Anexo [XX] – Requisitos de seguridad de los proveedores de BT

Contenido

PARTE 1: INTRODUCCIÓN

1 INTRODUCCIÓN

1.1 En este documento se establecen los requisitos de seguridad de BT.

1.2 En estos Requisitos de seguridad, se aplicarán las definiciones de la Parte 5, "**Definiciones"**, pero, por lo demás, los términos del Contrato se aplicarán a estos Requisitos de seguridad y todas las palabras y expresiones empleadas en estos Requisitos de seguridad tendrán el mismo significado que el otorgado en el Contrato.

1.3 Estos Requisitos de seguridad complementan y no van en detrimento de ninguna otra obligación del Proveedor en el Contrato (incluyendo, entre otros, sus obligaciones en las Condiciones tituladas "**Confidencialidad**", "**Protección de datos personal"** y "**Cumplimiento**").

PARTE 2: REQUISITOS DE ACCESO LIMITADO

2 REQUISITOS DE ACCESO LIMITADO

Esta sección se notificará, según sea preciso, cuando el Proveedor proporcione Suministros que impliquen el acceso limitado a Información de BT o del cliente de BT, o tenga acceso a nivel de usuario a los Sistemas administrativos de BT. Los Proveedores que se incluyan en esta categoría no tendrán que cumplir ninguna otra parte de este documento.

2.1 Sin perjuicio de ninguna de las obligaciones de confidencialidad que pueda tener, cuando el Proveedor o el Personal contratado tenga acceso a Información de BT, el Proveedor deberá:

2.2 Verificar que la Información de BT no sea divulgada por el Personal contratado, ni que dicho personal acceda a ella, salvo que sea necesario para la provisión de los Suministros; y

2.3 Implementar todos los sistemas y procesos (técnicos y organizativos) que sean necesarios conforme a las Buenas prácticas de seguridad del sector, con el fin de proteger la seguridad y la confidencialidad de la Información de BT y sus sistemas.

PARTE 3: REQUISITOS DE SEGURIDAD GENERALES

Obligatorios cuando en la Parte 2: No se hayan notificado los Requisitos de acceso limitado como aplicables.

3 SEGURIDAD GENERAL DE LA INFORMACIÓN

Seguridad general de la información

3.1 El Proveedor implementará sistemas y procesos (técnicos y organizativos) para:

3.1.1 proteger la seguridad y la confidencialidad de la Información de BT y sus sistemas, tal y como se estipula en estos Requisitos de seguridad; y

3.1.2 garantizar la disponibilidad, calidad, integridad y capacidad adecuada para entregar los Suministros sin interrupción, tal y como lo requieran las Buenas prácticas de seguridad del sector.

3.2 El Proveedor implementará un proceso de gestión del cambio informático documentado para garantizar que cualquier cambio que se haya realizado en los procesos y en los sistemas del Proveedor sean implementados de tal forma que el Proveedor siga cumpliendo estos Requisitos de seguridad.

3.3 El Proveedor pondrá a disposición de BT, tras solicitud por escrito por parte de BT, copias de cualquier certificación de seguridad y declaración de cumplimiento pertinentes para los Suministros con el fin de demostrar el cumplimiento de estos Requisitos de seguridad.

3.4 El Proveedor hará todo lo que sea razonable para garantizar el nombramiento de las personas adecuadas y encargarles la responsabilidad del Punto de contacto para Riesgos de seguridad, Gestión de incidentes y Gestión del cumplimiento. El Proveedor notificará al Contacto de seguridad de BT los datos de contacto de dichas personas y cualquier cambio que puedan sufrir. Los datos deberían incluir:

nombre, responsabilidad, función y dirección de e-mail del grupo y/o número de teléfono

3.5 El Proveedor confirma y acuerda que, cuando sea oportuno, BT puede realizar cambios razonables en los Requisitos de seguridad de BT cuando:

3.5.1 el Proveedor se vea sometido a una fusión, adquisición o a cambios materiales de titularidad o control;

3.5.2 se produzca un cambio de acuerdo con las normas de seguridad tecnológicas o industriales; o

3.5.3 se produzca cualquier cambio material en los Suministros o en la forma en la que se proporcionan,

(cada uno de ellos será un "**Cambio de requisito de seguridad**").

Tras recibir la notificación por escrito de BT de la necesidad de un Cambio de requisito de seguridad, el Proveedor se atendrá al Cambio de requisito de seguridad rápidamente y, en cualquier caso, en un plazo razonable (que deberá tener en cuenta la naturaleza del cambio y el riesgo que supone para BT).

3.6 El Proveedor revisará, como mínimo anualmente o cuando se produzca cualquier cambio material en los Suministros o en cómo se proporcionan, los Requisitos de seguridad para asegurar que sigan cumpliendo todos los Requisitos de seguridad aplicables.

3.7 Si el Proveedor subcontrata las obligaciones incluidas en el Contrato, deberá asegurar que todos los contratos con los Subcontratistas pertinentes incluyan condiciones escritas que obliguen al Subcontratista a cumplir los Requisitos de seguridad del proveedor de BT, en la medida que sean aplicables. Estas condiciones deben existir en la práctica entre el Proveedor y su Subcontratista antes de que el Subcontratista o cualquiera de sus empleados pueda acceder a los Sistemas y a la Información de BT.

Uso de la Información de BT

3.8 El Proveedor no utilizará la Información de BT para ningún otro fin que no sea para el que se le proporcionó al Proveedor y, en ese caso, siempre en la medida necesaria para permitir ejecutar el Contrato. Cuando el Proveedor procese Datos personales, no deberá utilizar ningún Dato personal que forme parte de la Información de BT para ningún fin que no sea el especificado en el Anexo de procesamiento.

3.9 La Información de BT se puede conservar tanto tiempo como sea necesario para ejecutar el Contrato, tras lo cual no se debería conservar más de dos años como máximo, salvo que BT y el Proveedor hayan acordado un período de conservación distinto o lo exija cualquier legislación aplicable. Para evitar cualquier duda, cuando el Proveedor procese Datos personales, no conservará ningún Dato personal que forme parte de la Información de BT durante más tiempo que el especificado en el Anexo de procesamiento o en la Condición titulada **"Protección de Datos personales**".

3.10 El Proveedor debe someterse a las políticas y normas aplicables en:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

3.11 Si los Suministros dependen directamente de un contrato público británico, el Proveedor debe cumplir la versión más reciente del programa Cyber Essentials Plus.

Tratamiento de la información

3.12 El Proveedor dispondrá y cumplirá los procesos de tratamiento de la información que sean materialmente uniformes con la Clasificación de información de terceros y la Especificación de tratamiento y que, como mínimo, garanticen que el Proveedor:

3.12.1 implementa los procesos adecuados para evitar la distribución no autorizada de la Información de BT en ningún formato, incluyendo e-mail, fax, redes sociales, formato impreso o publicaciones (por ejemplo, garantizando la existencia de una política de 'mesa y pantalla despejada' y que la información Estrictamente confidencial no se envíe por fax ni por e-mail);

3.12.2 no hable de Información de BT en las reuniones, salvo que los asistentes (i) estén autorizados a asistir a la reunión; (ii) necesiten conocer la información de la que se está hablando; y (iii) sean conscientes y tengan en cuenta sus obligaciones de confidencialidad;

3.12.3 no guarde Información de BT:

3.12.3.1 en la nube o en servicios de Internet incluyendo, entre otros, Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin o Facebook, salvo que se acuerde por escrito con BT;

3.12.3.2 en ningún portátil u otro dispositivo, salvo que esté protegido con una función de encriptación completa del disco (como BitLocker) que cumpla los estándares del párrafo 3.15; o

3.12.3.3 elimine o inutilice Información de BT de las actividades empresariales diarias de forma segura.

Control de acceso

3.13 El Proveedor mantendrán controles de acceso en los Sistemas del proveedor adecuados al entorno y a la naturaleza de los Suministros proporcionados a BT, incluyendo la garantía, cuando proceda, de que:

3.13.1 todos los usuarios, incluyendo los usuarios a nivel de administrador, deban tener ID exclusivas;

3.13.2 se requieran cambios regulares de las contraseñas (como mínimo, cada 90 días);

3.13.3 se implementen las protecciones adecuadas tras intentos de conexión fallidos para evitar ataques forzados;

3.13.4 se deshabiliten automáticamente las cuentas sin utilizar;

3.13.5 se utilicen contraseñas de la longitud adecuada (con un mínimo obligatorio de 8 caracteres que incluyan tres de las siguientes categorías: (i) mayúsculas; (ii) minúsculas; (iii) números; y (iv) no alfanuméricos, y se ejecute el historial de la contraseña para prohibir el uso de contraseñas anteriores en un período de 12 meses;

3.13.6 se implemente el acceso basado en roles a los Sistemas del proveedor con un acceso más restrictivo, como mínimo, para el acceso del administrador; y

3.13.7 se lleven a cabo revisiones periódicas y auditorías del acceso de los usuarios.

Acceso remoto

3.14 El Proveedor no está autorizado a permitir al Personal contratado el Acceso remoto a información clasificada como Estrictamente confidencial, salvo que se acuerde lo contrario por escrito con BT. Cuando el Acceso remoto esté permitido, el Proveedor se asegurará de que dicho Acceso remoto esté sujeto a controles de seguridad adecuados en el seno de la empresa del Proveedor, incluyendo, entre otras cosas, la verificación de que el Acceso remoto por parte de los usuarios esté sometido a una autenticación sólida de doble factor. Si se usa el Acceso remoto a través de redes públicas para fines de soporte, las conexiones se encriptarán de conformidad con los estándares estipulados en el párrafo 3.15.

Transmisión de datos

3.15 La transmisión de Registros masivos rutinarios de Información de BT se debería realizar a través de PGP o una plataforma de transferencia aprobada en el sector.

Encriptación

3.16 El Proveedor se asegurará de que la Información de BT Confidencial y Estrictamente confidencial se encripte cuando esté estacionaria y en tránsito, de conformidad con las Buenas prácticas de seguridad del sector, que garantice la no utilización de estándares desfasados por el sector pertinente. Los estándares de encriptación actuales aprobados por BT en la Fecha de entrada en vigor que cumplan los requisitos de este párrafo 3.15 se establecen en la Clasificación de información de terceros y Especificación de tratamiento.

Parches

3.17 El Proveedor dispondrá y seguirá un proceso de gestión de parches documentado que, como mínimo, garantice que el Proveedor:

3.17.1 despliegue parches en los siguientes calendarios:

Tipo de parche	Descripción	Calendario
Parches críticos	Parches necesarios para abordar aspectos vulnerables del día cero	En cuanto sea plausible y, en cualquier caso, en un plazo de 14 días a partir de la disponibilidad de un parche
Parches importantes	Puntos vulnerables clasificados como Altos 7,0 - 8,9 en la escala de calificación de la gravedad cualitativa del Sistema de puntuación de vulnerabilidad común (CVSS)	En un plazo de 30 días a partir de la disponibilidad de un parche
Otros parches	Todos los parches que no son importantes ni parches críticos	En un plazo de 8 semanas a partir de la disponibilidad de un parche

3.17.2 controla todos los distribuidores aplicables para los lanzamientos de parches;

3.17.3 usa los parches obtenidos de: distribuidores directamente para los sistemas patentados y parches que (i) están firmados digitalmente o (ii) están comprobados con el uso de un hash del distribuidor (no se deben utilizar hashes MD5) para el paquete de actualización, de tal forma que se pueda identificar el parche como procedente de una comunidad de soporte reconocida para software de fuente abierta;

3.17.4 prueba todos los parches en sistemas que representan de forma precisa la configuración de los sistemas de producción objetivo, antes del despliegue del parche en los sistemas de producción y que el funcionamiento correcto del servicio con parches esté comprobado después de cualquier actividad que implique el uso de parches; y

3.17.5 mantiene y actualiza los Sistemas del proveedor para garantizar que se puedan aplicar los parches de los distribuidores más actualizados.

3.18 Si no se puede usar un parche del Proveedor en un sistema, el Proveedor debe notificarlo a BT por escrito. Al recibir dicha notificación, BT revisará el riesgo para BT y para la Información de BT asociado con el uso continuado por el Proveedor del sistema y BT puede pedir al Proveedor que tome cualquier medida razonable (a coste del Proveedor) para abordar dichos riesgos.

Gestión de la vulnerabilidad

3.19 El Proveedor tendrá y seguirá un proceso de gestión de la vulnerabilidad que, como mínimo, garantice que el Proveedor:

3.19.1 realiza las acciones adecuadas (por ejemplo, escaneado) para identificar los puntos vulnerables;

3.19.2 realiza sus propias pruebas periódicas de penetración; y mantiene informes de dichas pruebas; y

3.19.3 reacciona a cualquier notificación de puntos vulnerables e implementa planes de acción para mitigar los puntos vulnerables conocidos de conformidad con los párrafos de 3.22 a 3.27.

Pruebas de penetración

3.20 El Proveedor deberá:

3.20.1 permitir a BT (o a los subcontratistas autorizados de BT) realizar pruebas de penetración razonables con un plazo de antelación razonable; y

3.20.2 proporcionar a BT acceso a los informes de pruebas de penetración del Proveedor pertinentes con respecto a los Suministros que se estén proporcionando.

Auditorías y Creación de registros

3.21 El Proveedor dispondrá y seguirá un proceso de auditorías y creación de registros que, como mínimo, garantice que el Proveedor registre (según corresponda) los siguientes eventos:

3.21.1 los puntos de inicio y finalización del proceso registrado;

3.21.2 cambios del tipo de eventos registrados, según lo precise el seguimiento de auditoría (por ejemplo, los parámetros de inicio y cualquier modificación de los mismos);

3.21.3 inicio y cierre del Sistema del proveedor;

3.21.4 inicios de sesión satisfactorios;

3.21.5 intentos de inicio de sesión fallidos (por ejemplo, ID del usuario o contraseña incorrectos);

3.21.6 todas las operaciones realizadas por usuarios con privilegios (por ejemplo, usuarios con acceso firme a instalaciones o aplicaciones del sistema);

3.21.7 escalación de privilegios satisfactoria y no satisfactoria;

3.21.8 todos los accesos por parte del Proveedor o del Personal contratado del Proveedor a información Estrictamente confidencial u operaciones sobre esa información; y

3.21.9 la creación, modificación y eliminación en o de cuentas de usuario.

3.22 Para cada evento auditable, el Proveedor mantendrá un seguimiento de auditoría a prueba de manipulación que permita la reconstrucción de dichos eventos.

3.23 Teniendo en cuenta la gravedad del componente/datos, el Proveedor inspeccionará periódicamente y analizará los registros de auditoría para detectar cualquier comportamiento sospechoso o anómalo y tomará las acciones adecuadas y/o dará la voz de alarma.

3.24 Todas las alarmas deben estar documentadas y se deberá actuar al respecto de manera oportuna, en función de la gravedad de la alarma.

3.25 El Proveedor conservará todos los archivos de registro durante tres meses (salvo que se vea obligado a borrarlos en virtud de la cláusula titulada "**Protección de Datos personales**") y presentará copias o permitirá el acceso a los archivos de registro a solicitud de BT en un formato acordado por ambas Partes.

Gestión de las amenazas y Tratamiento de incidentes

3.26 El Proveedor dispondrá y seguirá un proceso de gestión de incidentes de seguridad formal que incluya la definición de las responsabilidades para abordar un Incidente de seguridad relevante. Cualquier información relacionada con un Incidente de seguridad relevante se tratará como "**Confidencial**".

3.27 El Proveedor informará al Contacto de seguridad de BT y al Contacto comercial de BT, en un plazo de tiempo razonable tras tener constancia de cualquier Incidente de seguridad relevante y, en cualquier caso, no más tarde de doce (12) horas a partir de que al Proveedor le conste el Incidente de seguridad relevante.

3.28 Sin retraso no razonable, el Proveedor tomará rápidamente las acciones correctivas adecuadas y oportunas para mitigar cualquier riesgo y efecto relativos al Incidente de seguridad relevante para reducir la gravedad y la duración del incidente.

3.29 El Proveedor acuerda proporcionar toda la información que BT precise de manera razonable con relación al Incidente de seguridad relevante, incluyendo, entre otros:

3.29.1 la fecha y la hora;

3.29.2 la ubicación;

3.29.3 el tipo de incidente;

3.29.4 el impacto;

3.29.5 la clasificación de la información afectada;

3.29.6 el estado; y

3.29.7 el resultado (incluyendo la resolución, recomendaciones o acciones adoptadas).

3.30 El Proveedor se asegurará de la subsanación inmediata de los riesgos identificados en lo relativo a la confidencialidad, integridad o disponibilidad de la Información de BT en los procesos o Sistemas del Proveedor.

3.31 Si un Incidente de seguridad relevante constituye también una Infracción de los Datos personales, en ese caso el Proveedor también cumplirá las estipulaciones de la cláusula titulada "**Protección de los Datos personales**", además de lo estipulado en estos Requisitos de seguridad. Para evitar cualquier duda, el Proveedor también cumplirá lo estipulado en la cláusula titulada "**Protección de los Datos personales**" con relación a cualquier Infracción de Datos personales, independientemente de si la infracción pueda ser o no un Incidente de seguridad relevante.

4 SEGURIDAD DEL PERSONAL CONTRATADO

4.1 El Personal contratado no disfrutará de Acceso hasta que no haya realizado la Formación de seguridad de la Información de BT, a la que se puede acceder a través de https://workingwithbt.extra.bt.com o a través del sistema de aprendizaje de BT, en el que el Personal contratado tendrá asignado un número de identificación de BT. La Formación de seguridad de la Información de BT se debe actualizar oportunamente, tal y como se detalla en https://workingwithbt.extra.bt.com. El Proveedor conservará los registros de la formación y los pondrá a disposición de BT a efectos de auditoría.

4.2 El Proveedor se asegurará de que todo el Personal contratado firme acuerdos de confidencialidad que incluyan materialmente las mismas obligaciones que las impuestas al Proveedor en la Parte 2 anterior, antes de que cualquier miembro del Personal contratado empiece a trabajar en instalaciones de BT o en Sistemas de BT o tenga acceso a Información de BT. Estos acuerdos de confidencialidad los debe conservar el Proveedor y ponerlos a disposición de BT a efectos de auditoría.

4.3 El Proveedor abordará las infracciones de las políticas y los procedimientos de seguridad de BT y del Proveedor mediante procesos formales incluyendo la acción disciplinaria, que puede incluir la retirada de la persona de:

4.3.1 tener acceso a los Sistemas de BT o a la Información de BT; o

4.3.2 llevar a cabo tareas relativas a la provisión de los Suministros.

Además, el Proveedor debería garantizar que se disponga de los procesos pertinentes para asegurar que cualquier miembro del Personal contratado que haya sido retirado no vuelva a tener acceso posteriormente a los Sistemas de BT, a la Información de BT ni se le permita trabajar con relación a la provisión de los Suministros.

4.4 El Proveedor, en la medida que permita la ley, mantendrá un servicio de asistencia telefónica confidencial, disponible para todo su personal, que deberá utilizar el Personal contratado en caso de que se le indique que debe actuar de una forma no coherente o que infrinja estos Requisitos de seguridad. Al Contacto de seguridad de BT se le notificarán los informes pertinentes.

4.5 Cuando al Personal contratado ya no se le asignen los Suministros, el Proveedor se asegurará de que:

4.5.1 se revoque el acceso a la Información de BT; y

4.5.2 a elección de BT, cualquier Activo físico de BT o Información de BT en posesión del Personal contratado se debería:

4.5.2.1 devolver al equipo operativo de BT pertinente; o

4.5.2.2 ser destruido de conformidad con la versión más actual de la Clasificación de información de terceros y Especificación de tratamiento.

4.6 Salvo que se acuerde lo contrario por escrito con el Contacto de seguridad de BT, el Proveedor deberá implementar un procedimiento de salida controlada para el Personal contratado que incluya la solicitud escrita al Contacto de seguridad de BT para la retirada del acceso a los Sistemas de BT, la Información de BT y cualquier otro Acceso y accesos. El Personal contratado debería ser informado de que su acuerdo de confidencialidad seguirá siendo vigente y de que la información BT a la que ha tenido acceso por su trabajo con los Suministros no se debe divulgar.

4.7 Como parte de la concesión de Acceso, el Proveedor mantendrá y proporcionará registros de todo el Personal contratado que precise acceso o participe en la provisión de los Suministros a BT, incluyendo su nombre, ubicación en la que trabajan, dirección de e-mail del trabajo, número de teléfono profesional directo y extensión (si procede) y/o número de móvil, fecha de solicitud del número de ID de usuario (UIN) (en caso de que lo tengan), fecha en la que se les asignó la provisión de los Suministros a BT, fecha en la que realizaron la formación obligatoria, fecha en la que dejaron de proporcionar los Suministros y una declaración de comprobación del trabajo anterior. Será responsabilidad del Contacto de seguridad del Proveedor verificar que, en todo momento, solo el Personal contratado esté autorizado.

4.8 El Proveedor dispondrá de políticas y procesos para garantizar que el Personal contratado no use las redes sociales para publicar o hacer público online ninguna afirmación, comentario, contenido o imagen que;

4.8.1 pudiera atribuirse de forma razonable como propia de BT;

4.8.2 divulgue cualquier Información de BT que fuera Información confidencial, o estuviera identificada como “Confidencial” o “Estrictamente confidencial”; y

4.8.3 sea difamatorio/a para BT y pueda dañar la marca y la reputación de BT.

5 AUDITORÍAS Y REVISIÓN DE LA SEGURIDAD

5.1 Sin perjuicio de cualquier otro derecho de auditoría que BT pueda tener, con el fin de evaluar el cumplimiento por parte del Proveedor de estos Requisitos de seguridad y cuando proceda la Condición “**Protección de los Datos personales**”, BT o sus representantes nombrados se reservan el derecho a realizar una auditoría de cumplimiento de la seguridad cuando lo estimen oportuno, en cualquiera o todos los aspectos de las políticas del Proveedor, sus procesos y sistemas (con sujeción a la protección por parte del Proveedor de la confidencialidad de cualquier información no relacionada con la provisión de los Suministros a BT), mediante una revisión de la seguridad documentada o en las instalaciones del Proveedor y de cualquier Subcontratista pertinente que estén materialmente implicados en la provisión de los Suministros o en la ejecución del Contrato.

5.2 El Proveedor proporcionará a BT, o a sus representantes, acceso y asistencia según sea necesario y adecuado para permitir las revisiones de la seguridad documentadas o la realización de auditorías en las instalaciones. Antes de la realización *in situ* de la auditoría rutinaria, se notificará al Proveedor con una antelación mínima de 30 días laborables. Sin embargo, para evitar cualquier duda, en caso de una Infracción de los Datos personales o una Infracción de la seguridad relevante real o supuesta, BT no tendrá que respetar ese plazo de notificación.

5.3 El Proveedor colaborará con BT para implementar las recomendaciones acordadas y llevar a cabo cualquier acción correctiva que BT considere necesaria y se derive de una revisión documentada o de una auditoría en la sede, en un plazo de 30 días tras la notificación de dichas recomendaciones o acción correctiva por parte de BT o en el período acordado entre las Partes, a cargo del Proveedor.

5.4 En caso de que BT necesitara realizar una auditoría independiente del Proveedor y se descubriera que este último no cumple los principios y las prácticas de la norma ISO/IEC 27001:2013, en ese caso el Proveedor, a su propio cargo, llevará a cabo las acciones necesarias para conseguir el cumplimiento necesario y le reembolsará a BT todos los costes en los que BT haya incurrido por realizar dicha auditoría.

6 INVESTIGACIÓN

6.1 Si BT tiene motivos para sospechar que se ha producido una:

6.1.1 Infracción de los Datos personales;

6.1.2 Infracción de la seguridad relevante;

6.1.3 o una infracción de estos Requisitos de seguridad,

BT informará al Contacto de seguridad del Proveedor y el Proveedor acuerda, a su propia costa:

6.1.4 actuar inmediatamente para investigar la supuesta infracción e identificar, prevenir y procurar todo lo razonable para mitigar los efectos de dicha infracción; y

6.1.5 llevar a cabo cualquier acción de recuperación o de otro tipo que sea necesaria para subsanar la infracción.

6.1.6 proporcionar a BT los informes que BT requiera de forma razonable con relación a las investigaciones, hallazgos y acciones tomadas para subsanar o mitigar la infracción,

En caso de una infracción grave, el Proveedor colaborará plenamente con BT en cualquier investigación resultante o auditoría por parte de BT, un organismo normativo y/o cualquier organismo de aplicación de la ley, debiendo dicha investigación o auditoría incluir (tras una notificación razonable por parte de BT al Proveedor) acceso a la Información de BT mantenida en las instalaciones del Proveedor o en los Sistemas del proveedor

Durante cualquier investigación, el Proveedor colaborará con BT, proporcionando acceso y asistencia según sea necesario y adecuado para investigar la infracción. BT puede solicitar el aislamiento del Proveedor para evaluar cualquier activo tangible o intangible que pertenezca al Proveedor para ayudar en la investigación y el Proveedor no denegará ni retrasará de forma poco razonable dicha solicitud.

PARTE 4: REQUISITOS DE SEGURIDAD ESPECÍFICOS

7 POLÍTICA Y REQUISITOS DE SEGURIDAD GENÉRICOS

7.1 El Proveedor manifiesta y declara que los Sistemas del proveedor, los Suministros, los servicios asociados, los procesos y las sedes físicas cumplen y seguirán cumpliendo siempre la norma ISO/IEC 27001:2013 y cualquier versión futura o modificada de la norma que se emita. Este cumplimiento se debe garantizar, a criterio exclusivo de BT, mediante:

7.1.1 certificación del ISMS del Proveedor por un UKAS o un organismo certificador aprobado equivalente internacional en el que BT haya validado el alcance y la declaración de aplicabilidad; o

7.1.2 una auditoría bilateral y proceso de comprobación especificado por BT.

7.2 El Proveedor debe presentar un certificado ISO/IEC 27001 válido al inicio del Contrato y en futuras renovaciones de la certificación.

7.3 En caso de que el alcance del certificado o la declaración de aplicabilidad cambiaran en algún momento, el Proveedor debe enviar estos cambios para que se vuelvan a validar utilizando el procedimiento de control de cambios (o, en ausencia de dicho procedimiento, a través del proceso de variación). El Proveedor debe informar a BT en un plazo de dos días laborables de cualquier no conformidad importante identificada por el organismo certificador o el Proveedor.

8 SEGURIDAD FÍSICA - INSTALACIONES DE BT

El cumplimiento de esta sección es obligatorio si el Proveedor proporciona Suministros en las instalaciones de BT.

8.1 Todo el Personal contratado que trabaje en las instalaciones de BT estará en posesión de una tarjeta de identificación proporcionada por BT o por el Proveedor, que deberá llevar en un lugar destacado, que demuestre que el Personal contratado está autorizado (“**Tarjeta de acceso autorizado”**). Las Tarjetas de acceso autorizado incluirán una fotografía que deberá ser clara y mantener un parecido con el miembro del Personal contratado. Al Personal contratado también debe proporcionarse una tarjeta de acceso electrónico y/o una tarjeta de visitante de duración limitada, que se utilizará de acuerdo con las instrucciones de emisión locales.

8.2 Cuando se emita al Personal contratado una Tarjeta de acceso autorizado por parte de BT, el Proveedor debe avisar a BT a la mayor brevedad posible y, en cualquier caso, en un plazo de cinco días laborables, cuando dicho Personal contratado ya no precise acceder a las instalaciones de BT.

8.3 Solo está permitida la conexión directa (conexión al puerto LAN o conexión inalámbrica) a los dominios de BT por parte de servidores creados por BT, PC Webtop de BT y dispositivos finales de confianza. El Proveedor no conectará, sin la autorización previa por escrito del Contacto de seguridad de BT, ningún equipo no aprobado por BT a ningún Dominio de BT (y, cuando sea pertinente, se asegurará de que ningún miembro del Personal contratado lo haga). El Contacto de seguridad de BT solo proporcionará la autorización escrita al iniciar el proceso de concesión de la política de seguridad dentro de BT. En cualquier caso, el Proveedor debe garantizar que no se use ningún equipo de titularidad privada del Personal contratado o de cualquier otro trabajador (incluyendo contratistas, trabajadores temporales y trabajadores de agencias) para almacenar, acceder o procesar ningún dato de BT.

8.4 No se sacará ninguna Información de BT fuera de las instalaciones de BT, ni se sacará ni instalará ningún equipo ni software de las instalaciones de BT sin la autorización previa por parte de BT.

8.5 Se cumplirán la protección física y las directrices de trabajo en las instalaciones de BT, que incluirán, entre otras cosas, el acompañamiento del Personal contratado y la adopción de unas prácticas de trabajo adecuadas dentro de áreas seguras.

8.6 Cuando el Proveedor esté autorizado a proporcionar a su Personal contratado acceso sin alojamiento a áreas dentro de la propiedad de BT, el firmante autorizado de BT y el Personal contratado deben cumplir el documento orientativo "**Acceso del Proveedor a las sedes y edificios de BT**"

https://groupextranet.bt.com/selling2bt/working/third_party_access/default.htm.

8.7 Asimismo, el firmante no autorizado por BT y el Personal contratado deberán tener, como mínimo, verificaciones previas al empleo L2 https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

9 SEGURIDAD FÍSICA - INSTALACIONES DEL PROVEEDOR

El cumplimiento de esta sección es obligatorio si el Proveedor proporciona Suministros de instalaciones que no son de BT. (Por ejemplo, Proveedores o terceros del Proveedor)

9.1 El acceso a instalaciones que no sean de BT (sedes, edificios o áreas internas) en las que se proporcionen Suministros, o en las que se almacene o procese Información de BT, solo estará permitido cuando se utilice una tarjeta de identificación del Proveedor autorizado. Esta tarjeta se tiene que utilizar como medio de comprobación de la identidad en las instalaciones pertinentes en todo momento y, como tal, la fotografía que aparezca en ella debe ser clara y mantener un parecido con la persona. Las personas también pueden estar provistas de una tarjeta de acceso electrónico autorizado para acceder a las instalaciones pertinentes o un acceso de seguridad por teclado. El Proveedor debe tener procesos para: autorización, divulgación de cambios de código (que se deben realizar mensualmente, como mínimo); y cambios de código *ad hoc*.

9.2 El Proveedor se asegurará de que el acceso a instalaciones que no sean de BT de las que se saquen Suministros o en las que se almacene o procese Información de BT, esté autorizado y el Proveedor debe cumplir los procesos y procedimientos de seguridad para controlar y supervisar al Personal contratado, a los visitantes y a cualquier otra persona externa, incluyendo terceros con acceso físico a estas áreas (por ejemplo, mantenimiento del control medioambiental, empresas de alarmas, empresas de limpieza).

9.3 Si BT lo solicita, el Proveedor deberá asegurar que el Personal contratado sea segregado de forma segura del resto del personal del Proveedor. Además, el Proveedor debe garantizar que los sistemas y la infraestructura empleados para la entrega de los Suministros estén contenidos dentro de una red lógica específica. Esta red debe estar compuesta únicamente por los sistemas específicos para la prestación de un servicio de procesamiento de datos seguro.

9.4 Las áreas seguras de las instalaciones del Proveedor (por ejemplo, salas de comunicaciones de red) estarán separadas y protegidas por controles de acceso adecuados, para garantizar que solo el Personal contratado autorizado tenga acceso a tales áreas seguras. El acceso a estas áreas ejercido por cualquier miembro del Personal contratado debe ser auditado como mínimo una vez al mes. Además, se debe hacer una evaluación de reautorización de los derechos de acceso a estas áreas como mínimo anualmente.

El Proveedor proporcionará a BT una prueba de evaluación de riesgos, cuando BT así se lo solicite. Si no se facilita tras la solicitud de BT, a discreción de BT, BT o su representante realizarán una evaluación de los riesgos del entorno utilizado para prestar el Servicio (como centros de datos, áreas de procesamiento de datos, salas de ordenadores) antes de iniciar la prestación de los Suministros. Además, se debe informar a BT antes de cualquier obra importante en cualquier instalación que pudiera poner en peligro la seguridad de la Información de BT.

9.5 El Proveedor utilizará sistemas de seguridad CCTV y sus medios de grabación asociados en respuesta a posibles incidentes de seguridad, como herramienta de vigilancia de seguridad, como disuasión o como ayuda para la posible detención de presuntos delincuentes en el momento de cometer un delito. Las grabaciones efectuadas a través de sistemas CCTV (en cinta o digitalmente), se deben conservar al menos 20 días. No obstante, este período se puede ampliar en las siguientes situaciones:

9.5.1 Si se deben conservar pruebas en vídeo del CCTV para la investigación de un incidente o delito; o

9.5.2 Si se especifica que es un requisito necesario para cumplir la legislación.

9.5.3 Todas las grabaciones del CCTV se deben guardar en un armario bajo llave y la llave debe estar protegida y controlada. El acceso al armario debe estar restringido solo al personal autorizado.

9.6 Todos los sistemas de grabación de CCTV han de estar protegidos para evitar la modificación o la eliminación y la posibilidad de la visualización 'casual' de cualquier pantalla de CCTV según las directrices para el uso de sistemas CCTV, que se pueden consultar en

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

9.7 El Proveedor inspeccionará todas las áreas de las instalaciones del Proveedor utilizadas para la prestación de los Servicios y Suministros con el fin de detectar riesgos y amenazas al menos una vez al mes. El Proveedor debe haber considerado e implementado todas las medidas adecuadas para garantizar la seguridad física con relación a lo siguiente:

9.7.1 concienciación de amenazas locales incluyendo, entre otras, amenazas potenciales de industrias locales y proximidad de materiales peligrosos almacenados; y

9.7.2 catástrofes naturales, incluyendo riesgos de amenaza de inundaciones, corrimientos de tierra y condiciones climatológicas adversas, entre otros.

9.8 El Proveedor debe evaluar el cableado eléctrico y de telecomunicaciones que exista en las instalaciones del Proveedor y que transporte datos o se utilice para servicios de información o servicios de radio/satélite para la prestación de los Suministros, con el fin de comprobar el nivel de protección y evitar la interrupción de las operaciones comerciales. Se deben implementar medidas de protección de la seguridad física proporcionales a la gravedad empresarial de las operaciones para las que sirven, de la siguiente manera:

9.8.1 proteger el trayecto del cableado empresarial, apantallado de cables, pozos o cajas de paso que contengan los cables críticos para el negocio;

9.8.2 restringir el acceso a las cámaras de cables o armarios de cables en los edificios operativos con el uso de lectores de control de acceso electrónico o con una gestión efectiva con llave;

9.8.3 proteger físicamente, además de su entorno, los enlaces de comunicaciones informáticas y los equipos de comunicaciones de las instalaciones informáticas; y

9.8.4 proteger adecuadamente los enlaces de las comunicaciones por radio y satélite y el equipo de comunicaciones.

9.9 BT requerirá, salvo que se acuerde lo contrario entre el Proveedor y el Contacto de Seguridad de BT, la implementación de servicios de seguridad atendidos por parte del Proveedor para complementar la medida de seguridad física y electrónica en las instalaciones del Proveedor en las que:

9.9.1 La ubicación sea de importancia operativa (por ejemplo, Centros de contacto, centros de datos, sedes de redes clave, etc.)

9.9.2 La Información de BT procesada pueda afectar o ir en detrimento de la marca y reputación de BT

9.9.3 Se procese un gran volumen de Información de BT (por ejemplo, externalización de procesos empresariales)

9.9.4 Requisitos contractuales del cliente

9.9.5 Exista un riesgo/amenaza específicos en la sede

9.9.6 El Proveedor esté en posesión de Información de BT con un alto nivel de sensibilidad.

9.10 Para proteger el equipo de BT (como servidores o conmutadores BT) en las instalaciones del Proveedor de amenazas ambientales o peligros, y de la posibilidad de acceso no autorizado, el Equipo BT debe estar instalado en una zona protegida y separada del equipo utilizado para cualquier sistema que no pertenezca a la organización BT. El nivel de separación debería garantizar que la seguridad del equipo BT no pueda verse en peligro, ni deliberada ni accidentalmente como resultado del acceso facilitado a organizaciones que no sean BT y, por ejemplo, podría adoptar la forma de una pared divisoria segura, armarios que se puedan cerrar con llave o jaulas metálicas.

9.11 El Proveedor debe haber implementado las medidas adecuadas para garantizar la seguridad física en relación a lo siguiente:

9.11.1 medidas de prevención contra incendios, entre otros, alarmas, equipos de detección y extinción;

9.11.2 condiciones climáticas, teniendo en cuenta la temperatura, la humedad y la electricidad estática y la gestión, monitorización y respuesta asociadas para condiciones extremas (como apagado automático, alarmas);

9.11.3 equipo de control incluyendo, entre otros, aire acondicionado y detección de agua;

9.11.4 ubicación de los depósitos de agua, tuberías, etc., dentro de las instalaciones;

9.11.5 acceso auditable - cuando proceda, el acceso a los sistemas por parte del personal debe ser auditable; y

9.11.6 supervisión del Personal contratado no asociado normalmente a la gestión o al acceso a los sistemas de BT.

9.12 Se utilizarán perímetros de seguridad (barreras como paredes, vallas, verjas de acceso controladas por tarjeta o puestos de recepción atendidos), para proteger áreas que contengan Información de BT sensible o información del cliente de BT (incluyendo Datos personales) e instalaciones de procesamiento asociadas.

9.13 Se controlarán los puntos de acceso, como las áreas de entrega y carga, y otros puntos en los que personas no autorizadas puedan entrar en las instalaciones y, si es posible, se aislarán de las instalaciones de procesamiento de la información, para evitar el acceso no autorizado o ataques deliberados.

9.14 El Proveedor se asegurará de que el acceso físico a las áreas con acceso a Información de BT o a información del cliente de BT (incluyendo Datos personales) se realice con tarjetas inteligentes o de proximidad (o sistemas de seguridad equivalentes) y el Proveedor debe realizar auditorías internas mensuales, como mínimo, para garantizar el cumplimiento de estas estipulaciones.

9.15 El Proveedor deberá asegurarse de que esté prohibida la fotografía y/o captura de imágenes de cualquier Información de BT o información del cliente de BT (incluyendo Datos personales). En circunstancias excepcionales en las que, por requisitos empresariales, sea necesario capturar dichas imágenes, es necesario obtener una exención temporal a esta estipulación del Contacto de seguridad de BT.

9.16 El Proveedor observará la política de mesa y pantalla despejados para proteger la Información de BT.

10 PROVISIÓN DE EQUIPO DE ALOJAMIENTO (HOSTING)

El cumplimiento de esta sección es obligatorio si el Proveedor proporciona un entorno de alojamiento para el equipo de BT o del cliente de BT.

10.1 El Proveedor, cuando prevea un área de acceso segura en sus instalaciones para alojar equipo de BT o del cliente de BT («**Planta del proveedor**»):

10.1.1 se asegurará de que todo el Personal contratado que acceda a la Planta del proveedor esté en posesión de una tarjeta de identificación o de una tarjeta de control de acceso electrónico. Esta tarjeta se tiene que utilizar como medio de comprobación de la identidad en la Planta del proveedor en todo momento y, como tal, la fotografía que aparezca en ella debe ser clara y mantener una semejanza con el miembro del Personal contratado; y

10.1.2 Tendrá que haber puesto en marcha los debidos procedimientos para abordar las amenazas de seguridad dirigidas contra los equipos de BT o del cliente de BT o contra terceros que trabajen en representación de BT para salvaguardar la Información de BT y del cliente de BT en la Planta del proveedor; y

10.1.3 Utilizará los sistemas de seguridad CCTV y sus medios de grabación asociados en la Planta del Proveedor en respuesta a incidentes de seguridad, como herramientas de vigilancia de la seguridad, como disuasión y ayuda para la detención de presuntos delincuentes en el momento de cometer un delito. El Proveedor garantizará que existan grabaciones de CCTV de un mínimo de 20 días, para que sea efectiva como herramienta de investigación; y

10.1.4 Proporcionará a BT un plano de planta del espacio asignado en el área segura de la Planta del proveedor; y

10.1.5 Se asegurará de que los armarios de BT y del cliente de BT en la Planta del proveedor se mantengan cerrados con llave y solo pueda acceder a ellos personal de BT autorizado, representantes aprobados de BT y el Personal contratado pertinente; y

10.1.6 Implementará un proceso de gestión seguro de la llave en la Planta del proveedor; e

10.1.7 Inspeccionará el área local adyacente a la Planta del proveedor para detectar riesgos y amenazas de forma periódica; y

10.1.8 Documentará y mantendrá procedimientos operativos (en el idioma del país donde se origine el trabajo de BT) para descargar los requisitos de seguridad detallados en este párrafo 10 y, cuando así se solicite, proporcionará a BT acceso a dicha documentación.

10.2 BT proporcionará al Proveedor:

10.2.1 un registro de los activos físicos de BT y/o del cliente de BT mantenidos en la Planta del proveedor; y

10.2.2 detalles de los trabajadores de BT, subcontratistas y agentes que precisan acceder a la Planta del proveedor (de manera continuada).

11 DESARROLLO DE LOS SERVICIOS

El cumplimiento de esta sección es obligatorio si el Proveedor se encarga del desarrollo de los Suministros para su uso por parte de BT y/o los clientes de BT. Esto incluye "componentes existentes", configuración de software y fabricación de componentes para los Suministros.

11.1 El Proveedor implementará las medidas de seguridad acordadas en todos los componentes suministrados que constituyan los Suministros y/o los Servicios, de tal forma que salvaguarden la confidencialidad, disponibilidad e integridad de los Suministros, incluyendo lo siguiente:

11.1.1 Mantener la documentación adecuada (en el idioma del país donde se origine el trabajo de BT) con relación a la implementación de la seguridad y asegurar que dicha seguridad cumpla las mejores prácticas del sector;

11.1.2 minimizar las oportunidades de que personas no autorizadas (por ejemplo, hackers) consigan acceder a los Sistemas de BT, a la Información de BT, a las Redes de BT o a los Suministros de BT; y

11.1.3 minimizar el riesgo de un uso indebido de los Sistemas de BT, la Información de BT, las Redes de BT o los Servicios que pudieran provocar potencialmente una pérdida de ingresos o servicios.

11.2 El Proveedor demostrará, a solicitud, que cualquier versión de software o hardware suministrado (tanto patentado como comercial) facilitado a BT es el mismo que el acordado con BT. El Proveedor mantendrá la integridad de las versiones, incluyendo actualizaciones, sistemas operativos y aplicación de fábrica al escritorio.

11.3 El Proveedor se asegurará de que el desarrollo de sistemas para el uso por parte de BT o la versión y el mantenimiento de hardware propiedad de BT se refuercen de acuerdo con los Requisitos de seguridad informática de BT si los proporciona el equipo operativo de BT o se desarrollan según las mejores prácticas del sector.

11.4 El Proveedor se asegurará de que los sistemas y procesos utilizados para las actividades de prueba y desarrollo se separen de los sistemas de producción. Se debe emplear un proceso de control de los cambios para divulgar cualquier código al entorno de producción. Los datos de prueba proporcionados por BT deben ser eliminados después de un período determinado por el titular de los datos de BT y no se pueden utilizar datos en directo ni de producción en entornos de desarrollo o prueba.

11.5 Todos los puntos vulnerables de seguridad graves que se encuentren en las pruebas de seguridad y que se clasifiquen como riesgo medio o superior, se deben subsanar antes de cualquier operatividad. Cualquier punto débil en los Servicios identificado por BT o el Proveedor se subsanará a costa de este último en los plazos que BT requiera de manera razonable.

11.6 Los Suministros deben someterse a pruebas de penetración independientes encargadas por el Proveedor antes del lanzamiento, como mínimo anualmente y después de cambios o incidentes importantes a cargo del Proveedor.

11.7 Los Suministros desarrollados para uso por parte de BT o sus clientes deben ser desarrollados con un Ciclo de vida de desarrollo seguro (SDLC) estándar reconocido en el sector y documentado, para minimizar el riesgo de introducir puntos de vulnerabilidad en la seguridad en el entorno de producción y/o en los clientes. El SDLC debe incluir las siguientes puertas, con objetos tangibles derivados de cada revisión y disponibles para su inspección por parte de BT dentro del marco de la auditoría indicado en el párrafo 5 de la Parte 3 de estos Requisitos de seguridad:

11.7.1 revisión de seguridad de los requisitos empresariales;

11.7.2 revisión de seguridad del diseño;

11.7.3 revisión de seguridad del código fuente - automática y/o manual; y

11.7.4 auditoría de seguridad de la solución antes de su despliegue (para incluir ataques simulados) según un plan de auditoría específico del proyecto y documentado, basado en los informes derivados de las revisiones de seguridad de los requisitos empresariales, de diseño y de código.

Más información en las Normas orientativas de terceros de la industria sobre 'Codificación segura':

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm

12 GARANTÍA

Ahora incluida dentro del contrato principal.

13 ACCESO A LOS SISTEMAS DE BT

El cumplimiento de esta sección es obligatorio si el Personal contratado del Proveedor tiene que acceder a los Sistemas de BT para proporcionar los Suministros.

13.1 BT puede permitir, según su criterio exclusivo, un Acceso limitado según sea estrictamente necesario para la provisión de los Suministros.

13.2 Con relación al Acceso, el Proveedor cumplirá todas las políticas pertinentes de BT, las normas y las instrucciones proporcionadas al Proveedor y deberá (y se asegurará de que todo el Personal contratado también lo haga):

13.2.1 asegurar que la identificación del usuario, las contraseñas, los PIN, los identificadores y los accesos a conferencias sean individuales para el Personal contratado y no se compartan. Los datos se deben almacenar de forma segura y separados del dispositivo para cuyo acceso se utilicen. Si otra persona conoce la contraseña, se debe cambiar inmediatamente;

13.2.2 cuando se lo solicite de forma razonable, debe proporcionar a BT los informes que pueda precisar sobre el Personal contratado autorizado para acceder a los Sistemas de BT;

13.2.3 la vinculación entre dominios a los Sistemas de BT no está permitida salvo que se apruebe específicamente y esté autorizado por el Contacto de seguridad de BT;

13.2.4 se hará todo lo razonablemente posible para garantizar la no presencia de virus ni códigos maliciosos (tal y como se entienden en general esas expresiones en el sector informático) para minimizar el riesgo de corrupción de los Sistemas de BT o de la Información de BT por cualquier medio; y

13.2.5 se hará todo lo razonablemente posible para garantizar que los archivos que contengan información, datos o medios que no sean relevantes para los Suministros no se guarden en Equipos de BT, servidores de BT, portátiles y ordenadores de sobremesa proporcionados por BT, instalaciones de almacenamiento centralizadas de BT o Sistemas de BT.

13.2.6 cuando BT haya facilitado al Proveedor acceso a Internet o a la intranet de BT, deberá garantizarse que el Personal contratado solo acceda a Internet o a la intranet de BT de forma adecuada y solo para que se puedan facilitar los Suministros pertinentes y bloquear sitios no aceptables o peligrosos del usuario. Es responsabilidad del Proveedor garantizar que comunique al Personal contratado, como mínimo anualmente, orientación sobre Internet y el abuso del e-mail. Esta orientación debe requerir que:

13.2.6.1 los usuarios no:

(i) Puedan acceder a ningún contenido ofensivo, sexual, sexista, racista o políticamente ofensivo;
(ii) Lleven a cabo ningún acto que pueda comprometer la reputación de BT o de personas físicas;
(iii) Mantengan un negocio privado;
(iv) (d) infrinjan ningún derecho de copyright; o
(v) sorteen o atraviesen el firewall de BT u otros mecanismos de seguridad;

13.2.6.2 El Personal contratado no contribuirá a los sitios ni publicará afirmaciones online que puedan atribuirse como opiniones propias de BT.

13.3 El Proveedor debe llevar a cabo revisiones periódicas para garantizar que el Acceso sea para para desempeñar el cargo. Debe haber disponibles copias de la documentación de revisión para su inspección por parte de BT dentro del marco de la auditoría descrito en el párrafo 5.1:

13.4 El Proveedor debe notificar a BT enseguida y, en cualquier caso, en un plazo de cinco días laborables, si un trabajador, incluyendo los contratistas, los trabajadores temporales y los trabajadores de agencia, ya no deban acceder más acceder a los Sistemas de BT, por ejemplo, cuando los trabajadores abandonan la empresa o cambian de puesto de trabajo.

14 ACCESO A LA INFORMACIÓN DE BT EN LOS SISTEMAS DEL PROVEEDOR

El cumplimiento de esta sección es obligatorio si se guarda o procesa Información de BT en los Sistemas del proveedor.

14.1 Si se otorga al Personal contratado Acceso a los Sistemas del proveedor al efecto de proporcionar los Suministros y/o Servicios, el Proveedor deberá demostrar la responsabilidad de dicho Acceso (incluyendo, entre otros, el uso de cuentas de usuario únicas, gestión de las contraseñas y un seguimiento de auditoría/registro claro de todos los actos del Personal contratado.

14.2 El Proveedor mantendrá sistemas que detecten y registren cualquier intento de daño, modificación o acceso no autorizado a la Información de BT en los Sistemas del proveedor. Ejemplos de ello incluyen, entre otros, procesos de registros en sistemas y auditorías, IDS e IPS, etc.

14.3 El Proveedor mantendrá controles para detectar y proteger frente a software malicioso, virus y códigos maliciosos en los Sistemas del proveedor y se asegurará de que se implementen los debidos procedimientos de concienciación del usuario.

14.4 El Proveedor se asegurará de que se identifique y elimine cualquier software no autorizado de los Sistemas del proveedor que tenga, procese o acceda a Información de BT, como mínimo una vez al mes.

14.5 El Proveedor se asegurará de que se controle de forma segura el acceso a los puertos de diagnóstico y de gestión, además de a las herramientas de diagnóstico.

14.6 El Proveedor se asegurará de que se limite el acceso a las herramientas de auditoría del Proveedor al Personal contratado y de que se monitorice su uso.

14.7 El Proveedor se asegurará de que se realicen revisiones del código y pruebas de penetración en todo el software producido internamente (incluyendo cualquier Software) empleado para procesar Información de BT por parte de un equipo independiente que no debe incluir a los desarrolladores del software.

14.8 En la medida que se utilicen servidores para proporcionar los Suministros, no se deben implementar en redes que no sean de confianza (redes fuera de su perímetro de seguridad, que escapen a su control administrativo, por ejemplo, orientadas a Internet) sin los controles de seguridad adecuados.

14.9 El Proveedor se asegurará de que se controlen los cambios en los Sistemas del proveedor individuales que tienen y procesan Información de BT y/o que se utilicen para proporcionar los Suministros y estén sometidos a procedimientos de control de los cambios formales.

14.10 El Proveedor debe garantizar que todos los relojes y horas del sistema estén sincronizados utilizando la última versión de NTP o una tecnología de sincronización horaria similar.

14.11 Cuando el Proveedor proporcione sistemas que permitan el acceso en línea a los Clientes de BT:

14.11.1 Las credenciales online para los Clientes de BT deben contener, como mínimo, lo siguiente:

14.11.1.1 ID del usuario;

14.11.1.2 contraseña online;

14.11.1.3 tres preguntas de autenticación y respuestas para respaldar el acceso a la cuenta; y

14.11.1.4 una forma de contacto alternativa a efectos de autenticación.

14.11.2 El Cliente de BT debe poder elegir una ID de usuario única para sus credenciales online y la contraseña online no debe contener su ID de usuario única.

14.11.3 La contraseña online del Cliente de BT debe tener una longitud mínima de 8 caracteres y contener al menos 1 carácter de 3 de los siguientes grupos: (i) número decimal (0-9), (ii) letra en mayúsculas (A-Z), (iii) letra en minúsculas (a-z), (iv) no alfanumérico

14.11.4 Para cambiar una contraseña online, el Cliente de BT debe proporcionar su contraseña actual seguida por la entrada duplicada de la nueva contraseña.

14.11.5 En caso de olvido de la ID del usuario o contraseña de un Cliente de BT, el sistema proporcionado por el Proveedor debe generar un mensaje de e-mail a la dirección de e-mail registrada del Cliente de BT que incluya el enlace de la solicitud para restablecer la contraseña o la ID del usuario después de introducir correctamente en el formulario online lo siguiente:

14.11.5.1 MSISDN o número de teléfono fijo

14.11.5.2 Contraseña online

14.11.5.3 ID del usuario del Cliente de BT

14.11.6 El enlace de la solicitud para restablecer la contraseña debe tener una duración de validad limitada de 30 minutos como máximo, antes de que expire y se tenga que realizar una nueva solicitud de contraseña online.

14.11.7 Tras restablecer correctamente la contraseña, el Cliente de BT debe estar obligado a elegir una contraseña nueva.

14.11.8 La recuperación de las credenciales de usuario del Cliente de BT cuando se olvide la ID del usuario y la contraseña online, debe generar un mensaje de e-mail a la dirección de e-mail registrada que contenga la ID del usuario y un enlace de solicitud para restablecer la contraseña después de introducir correctamente el nombre y el apellido, el número de teléfono y la dirección de e-mail del Cliente de BT.

14.11.9 Puede que sean precisos niveles adicionales de autenticación del cliente en función de la sensibilidad de los datos y de la funcionalidad a la que se tiene que acceder.

15 ALOJAMIENTO DE INFORMACIÓN DE BT POR PARTE DEL PROVEEDOR

El cumplimiento de esta sección es obligatorio cuando el Proveedor aloje externamente Información de BT clasificada como 'Confidencial' o 'Estrictamente confidencial' en un entorno de servicios en la nube o en un entorno de servidor del Proveedor o del Subcontratista.

15.1 El Proveedor deberá asegurarse, con relación a los Suministros, que los entornos en los que se aloje Información de BT cumplan con los Requisitos de alojamiento de datos externos de terceros, disponibles en:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

16 SEGURIDAD EN LA RED

El cumplimiento de esta sección es obligatorio si el Proveedor crea, desarrolla o soporta Redes de BT o Activos de red.

16.1 El Proveedor, con relación a los Suministros, deberá implementar las medidas de seguridad acordadas en todos los componentes suministrados, de forma que se salvaguarde la confidencialidad, disponibilidad e integridad de las Redes de

BT y/o los Activos de 21CN. El Proveedor proporcionará a BT documentación completa con relación a la implementación de la Seguridad de la red con relación a los Suministros y se asegurará de que:

16.1.1 cumpla, y garantice, todos los requisitos jurídicos y normativos de la Seguridad de la red de la que el Proveedor seas el responsable; y

16.1.2 haga todo lo posible para evitar que personas no autorizadas (por ejemplo, hackers) consigan acceder a los Elementos de gestión de la red y a otros elementos a los que se accede a través de las Redes de BT y/o 21CN; y

16.1.3 haga todo lo posible para reducir el riesgo de uso indebido de las Redes de BT y/o 21CN por las personas autorizadas a acceder a ellas, que podría provocar potencialmente una pérdida de ingresos o servicios; y

16.1.4 haga todo lo posible para detectar cualquier infracción de la seguridad que pueda producirse, garantizando la subsanación rápida de cualquier infracción, junto con la identificación de las personas que consiguieron acceder y el establecimiento de cómo lo consiguieron; y

16.1.5 minimice el riesgo de posible configuración incorrecta de las Redes de BT, por ejemplo, otorgando los permisos mínimos necesarios para cumplir con la tarea encomendad.

16.2 El Proveedor debe hacer todo lo que sea razonable para proteger todas las interfaces de los Suministros y/o los Servicios y no debería asumir que los componentes suministrados operan en un entorno seguro.

16.3 El Proveedor deberá proporcionar al Contacto de seguridad de BT los nombres, las direcciones (y cualquier otro dato que BT pueda precisar) de todos los miembros del Personal contratado que, cuando sea oportuno, participe directamente en la implementación, el mantenimiento y/o la gestión de los Suministros antes de que realicen dicha implementación, mantenimiento y/o gestión.

16.4 Con relación a las actividades de soporte radicadas en el Reino Unido, el Proveedor tendrá un equipo de seguridad cualificado compuesto por, al menos, un nacional británico que deberá estar disponible para comunicarse con el Contacto de seguridad de BT (o las personas que designe) y el equipo asistirá a las reuniones que el Contacto de seguridad de BT precise cuando lo estime oportuno de forma razonable.

16.5 El Proveedor proporcionará al Contacto de seguridad de BT un calendario (actualizado según sea necesario oportunamente) de todos los componentes activos incluidos en los Suministros y/o los Servicios y sus correspondientes fuentes.

16.6 El Proveedor proporcionará detalles de su personal que se vincule con el equipo de gestión de los puntos vulnerables de BT (CERT) en relación al debate sobre los puntos vulnerables identificados por BT y el Proveedor en los Suministros y/o en los Servicios. El Proveedor proporcionará a BT información puntual sobre los puntos vulnerables y cumplirá (a cargo del Proveedor) los requisitos razonables con relación a los puntos vulnerables que le puede notificar el Contacto de seguridad de BT cuando lo estime oportuno. El Proveedor informará a BT de cualquier punto vulnerable con la antelación suficiente para permitir la aplicación o instalación de controles paliativos antes de que el Proveedor divulgue públicamente esos puntos vulnerables.

16.7 El Proveedor permitirá al Contacto de seguridad de BT y a las personas nombradas por él, cuando lo estime oportuno, acceder de forma plena e ilimitada a cualquier instalación en la que se desarrollen, fabriquen o creen los Suministros para realizar pruebas de cumplimiento de la seguridad y/o evaluaciones, y el Proveedor colaborará en dichas pruebas de cumplimiento de la seguridad (y se asegurará de que todo el Personal contratado pertinente colabore).

16.8 El Proveedor se asegurará de que cualquier componente relacionado con la seguridad incluido en los Suministros que identifique BT cuando sea oportuno, se evalúe externamente a cargo del Proveedor a satisfacción razonable de BT.

16.9 Con relación a cualquier información proporcionada u obtenida de BT identificada como '**ESTRICTAMENTE CONFIDENCIAL'** o que se interprete fácilmente que es confidencial, el Proveedor se asegurará de que:

16.9.1 se proporcione acceso a ella solo a los miembros del Personal contratado específicamente autorizados por BT para visualizar y manejar y se guardará un registro de ese acceso;

16.9.2 se maneje, use y guarde con estricto cuidado, y también se encripte antes de su almacenamiento utilizando PGP o WinZip 9, y en unas condiciones que ofrezcan un alto nivel de resistencia a un riesgo deliberado (por ejemplo, utilizando el algoritmo de encriptación más sólido disponible/contraseña segura) y que permitan detectar de manera muy fácil un peligro real o una tentativa de peligro;

16.9.3 cuando sea transmitida, se aplique un sistema de seguridad adecuado, mediante encriptación Secure Email, PGP o WinZip 9; y

16.9.4 no se exporte sin el permiso por escrito de BT, fuera del Espacio Económico Europeo.

16.10 El Proveedor deberá proporcionar rápidamente y, en cualquier caso, en un plazo de 7 días laborables, al Contacto de seguridad de BT todos los datos de cualquier función y/o funcionalidad en cualquiera de los Suministros (o que estén planificadas en el mapa de ruta de cualquiera de los Suministros) que, cuando sea oportuno:

16.10.1 el Proveedor conozca; o

16.10.2 el Contacto de seguridad de BT crea de forma razonable que están diseñadas, o se podrían utilizar, para la interceptación legítima o cualquier otra interceptación del tráfico en las telecomunicaciones, y así lo informe al Proveedor. Dichos datos deberán incluir toda la información que sea razonablemente necesaria para permitir al Contacto de seguridad de BT entender plenamente la naturaleza, la composición y el alcance de dichas funciones y/o funcionalidad.

16.11 Para mantener el acceso a las Redes de BT y/o a los sistemas, el Proveedor notificará a BT inmediatamente cualquier cambio en su método de Acceso a través de firewalls, incluyendo la provisión de la traducción de la dirección de red.

16.12 El Proveedor no debe utilizar ninguna herramienta de monitorización de la red que pueda visualizar información de la aplicación.

16.13 El Proveedor se asegurará de que la funcionalidad IPv6 incluida en los sistemas operativos esté deshabilitada en los hosts (por ejemplo, en los dispositivos del usuario final o en los servidores) que se conectan a la Red de BT y a los dominios cuando no sea necesaria.

16.14 El Proveedor deberá cumplir y asegurar que los Suministros o Servicios cumplan las políticas de BT si se las han facilitado y los Requisitos de seguridad. Cualquier incumplimiento deberá acordarse en la firma del contrato o a través de un proceso de control de cambios (o equivalente).

16.15 El Proveedor debe garantizar que todo el Personal contratado haya pasado las debidas comprobaciones antes de la contratación adecuadas para el nivel de Acceso estipulado en

https://groupextranet.bt.com/selling2bt/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

Los Proveedores que creen, desarrollen o soporten Redes de BT o Activos de red deberán garantizar que todo el Personal contratado haya superado las comprobaciones mínimas L2 antes de la contratación. Las comprobaciones previas a la contratación L3 serán precisas para los cargos identificados por el Contacto de seguridad de BT. Si el Proveedor no tiene la capacidad para revelar directamente cuestiones de seguridad con respecto al Personal contratado como parte de las comprobaciones L3, BT le ayudará a ello y el Proveedor correrá con los costes correspondientes.

16.16 El Proveedor mantendrá el hardware y el software de acuerdo con las especificaciones del fabricante.

16.17 El Proveedor no utilizará medios extraíbles (discos, unidades USB, etc.) previstos para el soporte y mantenimiento para ningún otro fin.

17 SEGURIDAD EN LA RED DEL PROVEEDOR

El cumplimiento de las Condiciones de esta sección es obligatorio cuando se utilice la red del Proveedor para proporcionar los Suministros (aquí se incluyen la red LAN, WAN, Internet y redes inalámbricas y de radio).

17.1 El Proveedor, con relación a los Suministros o los Servicios, implementará medidas de seguridad en sus redes, con el fin de salvaguardar la confidencialidad, disponibilidad e integridad de la Información de BT. Las medidas, y el Proveedor:

17.1.1 cumplirán todos los requisitos legales y normativos; y

17.1.2 harán todo lo posible para evitar que personas no autorizadas (por ejemplo, hackers) consigan acceder a las Redes del proveedor;

17.1.3 harán todo lo posible para reducir el riesgo de uso indebido de las Redes del proveedor por las personas autorizadas a acceder a ellas, que podría provocar potencialmente la pérdida de ingresos o servicios; y

17.1.4 harán todo lo posible para detectar cualquier Infracción de seguridad relevante y garantizar la subsanación rápida de cualquier infracción, junto con la identificación de las personas que consiguieron acceder y el establecimiento de cómo lo consiguieron.

17.2 Deben existir medidas adecuadas para garantizar la seguridad de los componentes, incluyendo entre otros:

17.2.1 el uso de principios efectivos de '**defensa en profundidad**';

17.2.2 el uso de controles aplicados que eviten cualquier ataque intencionado;

17.2.3 el uso de firewalls, routers, conmutadores;

17.2.4 comunicaciones seguras entre dispositivos y estaciones de gestión;

17.2.5 comunicaciones seguras entre dispositivos según proceda, incluyendo la encriptación de todos los accesos de administrador que no sean desde la consola;

17.2.6 diseño arquitectónico sólido, dividido en niveles y por zonas, con una gestión de la identidad firme y efectiva y una configuración del sistema operativo que se debe reforzar y documentar adecuadamente;

17.2.7 la deshabilitación (cuando sea factible) de servicios, aplicaciones y puertos que no se vayan a utilizar.

17.2.8 la deshabilitación o eliminación de cuentas de visitante;

17.2.9 la instalación de los parches de seguridad más recientes en las Redes del proveedor y en sus sistemas en cuanto sea factible tras la realización de las comprobaciones. Cualquier excepción debe ser comunicada a BT, quien evaluará el riesgo que suponga. BT se reserva el derecho a obligar al Proveedor a instalar parches tras una evaluación de riesgos;

17.2.10 evitar relaciones de confianza entre servidores;

17.2.11 el uso del principio de seguridad de las mejores prácticas de **'el menor privilegio'** para realizar una función;

17.2.12 garantizar la aplicación de medidas adecuadas para gestionar el rechazo de ataques al servicio;

17.2.13 garantizar la aplicación de medidas adecuadas para la detección de intrusiones y/o protección;

17.2.14 monitorizar a todos los distribuidores aplicables y otras fuentes de información pertinentes para detectar alertas de vulnerabilidad;

17.2.15 cuando proceda, presentar una monitorización de la integridad para detectar cualquier adición, modificación o eliminación de archivos o datos críticos del sistema; y

17.2.16 cambiar todas las contraseñas por defecto y las proporcionadas por los representantes antes de que los componentes de la red se hagan públicos.

18 SEGURIDAD EN LA NUBE

El cumplimiento de las Condiciones de esta sección es obligatorio cuando el Proveedor preste Servicios en la nube a BT.

18.1 El Proveedor cumplirá:

la última versión de la Matriz de Control en la Nube de Cloud Security Alliance (CCM); los requisitos de seguridad de alojamiento externo de BT, disponibles en:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm

Los contratos de nivel de servicio de la red y las infraestructuras (internos o externalizados) deberán documentar de manera clara los controles de seguridad, la capacidad y los niveles de servicio, así como los requisitos empresariales o del cliente.

18.2 El Proveedor aplicará las medidas de seguridad acordadas en todos los componentes suministrados, con el fin de salvaguardar la confidencialidad, disponibilidad, calidad e integridad de los Suministros minimizando la oportunidad de personas no autorizadas (por ejemplo, otros clientes de servicios en la nube) de lograr acceder a Información de BT y a los Suministros de BT.

19 CENTRO DE CONTACTO

El cumplimiento de las Condiciones de esta sección es obligatorio cuando el Proveedor trabaje para un centro de contacto para BT.

19.1 El Proveedor, con relación a los Suministros, se asegurará de que los entornos en los que se almacene, procese o visualice la Información de BT cumplan la versión más actual de la Norma de terceros del Centro de contacto, disponible en:

https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm.

PARTE 5: DEFINICIONES

En estos Requisitos de seguridad, se aplicarán las siguientes definiciones pero, por lo demás, los términos del Contrato se aplicarán a estos Requisitos de seguridad y todas las palabras y expresiones empleadas en estos Requisitos de seguridad tendrán el mismo significado que el que se les otorga en el Contrato:

«**Acceso**»: el procesamiento, tratamiento o almacenamiento de Información de BT por uno o más de los siguientes métodos:

- Por interconexión con los Sistemas de BT

- Proporcionado en papel o en formato no electrónico
- Información de BT en los Sistemas del proveedor
- Por medios móviles

y/o acceso a las instalaciones de BT para la provisión de los Suministros, excluida la entrega de hardware y la asistencia a reuniones).

«**Autorizado**»: BT ha aprobado el Acceso como parte del proceso de interconexión del Sistema de BT o se ha recibido una autorización por escrito del Contacto de seguridad de BT. «**Autorización**» se interpretará en consecuencia. El nivel de acceso proporcionado será pertinente y estará limitado al necesario para proporcionar los Suministros.

«**Sistemas administrativos de BT**»: significará la plataforma de facturación de BT (en estos momentos, iSupplier) o cualquier otro sistema acordado con BT que sea meramente administrativo;

«**Cliente de BT**»: incluirá a efectos de estos Requisitos de seguridad una empresa o una persona física a quien BT proporciona bienes o servicios.

«**Información de BT**»: toda la información relacionada con BT o un Cliente de BT proporcionada al Proveedor y toda la información que procese o maneje el Proveedor en representación de BT o de un Cliente de BT en virtud del Contrato.

«**Redes de BT**»: la red controlada o administrada por BT.

«**Activos físicos de BT**»: todos los activos físicos (incluyendo, entre otros, routers, conmutadores, servidores, llaves de armarios, portátiles, identificadores, tarjetas de paso, planos o documentación) en posesión del Proveedor y que pertenezcan a BT.

«**Seguridad de BT**»: la organización de seguridad basada en BT.

«**Contacto de seguridad de BT**»: el profesional de garantía de la información dentro de Seguridad de BT o Contacto de BT comercial si se le notifica al Proveedor o a la Seguridad central 0800 321999 [+44 1908 641100] que será el único punto de contacto para cualquier cuestión relacionada con estos Requisitos de seguridad y cualquier Incidente de seguridad relevante.

«**Sistemas de BT**»: los servicios y los componentes de servicio, productos, redes, servidores, procesos, sistema en papel o sistemas informáticos (en parte o en su totalidad) propiedad y/u operados por BT o cualquier otro sistema que pueda alojarse en las Instalaciones de BT, incluyendo iSupplier (tal y como se define en la cláusula titulada «**Pago y Facturación**»).

«**Registros masivos**»: significa más de 1000 registros individuales de Información de BT clasificados como «Confidencial» o 100 registros individuales de Información de BT clasificados como 'Estrictamente confidencial'.

«**CCTV**»: circuito cerrado de televisión.

«**Personal contratado**», «**Personal contratado pertinente**»: tal y como se define en el Contrato.

«**Cyber Essentials Plus**»**:** significa el programa sustentado por el gobierno británico para ayudar a las empresas a protegerse frente a los ciberataques comunes, actualmente disponible en https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

«**Buenas prácticas de seguridad del sector**»: significa, con relación con cualquier compromiso y circunstancia, la implementación de prácticas de seguridad, políticas, normas y herramientas que se podrían esperar de forma razonable y cotidiana de una persona cualificada y experimentada que participe en el mismo tipo de actividad bajo las mismas circunstancias o similares.

«**Información**»: información, tangible o en otro formato, incluyendo, entre otros, las especificaciones, informes, datos, notas, documentación, planos, software, resultados informáticos, diseños, diagramas de circuitos, modelos, patrones, muestras, invenciones (independientemente de si se pueden patentar o no) y los conocimientos y medios (de haberlos) en los que se suministra dicha información.

«Interna», «Pública», «Confidencial» y «Estrictamente confidencial»: tienen el significado que se les otorga en la Clasificación de la información de terceros y Especificación de tratamiento.

«**ISO 27001**»: la versión actual de la norma internacional para los sistemas de gestión de la seguridad internacionales, establecida por la Organización Internacional de Estandarización y la Comisión Electrotécnica Internacional.

«**Activos de red**»: dispositivo, u otro componente de la Red de BT, que es compatible con actividades relacionadas con la red.

«**Seguridad de la red**»: la seguridad de las rutas de comunicación de interconexión y los nodos que conectan de forma lógica las tecnologías del usuario final de forma conjunta y los sistemas de gestión asociados.

«Procesar», «Procesado(s)», «Procesamiento», «Anexo de procesamiento» y **«Datos personales»**: tendrán los significados que se les otorga en la sección titulada **«Protección de Datos personales»**.

«**Incidente de seguridad relevante**»: un punto débil de seguridad observado o supuesto en los sistemas o en los servicios, y eventos de seguridad que afectan a los Suministros o a la ejecución del Contrato (incluyendo la pérdida real o supuesta, daños, robo o uso indebido de la Información de BT o los Sistemas de BT), incluyendo entre otros:

- pérdida de servicio, equipo o instalaciones;

- corrupción, daño o uso indebido de los Activos físicos de BT;
- averías o sobrecargas del sistema;
- errores humanos;
- incumplimientos de los Requisitos de seguridad descritos en este documento;
- infracciones de las disposiciones de la seguridad física;
- cambios del sistema sin controlar;
- averías del software o del hardware;
- infracciones de acceso; y
- pérdidas de datos conocidas o supuestas relacionadas con los sistemas asociados a BT y las conexiones entre BT y el Proveedor.

«**Acceso remoto**»: acceso remoto desde casa u otra ubicación a través de una red pública (por ejemplo, Internet) o el acceso remoto por parte de la red del Proveedor al Sistema de BT.
«**Requisitos de seguridad**»: significa estos requisitos de seguridad de BT debidamente actualizados de forma oportuna.
«**Suministros**»: significará cualquiera de los **«Servicios», «Suministros», «Bienes»** y **«Trabajo»** definidos en el Contrato y cualquier ejecución del Contrato.
«**Sistemas del proveedor**»: cualquier ordenador propiedad del Proveedor, aplicación o sistemas de red empleados para acceder, almacenar o procesar Información de BT o implicados en la provisión de los Suministros.
«**Contacto de seguridad del proveedor**»: aquella persona cuya información de contacto notificará el Proveedor a BT cuando sea oportuno y que será el único punto de contacto para cuestiones relacionadas con estos Requisitos de seguridad y cualquier Incidente de seguridad relevante.
«**Transferir**» o «**Transferido**»: el traslado de Información de BT en posesión del Personal contratado (incluyendo, entre otros, Datos personales) desde una ubicación o persona a otra, ya sea por medios físicos, de voz o electrónicos; y el otorgamiento de Acceso a la Información de BT en posesión del Personal contratado (incluyendo, entre otros, Datos personales) de una ubicación o persona a otra, ya sea por medios físicos, de voz o electrónicos.
«**Clasificación de la información de terceros y Especificación de tratamiento**» significa los requisitos para el tratamiento de la información del Proveedor tal y como se estipulan en https://groupextranet.bt.com/selling2bt/working/ThirdPartySecuritystandards/index.htm según se actualice puntualmente.