Contenido

1. Introducción

1.1 Este documento establece los requisitos de seguridad de BT y es aplicable a todos aquellos terceros que trabajan para o en nombre del Grupo BT, incluidos Openreach, EE y PlusNet, a los que se referirá en adelante en el resto del documento como "BT".

1.2 Estos requisitos de seguridad son adicionales y sin perjuicio de cualquier otra obligación del tercero establecida en el Contrato.

1.3 Todos los estándares referidos en este documento se pueden encontrar en la siguiente ubicación. Estándares para terceros

2. Requisitos de acceso limitado

2.1 Sin perjuicio de las obligaciones de confidencialidad que pueda tener, si el personal del tercero tiene acceso a información de BT, dicho tercero deberá:

2.2 Asegurar que el personal de terceros no revele ni acceda a la información de BT salvo que sea preciso para la prestación del servicio; y

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

3. Seguridad de la información general

3.1 Previa solicitud razonable de BT, el tercero deberá poner a disposición de BT copias de las certificaciones de seguridad y una declaración de cumplimiento relevante para el Servicio, que demuestre el cumplimiento de estos Requisitos de seguridad.

3.2 Si se produjeran cambios significativos bien tecnológicos o industriales, en los Servicios o en la forma en que se prestan, BT podrá realizar una modificación del Contrato durante el período de vigencia del mismo, si fuera preciso realizar un cambio en los Requisitos de seguridad aplicables. El tercero deberá cumplir la modificación del contrato acordada en un plazo razonable, teniendo en cuenta la naturaleza del cambio y el riesgo para BT.

3.3 El tercero deberá revisar estos Requisitos de seguridad y los estándares asociados como mínimo anualmente o 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 virtud del 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 partes relevantes de estos requisitos de seguridad o de requisitos de seguridad de terceros equivalentes.

3.5 La información de BT podrá conservarse durante el tiempo que sea necesario para ejecutar 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 los límites de las leyes pertinentes.

3.6 Si los Servicios son un soporte directo de un contrato con el Gobierno del Reino Unido, el tercero debe cumplir con la versión más actual de Cyber Essentials Plus.

3.7 El tercero deberá garantizar que la información de BT se gestiona de acuerdo con los controles incluidos en los siguientes estándares:

Norma de Clasificación de la Información y Gestión de Datos de Terceros V4.0

- Nuestra norma sobre controles de terceros V1.1 - Secciones

Sección 1 Funciones y responsabilidades.

Sección 2 Gobernanza.

Sección 3 Gestión de Incidentes.

Sección 4 Gestión de cambios.

Sección 5 Gestión de Amenazas y Ciberseguridad

Sección 6 Gestión de Identidades y Control de Acceso.

Sección 10 Clasificación y protección de los datos.

Sección 12 Prevención de la fuga de datos.

Sección 13 PCI-DSS (si está en el ámbito del Servicio).

Sección 19 Gestión de vulnerabilidades.

Sección 22 Registro y monitorización continua de la seguridad.

4. Seguridad del personal del tercero

4.1 El tercero deberá garantizar que todo el personal del tercero haya firmado acuerdos de confidencialidad antes de comenzar a trabajar en los edificios de BT o en los sistemas de BT o tenga acceso a la información de BT. El tercero deberá conservar los acuerdos de confidencialidad y poner las pruebas a su disposición para auditorías.

4.2 El tercero se ocupará de los incumplimientos de los controles y estándares de seguridad de los terceros y de BT aplicables, a través de procesos formales que incluyen medidas disciplinarias que pueden incluir la expulsión del individuo:

4.2.1 tener acceso a los sistemas de BT o a la información de BT; o

4.2.2 realizar trabajos relacionados con la prestación del Servicio.

Además, el tercero procurará que se hayan implementado los procesos pertinentes para garantizar que todo el personal del tercero que haya sido retirado no tenga posteriormente acceso a los sistemas de información de BT y que no se le permita trabajar en relación con la prestación del servicio.

4.3 El tercero deberá, en la medida en que lo permita la ley, contar con un mecanismo de confidencialidad 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. Informes relevantes que deben notificarse a BT.

- **A criterio de BT, cuando el personal del tercero ya no esté asignado al servicio, los activos físicos o la información de BT en su poder deberán: devolverse al equipo operativo de BT pertinente;
- destruirse de acuerdo con el Estándar de Clasificación de la información y gestión de datos de Terceros V4.0

4.4 El tercero deberá garantizar que se han implementado los procesos apropiados en relación con el personal del tercero para cumplir los controles de las siguientes normas:

- Nuestro estándar de controles de terceros V1.1 - Secciones

  Sección 15 Redes Sociales

  Sección 23 Formación y sensibilización

5. Auditoría y revisión de la 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 estos requisitos de seguridad y los estándares asociados, que 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 prevé un preaviso de 30 días laborables al tercero para realizar una auditoría in situ rutinaria.

El alcance de la auditoría consistirá en revisar todos los aspectos de las políticas, procesos y sistemas del tercero (siempre que el tercero proteja la confidencialidad de cualquier información no relacionada con la prestación del servicio a BT), que sean relevantes para el servicio prestado.

5.2 El tercero colaborará 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 en un plazo de 30 días a partir de la notificación 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 está incumpliendo los principios y las prácticas de la norma ISO/IEC 27001:2013, 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 realización de dicha auditoría.

6. Derecho de inspección

6.1 El tercero debe conceder a BT el derecho de inspección de acuerdo con:

- Nuestro Estándar de Controles de Terceros V1.1 –

  Sección 24 Derecho de inspección

7. Certificaciones de seguridad

7.1 Los sistemas de terceros, el servicio, los servicios asociados, los procesos y las ubicaciones físicas deben cumplir y seguir cumpliendo de manera continuada la norma ISO/IEC 27001:2013 (o certificaciones que demuestren controles equivalentes, sustentados con el informe de un auditor independiente) y con cualquier versión modificada o futura de la norma que se emita. Este cumplimiento debe garantizarse mediante:

7.1.1 La certificación del ISMS del tercero por una parte de UKAS o un organismo certificador internacional equivalente aprobado cuyo alcance y declaración de aplicabilidad hayan sido validados por BT; o

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

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

7.3 Si el alcance del certificado o la declaración de aplicabilidad variaran con el tiempo, el tercero debe enviar dichos cambios para su revalidación empleando el procedimiento de control de cambios (o, a falta de este, el proceso de modificación). El tercero deberá informar a BT en un plazo de 2 días laborables de cualquier incumplimiento importante identificado por el organismo de certificación o el tercero.

8. Seguridad física - Instalaciones de BT

8.1 Si el tercero está trabajando en las instalaciones de BT, se aplicará el control estándar siguiente:

- Nuestro estándar sobre controles de terceros V1.1

Sección 25. Seguridad física - Instalaciones de BT

9. Seguridad física - Instalaciones de terceros

9.1 Si se usan instalaciones de terceros para prestar el Servicio, se aplicará el siguiente control estándar.

- Nuestro estándar de controles de terceros V1.1

Sección 9. Seguridad física en locales de terceros, **excluyendo** los controles 9.10 y 9.11 para la provisión del entorno de alojamiento para los equipos de BT.

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

10.1 Si se usan instalaciones de terceros para suministrar un entorno de alojamiento de equipos, se aplicará el siguiente control estándar.

- Nuestro estándar sobre controles de terceros V1.1

Sección 9. Seguridad física en las instalaciones de terceros - controles 9.10 y 9.11 para la provisión del entorno de alojamiento para los equipos de BT.

11. Desarrollo del software seguro

11.1 Si el tercero suministra software o sistemas, se aplicará el siguiente control estándar.

- Nuestro estándar sobre controles de terceros V1.1

Sección 17. (17.1 y 17.2) Desarrollo de software seguro

12.ESCROW

12.1 Si se precisa un ESCROW para proteger a todas las partes, se aplicarán los controles del siguiente estándar:

- Nuestro estándar de controles de terceros V1.1

Sección 17. (sólo 17.3) Desarrollo de software seguro

13.Acceso a los sistemas de BT

13.1 Si los sistemas o el personal del tercero precisan acceder/ conectarse a los sistemas de BT, se aplicarán los controles del siguiente estándar:

- Nuestro estándar sobre controles de terceros V1.1

Sección 8. Acceso a los sistemas de BT

14.Sistemas de terceros que contienen información de BT

14.1 Si se usan sistemas de terceros para alojar información de BT, se aplicarán los controles del siguiente estándar:

Estándar de clasificación y tratamiento de datos de terceros V4.0

- Nuestro estándar sobre controles de terceros V1.1 – Secciones

Sección 7. Gestión de activos de información.

Sección 11. Criptografía.

Sección 16. Configuración del sistema.

Sección 18. Protección anti-malware.

Sección 21. Mitigación de las Denegaciones de Servicio.

15. Terceros que alojan información de BT

15.1 Si el tercero aloja información de BT, las instalaciones deben contar con una certificación ISO/IEC 27001 válida para la gestión de la seguridad (o certificaciones que demuestren controles equivalentes, respaldados por un informe de un auditor independiente).

15.2 Se aplicarán los controles de los siguientes estándares:

- Estándar de Clasificación de la Información y Manejo de Datos de Terceros V4.0
- Nuestro estándar de controles de terceros V1.1 – Secciones
  Sección 7. Gestión de activos de información.
  Sección 11. Criptografía.
  Sección 16. Configuración del sistema.
  Sección 18. Protección anti-malware.
  Sección 21. Mitigación de la Denegación de Servicio.

16.Seguridad de la red - Red propia de BT

16.1 Si el tercero va a instalar equipos, configurar, mantener, reparar o monitorizar la red propia de BT, se aplicarán los controles del siguiente estándar:

- Nuestro estándar de controles de terceros V1.1

  Sección 26. Seguridad de la red - Red propia de BT.

17. Seguridad de redes de terceros

17.1 Si se usa la red de un tercero para acceder a la información de BT o para prestar el servicio, se aplicarán los controles del siguiente estándar:

- Nuestro estándar de controles de terceros V1.1 – Secciones

  Sección 16 Configuración del sistema.

Sección 20 Integridad de la red

18.Seguridad en la nube

18.1 Si el tercero va a prestar a BT servicios en la nube, se aplicará el control del siguiente estándar:

- Nuestro estándar sobre controles de terceros V1.1

  Sección 14. Computación en la nube/online.

19.Centro de Contacto

19.1 Si el tercero va a prestar a BT servicios de centro de contacto, se aplicará el control del siguiente estándar:

- Estándar de centros de contacto de terceros V2.0

20.Términos definidos e interpretación

20.1 Salvo que se defina otra cosa más abajo, las palabras y expresiones utilizadas en estos Requisitos de seguridad tendrán el mismo significado que en el Contrato:

"Acceso" significa el tratamiento, gestión o almacenamiento de la Información de BT por uno o varios de los siguientes métodos:

a. por interconexión con los sistemas de BT;
b. en papel o en un formato no electrónico
c. Información BT en los sistemas del proveedor; o
d. por medios móviles

y/o Acceso a las instalaciones de BT para la prestación de los Suministros, excluyendo el suministro de hardware y la asistencia a reuniones.

"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 razonablemente y de forma ordinaria se esperarían de una persona capacitada y con experiencia en el mismo tipo de actividad bajo las mismas o similares circunstancias.

"Contrato" significa el Contrato suscrito por las Partes para el suministro de bienes, software o Servicios que hace referencia a los presentes Requisitos de Seguridad.

"Cyber Essentials Plus" se refiere al programa por el Gobierno del Reino Unido para ayudar a las organizaciones a protegerse de ataques informáticos comunes.

"Declaración de información sensible" significa la declaración escrita que debe aportar el Proveedor con respecto a los puestos que este identifique como con acceso a información clasificada como "Oficial Sensible" o con privilegios elevados para infraestructuras que almacenan, procesan o transmiten información clasificada como "Oficial Sensible", de la que se adjunta una plantilla en el Anexo 1.

"Escrow" significa el acuerdo de depósito de código fuente celebrado de conformidad con el Contrato, para utilizar, copiar, mantener y modificar dicho código fuente para los fines comerciales de BT (incluido el derecho a compilar dicho código fuente).

"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.

"Personal del tercero" significa cualquier persona que el Proveedor o sus Subcontratistas contraten para la ejecución de las obligaciones del Proveedor con arreglo al Contrato.

"Requisitos de seguridad" significa este documento, tal y como se actualice de forma puntual.

"Seguridad de la red" significa la seguridad de los nodos y las rutas de comunicaciones interconectadas que conectan lógicamente las tecnologías de los usuarios finales y los sistemas de gestión asociados.

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

"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 alojarse en instalaciones de BT.

"Sistemas de terceros" significa cualquier ordenador, aplicación o sistema de redes propiedad del Proveedor que se usen para acceder, almacenar o tratar información de BT o que participen en la provisión de Suministros.

"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.

Interpretación

20.2 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 el término que preceden a esos términos.

20.3 Siempre que un derecho u obligación de una de las Partes se exprese como algo que "puede" ejercer o cumplir, la opción de ejercerlo o ejecutarlo quedará a la entera discreción de esa Parte.

20.4 Si se incluye un hipervínculo ("URL"), dicha referencia se aplicará al recurso online accesible a través de ese URL o a cualquier otro URL de sustitución tal y como se haya notificado a la Parte correspondiente en forma puntual.

Versión	Descripción	Autor	Fecha
4.0	Nuevo	Karen Tanner	02/02/20
4.1	Cláusula adicional para información confidencial alta	Karen Tanner	20/02/20