Contenidos

1. Introducción

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

1.2 Estos Requisitos de seguridad son adicionales y sin perjuicio de cualquier otra obligación de Terceros establecida en el Contrato.

2. Requisitos de Acceso Limitado

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

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

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

3. Seguridad de la Información General

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

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

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

3.4 Si el Tercero subcontrata obligaciones en el Contrato, deberá asegurarse de que todos los Contratos con los Subcontratistas en cuestión y los Subcontratistas de estos incluyan condiciones escritas que insten al Subcontratista a cumplir las secciones relevantes de estos Requisitos de seguridad o los requisitos equivalentes de seguridad de Terceros.

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

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

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

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

Gestión de la Información de BT

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

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

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

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

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

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

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

documentos de trabajo una vez estén en formato de papel.

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

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

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

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

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

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

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

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

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

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

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

- Solo se permite en dispositivos con encriptado de disco duro, como Bitlocker.
- Todos los documentos deben encriptarse individualmente.
- Debe aplicarse la Gestión de Derechos de la Información (IRM) al documento.
- Si se incluye, la información debe conservar la etiqueta de clasificación de BT.

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

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

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

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

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

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

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

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

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

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

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

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

Funciones y responsabilidades

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

Gobernanza

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

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

3.26 El Tercero debe garantizar que se definan e implementen funciones y responsabilidades apropiadas para la información y ciberseguridad que incluyan:

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

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

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

Gestión de incidentes

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

- Garantizar que el personal conozca sus funciones y el orden de las operaciones cuando se necesite una respuesta.
- Garantizar que los incidentes se comuniquen de acuerdo con los criterios establecidos.
- Garantizar que el impacto del incidente se comprenda.
- Garantizar que se ejecuten los procedimientos forenses cuando sean precisos internamente o a través de una función especializada.
- Garantizar que se integren las lecciones aprendidas de los incidentes en los casos de buenas prácticas.
- Garantizar que la información relacionada con un incidente que afecte a BT sea tratada como «Confidencial».

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

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

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

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

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

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

Gestión del cambio

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

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

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

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

Gestión de amenazas y ciberseguridad

3.39 El Tercero debe garantizar que exista un marco para la evaluación de las amenazas y los riesgos de Ciberseguridad implementado para que el perfil de riesgo de Ciberseguridad de las operaciones, los activos, las instalaciones y los miembros de la organización sea comprendido y gestionado mediante:

- La evaluación de las vulnerabilidades de los activos.
- La identificación de las amenazas tanto internas como externas.
- La sensibilidad de la información/datos en cuestión.
- La evaluación de los posibles impactos empresariales.

- Se utilizan las amenazas, vulnerabilidades, probabilidades e impactos para determinar el riesgo.
- Garantizar que el marco de gestión de amenazas y Ciberseguridad se acuerda a un nivel adecuado en la organización.

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

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

Gestión de identidades y control de acceso

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

- La concesión, reactivación, modificación y desactivación de los derechos de acceso basándose únicamente en aprobaciones documentadas y autorizadas.
- Garantizar que las cuentas durmientes estén deshabilitadas.
- Deshabilitar las cuentas del personal que ya no esté empleado en la empresa.
- Implementar procesos y herramientas para seguir, controlar, prevenir, corregir el uso, asignación y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.
- Se realizan revisiones de acceso periódicas para garantizar que ese acceso sea adecuado a su objetivo.
- Se exige que las cuentas de usuario se recertifiquen al menos anualmente y que las cuentas privilegiadas lo hagan trimestralmente.
- Garantizar que los secretos y credenciales permanentes (por ejemplo, el acceso mediante cuentas de acceso de emergencia de tipo “break-glass”) estén protegidos dentro de un almacenamiento protegido mediante hardware y que solo estén a disposición de la(s) persona(s) responsable(s) en caso de emergencia.

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

- La autenticación de doble factor debe lograrse con una ID de usuario, una contraseña y uno de los siguientes métodos:
- Generador de contraseñas de un solo uso: requiere un PIN/contraseña específica del usuario para visualizar la contraseña de un solo uso.

- Una tarjeta inteligente con un chip según la norma ISO 7816, y con el correspondiente lector y software de lectura de tarjetas. Las tarjetas inteligentes sin contacto no están permitidas.
- Autenticación basada en certificados emitidos de acuerdo con la política de certificados de Infosec).

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

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

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

3.46 El Tercero debe garantizar que toda la autenticación se gestione de forma acorde al riesgo de la transacción, es decir, la contraseña con la adecuada complejidad y longitud, frecuencia en el cambio de contraseñas, autenticación multifactorial, gestión segura de las credenciales de la contraseña, entre otros controles. El acceso privilegiado se realizará mediante cuentas protegidas con autenticación multifactorial. Las cuentas de acceso de emergencia de tipo “break-glass” contar con credenciales seguras exclusivas para cada punto de acceso de equipo de la red.

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

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

Protección y clasificación de los datos

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

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

Prevención de la fuga de datos

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

- E-mail, internet / pasarela web (incluyendo el almacenamiento en línea y correo web), USB, óptico y otros tipos de puertos / almacenamiento portátil, etc.,

informática móvil y BYOD, servicios de acceso remoto, mecanismos para compartir archivos y redes sociales.

- Los dispositivos no autorizados no deben conectarse a la red (ya sea a la red corporativa del vendedor o a los sistemas/red de BT) ni emplearse para acceder a información no pública.

PCI DSS

3.51 El Tercero debe garantizar que, si está involucrado con la gestión de datos relacionados a las tarjetas de pago, cumplirá como corresponda con lo indicado en los estándares PCI-DSS. Asimismo, el Tercero deberá registrar las actividades de tarjetas de pago con el Equipo de Gobernanza y Garantía de PCI, por e-mail a Group PCI Compliance group.pci.compliance@bt.com.

Gestión de vulnerabilidades.

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

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

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

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

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

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

Registro y monitorización continua de la seguridad.

3.55 El Tercero debe garantizar que exista un marco de gestión de registros y auditoría consolidado y uniforme que garantice que los sistemas clave que incluyan aplicaciones se configuran para registrar eventos clave (incluyendo los accesos privilegiados y la actividad del personal), y dichos registros deberán conservarse durante un período mínimo de 13 meses. Los registros para el equipo de red con Funciones críticas de seguridad deben registrarse por completo y estar disponibles para ser auditados durante 13 meses. Como mínimo, el Tercero debe garantizar que los registros (si procede) contengan los siguientes elementos:

- Una auditoría establecida y consistente, además del punto de inicio y fin del proceso registrado.
- Cambios en el tipo de eventos registrados tal y como exija el rastreo de auditoría (por ej., los parámetros de arranque y cualquier cambio en los mismos).
- Arranque y apagado del sistema.
- Registros satisfactorios.
- Intentos de registro fallidos (por ej., ID o contraseña de usuario incorrecta).
- Creación, modificación y borrado en/de cuentas de usuario.
- El activo al que se está accediendo (por ejemplo, datos).
- Dónde se accedió al activo (por ejemplo, dirección IP).
- Cuándo (por ejemplo, indicación de fecha y hora).

3.56 El marco de gestión de registros y auditoría debe incluir los siguientes componentes:

- Los registros de eventos clave se revisarán mediante una función independiente al menos una vez al mes para detectar posibles actividades no autorizadas, y objetivos y métodos de ataque.
- Las excepciones se consignarán e investigarán hasta su resolución.
- Se recopilarán y correlacionarán registros de diferentes fuentes y sensores, y se almacenarán de forma segura y a prueba de manipulación para permitir la reconstrucción de dichos eventos.
- El impacto de los eventos se determina mediante unos umbrales de alerta de incidentes establecidos y se actúa puntualmente según la gravedad de la alarma.

4. Seguridad del Personal del Tercero

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

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

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

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

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

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

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

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

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

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

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

5. Revisión de auditoría y seguridad

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

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

5.2 El Tercero trabajará con BT para implementar las recomendaciones acordadas y llevar adelante cualquier acción correctiva que se considere necesaria y que derive de una

revisión de seguridad basada en documentos o una auditoría in situ dentro de los 30 días posteriores a la notificación por parte de BT o el período que se haya acordado entre las partes.

5.3 Si BT necesitara realizar una auditoría independiente del Tercero y se descubriera que este está incumpliendo los principios y prácticas establecidos en la norma ISO/IEC 27001, el Tercero deberá, asumiendo el coste, realizar las acciones necesarias para alcanzar el nivel necesario de cumplimiento y reembolsar todos los gastos en que incurra BT por la obtención de dicha auditoría.

6. Derecho de Inspección

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

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

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

7. Certificaciones de seguridad

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

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

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

8. Seguridad física - Instalaciones de BT

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

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

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

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

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

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

9. Seguridad física - Instalaciones de Terceros

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

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

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

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

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

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

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

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

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

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

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

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

10.2 BT proporcionará al Tercero:

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

11. Desarrollo de software seguro

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

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

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

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

12. Custodia

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

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

13. Acceso a los Sistemas de BT

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

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

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

Conectividad entre Sistemas

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

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

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

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

14. Sistemas de Terceros que alojan Información de BT

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

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

14.2 El Tercero debe garantizar que, al menos una vez al año, se encargará de realizar una prueba de penetración/evaluación de la seguridad informática de carácter independiente sobre su infraestructura y las aplicaciones informáticas empleadas para prestar servicios que incluya sitios de Recuperación ante desastres para identificar vulnerabilidades que podrían aprovecharse para filtrar datos/servicios y prevenir cualquier infracción de seguridad a través de ciberataques. El Tercero debe permitir a BT, previa solicitud razonable, acceder a los informes de las pruebas de penetración correspondientes a los servicios que se estén prestando.

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

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

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

Gestión de activos

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

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

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

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

Criptografía

14.9 El Tercero deberá asegurarse de que la información de BT clasificada como Confidencial o con mayor grado de confidencialidad está adecuadamente encriptada (en tránsito y en reposo), y que el cifrado se realiza íntegramente con algoritmos criptográficos y cifrados modernos y seguros que utilicen mecanismos robustos de protección de la integridad y que cumplan los estándares de la industria para la negociación segura de

protocolos y claves y la gestión de claves. Las siguientes opciones TLS no están permitidas para datos en tránsito: TLS v1.0, TLS v1.1 y SSL (en cualquier versión). Las siguientes opciones de IPSec no están permitidas: IKE versión 1.

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

- Las claves simétricas (como AES) deben tener una longitud de al menos 256 bits.
- Las claves asimétricas (como RSA) deben tener una longitud de al menos 2048 bits.
- Las claves de curva elíptica deben tener una longitud de al menos 224 bits.

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

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

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

Configuración de sistemas

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

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

Protección contra malware

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

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

Mitigación de las denegaciones de servicio

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

15. Terceros que alojan Información de BT

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

16. Seguridad de la red – Red propia de BT

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

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

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

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

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

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

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

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

- conozca el Tercero; o
- BT crea de forma razonable y, por tanto, informe al Tercero de que están diseñadas para, o podrían usarse para, la interceptación legal o cualquier otra interceptación del tráfico de telecomunicaciones. En esos detalles se deberá incluir toda la información que sea razonablemente necesaria para que BT conozca en profundidad la naturaleza, la composición y la envergadura de tales funciones y/o funcionalidades.

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

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

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

Ley de (Seguridad en las) Telecomunicaciones 2021 (TSA)

Cuando el servicio del Tercero esté en el ámbito de la Ley de (Seguridad en las) Telecomunicaciones 2021 (TSA), se aplicarán los controles de seguridad siguientes

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

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

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

16.12 Al proporcionar un equipo de red, los Terceros deben facilitar a BT una «declaración de seguridad» que detalle la producción del equipo seguro y el modo en que se garantiza la seguridad del equipo durante toda la vida útil del mismo. Esta declaración de seguridad cubrirá los requisitos de la Evaluación de Seguridad del Proveedor publicada en el Anexo B del Código de Conducta de Seguridad para Telecomunicaciones.

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

- El Tercero garantiza que se atendrá a un estándar no inferior al especificado en la «declaración de seguridad» publicada.
- El Tercero proporcionará una guía actualizada que describa la implementación segura del equipo.
- El Tercero ofrecerá soporte para todo el equipo y todos los subcomponentes de software y hardware durante toda la duración del contrato.

- El Tercero facilitará información sobre todos los principales componentes y dependencias de Terceros, incluyendo, pero sin limitarse al producto y a la versión, a los componentes de código abierto, al nivel de soporte y al periodo.
- El Tercero solucionará cualquier problema de seguridad descubierto en sus productos que suponga un riesgo de seguridad para un servicio o red de un proveedor dentro de un plazo razonable a partir de la notificación del mismo, y mientras tanto ofrecerá actualizaciones periódicas sobre el progreso. El plazo anteriormente mencionado se negociará entre BT y el Tercero de modo razonable por ambas partes. Esto incluirá todos los productos afectados por la vulnerabilidad, y no solo el producto por el que se reportó la vulnerabilidad.

16.14 Si el Tercero ha obtenido certificaciones o evaluaciones de seguridad reconocidas internacionalmente para el equipo (por ejemplo, Common Criteria o NESAS), las mismas deberán hacerse públicas con todas las conclusiones que validan dicha evaluación o certificación.

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

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

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

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

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

17. Seguridad de redes de Terceros

17.1 El Tercero debe asegurarse de que se establezca y se mantenga la integridad de la red garantizando el adecuado control de los siguientes componentes:

- Las conexiones externas con la red documentadas, dirigidas a través de un cortafuegos y verificadas y aprobadas antes de que se establezcan las conexiones para impedir violaciones de la seguridad de los datos.
- La red está debidamente diseñada usando principios de «defensa en profundidad» para garantizar que las infracciones de ciberseguridad se minimicen garantizando la existencia de controles apropiados que eviten cualquier ataque intencionado como la «segmentación de redes».
- El diseño e implementación de la red se revisa al menos anualmente.
- Todo el acceso inalámbrico a las redes estará supeditado a protocolos de autorización, autenticación, segmentación y encriptación para evitar violaciones de seguridad.
- Uso de comunicaciones seguras entre dispositivos y estaciones de gestión.

- Uso de comunicaciones seguras entre dispositivos; incluyendo la encriptación de todos los accesos de administrador sin consola.
- Uso de un diseño sólido de arquitectura, dividido en capas y zonas y equipada con un sistema eficaz de gestión de identidades y configuración del sistema operativo que debe estar adecuadamente protegido y documentado
- Mediante la desactivación (cuando se pueda) de servicios, aplicaciones y puertos que no se usen.
- Mediante la desactivación o eliminación de cuentas de invitados.
- No autorizando relaciones de confianza entre servidores.
- Uso del principio de seguridad de buenas prácticas de «privilegio mínimo» para realizar una función.
- Garantizando la implementación de medidas apropiadas para la detección de intrusión y/o protección.
- Donde proceda, monitorización de la integridad de los archivos para detectar cualquier adición, modificación o eliminación de datos o archivos de sistema críticos.
- Cambiar todas las contraseñas por defecto y suministradas por los proveedores antes de que los componentes de red operen.

17.2 Cuando el Tercero esté prestando servicios sujetos a la Ley de (Seguridad en las) Telecomunicaciones 2021, se aplicarán los controles adicionales de seguridad siguientes:

- Los sistemas orientados al exterior, excluyendo el Equipo en las Instalaciones del Cliente (CPE), se someten a pruebas de seguridad cada dos años o cuando se produzca un cambio significativo.
- Los conjuntos de datos sensibles y las funciones sensibles o críticas no se alojan en equipos situados en el Borde expuesto de la red.
- Si no está protegido criptográficamente, deberá implementarse una separación física y lógica entre el Borde expuesto y las funciones sensibles o críticas.
- Deberá implementarse una separación de seguridad mediante funciones de cumplimiento de seguridad entre el Borde expuesto y las funciones sensibles o esenciales.

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

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

18. Seguridad de la =Nube

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

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

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

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

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

19. Servicios de telefonía móvil

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

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

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

20.1 Cuando el Proveedor necesite acceder, almacenar, tratar o transmitir información clasificada como OFICIAL del Gobierno de Reino Unido (HMG) superior, el Proveedor realizará una Evaluación de Riesgos de Seguridad del Personal en todos los puestos identificados en la Declaración Oficial de Sensibilidad párrafo 2, de conformidad con los requisitos estipulados en el documento «CPNI National Security Clearance - A guide» (4ª Edición - Junio de 2013 o posterior).

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

20.3 El Tercero deberá garantizar que los sistemas y la infraestructura utilizados para prestar el Servicio estén contenidos en una red lógica específica. Esta red solo debe constar de los sistemas dedicados a la prestación de un servicio seguro de tratamiento de datos del cliente.

21. Términos definidos e interpretación

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

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

a. por interconexión con los Sistemas de BT;

b. en papel o formato no electrónico;

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

d. por medios móviles

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

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

«Parte interesada de BT» significa el representante de BT que tenga la propiedad del ámbito del trabajo en cuestión

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

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

«BYOD» significa «traiga su propio dispositivo».

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

«Equipo en las instalaciones del cliente» significa equipo suministrado al cliente y

gestionado por el proveedor que se use, o se pretenda usar, como parte de la red o servicio. Esto excluye los dispositivos electrónicos de consumo como teléfonos móviles y tabletas, pero incluye dispositivos como cortafuegos en el borde, equipo SD-WAN o kit de acceso inalámbrico fijos.

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

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

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

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

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

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

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

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

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

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

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

Anexo 1.

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

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

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

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

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

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

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

«Tercero» significa un Proveedor de BT.

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

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

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

Interpretación

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

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

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

Versión	Descripción	Autor	Fecha
4.0	Nuevo	Karen Tanner	02/02/2020
4.1	Cláusula adicional para el conjunto de cláusulas 20 del HMG	Karen Tanner	20/02/2020
5.1	Ley de (Seguridad en las) Telecomunicaciones 2021 (TSA) Legislación y adopción de CIS por parte de BT	Jemma Turner	25/10/2022

ANEXO 1 – Requisitos de Seguridad Adicionales

Si el Tercero debe Acceder, almacenar, tratar o transmitir información «Oficial Sensible del HMG», deberá cumplir los presentes Requisitos de Seguridad junto con los requisitos que se recogen en este Anexo 1 y proporcionar a BT la Declaración de información Oficial Sensible cumplimentada antes de firmar el Contrato. En todos los casos, el control del máximo nivel sustituirá a los requisitos documentados en otros puntos de estos Requisitos de seguridad para Servicios y sistemas incluidos en la Declaración de información oficial sensible.

1. EMPLEADOS

1.1. Todos los puestos identificados por el Tercero como el de Acceso a información clasificada de «Oficial Sensible» o con privilegios elevados a infraestructuras que almacenen, traten o transmitan información clasificada como «Oficial Sensible» deberán documentarse en la Declaración de información Oficial Sensible.

1.2. El Personal del Tercero empleado en puestos identificados en la Declaración de información Oficial Sensible:

1.2.1. como mínimo deberá someterse al cribado preempleo de acuerdo con el Estándar de Seguridad Básico para el Personal (BPSS);

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

1.2.3. si no puede obtener las autorizaciones de seguridad necesarias, se le debe impedir el acceso a la información o a los sistemas.

2. FORMACIÓN EN SEGURIDAD

2.1. El Tercero exigirá una formación en seguridad después de la contratación y al menos anualmente, que incluya los requisitos de gestión para la información clasificada como «Oficial» u «Oficial Sensible» de acuerdo con los requisitos del Programa de clasificación de seguridad del Gobierno de Reino Unido tal y como se detalla en la Guía de BT para la protección de la información del HMG para Terceros

2.2. El Tercero actualizará las descripciones laborales de los puestos de trabajo documentados en la Declaración de información oficial sensible para exigir la participación en la formación indicada en el apartado 2.1 anterior. El Tercero mantendrá un registro de la formación que deberá poner a disposición de BT previa solicitud.

3. CONTROL DE ACCESO

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

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

3.3. Si los empleados del Tercero, incluyendo Contratistas, empleados temporales y trabajadores de agencia, tienen tarjetas de Acceso permanente a las instalaciones de BT, el Tercero deberá enviar una notificación escrita a BT en el plazo de 1 Día

Laborable desde el momento en que ya no tengan que Acceder a las instalaciones de BT (por ej., si un empleado deja la empresa o cambia de puesto).

4. VALORACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS

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

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

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

6. AUDITORÍA, PRUEBAS Y MONITORIZACIÓN

6.1. El Tercero implementará monitorización de seguridad 24/7 cuando BT así lo especifique.

6.2. La infraestructura del Tercero sometida a una monitorización de seguridad de 24 horas al día, 7 días a la semana se documentará en la Declaración de información Oficial Sensible.

7. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES

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

8. LOCALIZACIÓN

8.1. Salvo que BT especifique otra cosa, el Servicio deberá estar físicamente localizado dentro de las fronteras físicas del Reino Unido o, si fuera aplicable, del Espacio Económico Europeo (EEE).

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

1. Sistemas/Servicios en cuestión

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

Sistema	Servicio

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

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

3. Gestión de Vulnerabilidades

Sistema	Tipo de Evaluación de vulnerabilidad	Frecuencia

4. Auditoría, Pruebas y Monitorización

Sistemas a monitorizar 24/7 según indicaciones de BT

23. ANEXO 2, Ley de (Seguridad en las) Telecomunicaciones 2021 (TSA) - Código de Conducta para la conversión de Requisitos de Seguridad

Código de Conducta Ref.	Cláusula de seguridad de BT Ref.
M21.04 Cuando se almacenen datos en el extranjero, el proveedor deberá mantener una lista de las ubicaciones en las que se mantienen los datos. El riesgo derivado del mantenimiento de los datos en estas ubicaciones, incluyendo cualquier riesgo asociado con las leyes locales de protección de datos, se gestionará como parte de los procesos de gestión de riesgos del proveedor.	3.8
M10.46 Los proveedores se asegurarán de que sus contratos permitan compartir información sobre cuestiones de seguridad según sea necesario para ayudar a la identificación y a la reducción de riesgos donde la seguridad se vea comprometida en relación con la red pública de comunicaciones electrónicas o el servicio público de comunicaciones electrónicas, como resultado de acciones u omisiones por parte de Terceros proveedores.	3.31
M10.13 Los proveedores deberán exigir contractualmente a los proveedores de Terceros la localización y la comunicación de la causa de origen de cualquier incidente de seguridad que pudiera comprometer la seguridad en el Reino Unido en un plazo de 30 días, y además deberán rectificar cualquier debilidad descubierta.	3.33
M5.05 Además de los requisitos de CAF D.2, los proveedores deberán realizar un análisis de la causa de origen de todos los incidentes de seguridad. Los resultados de este análisis deberán ser comunicados a un nivel adecuado, que puede incluir la junta del proveedor.	3.34
M11.02 Garantizar que los secretos y credenciales permanentes (por ejemplo, relacionados con el acceso de emergencia o “break-glass”) estén protegidos y que no estén a disposición de nadie más que la(s) persona(s) responsable(s) en caso de emergencia.	3.42
M6.02 El acceso privilegiado se realizará mediante cuentas con ID de usuario y credenciales de autenticación únicas para cada usuario que no deberán compartirse.	3.45
M6.04 Las cuentas de usuario privilegiadas de acceso de emergencia o “break-glass” deben contar con credenciales seguras únicas para cada equipo de la red.	3.46
M10.24 Los proveedores deberán exigir contractualmente que los administradores de Terceros implementen controles técnicos para evitar que un proveedor o su red puedan afectar negativamente a cualquier otro proveedor o red.	16.10
M10.25 Los proveedores deberán exigir contractualmente que los administradores de Terceros implementen una separación lógica dentro de la red del administrador de Terceros para separar los datos y las redes de clientes.	16.11
M10.26 Los proveedores deberán exigir contractualmente que los administradores de Terceros implementen una separación lógica entre los entornos de gestión del administrador de Terceros utilizados para las redes de distintos proveedores.	16.11
M10.27 Los proveedores deberán exigir contractualmente que los administradores de Terceros implementen y hagan cumplir funciones de cumplimiento de seguridad en el límite entre la red del administrador de Terceros y la red del proveedor.	16.11

M10.28 Los proveedores deberán exigir contractualmente que los administradores de Terceros implementen controles técnicos para limitar el potencial de que usuarios o sistemas tengan un impacto negativo en más de un proveedor.	16.11
M10.29 Los proveedores deberán exigir contractualmente que los administradores de Terceros implementen estaciones de trabajo con acceso privilegiado lógicamente independientes para cada proveedor.	16.11
M10.30 Los proveedores deberán exigir contractualmente que los administradores de Terceros implementen cuentas y dominios administrativos independientes para cada proveedor.	16.11
M10.36 Los proveedores deberán exigir contractualmente que los proveedores de equipos de red compartan con ellos una «declaración de seguridad» que detalle la producción del equipo seguro y el modo en que se garantiza la seguridad del equipo durante toda la vida útil del mismo. Se recomienda que cualquier declaración de este tipo cubra todos los aspectos descritos en la Evaluación de Seguridad del Proveedor (VSA) (véase Anexo B), y los proveedores deben animar a sus proveedores a publicar una respuesta a la VSA.	16.12
M10.38 Los proveedores deberán garantizar, mediante disposiciones contractuales, que se firme la declaración de seguridad del proveedor de equipos de red a un nivel de gobernanza adecuado.	16.12
M10.40 Los proveedores deberán exigir contractualmente al proveedor de equipos de red que se atenga a un estándar no inferior al especificado en la «declaración de seguridad» del proveedor de equipos de red.	16.13
M10.41 Los proveedores deberán exigir contractualmente a los proveedores de equipos de red que proporcionen una guía actualizada que describa la implementación segura del equipo.	16.13
M10.42 Los proveedores deberán exigir contractualmente a los proveedores de equipos de red que ofrezcan soporte para todo el equipo y todos los subcomponentes de software y hardware durante toda la duración del contrato. El periodo de soporte tanto del hardware como del software deberá constar por escrito en el contrato.	16.13
M10.43 Los proveedores deberán exigir contractualmente a los proveedores de equipos de red que proporcionen información (producto y versión) sobre los principales componentes y dependencias de Terceros, incluyendo los componentes de código abierto, y el periodo y nivel de soporte.	16.13
M10.44 Cuando sea relevante para el uso particular de equipos de un proveedor, los proveedores deberán exigir a los proveedores de Terceros que solucionen cualquier incidencia de seguridad descubierta en sus productos que suponga un riesgo de seguridad para un servicio o la red de un proveedor dentro de un plazo razonable desde la notificación del mismo, y mientras ofrecerá actualizaciones periódicas sobre el progreso. Esto incluirá todos los productos afectados por la vulnerabilidad, y no solo el producto por el que se reportó la vulnerabilidad.	16.13
M10.39 Cuando el proveedor de equipos de red declare haber obtenido cualquier certificación o evaluación de seguridad reconocida internacionalmente para su equipo (por ejemplo, Common Criteria o NESAS), los proveedores deberán exigir contractualmente a los proveedores de equipos que compartan con ellos la totalidad de las conclusiones que demuestran dicha evaluación o certificación.	16.14
M10.35 Los proveedores exigirán que las redes del administrador de Terceros que pudieran afectar al proveedor sean sometidas al mismo nivel de pruebas aplicado por el propio proveedor (por ejemplo, pruebas TBEST, según estipule Ofcom periódicamente al proveedor).	16.15

M10.46 Los proveedores se asegurarán de que sus contratos permitan compartir información sobre cuestiones de seguridad según sea necesario para ayudar a la identificación y a la reducción de riesgos donde la seguridad se vea comprometida en relación con la red pública de comunicaciones electrónicas o el servicio público de comunicaciones electrónicas, como resultado de acciones u omisiones por parte de Terceros proveedores.	16.16
M21.02 Las medidas tomadas por el proveedor en virtud del Reglamento 3(3)(f) deberían incluir normalmente la garantía, siempre que sea factible, de que el equipo que realiza las Funciones de Supervisión de Red del proveedor esté ubicado en el Reino Unido y el personal que intervenga esté localizado en el Reino Unido.	16.18
M21.02 Las medidas tomadas por el proveedor en virtud del Reglamento 3(3)(f) deberían incluir normalmente la garantía, siempre que sea factible, de que el equipo que realiza las Funciones de Supervisión de Red del proveedor esté ubicado en el Reino Unido y el personal que intervenga esté localizado en el Reino Unido. M16.07 Los sistemas que recopilen y traten los registros y los datos de monitorización deberán ser tratados como Funciones de Supervisión de Red.	16.18 y 16.19
M1.02 Deberían realizarse pruebas de seguridad en los sistemas que tengan contacto con el exterior, excluyendo el CPE, al menos cada dos años, o en cualquier caso poco después de producirse cualquier cambio significativo.	17.2
M1.03 El equipo en el borde expuesto no deberá alojar datos sensibles ni Funciones Críticas de Seguridad.	17.2
M1.04 Deberá implementarse una separación física y lógica entre el borde expuesto y las Funciones Críticas de Seguridad. (Téngase en cuenta que este requisito puede no ser necesario una vez pueda protegerse criptográficamente los conjuntos de datos y las funciones que puedan verse comprometidos)	17.2
M1.05 Deberán existir límites de seguridad entre el borde expuesto y las funciones críticas o sensibles que implementen medidas de protección.	17.2
M8.12 En el caso de las tarjetas SIM de perfil fijo, el proveedor deberá garantizar que los datos SIM sensibles estén protegidos adecuadamente durante todo su ciclo de vida, tanto por parte del distribuidor de la tarjeta SIM como dentro de la red del operador, dado el riesgo para la resiliencia y la confidencialidad de la red si se perdiese esta información.	19.1
M8.13 En el caso de las tarjetas SIM de perfil fijo, la integridad, la confidencialidad y la disponibilidad de los datos sensibles de la tarjeta SIM compartidos con el distribuidor de la tarjeta SIM deberán estar protegidas en cada paso de su ciclo de vida.	19.1