según corresponda, en busca de riesgos y amenazas.

9.7 El proveedor debe evaluar el nivel de protección del cableado eléctrico y de telecomunicaciones que transporta datos o soporta servicios de información o de radio/satélite empleado en la provisión de los suministros con el fin de impedir la interrupción de las operaciones comerciales. Las medidas de protección de la seguridad física acordes con la criticidad comercial de las operaciones a las que sirven, deben aplicarse de la siguiente manera:
i) Deben protegerse las carreteras críticas de la empresa, el blindaje de los cables, las arquetas o las cajas en las aceras que lleven cables críticos de la empresa.
ii) El acceso a las cámaras de cables o armarios verticales de cables dentro de los edificios operativos debe restringirse con el uso de lectores electrónicos de control de acceso o con una gestión eficaz de las llaves.
iii) Hay que proteger física y medioambientalmente los enlaces de comunicaciones para PC y los equipos de comunicaciones dentro de las instalaciones de ordenadores.
iv) Los enlaces de comunicaciones por radio y satélite y los equipos de comunicaciones deben ser protegidos adecuadamente.

9.8 Los servicios de seguridad dotados de personal se consideran necesarios para complementar las medidas de seguridad electrónicas y físicas en las instalaciones del proveedor en las siguientes circunstancias:

- La ubicación es de importancia operativa.
- La información de BT procesada puede afectar a la marca y a su reputación.
- Un gran volumen de información de BT procesada (por ejemplo, externalización de procesos empresariales)
- Requisitos contractuales del cliente
- Riesgo o amenaza específicas al sitio
- El proveedor está en posesión de información de BT con un alto nivel de confidencialidad.

9.9 Para proteger los equipos de BT (como servidores o switches de BT) sitos en instalaciones de los proveedores de las amenazas o peligros ambientales, y de la posibilidad de accesos no autorizados, los equipos de BT deberán ubicarse en una zona protegida y separada de los equipos utilizados por los sistemas de organizaciones ajenas a BT. El nivel de separación debe garantizar que la seguridad de los equipos de BT no quede comprometida, ni deliberada ni accidentalmente, como resultado del acceso concedido a organizaciones ajenas a BT. Dicha separación podría ser, por ejemplo, una pared divisoria segura, armarios con cerradura o jaulas metálicas.

9.10 Se emplearán medidas de prevención y de detección para evitar errores de instalación causados por la interrupción de los servicios esenciales u otras influencias ambientales.

- Fuego
- Gas
- Inundación
- Apagón eléctrico

Las alarmas deben instalarse y conectarse de nuevo a una posición dotada de personal de forma permanente para permitir la detección de los siguientes:

- Fuego
- Gas
- Apagón eléctrico
- Fallo en el suministro ininterrumpido de energía eléctrica (SAI),
- Fallo en el control de temperatura del aire acondicionado/humedad

9.11 Los perímetros de seguridad (barreras como paredes, vallas, puertas de entrada controladas con tarjeta o mostradores de recepción con personal) se utilizarán para proteger zonas que contengan información de BT e instalaciones de procesamiento de información.

9.12 Los puntos de acceso como zonas de entrega y carga de mercancía y otros puntos en los que personas no autorizadas pudieran entrar en los locales deben controlarse y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado o ataques deliberados.

9.13 Asegúrese de que el acceso físico a las zonas que tienen acceso a información de BT se haga exclusivamente con tarjetas inteligentes o de proximidad (o sistemas de seguridad equivalentes) y que el proveedor lleve a cabo auditorías internas regularmente para garantizar el cumplimiento de estas disposiciones.

9.14 El proveedor se asegurará de prohibir la fotografía o captura de imagen de cualquier información de BT o información de clientes de BT. En circunstancias excepcionales, si hubiera requisitos empresariales para capturar esas imágenes, hay que obtener por escrito la exención temporal de esta cláusula de parte del contacto de seguridad de BT usando el Anexo 3.

9.15 El proveedor mantendrá una política de escritorio y pantalla despejados para proteger la información de BT.

10. Disposición del entorno de alojamiento

Se exige el cumplimiento de las cláusulas de la sección 10 si el proveedor está proporcionando un entorno de alojamiento a equipos de BT o de clientes de BT.

10.1 El proveedor deberá, en los casos en que el proveedor esté proporcionando una zona de acceso seguro a sus instalaciones para alojar equipos de BT o de los clientes de BT ("Sitio del proveedor"):
(a) garantizar que todo el personal contratado que acceda al sitio del proveedor esté en posesión de una tarjeta de identificación o tarjeta de control de acceso electrónico. Esta tarjeta se utilizará como medio de verificación de la identidad en el sitio del proveedor en todo momento e incluirá una imagen fotográfica nítida que se parezca realmente al miembro del personal contratado;
(b) haber implementado procedimientos para tratar con seguridad las amenazas dirigidas contra el equipo de BT o de los clientes de BT o contra un tercero que trabaje en nombre de BT para salvaguardar la información de BT y del cliente de BT en el sitio del proveedor;
(c) utilizar sistemas de seguridad de CCTV y su medio de registro asociado en el sitio del proveedor en respuesta a incidentes de seguridad, como una herramienta de vigilancia de seguridad o elemento disuasorio y como una ayuda para la posible detención de individuos capturados en el acto de cometer un delito. El proveedor se asegurará de que se graben 20 días de CCTV para que esta sea una herramienta efectiva de investigación;
(d) proporcionar a BT un plano por plantas del espacio asignado en la zona segura del sitio del proveedor y
(e) asegurarse de que los armarios de BT y los de los clientes de BT en el sitio del proveedor se mantengan bloqueados y accesibles únicamente para personal autorizado de BT, representantes aprobados de BT y el personal contratado pertinente;
(f) implementar un proceso de gestión segura de llaves en el sitio del proveedor;
(g) inspeccionar regularmente la zona que rodea el sitio del proveedor en busca de riesgos y amenazas;
(h) documentar y mantener procedimientos de operación (en el idioma del país que origina la tarea de BT) para descargar los requisitos de seguridad detallados dentro de este párrafo 12 y a petición de que BT tengan acceso a dicha documentación.

10.2 BT le proporcionará al proveedor:
(a) un registro de los activos físicos de BT y de los clientes de BT llevado a cabo en el sitio del proveedor;
(b) datos de empleados, subcontratistas y agentes de BT que necesiten acceder al sitio del proveedor (en curso).

11. Desarrollo de suministros

Se exige el cumplimiento de estas cláusulas de la sección 11 si el proveedor se ocupa del desarrollo de los suministros para el uso de BT y/o los clientes de BT. (Esto incluye "componentes disponibles comercialmente", configuraciones de software y fabricación de componentes para los suministros)

11.1 El proveedor aplicará las medidas de seguridad acordadas en todos los componentes suministrados, de manera que se salvaguarde la confidencialidad, disponibilidad e integridad de los suministros al:

(i) mantener la documentación correspondiente (en el idioma del país de origen del trabajo de BT) en relación con la implementación de la seguridad y asegurarse de que esta documentación y la mencionada seguridad estén de acuerdo con las prácticas recomendables del sector

(ii) reducir al mínimo la posibilidad de que personas no autorizadas (por ejemplo: hackers) tengan acceso a los sistemas y a la información de BT, a las redes o a los servicios de BT, y

(iii) minimizar el riesgo de un mal uso de los sistemas y la información de BT, las redes o los servicios de BT que, potencialmente, pudieran causar una pérdida de ingresos o servicios.

11.2 El proveedor deberá demostrar, siempre que se le solicite, que cualquier ensamblaje de software o hardware suministrado (tanto propietario como los disponibles comercialmente) entregado a BT sea el mismo que se acordó con BT. El proveedor deberán mantener la integridad de los ensamblajes incluyendo actualizaciones, sistemas operativos y aplicaciones desde la fábrica hasta el escritorio.

11.3 El proveedor se asegurará de que el desarrollo de sistemas para el uso de BT o el ensamblaje y mantenimiento del hardware propiedad de BT cumpla los requisitos de seguridad de TI de BT, si los facilitó el equipo operativo de BT, o siga las prácticas recomendables del sector.

11.4 El proveedor se asegurará de que los entornos de desarrollo y pruebas no contengan datos en vivo y estén separados de los entornos en vivo. Los datos de prueba facilitados por BT deben eliminarse tras un período determinado por el propietario de los datos de BT.

11.5 El proveedor garantiza que se han hecho todos los esfuerzos razonables para asegurar que el software y/o el hardware (y la documentación proporcionada en formato electrónico) esté libre, entre otras, de todas las formas de

(i) "posesión electrónica" y "bombas lógicas";

(ii) "virus" y "gusanos" que podrían haberse detectado con la última versión (en la fecha de expedición) del software de detección de virus disponible en el mercado;

(iii) "spyware", "adware" y otros tipos de programas maliciosos.

(estas expresiones tendrán los significados que generalmente se entienden dentro del sector informático). El proveedor garantiza, en el momento de su aceptación y después, que el software y/o el hardware se presentarán de acuerdo con la especificación funcional durante el período de garantía. El proveedor deberá emplear únicamente materiales de buena calidad, técnicas y requisitos de seguridad en la ejecución del contrato y, en todo momento, deberá aplicar los Requisitos de seguridad de atención, habilidad y diligencia necesarias en las buenas prácticas informáticas y las metodologías de codificación segura.

11.6 El proveedor deberá trabajar con BT para asegurar el cumplimiento de los Requisitos de seguridad en el marco o marcos adecuados de seguridad a expensas del proveedor; de

vez en cuando esto puede requerir que los suministros realicen pruebas de seguridad en consonancia.

11.7 Cualquier debilidad de seguridad identificada por BT o el proveedor en los suministros se remediará por cuenta del proveedor dentro de los plazos que BT exija razonablemente.

12. Acceso a la información

Aplicable si se especifica en los Requisitos.

12.1 En un plazo de 14 días desde la solicitud por escrito de BT y a elección de BT:
(a) las partes deberán, asumiendo sus correspondientes gastos, ejecutar y entregar a la otra un acuerdo de acceso a la información en forma del Acuerdo de acceso a la información que figura en el Anexo 3; o
(b) el proveedor deberá, por cuenta propia, concertar un acuerdo de depósito de custodia sustancialmente en la forma de acuerdo que figura en el Anexo 21 respecto a la totalidad de la información y la documentación relacionada con los suministros (incluyendo, entre otros, en lo que al software se refiere, todo el código fuente, los datos de enlace, listados de software, datos técnicos completos, notas del programador, toda la información y documentación relacionada con el software que sea necesaria para mantener, modificar y corregir el software y facilitar todos los niveles de asistencia al software) ("la información en custodia") y depositar en custodia con NCC Escrow International Limited (el "agente de custodia ") una copia actualizada de la información en custodia. El proveedor deberá garantizar que la información en custodia permita a BT y/o terceros competentes que representen a BT:

(i) completar todas las obligaciones pendientes del proveedor en virtud del contrato, incluyendo, en otras, las obligaciones que hubieran existido (incluida la obligación de servir todos los pedidos que BT hubiera formalizado de otro modo en virtud del contrato) si el contrato no lo hubiera terminado BT (de forma distinta al párrafo 4 de la condición titulada "Terminación") antes de la expiración de su plazo natural (lo que incluirá cualquier plazo ampliado en virtud de cualquier opción de BT de extender el plazo inicial);
(ii) entender con facilidad la información en custodia, mantener (incluyendo la actualización), modificar, mejorar y corregir la información en custodia y los suministros.

12.2 El proveedor garantizará que la información en custodia depositada en BT o en el agente de custodia, lo que proceda, sea y se conserve lo suficiente como para permitir que un programador o analista razonablemente experto mantenga o mejore el software sin la ayuda de ninguna otra persona o referencia, y el proveedor se compromete, además, a mantener plenamente actualizada la información en custodia durante todo el plazo.

12.3 En caso de que se produzca algún evento que autorice a BT o al agente de custodia, lo que proceda, a utilizar y/o divulgar la información de custodia, el proveedor proporcionará inmediatamente a BT, a sus expensas y por un período razonable, asesoramiento, apoyo, asistencia, datos, información, acceso al personal clave del proveedor o de su otorgante de licencia de software con el propósito de comprender, mantener (incluida la actualización), mejorar, modificar y corregir cualquier parte de la información en custodia y/o del software.

12.4 Sin perjuicio de cualquier otro derecho que pueda tener, BT tendrá automáticamente el derecho no exclusivo, perpetuo, irrevocable, mundial y gratuito de usar la información en custodia, después de su divulgación, con el fin de mantener y dar asistencia a los elementos suministrados y con el derecho no exclusivo, perpetuo, irrevocable, mundial y gratuito de usar, copiar, mantener (incluida la actualización), modificar, adaptar, mejorar y corregir los suministros y cualquier suministro modificado, adaptado, mejorado y/o corregidos, y de otorgar licencias a terceros (sujetas a las limitaciones de las licencias para el proveedor), junto con el derecho a autorizar a terceros a realizar cualquiera de las acciones anteriores en nombre de BT.

12.5 Esta condición perdurará más allá de la expiración o terminación del contrato.

12.6 Si es necesario con el fin de asegurar el cumplimiento en las cuestiones de seguridad, el contacto de seguridad de red de BT (y/o las personas designadas por él, que deberán ser todos empleados de BT) tendrán derechos similares (mutatis mutandis) si se solicita como parte de los suministros, de familiarización y validación (como se definen en el acuerdo de acceso a la información) con respecto al material de origen (como se define en el acuerdo de acceso a la información).

13. Acceso a los sistemas de BT

Se exige el cumplimiento de las cláusulas de la sección 13 si el personal contratado del proveedor necesita acceder a los sistemas de BT para proporcionar los suministros.

13.1 BT puede permitir el acceso para la provisión de los suministros mientras el proveedor esté autorizado a ello.

13.2 En relación con el acceso, el proveedor deberá (y, si corresponde, se asegurará de que todo el personal contratado lo haga):

a) garantizar que la identificación de usuarios, las contraseñas, números PIN, dispositivos y el acceso a las teleconferencias sean exclusivas para cada uno de los miembros del personal contratado y no se compartan. Los detalles se deben almacenar de forma segura y por separado desde el dispositivo que ellos utilicen para el acceso. Si otra persona distinta conoce una contraseña, esta debe cambiarse inmediatamente.

b) Ofrecer a BT, siempre que BT lo solicite de forma razonable, los informes que necesite relacionados con el personal contratado autorizado para acceder a los sistemas de BT.

c) Vincular dominios a los sistemas de BT está prohibido salvo que el contacto de seguridad de BT lo apruebe y autorice utilizando el Anexo 3.

d) Realizar todos los esfuerzos razonables para garantizar la ausencia de virus o códigos maliciosos (como estas expresiones se entienden generalmente en el sector informático) y minimizar el riesgo de corrupción de los sistemas o la información de BT.

e) Realizar los esfuerzos que sean razonables para garantizar que los archivos personales que contengan información, datos o medios sin relevancia para los suministros no se almacenen en servidores de BT, en portátiles y equipos de sobremesa suministrados por BT, en instalaciones de almacenamiento centralizado de BT o en los sistemas de BT.

13.3 Si BT ha proporcionado al proveedor acceso a Internet/Intranet, el proveedor accederá a Internet/Intranet adecuadamente (y se asegurará de que el personal contratado lo haga) para habilitarlo y proporcionar los suministros, según sea el caso. Es responsabilidad del proveedor asegurarse de que se comunican las siguientes instrucciones sobre el abuso de internet y el correo electrónico al personal contratado pertinente como mínimo una vez al año.

No se debe acceder a material que pueda considerarse como: -

a. ofensivo, sexual, sexista, racista, políticamente ofensivo;
b. un acto que pueda acarrear descrédito para BT o las personas;
c. gestionar una empresa privada;
d. una violación de los derechos de autor;
e. telefonía o mensajería por Internet, como Skype;
f. superar los cortafuegos u otros mecanismos de seguridad de BT;
g. que coopere con sitios web o que se pronuncie en línea de forma que pudieran, razonablemente, atribuirse a BT.
h. inaceptable o peligroso y cuyo acceso se bloqueará al usuario.

13.4 El proveedor notificará inmediatamente a BT si algún miembro del personal contratado pertinente ya no necesitara derechos de acceso a los sistemas de BT o si cambiara su función por alguna de las razones del acuerdo permitiendo a BT desactivar o modificar los derechos de acceso a los sistemas de BT.

14. Acceso a la información de BT en los sistemas del proveedor

Se exige el cumplimiento de las cláusulas de la sección 14 si la información de BT se está almacenando o procesando en los sistemas del proveedor.

14.1 Si el personal contratado tiene concedido el acceso a los sistemas del proveedor relacionados con la entrega de productos y/o servicios a BT por parte del proveedor, este último deberá:

a) asegurarse de que cada individuo tenga una identificación única de usuario y una contraseña (que se ajuste a la práctica estándar recomendable del sector) conocida solo por dicho individuo para su uso exclusivo como parte del proceso seguro de inicio de sesión.

b) permitir el acceso a los sistemas propiedad del proveedor que mantengan o accedan a la información o a los sistemas de BT solo en la mínima medida necesaria para permitir que el personal contratado realice sus obligaciones en virtud del acuerdo.

c) mantener los procedimientos formales para controlar la asignación, revisión y revocación y/o terminación de los derechos de acceso.

d) garantizar que la asignación y uso de privilegios mejorados y acceso a las herramientas e instalaciones sensibles de los sistemas del proveedor estén controlados y limitados únicamente a aquellos usuarios que tengan una necesidad empresarial. Las consolas del sistema deben acceder y funcionar en un entorno seguro que esté en consonancia con los activos que se utilizan para la gestión. Debe establecerse una seguridad física adecuada que garantice que no pueda producirse un acceso no autorizado.

e) garantizar que la asignación de contraseñas de usuario a los sistemas propiedad del proveedor que mantengan o accedan a la información de BT se controle a través de un proceso formal auditable de gestión.

f) llevar a cabo revisiones regulares de los derechos de acceso de usuario.

g) garantizar que el acceso físico al equipo informático que almacene o tenga acceso a la información de BT se haga exclusivamente con tarjetas inteligentes o de proximidad (o sistemas de seguridad equivalentes) y que el proveedor lleve a cabo auditorías internas regularmente para garantizar el cumplimiento de estas disposiciones.

h) demostrar que los usuarios siguen las prácticas recomendables de seguridad en la gestión de sus contraseñas.

i) implementar un sistema de gestión de contraseñas que proporcione una instalación interactiva segura y efectiva que garantice contraseñas de calidad.

j) garantizar que las sesiones de usuario se cierren tras un periodo definido de inactividad.

k) garantizar que los registros de auditoría se generen para grabar la actividad de los usuarios y los eventos relevantes para la seguridad y que se administren con seguridad. Los registros deberán conservarse durante un período razonable para facilitar cualquier investigación, con nula capacidad por parte del proveedor de permitir cualquier acceso no autorizado o la modificación de los registros de auditoría.

l) garantizar que sea personal del proveedor independiente de aquellos usuarios que se monitorizan quien lleve a cabo la supervisión de los registros de auditoría y eventos y los informes de análisis por si hubiera comportamientos anómalos y/o intentos de acceso no autorizado.

14.2 El proveedor conservará los sistemas que detecten y registren cualquier intento de daño, modificación o acceso no autorizado a la información de BT en los sistemas del proveedor. Los ejemplos incluyen, entre otros, los procesos de inicio de sesión y auditoría del sistema, IDS, IPS, etc.

14.3 Mantendrá los controles para detectar y protegerse del software malicioso y asegurarse de que se implementen los procedimientos adecuados para la toma de conciencia del usuario.

14.4 Garantizará que al menos cada mes cualquier el software no autorizado se identifique y elimine de los sistemas del proveedor que conserven, procesen o accedan a la información de BT.

14.5Garantizará que el acceso a los puertos de diagnóstico y gestión, así como las herramientas de diagnóstico, estén controlados de forma segura.

14.6 Garantizará que el acceso a las herramientas de auditoría del proveedor esté restringido al personal contratado pertinente y se controle su uso.

14.7 Garantizará que las revisiones del código y las pruebas de penetración en todo el software producido en la casa que se emplee para procesar la información de BT las realice un equipo independiente de los desarrolladores.

14.8 En la medida en que los servidores se utilicen para proporcionar los suministros, no deben instalarse en redes que no sean de confianza (redes fuera de su perímetro de

seguridad, que están más allá de su control administrativo, como por ejemplo, la conexión a Internet) sin los controles de seguridad apropiados.

14.9 Los cambios en los sistemas propios del proveedor que conserven y procesen información de BT y/o que se utilicen para proporcionar los productos o servicios a BT, deben controlarse y quedar sujetos a los procedimientos formales del control de cambios.

14.10 Todos los sistemas deben tener sus relojes internos sincronizados a una fuente de confianza.

15. Proveedores que alojan información de BT

Se exige el cumplimiento de las cláusulas de la sección 15 si el proveedor aloja externamente información de BT clasificada como confidencial o superior en un entorno de servicios en la nube o en el entorno de un servidor de proveedores o subcontratistas.

15.1 El proveedor deberá garantizar, en relación con los suministros, que los entornos donde se aloje información de BT cumplan los requisitos del Anexo 5.

16. Seguridad en la red

Se exige el cumplimiento de las cláusulas de la sección 16 a los proveedores que construyan, desarrollen o soporten las redes de BT o los activos de red.

16.1 El proveedor aplicará, en relación con los suministros, las medidas de seguridad acordadas en todos los componentes suministrados, de modo que salvaguarde la confidencialidad, disponibilidad e integridad de las redes de BT y/o de los activos 21CN. El proveedor proporcionará a BT la documentación completa sobre la implementación de la seguridad en la red relacionada con los suministros y garantizará que la documentación y la mencionada seguridad:

(a) cumplan todos los requisitos legales y normativos;
(b) se esforzará al máximo para impedir que personas no autorizadas (p. ej. hackers) accedan a los elementos de gestión de la red y otros elementos a los que se accede a través de las redes de BT y/o 21CN;
(c) se esforzará al máximo para reducir el riesgo de mal uso de las redes de BT y/o 21CN por parte de aquellos individuos que están autorizados para acceder a ella, lo que, potencialmente, podría causar una pérdida de ingresos o de servicios;
(d) se esforzará al máximo para detectar las infracciones de seguridad que se produzcan, permitiendo la rápida rectificación de cualquier problema derivado, la identificación de los individuos que obtuvieron acceso y la determinación de cómo se obtuvo;
(e) minimicen el riesgo de errores de configuración de las redes de BT, por ejemplo, se puede lograr mediante la concesión de los permisos mínimos necesarios para cumplir la función contratada.

16.2 El proveedor debe tomar todas las medidas razonables para que todas las interfaces de los componentes suministrados funcionen con seguridad y no debe presuponer que los componentes suministrados se activan en un entorno seguro.

16.3 El proveedor deberá proporcionar al contacto de seguridad de red de BT los nombres, direcciones (y demás datos que BT solicite) de todos los miembros del personal contratado que estén, de manera ocasional, directamente involucrados en la implementación, mantenimiento y/o gestión de los suministros antes de que participen respectivamente en dicha implementación, mantenimiento y/o gestión.

16.4 En relación con sus actividades de asistencia con sede en el Reino Unido, el proveedor mantendrá un equipo de seguridad especializado, compuesto por al menos un ciudadano del Reino Unido, que estará disponible como enlace con el contacto de seguridad de red de BT (o sus representantes) y asistirá a las reuniones conforme el contacto de seguridad de red de BT lo requiera ocasionalmente de forma razonable.

16.5 El proveedor proporcionará al contacto de seguridad de red de BT un horario (actualizado según sea necesario) de todos los componentes activos en los suministros y sus respectivas fuentes.

16.6 El proveedor proporcionará los datos de los miembros de su personal que se enlacen con el equipo de gestión de la vulnerabilidad de BT (CERT) en lo relacionado con el debate en torno a las vulnerabilidades identificadas por BT y el proveedor en los suministros. El proveedor proporcionará a BT la oportuna información sobre vulnerabilidades y cumplirá dichos requisitos razonablemente en relación con las vulnerabilidades que el contacto de seguridad de red de BT pueda notificar de vez en cuando, a expensas del proveedor. El proveedor deberá informar a BT de cualquier vulnerabilidad con tiempo suficiente para poder mitigar los controles que el proveedor establezca tras la divulgación pública de las vulnerabilidades.

16.7 El proveedor debe permitir de vez en cuando al contacto de seguridad de red de BT y sus representantes acceso completo e ilimitado a cualquier local donde los suministros se desarrollen, fabriquen o manufacturen para realizar pruebas y/o evaluaciones de cumplimiento normativo de seguridad y el proveedor deberá cooperar (y asegurarse de que todo el personal contratado pertinente lo haga) en dichas pruebas.

16.8 El proveedor garantizará que cualquier componente relacionado con la seguridad que forme parte de los suministros, conforme BT los identifique o se le atribuyan a BT de vez en cuando, se evalúe de forma externa, a expensas del proveedor, a entera satisfacción de BT.

16.9 En lo referente a cualquier información proporcionada u obtenida de BT que esté marcada con "ESTRICTAMENTE CONFIDENCIAL" o que fácilmente se interprete como confidencial, el proveedor deberá garantizar que:

(a) se le facilite el acceso únicamente al personal contratado específicamente autorizado por BT para verla y gestionarla y que se mantenga un registro de tal acceso;
(b) se gestione, utilice y almacene con mucho cuidado y se cifre antes de su almacenamiento con PGP o WinZip 9 en las condiciones que ofrezcan un alto grado de resistencia a su exposición intencional (es decir, utilizando el algoritmo disponible de cifrado más intenso o usando una contraseña segura) y que hagan que la exposición, real o frustrada, se detecte muy probablemente;

(c) cuando se transmita, se le aplique una seguridad adecuada mediante cifrado con Secure Email, PGP o WinZip 9;
(d) no se puede exportar, sin el permiso escrito de BT, fuera del Espacio Económico Europeo.

16.10 El proveedor deberá, sin demora, y en todo caso en un plazo de 7 días laborables, proporcionar al contacto de seguridad de red de BT datos completos de las características y/o funcionalidad en cualquiera de los suministros (o que estén previstas en el Plan de trabajo para cualquiera de los suministros) que, ocasionalmente:

(a) el proveedor conozca; o
(b) el contacto de seguridad de la red de BT considere razonable, y así lo comunique al proveedor, que se hayan diseñado, o se puedan utilizar, para realizar una interceptación legal o cualquier otra interceptación del tráfico de las telecomunicaciones. Dichos datos deberán incluir toda la información que sea razonablemente necesaria para que el contacto de seguridad de red de BT comprenda totalmente la naturaleza, composición y alcance de tales características y/o funcionalidad.

16.11 Con el fin de mantener el acceso a las redes y/o sistemas de BT, el proveedor notificará a BT inmediatamente cualquier cambio en su método de acceso a través de los cortafuegos, incluido el suministro de la traducción de la dirección de la red.

16.12 Las herramientas de monitorización de la red que pueden ver información de la aplicación no se deben utilizar.

16.13 La funcionalidad IPv6 incluida en los sistemas operativos debe desactivarse en los sistemas hosts (dispositivos de usuario final, servidores) que se conecten con los dominios de la red de BT y se debe desactivar cuando no sea necesarios.

16.14 El proveedor cumplirá (y se asegurará de que los suministros cumplan) las políticas de BT, si las hubiera, y los Requisitos de seguridad. Cualquier incumplimiento debe acordarse a la firma del contrato o en virtud del control de cambios.

16.15 El proveedor garantizará que todo el personal contratado pase las comprobaciones previas al empleo adecuadas a su nivel de acceso
http://www.selling2bt.bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf

Los proveedores que construyan, desarrollen o soporten las redes de BT o los activos de red deben garantizar que todo el personal contratado pase como mínimo las comprobaciones previas al empleo de nivel L2. Se exigirán las comprobaciones previas al empleo de nivel L3 a los puestos de trabajo identificados por el contacto de seguridad de red de BT. Cuando el proveedor no tenga la capacidad de acreditar directamente la seguridad del personal contratado como parte de las comprobaciones L3, entonces BT ayudará a obtener una acreditación cuyo coste correrá a cargo del proveedor.

17. Seguridad en la red del proveedor

Se exige el cumplimiento de las cláusulas de la sección 17 cuando la red del proveedor se utilice con el fin de proporcionar los suministros (Esto incluye las redes LAN, WAN, Internet, redes inalámbricas y de radio)

17.1 El proveedor aplicará, en relación con los suministros, medidas de seguridad en todas sus redes, de modo que se salvaguarde la confidencialidad, disponibilidad e integridad de la información de BT. Las medidas deberán:

(a) cumplir todos los requisitos legales y normativos;
(b) hacer todo lo posible para evitar que personas no autorizadas (por ejemplo: hackers) tengan acceso a la Red y
(c) hacer todo lo posible para reducir el riesgo de mal uso de las redes que pudieran, potencialmente, causar una pérdida de ingresos o de servicios, por parte de aquellos individuos que están autorizados a acceder a ella;
(d) hacer todo lo posible para detectar las infracciones de seguridad que se produzcan, permitiendo la rápida rectificación de cualquier problema derivado, la identificación de los individuos que obtuvieron acceso y la determinación de cómo se obtuvo.

18. Seguridad en la nube

También se exige el cumplimiento de las cláusulas de la sección 18 si el proveedor está proporcionando a BT servicios relacionados con la nube. La definición de nube se puede encontrar en la publicación NIST http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf)

18.1 Los proveedores deberán presentar pruebas de que los servicios en la nube que suministran cumplen los requisitos de control de la Cloud Security Alliance Nube Controls Matrix (CCM) en la última edición de la versión disponible en https://cloudsecurityalliance.org además de respetar el Anexo 5 de estos Requisitos de seguridad.

18.2 La información de BT implicada en el comercio electrónico que se transmita por las redes públicas estará protegida, de conformidad con el Anexo 1, mientras se encuentre en tránsito y almacenada (incluso las copias de seguridad) frente a actividades fraudulentas, divulgación no autorizada, acceso y modificaciones.

18.3 Los acuerdos de nivel de servicio de red e infraestructura (internos o subcontratados) deberán documentar claramente los controles de seguridad, los niveles de capacidad y de servicio y los requisitos empresariales o del cliente.

18.4 El proveedor permitirá pruebas de penetración y/o acceso a los informes existentes de pruebas de penetración del proveedor en relación con los suministros que proporciona. El alcance y el calendario de las pruebas se acordarán con BT.

18.5 El proveedor implementará las medidas de seguridad acordadas para todos los componentes suministrados, de manera que se salvaguarden la confidencialidad, disponibilidad, calidad e integridad de los suministros y se minimice la posibilidad de que

personas no autorizadas (por ejemplo, otros clientes de la nube) tengan acceso a la información y los servicios de BT.

Glosario

En estos Requisitos de seguridad se aplicarán las siguientes definiciones; aunque las cláusulas del contrato se aplicarán a estos Requisitos de seguridad y todas las palabras y expresiones utilizadas en estos Requisitos de seguridad tendrán el mismo significado que se les haya dado en el contrato:

"**Acceso**": el procesamiento, gestión o almacenamiento de la información de BT por uno o más de los siguientes métodos:

- Por interconexión con los sistemas de BT
- Facilitada en papel o formato no electrónico
- Información de BT en los sistemas del proveedor
- Por el teléfono móvil

y/o el acceso a los edificios de BT para la prestación de servicios (excepto la entrega de hardware y la asistencia a reuniones)]

["**Autorizado/a**": BT ha aprobado el acceso, ya sea como parte del proceso de interconexión al sistema de BT o como autorización por escrito recibida de la empresa BT o del propietario del proyecto de BT; la "**autorización**" se asignará en consecuencia. El nivel de acceso facilitado será relevante y estará limitado a proporcionar los suministros.]

"**Artículos de BT**": todos los artículos proporcionados por BT al proveedor y todos los artículos en poder del proveedor que pertenezcan a BT. (por ejemplo, llaves de armarios, equipos portátiles, tarjetas de paso, planes, documentos de proceso.)

"Contacto de seguridad de red de BT": profesional asegurador de la información procedente del equipo de seguridad de BT, con el que se contacta completando y enviando el formulario de solicitud del Anexo 3, o cualquier otra persona cuya identidad y datos de contacto puedan notificarse al contacto comercial del proveedor ocasionalmente.

"**Activos físicos de BT**": todos los activos físicos en posesión del proveedor que pertenezcan a BT. (Por ejemplo: routers, switches, servidores o documentación)

"**Seguridad de BT**": la organización de seguridad con sede en el interior de BT.

"**Contacto de seguridad de BT**": profesional asegurador de la información procedente del equipo de seguridad de BT, con el que se contacta completando y enviando el formulario de solicitud del Anexo 3.

"**Política de Seguridad de BT**": es la política relevante de seguridad de la red de BT conforme a la suministrada por BT.

"**Sistemas de BT**": los servicios y componentes de servicio, productos, redes, servidores, procesos, sistema basado en papel o sistemas de TI (en todo o en parte) que sean propiedad de BT, se accionen por BT o por sus representantes, BT Group plc o cualquier entidad del grupo BT Group plc; o cualesquiera otros sistemas que puedan alojarse en locales de BT (incluyendo iSupplier (como se define "iSupplier" en la sección del acuerdo titulada "Pago y facturación") utilizados en el contexto de "acceso" (tal como se define más arriba).

"**CCTV**": significa circuito cerrado de televisión

"**Fecha de inicio**": tal como se define en el contrato.

"**Personal contratado**", "**Personal contratado pertinente":** tal como se define en el contrato.

"**Información**": significa información ya sea material o de cualquier otra forma, incluyendo, entre otros: especificaciones, informes, datos, notas, documentación, dibujos, software, políticas, procedimientos, procesos, normas, salidas informáticas, diseños, diagramas de circuitos, modelos, patrones, muestras , invenciones (con capacidad de patentarse o no), el conocimiento específico y los soportes (si los hubiera) en los que dicha información se facilita.

"**ISO 27001**": norma internacional para los sistemas de gestión de seguridad de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

"**Pedido o pedidos**": una petición realizada por BT al proveedor para obtener suministros de conformidad con el contrato.

"**Seguridad de la red**": significa la seguridad de las rutas y nodos de interconexión de comunicaciones que conectan lógicamente las tecnologías de usuario final con los sistemas de gestión asociados.

"**Datos personales**": tendrán el significado que se les atribuye en la Directiva 95/46/CE o de cualquier legislación posterior en relación al mismo ("la Directiva").

"Proceso", "procesado/a" o "procesamiento": significa cualquier operación o conjunto de operaciones que se realice con la información de BT, ya sea con medios automatizados o no, como la recopilación, registro, organización, almacenamiento, adaptación o alteración, extracción, consulta, utilización, divulgación por transmisión, difusión o cualquier otra puesta a disposición, ajuste o combinación, bloqueo, supresión, devolución o destrucción.

"**Información sensible**": cualquier información de BT clasificada o marcada como "Confidencial" o superior, incluidos los datos personales.

"**Subcontratista**": tal como se define en el contrato.

"**Sistemas del proveedor**": cualquier equipo informático, aplicación o sistemas de red propiedad del proveedor utilizado para acceder, almacenar o procesar información de BT o implicado en la provisión de los suministros.

"**Contacto de seguridad del proveedor**": persona cuya información de contacto notificará el proveedor a BT de vez en cuando y que será el único punto de contacto para las cuestiones relacionadas con la seguridad.

"**Suministros**": todos los componentes, materiales, instalaciones, herramientas, equipos de prueba, documentación, firmware, software, piezas, repuestos y cosas que se deben proporcionar a BT en virtud del contrato, junto con toda la información y el trabajo que el contrato exige que se suministre o se preste a BT.

"**Transferencia" o "Transferido/a**": significa

(a) el traslado de la información de BT en posesión del personal contratado (incluidos, entre otros, los datos personales) de un lugar o persona a otro, ya sea físicamente, con la voz o por medios electrónicos;

(a) la concesión de acceso a la información de BT en posesión del personal contratado (incluidos, entre otros, los datos personales) de un lugar o persona a otro, ya sea físicamente, con la voz o por medios electrónicos.

Anexo 1: Clasificación de la información

Introducción

Dentro de BT todos los datos y la información tienen un responsable de negocio que se encarga de clasificar los documentos o los datos.

Todos los usuarios que entran en contacto con los datos y la información deben protegerlos. Como usuario de la información de BT, usted es responsable de asimilar los controles de clasificación de seguridad de este documento y los requisitos del proyecto concreto especificados por BT. Solo debe utilizar el documento o los datos para su propósito original y obtener la aprobación del propietario de los datos si desea permitir que más personas accedan a ellos.

Si usted recibe información de BT que no se haya clasificado debe comunicarse con el remitente o su gerente de BT para confirmar la clasificación, en caso contrario, póngase en contacto con seguridad de BT como indica el Anexo 3 de los Requisitos de seguridad.

Nota: Si usted tiene acceso a la red de área local (LAN) BT Greenside o se le exige que cree documentos para BT que incluyan cualquier información de BT, entonces usted necesita hacer referencia a la Política de seguridad 4, de lo contrario se le aplicará lo siguiente:

Clasificaciones de la información

Hay 4 clasificaciones de la información:

- Pública
- Interna
- Confidencial
- Estrictamente confidencial

Pública

La información pública no requiere controles o se destina al consumo público.

Interna

La información interna está disponible para personal de BT y otras personas que tengan acceso a la red de información de BT, suponiéndole dicho acceso algo de riesgo empresarial a BT.

Confidencial

La información confidencial tiene un público concreto: se impone estrictamente el principio de la necesidad de saber (controles de acceso). La divulgación no autorizada de información confidencial puede afectar a la reputación de BT o ser perjudicial para las personas.

Algunos ejemplos son:

- Información personal acerca de individuos, ya sea personal de BT, terceros o clientes;
- Datos de registro del sistema;
- Datos de ventas y comercialización;
- Planes de negocios locales;
- Datos de riesgo;

- Contraseñas;
- Información que es legalmente confidencial.

Colección de varios documentos confidenciales

Si tiene una colección de documentos confidenciales en una sola ubicación, es posible que la clasificación necesite actualizarse, lo que puede dar lugar a la reclasificación de documentos individuales como "estrictamente confidenciales" o requerir medidas adicionales de seguridad para garantizar la ubicación si:

- Juntos pudieran causar un daño excepcional a BT en caso de filtración;
- Cuando se utilizan con otras combinaciones de datos individuales, como nombre y dirección, y/o existen numerosos registros bancarios detallados en un sistema, pueden resultar un objetivo atractivo.

Si le preocupa la información que está en su posesión, hable con su contacto de BT.

Estrictamente confidencial

La información o los datos estrictamente confidenciales tienen una circulación definida y pequeña en número; se impone estrictamente el principio de la necesidad de saber (usted debe saber quién tiene copias y quién tiene acceso). La divulgación no autorizada podría causar daños excepcionales a BT. Hay que considerar cuidadosamente si la información es estrictamente confidencial ya que esta requiere los controles de seguridad más rigurosos.

Controles de seguridad

Términos definidos:

Cifrado

Requisitos mínimos:

- Utilice cifrado AES de 256 bits.
- Las claves simétricas deben tener una longitud mínima de clave de 256 bits.
- Las claves asimétricas (por ejemplo, RSA) deben tener una longitud de clave de al menos 2048 bits.
- Utilice solo códigos criptográficos conocidos y de confianza.
- No use certificados autofirmados.

Contraseña/frase de acceso (para el cifrado)

No debe ser fácilmente predecible (es decir, debe ser lo más aleatoria posible, sin relación con el ID de usuario, los usuarios, la identidad, la fecha, etc.) y no ser detectable usando diccionarios de contraseñas comúnmente utilizadas. Sin embargo, deben tener como mínimo:-

- Al menos 8 caracteres de longitud.
- Contener al menos dos de los siguientes elementos:
  - Elementos no alfanuméricos, p. ej: !, £,", $, %,^, &,*, (,), -,_, +, =, :, `, @, ~, #, ?, <, >
  - Números decimales: (0... 9)
  - Letras mayúsculas: (A... Z)
- Las claves privadas deben protegerse con una frase de acceso que utilice una mezcla de caracteres alfanuméricos y símbolos, tal como se ha definido arriba.

Nota: Para evitar dudas, los requisitos contractuales específicos del cliente contenidos en un contrato de cliente que requieran un mayor nivel de seguridad tendrán prioridad sobre los siguientes controles.

	Controles de seguridad	Interna	Confidencial	Estrictamente confidencial
1	**Legislación nacional sobre protección de datos: datos personales y datos personales sensibles**	No deben ser tratados como información interna. Proteja los registros individuales como confidenciales.	Proteja los registros individuales como confidenciales.	Proteja los registros individuales como estrictamente confidenciales.
2	**Seguimiento de los movimientos y control de la distribución de la documentación empresarial (Word, Excel, etc.)**	No son necesarios el control ni el seguimiento. Ponga la marca "**BT INTERNO**" en cada página, o "**OPENREACH INTERNO**" si es solo para compartir en Openreach.	Ponga "**CONFIDENCIAL** " en cada página del documento, asegúrese de seguir el "**principio de la necesidad de saber**" y considere el uso de una **lista de distribución.** **Se requiere cifrado según los términos "Cifrado" y**	Ponga "ESTRICTAMENTE CONFIDENCIAL" en cada página del documento. Incluya una **lista de distribución** de personas dentro del documento. El propietario debe asegurarse de seguir el "**principio de la necesidad de saber**".

			"Contraseña/frase de acceso**" definidos anteriormente.**	**Se requiere cifrado antes del almacenamiento utilizando software que respete los términos de "Cifrado" y "**Contraseña/frase de acceso**" definidos anteriormente cuando** los datos no se almacenan en un PC o portátil suministrado por BT con disco duro cifrado, es decir, soportes extraíbles. Lo mismo se aplica cuando lo envía por correo electrónico a cualquier persona, de BT o ajena a BT.
3	**Almacenamiento seguro en ordenador portátil y PC**	Se requiere almacenamiento seguro, por ej. con PGP, WinZip 9.	Cifrado de disco completo **según los términos definidos de "Cifrado" y "**Contraseña/frase de acceso**" anteriormente.**	Cifrado de disco completo **según los términos definidos de "Cifrado" y "**Contraseña/frase de acceso**" anteriormente.**
4	**Almacenamiento seguro en servidor y bases de datos (fijo - disco o cinta)**	No se requiere almacenamiento seguro si cumplen todos los requisitos físicos del apéndice SBCA, de lo contrario se exige el almacenamiento seguro, por ej. con PGP, WinZip 9	La información de BT debe cifrarse **tal como se define en los términos "Cifrado" y "**Contraseña/frase de acceso**" mencionados anteriormente**.	La información de BT debe cifrarse **tal como se define en los términos "Cifrado" y "**Contraseña/frase de acceso**" mencionados anteriormente.**
5	**Almacenamiento seguro en Blackberry, Windows Mobile, dispositivos PDA, tabletas (iPads, etc.), teléfonos móviles y reproductores de MP3**	Está prohibido almacenar información interna en estos dispositivos a menos que el dispositivo lo suministre BT o sea una concesión aprobada por	Está prohibido almacenar información confidencial en estos dispositivos a menos que el dispositivo lo suministre BT o sea una concesión aprobada por	Está prohibido almacenar ISC en estos dispositivos.

		seguridad de BT. Estos dispositivos no deben configurarse para acceder a cuentas de correo electrónico BT.com (se permite el acceso al correo electrónico bt.com a través de webmail).	seguridad de BT. Estos dispositivos no deben configurarse para acceder a cuentas de correo electrónico BT.com (se permite el acceso al correo electrónico bt.com a través de webmail).	
6	**Almacenamiento seguro en:** **Soportes extraíbles como tarjetas de memoria, memoria flash, CD/DVD, discos duros USB, tarjetas digitales seguras, disquetes y otros dispositivos similares.**	La información de BT debe cifrarse cuando se almacene en dichos dispositivos **tal como se define en los términos "Cifrado" y "**Contraseña/frase de acceso**" mencionados anteriormente**.	La información de BT debe cifrarse cuando se almacene en dichos dispositivos **tal como se define en los términos "Cifrado" y "**Contraseña/frase de acceso**" mencionados anteriormente.**	Está prohibido almacenar ISC en estos dispositivos.
7	**Almacenamiento web/en línea o en cualquier instalación de almacenamiento de Internet**	Prohibido	Prohibido	Prohibido
8	**Colaboración web externa**	Cualquier plataforma MS LiveMeeting o Webjoin	Prohibido	Prohibido
9	**Envío mediante correo electrónico**	No se requiere cifrado.	Cifrado para los destinatarios (cuando el destino no es una dirección de correo electrónico de bt.com) **según los términos "Cifrado" y "**Contraseña/frase de acceso**" definidos anteriormente.**	**Se requiere cifrado según los términos "Cifrado" y "**Contraseña/frase de acceso**" definidos anteriormente.**
10	**Reenvío automático de correo electrónico**	Prohibido	Prohibido	Prohibido
11	**Transmisión de red**	No se requiere cifrado.	Cifrado para la transmisión externa e interna,	Cifrado para la transmisión externa e interna,

			según los términos "Cifrado" y "Contraseña/frase de acceso**" definidos anteriormente.**	**según los términos "Cifrado" y "**Contraseña/frase de acceso**" definidos anteriormente.**
12	**Transferencia de archivos**	Utilice la transferencia segura de archivos, como SFTP, XFB.	Utilice la transferencia segura de archivos, como SFTP, XFB.	Utilice la transferencia segura de archivos, como SFTP, XFB.
13	**Borrado/eliminación de datos**	Use las funcionalidades de eliminación de la aplicación o del sistema operativo.	Borre físicamente los datos sobreescribiendo todos los sectores al menos una vez con cadenas binarias aleatorias utilizando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD.	Borre físicamente los datos sobreescribiendo todos los sectores al menos una vez con cadenas binarias aleatorias utilizando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD.
14	**Eliminación o reutilización de equipos informáticos (con información de BT)** **Incluye, entre otros:** **- La eliminación de piezas** **- La destrucción de equipos del proveedor** **- Los requisitos de destrucción de copias de seguridad** **- Piezas del servidor que enviaron de vuelta al fabricante para su reparación**	Utilice una solución de borrado de software verificable y probada en la que se emita un certificado formal para verificar el borrado. Cualquier equipo que no pueda borrarse debe ser destruido, debiendo recibirse/facilitarse una certificación formal con al menos un registro del número de serie del equipo como prueba del borrado. La solución anterior no puede utilizarse con unidades de estado sólido (SSD) que deben destruirse y recibir/facilitar una	Los discos (u otros soportes de almacenamiento, incluidos, entre otros, tarjetas compact flash, dispositivos SSD) se deben borrar sobreescribiendo todos los sectores con cadenas binarias aleatorias, al menos una vez, usando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD. Si no se puede conseguir el borrado o este no es correcto, entonces el disco (u otros soportes de almacenamiento, incluidos, entre otros, tarjetas	Los discos (u otros soportes de almacenamiento, incluidos, entre otros, tarjetas compact flash, dispositivos SSD) se deben borrar sobreescribiendo todos los sectores con cadenas binarias aleatorias, al menos una vez, usando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD. Si no se puede conseguir el borrado o este no es correcto, entonces el disco (u otros soportes de almacenamiento, incluidos, entre

		certificación formal. Consulte BS EN 17513 para obtener más información.	compact flash, dispositivos SSD) deben destruirse con una funcionalidad de destrucción de discos. Debe emitirse un certificado formal para verificar el borrado o la destrucción.	otros, tarjetas compact flash, dispositivos SSD) deben destruirse con una funcionalidad de destrucción de discos. Debe emitirse un certificado formal para verificar el borrado o la destrucción.
15	**Impresión**	Utilice una impresora conectada al PC o esté presente junto a la impresora de red, mientras dura la impresión.	Utilice una impresora controlada con un PIN, una impresora conectada al PC o una impresora situada en una sala de acceso controlado. Compruebe cuál es la impresora que va a utilizar y no deje documentos en la bandeja de impresión.	Utilice una impresora controlada con un PIN, una impresora conectada al PC o una impresora situada en una sala de acceso controlado. Tenga cuidado cuando esté imprimiendo. Compruebe cuál es la impresora que va a utilizar y no deje documentos en la bandeja de impresión.
16	**Servicios postales/de mensajería entre BT y el proveedor**	Un único sobre.	Utilice sobres dobles y envíe por correo certificado solo al destinatario; no escriba "Confidencial" en el primer sobre.	Utilice sobres dobles y envíe por correo certificado solo al destinatario; no escriba "Estrictamente confidencial" en el primer sobre.
17	**Divulgación externa**	Busque la autoridad del contacto de seguridad de BT. Consulte el Anexo 3.	Busque la autoridad del contacto de seguridad de BT. Consulte el Anexo 3.	Busque la autoridad del contacto de seguridad de BT. Consulte el Anexo 3.
18	**Utilizado en formación, desarrollo o pruebas**	BT debe anonimizarlo respetando la guía BP001 de prácticas recomendadas para anonimizar datos de BT.	BT debe anonimizarlo respetando la guía BP001 de prácticas recomendadas para anonimizar datos de BT.	Prohibido

19	**Eliminación de papel**	Cortado con trituradoras de corte transversal.	Cortado con trituradoras de corte transversal.	Cortado con trituradoras de corte transversal a 4 x 15 mm.
20	**Zonas públicas**	No hable sobre información interna en público.	No hable sobre información confidencial en público. No trabaje con documentos en espacios públicos donde se le pueda espiar.	No hable sobre información estrictamente confidencial en público. No trabaje con documentos en espacios públicos.

Anexo 2: Formación obligatoria

Los proveedores externos que presten servicios a BT deben ser conscientes de la política sobre seguridad de la información de BT.

La formación en seguridad obligatoria de BT se encuentra accesible en: http://regulatorycompliance.intra.bt.com/compliance/Training/3rdPartySupplierTraining/index.htm o http://workingwithbt.extra.bt.com/index_new.html para terceros sin acceso a la red de BT.

*Título del curso**	*Tipo de formación*	*Código del curso*	*Requisito (para todo tipo de puestos)*	*Duración estimada*	*Aprobado %*	*Frecuencia*
Seguridad de BT	*Seguridad*	*BTSEC002*	*Obligatorio*	*1 hora*	*100%*	*Una sola vez*
Política de seguridad de BT - Lista de verificación anual	*Seguridad*	*BTSEC003*	*Obligatorio*	*30 minutos*	*100%*	*Cada año*

El acceso a este sitio es seguro y se concede a cada dirección IP de la empresa. Póngase en contacto con su representante de BT si no se ha configurado este acceso.

Si ha solicitado el acceso y todavía no puede acceder al sitio, compruebe lo siguiente:

- Que está tratando de acceder a la dirección URL correcta http://workingwithbt.extra.bt.com/index.html
- Que está accediendo a Internet a través de la red de su empresa y no utilizando cualquier portal de BT como iDesk o un ordenador personal sin conexión a la red de la empresa.
- Compruebe la dirección IP que su cortafuegos deja ver en Internet. Puede encontrar la dirección IP en http://www.whatismyip.com/, copie y pegue la dirección IP que aparece y envíela por correo electrónico a bill.wp.brown@bt.com

Si accede al sitio, pero al abrir un curso aparece una página en blanco, pruebe lo siguiente:
En Internet Explorer, haga clic en **Herramientas**...haga clic en **Opciones de Internet** ….seleccione la pestaña **Opciones avanzadas**...desplácese hasta **Seguridad**...compruebe que esté marcada la casilla **No guardar las páginas cifradas en el disco**...haga clic en **Aceptar**

Si sigue viendo una página en blanco o la página no hace nada después de hacer clic en 'Enviar', pruebe lo siguiente:
Si utiliza una configuración de doble pantalla:

- Desactive la configuración de doble pantalla
- Asegúrese de arrastrar cualquier ventana de Internet Explorer que se abra en la pantalla secundaria a la pantalla principal. Luego, cierre las ventanas de Internet Explorer y vuelva a empezar con una nueva ventana. Repita lo anterior para cualquier ventana que se abra en la pantalla secundaria.
Repita lo anterior para cualquier ventana que se abra en la pantalla secundaria.

Si no puede obtener un certificado después de completar el curso, intente lo siguiente:
Desactive todos los bloqueadores de ventanas emergentes. Estos componentes pueden impedir que se abra la ventana de certificación y registro. Tenga en cuenta que es posible tener más de un bloqueador en su PC.

Si nada de lo anterior ha resuelto el problema o no se contempla su problema

Envíe su consulta a compliance.helpdesk@bt.com asegurándose de que "Extranet" sea la primera palabra que figure en el campo del asunto.

Anexo 3: Envío de notificaciones/solicitudes al contacto de seguridad de BT

El proveedor debe rellenar la sección 1.
(envíe por correo electrónico el formulario de consulta relleno a security@bt.com, en el campo Asunto escriba "BT Security Contact required for Security clause query/Incident")

Sección 1.

1. Indique la naturaleza de la consulta en materia de cláusulas de seguridad con el contacto de seguridad de BT utilizando las descripciones de cláusulas que se indican a continuación y marque la casilla apropiada a la consulta. Será más fácil para nosotros responderle si nos proporciona algún detalle en relación con su solicitud.

Ref. de la cláusula	Descripción de la cláusula	Casilla que debe seleccionarse
3.1	El proveedor notificará inmediatamente a BT los datos del contacto de seguridad del proveedor y cualquier cambio que se produzca en los mismos. **Introduzca los datos a continuación:** Seleccione un elemento.	☐
3.2	Al inicio del contrato, el proveedor notificará por escrito al contacto de seguridad de BT, utilizando el anexo 3, las ubicaciones geográficas en las que se prestan los principales servicios, dónde se encuentra el personal contratado pertinente o dónde se procesa o guarda la información de BT. Durante el contrato, el proveedor también deberá notificar cualquier propuesta de cambio de ubicación geográfica al contacto de seguridad de BT, mediante el Anexo 3, de forma que BT pueda volver a evaluar cualquier riesgo para BT o para la información de los clientes de BT. El proveedor deberá garantizar que todos los contratos con subcontratistas relevantes incluyan las cláusulas escritas que exigen que el subcontratista cumpla los Requisitos de seguridad para proveedores de BT en la medida en que sean aplicables. Estos términos deben acordarse entre el proveedor y su subcontratista antes de que el subcontratista o cualquier miembro de su personal pueda acceder a los sistemas y a la información de BT. **Introduzca los datos de ubicación a continuación:** Seleccione un elemento.	☐
3.5	El proveedor notificará al contacto de seguridad de BT, utilizando el Anexo 3, si el proveedor va a ser objeto de una fusión, adquisición o sufrirá cambios en la propiedad, de forma que podamos volver a evaluar cualquier riesgo para BT, para la información de BT o de sus clientes. **Introduzca los datos a continuación:** Seleccione un elemento.	☐

3.8	El proveedor deberá contar, en lo que respecta a la entrega de los suministros, con los procedimientos formales de gestión de incidentes de seguridad con responsabilidades definidas. Cualquier información sobre cualquier incidente de seguridad se considerará "Confidencial". El proveedor informará al contacto de seguridad de BT mediante el Anexo 3, en un plazo de tiempo razonable tras la toma de conciencia de cualquier incidente: i) relacionado con pérdidas materiales, corrupción, daños o mal uso de la información de BT, activos físicos y artículos de BT o acceso indebido o no autorizado a los sistemas o a la información de BT o incumplimiento de cualquiera de las obligaciones del proveedor en virtud de estos Requisitos de seguridad; o ii) relacionado con la imposibilidad de entregar los suministros de conformidad con el contrato. iii) cualquier acción que incumpla los requisitos de este documento de seguridad). Tras una razonable solicitud, el proveedor deberá proporcionar a BT lo antes posible un informe escrito con un plan corrector que incluya un calendario y las medidas que deban tomarse para evitar la repetición del incidente. **Introduzca los datos de alto nivel a continuación:**	☐
4.4	El proveedor deberá mantener un servicio de atención telefónica confidencial para todo su personal, en la medida permitida por la ley, para que lo utilice el personal contratado si son instruidos para actuar de manera incoherente, infringiendo estos Requisitos de seguridad. Los informes relevantes se notificarán al contacto de seguridad de BT mediante el Anexo 3. **Introduzca los datos de alto nivel a continuación:**	☐
8.2	Solo se permite la conexión directa (en el puerto LAN o conexión inalámbrica) con los dominios de BT a los servidores de integración continua de BT aprobados, a los PC webtop de BT y a los dispositivos finales de confianza. El proveedor no conectará (y, si procede, se asegurará de que ningún miembro del personal contratado lo haga) ningún equipo no aprobado por BT a ningún dominio de BT sin la autorización previa por escrito del contacto de seguridad de BT (utilizando el Anexo 3). El contacto de seguridad de BT deberá presentar la autorización por escrito al iniciar el proceso de concesión de la política de seguridad en BT. **Introduzca los datos de alto nivel a continuación:**	☐
9.14	El proveedor se asegurará de prohibir la fotografía o captura de imagen de cualquier información de BT o información de clientes de BT. En circunstancias	☐

	excepcionales, si hubiera requisitos empresariales para capturar esas imágenes, hay que obtener por escrito la exención temporal de esta cláusula de parte del contacto de seguridad de BT usando el Anexo 3. **Introduzca los datos de alto nivel a continuación:**	
12.6	Si es necesario con el fin de asegurar el cumplimiento en las cuestiones de seguridad, el contacto de seguridad de red de BT (y/o las personas designadas por BT, que deberán ser todos empleados de BT) tendrán derechos similares (mutatis mutandis), si se solicita como parte de los suministros, de familiarización y validación (como se definen en el Acuerdo de acceso a la información) con respecto al material de origen (como se define en el Acuerdo de acceso a la información). **Introduzca los datos de alto nivel a continuación:**	☐
13.2c	Vincular dominios a los sistemas de BT está prohibido salvo que el contacto de seguridad de BT lo apruebe y autorice utilizando el Anexo 3. **Introduzca los datos de alto nivel a continuación:**	☐
16.3	El proveedor deberá proporcionar al contacto de seguridad de red de BT los nombres, direcciones (y demás datos que BT solicite) de todos los miembros del personal contratado que estén, de manera ocasional, directamente involucrados en la implementación, mantenimiento y/o gestión de los suministros antes de que participen respectivamente en dicha implementación, mantenimiento y/o gestión. **Introduzca los datos de alto nivel a continuación:**	☐
16.5	El proveedor proporcionará al contacto de seguridad de red de BT un horario (actualizado según sea necesario) de todos los componentes activos en los suministros y sus respectivas fuentes. **Introduzca los datos de alto nivel a continuación:**	☐
16.10	El proveedor deberá, sin demora, y en todo caso en un plazo de 7 días laborables, proporcionar al contacto de seguridad de red de BT datos completos de las características y/o funcionalidad en cualquiera de los suministros (o que estén previstas en el Plan de trabajo para cualquiera de los suministros) que, ocasionalmente: **Introduzca los datos de alto nivel a continuación:**	☐
Inespecífico	No se puede identificar la cláusula específica o una consulta adicional relacionada con la seguridad. **Introduzca los datos de alto nivel a continuación:**	☐

Anexo 1	Aprobaciones exigidas por el contacto de seguridad de BT en lo referente a la clasificación de la información de BT Introduzca los datos de alto nivel a continuación:	☐

2. Complete lo siguiente para que esa consulta se puede asignar lo más rápidamente posible al contacto de seguridad apropiado.

1	**Nombre de la empresa del proveedor**	
2	**Nombre del contacto del proveedor**	
3	**Número de teléfono**	
4	**Correo Electrónico**	
5	**Número de contrato**	
6	**Fecha de la consulta/incidente**	
7	**Nombre del principal contacto de BT para el proveedor** (*Persona con la que trata el proveedor regularmente para abordar cuestiones laborales de BT*)	
8	**Número de teléfono del contacto de BT**	
9	**Información de la consulta**	

Sección 2 (uso exclusivo de BT)

Fecha de recepción de la consulta		Número de referencia del servicio de asistencia (helpdesk)	

1. Compruebe que el proveedor haya seleccionado al menos una cláusula de seguridad de la primera tabla. De la segunda tabla, el proveedor debe haber completado las filas 1 a 7 y 9 como mínimo. Si falta algún dato, será necesario ponerse en contacto con el proveedor para obtener la información que falta.

2. Si el proveedor ha seleccionado una cláusula de seguridad resaltada en verde, esta tendrá que gestionarla el equipo de seguridad CERT de BT, registrándose en Raptor y enviando por correo electrónico este formulario de solicitud de proveedor al equipo CERT.

3. Si el proveedor ha seleccionado una cláusula de seguridad resaltada en azul, esta tendrá que gestionarla el equipo de seguridad de red enviando este formulario por correo electrónico a Kevin Waterfall y Neil Trask

4. Las demás cláusulas de seguridad serán gestionadas por el equipo de seguridad IA de BT. Este formulario de captura de datos puede enviarse ahora al equipo de seguridad IA de BT.

    a. En el campo Asunto, copie y pegue los contenidos de las dos primeras columnas de la primera tabla que se correspondan con la casilla de verificación que el proveedor seleccionó y añada el nombre del proveedor. por ejemplo, 0800 3.1) – Nombre del proveedor
    (*Esto es importante ya que la cuenta de correo electrónico receptora ejecutará una secuencia de comandos utilizando los datos del campo Asunto*)

    b. Adjunte el formulario de solicitud del proveedor y envíelo a Risk & Compliance G

Anexo 4: Acceso a sitios y edificios de BT para organizaciones ajenas a BT (Reino Unido solamente)

N/D (aplicable únicamente a sitios del Reino Unido)

Anexo 5: Requisitos de alojamiento externo de datos

Estos requisitos son aplicables al alojamiento de todas las aplicaciones y datos de **BT** marcados como **'Confidencial'** o **'Estrictamente confidencial'**, en cualquier ubicación, que no sean propiedad de BT ni los gestione BT. Esto incluye, entre otros, los servicios en la nube donde: a) los datos en tránsito están seguros y protegidos de una interceptación empleando, normalmente, un protocolo cifrado; y b) los datos almacenados de BT están cifrados dentro del servicio en la nube.

Las siguientes condiciones se aplican a datos y aplicaciones confidenciales alojados fuera de BT:

- El centro de datos debe tener una certificación válida ISO 27001 (u otras certificaciones que demuestren controles equivalentes) para la gestión de la seguridad o cumplir los requisitos de seguridad de la certificación ISO 27001 o de las políticas de seguridad alineadas con ISO27001 y/o trabajar hacia la consecución de la norma ISO27001 en un plazo acordado con BT;
- Los datos 'en tránsito' deben cifrarse en alta intensidad para proteger los datos de BT entre el punto de salida de BT y el límite de DC (normalmente el balanceador de carga y el dispositivo de cifrado situado detrás del cortafuegos del límite de DC);
- Los técnicos de DC con acceso físico a los servidores no deben tener acceso lógico al entorno de producción y los administradores con acceso lógico a los sistemas, no deben tener acceso físico al DC.
- Todos los accesos lógicos deben controlarse con un sistema de seguridad de cuentas para garantizar que la gestión de contraseñas esté controlada y se implemente el proceso de autorización adecuado que garantice la identidad del solicitante, por ejemplo: CyberArk.
- Para el acceso privilegiado (incluido, entre otros, DBA), la gestión de contraseñas debería ser de tiempo limitado y cuando sea posible deberían aplicarse restricciones adicionales sobre la dirección IP de origen;
- Cualquier acceso privilegiado, como por ejemplo: DBA, ASG, etc. a los sistemas que procesan la información de BT debe cumplir los requisitos del Anexo 1: clasificación de la información;
- Para el acceso remoto, debe utilizarse una red privada virtual segura junto con una autenticación de dos factores basada en la función; además, todo acceso privilegiado remoto de terceros solo puede acceder a los sistemas si los datos de BT están en tránsito o almacenados dentro del mismo país que el DC, o un país o territorio que garantice un adecuado nivel de protección para los datos de BT;
- Implemente los procesos completos de gestión de claves criptográficas que se consideren las prácticas recomendables del sector;
- Cualquier acceso físico a las áreas o equipos donde se almacena o se procesa información de BT debe tener un proceso auditable, por ejemplo: una solicitud de cambio, para garantizar que el acceso se conceda solo para la duración mínima necesaria, por ejemplo, un acceso no permanente;
- El almacenamiento de los datos de la copia de seguridad fuera del sitio debe estar cifrado en línea con los requisitos del Anexo 1;
- Los controles deben funcionar para mitigar, detectar y prevenir el acceso no autorizado. Los controles deben crear un rastro de auditoría utilizando el principio de "Quién, qué, dónde, cuándo";
- Quién era el usuario, por ejemplo: el identificador de cuenta del usuario;
- Qué activos fueron los que se vieron, por ejemplo: datos;
- Desde dónde accedieron al activo, por ejemplo: la dirección IP; y
- Cuándo, por ejemplo: registro de tiempo.
- Todo acceso físico y lógico debe quedar registrado en archivos de registro que se conserven durante un año (como mínimo);
- En caso de una infracción en la que los datos de BT se vean comprometidos, robados o modificados, debe establecerse un proceso para garantizar que se notifique a BT dentro de un período razonable de tiempo, con el suficiente nivel de detalle;

En caso de tratarse de información de ISC, se aplica además lo siguiente:

- El centro de datos debe pasar una inspección de seguridad in situ;
- Los servidores de aplicaciones, bases de datos, etc. deben estar en una infraestructura dedicada, sin multitenencia y deben alojarse en un estante dedicado dentro de una jaula segura. En caso de que no se pueda cumplir este requisito, hay que proceder con una evaluación de riesgo de BT que demuestre la adecuada separación de los datos de BT de los de otros clientes que compartan el mismo entorno, garantizando que los DBA no tengan acceso lógico a las instancias del cliente y no vean los datos del cliente de manera conjunta. Las tablas y filas de la base de datos no deben reflejar la visión de una única instancia del cliente.
- Los procesos deben establecerse para garantizar que los datos de ISC se borren de manera segura al final de su ciclo de vida en la nube. Todos los dispositivos de almacenamiento que contengan datos de ISC deben borrarse o eliminarse como se especifica en el Anexo 1.