Public (Público)

PROTEGER BT

Nuestro estándar de Controles de terceros

Versión: 1.1

Responsable: Mark Tilston

Este estándar establece los controles de seguridad básicos para nuestros terceros.

El estándar se publica y se comunica a todas las partes relevantes y será responsabilidad de los 'expertos en la materia' revisar y garantizar al menos una vez al año que se sigan cumpliendo los requisitos de las partes interesadas y nuestros objetivos empresariales descritos en el ISMS de BT.

Se aplica a todos los terceros que trabajan para o en nombre del Grupo BT, incluyendo Openreach, EE y Plusnet.

Para simplificar las cosas, mencionaremos simplemente «BT» en el resto del documento.

Si una actividad va a ser realizada por una Parte interesada de BT, se marcará en gris.

Introducción

BT tiene el compromiso de proporcionar un entorno seguro en el que nuestros clientes y empleados puedan confiar. Nuestro objetivo es proteger toda nuestra información y nuestros sistemas de las destrucciones accidentales o maliciosas, daños, modificaciones o la revelación. Para ello, nos aseguramos de implementar las medidas de control adecuadas a los terceros para proteger la confidencialidad, integridad y disponibilidad de nuestra información y sistemas.

¿A quién afecta?

Este estándar afecta a todos los terceros que trabajen para o en nombre de BT, que entren en contacto con información o datos de BT generados, procesados, almacenados o distribuidos por ellos. Podremos modificar ocasionalmente este estándar de acuerdo con los procesos internos de consultas acordados.

Definición de los términos:

Término	Explicación
deber	Esta palabra, junto con los términos «SER PRECISO» «DEBER» o «EXIGIDO», significarán que la definición constituye un requisito absoluto
no deber	Esta frase, o la frase «ABSTENERSE DE», significarán que la definición constituye una prohibición absoluta
poder	Esta palabra, o el adjetivo «OPCIONAL» significa que un elemento es verdaderamente opcional
debería	Esta palabra, o el adjetivo «RECOMENDADO», significa que existe un motivo válido para, en determinadas situaciones, no cumplir algo específico, pero las implicaciones se deben comprender y evaluar detenidamente antes de elegir otra opción.
no debería	Esta frase, o la frase «NO RECOMENDADO», significa que se hará todo lo posible para cumplir los requisitos de un control, aunque no siempre será posible evitar la acción descrita en todos los casos. Si resulta imposible cumplir un control, será preciso evaluar y comprender todas las implicaciones.

Alcance

Este documento describe de forma precisa los controles de seguridad mínimos necesarios para gestionar la seguridad dentro de la cadena de suministro de terceros de BT.

El personal de BT puede encontrar estándares complementarios, así como los documentos de proceso y directrices que describen la implementación de los controles y que deben leerse junto con este estándar, en el sitio web de seguridad.

Las Partes interesadas de BT que requieran una exención con respecto a este estándar para un tercero deberán presentar una solicitud a través del Proceso de exenciones

¿Qué incluye este documento?

1.	Roles & Responsibilities.	4
2.	Governance.	4
3.	Incident Management.	4
4.	Change Management.	5
5.	Cyber Risk and Threat Management	6
6.	Identity Management and Access Control	6
7.	Information Asset Management	7
8.	Access to BT Systems	8
9.	Physical Security in 3rd Party Premises	8
10.	Data Classification and Protection.	10
11.	Cryptography.	10
12.	Data Leakage Prevention.	13
13.	PCI DSS	14
14.	Cloud / Online Computing.	14
15.	Social Media	14
16.	System Configuration.	14
17.	Secure Software Development.	15
18.	Anti-Malware Protection.	15
19.	Vulnerability Management.	16
20.	Network Integrity.	17
21.	Denial of Service Mitigation.	18
22.	Security Continuous Logging and Monitoring.	18
23.	Training and Awareness.	18
24.	Right of Inspection.	19
25.	Physical Security – BT Premises.	19
26.	Network Security – BT's own Network.	19
27.	Glossary.	21
28.	Change history.	22
29.	Document sign off	22
30.	Compliance	22
31.	Useful Links and Information	22
32.	Ownership and Confidentiality	23

1. Funciones y responsabilidades.

Todos los terceros deben conocer y comprender los requisitos de este estándar y garantizar que todas las personas involucradas en la prestación de un servicio a BT estén familiarizadas y cumplan los requisitos relevantes de este estándar.

Las Partes interesadas de BT tienen la responsabilidad de supervisar el cumplimiento de este estándar y trabajar con su tercero para mejorar el cumplimiento y la implementación cuando se identifiquen lagunas.

Los directivos de BT son los responsables de que sus empleados estén familiarizados y cumplan los requisitos de este estándar y las políticas y estándares relacionados.

2. Gobernanza.

2.1. El tercero en cuestión debe contar con un marco de seguridad industrial consolidado y uniforme para la gobernanza de la información y la ciberseguridad 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 relevantes relativos a la información y la ciberseguridad (incluyendo la privacidad) comprendidos y gestionados
- Procesos de gobernanza y gestión de los riesgos que aborden los riesgos de la información y ciberseguridad

2.2. 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 seguridad de la información con funciones y responsabilidades adecuadas y definidas

2.3. 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

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

3. Gestión de incidentes.

3.1. El tercero debe contar con un marco de gestión de incidentes consolidado y uniforme para garantizar que estos se gestionen, contengan y 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 criterios establecidos
- Garantizar que el impacto del incidente se comprenda

- Garantizar que se ejecuten procedimientos forenses cuando sea preciso internamente o a través de una función especializada
- Garantizar que se integren las lecciones aprendidas de los incidentes en las buenas prácticas.
- Garantizar que la información relacionada con un incidente que afecte a BT sea tratada como «Confidencial».

3.2. 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 para la seguridad, gestión de incidentes y gestión del cumplimiento. El tercero debe notificar a la Parte interesada de BT, los datos de contacto de esas personas y los posibles cambios que puedan haber. Los datos deben incluir: -
Nombre, responsabilidad, puesto y número telefónico y/o dirección de correo electrónico del grupo

3.3. El tercero informará a la Parte interesada de BT, en un plazo razonable a partir de 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 doce (12) horas desde el momento en el que el tercero tenga conocimiento del mismo.

3.4. 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.

3.5. El tercero presentará 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
- clasificación de la información afectada (ver Estándar de clasificación de la información y gestión de datos para terceros)
- estatus
- resultado (incluyendo las recomendaciones de resolución o medidas implementadas).

3.6. 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 la información. El tercero procurará mantener una relación contractual con dicha cuarta parte y garantizar que esa cuarta parte disponga de un marco de seguridad estándar en la industria.

4. Gestión del cambio.

4.1. El tercero debe garantizar que todos los cambios a 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 proceso para realizar actualizaciones de emergencia de manera controlada.

4.2. El tercero deberá garantizar que los cambios se reflejen en los entornos de producción y DR.

4.3. El tercero deberá notificar a BT inmediatamente cualquier cambio sustancial en el servicio como (entre otros) los cambios en sus métodos de acceso a través de los cortafuegos, incluyendo la provisión de traducción de las direcciones de redes.

4.4. El tercero deberá garantizar que el mantenimiento y reparación de los activos de la organización se realiza y registra con herramientas controladas y aprobadas.

4.5. El tercero deberá garantizar que el mantenimiento remoto de los activos organizativos se aprueba, registra y ejecuta de forma que se impida el acceso no autorizado.

5. Gestión de amenazas y ciberseguridad

5.1. 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, activos y 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.

5.2. 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.

5.3. 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.

6. Gestión de identidades y control de acceso

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

- La concesión, reactivación, modificación y deshabilitación 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.

- Se realizan revisiones de acceso periódicas para garantizar que ese acceso sea adecuado a su objetivo.
- Las cuentas de usuario vuelven a certificar el acceso al menos anualmente y las cuentas privilegiadas lo hacen trimestralmente.

6.2 El tercero debe garantizar que el acceso remoto se gestione de manera que solo las personas aprobadas 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 multifactorial.

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

- Generador de contraseñas de un solo uso; requiere un PIN/contraseña específico del usuario para visualizar la contraseña de un solo uso.
- Una tarjeta inteligente con un chip según la norma ISO 7816 y lector y software de lectura de tarjetas asociados. 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 acceso privilegiado para el soporte a través de acceso remoto, debe realizarse mediante una conexión segura y utilizar autenticación de doble factor.

6.3 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.

6.4 El tercero debe garantizar que todas las transacciones puedan vincularse a una sola persona identificable y, si existen credenciales compartidas, que existan unos controles de compensación adecuados (incluyendo procedimientos de rotura de cristal).

6.5 El tercero debe garantizar que toda la autenticación se gestione de forma acorde al riesgo de la transacción, es decir, longitud y complejidad adecuadas de la contraseña, frecuencia de los cambios de contraseña, autenticación multifactorial, gestión segura de credenciales de contraseña y otros controles.

6.6 Deben aplicarse controles apropiados para gestionar las autenticaciones fallidas, incluyendo notificaciones en pantalla, registro de fallos y bloqueo de usuarios.

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

7. Gestión de activos de la información

7.1. El tercero debe contar con un inventario de activos de la información (que, si procede, debe incluir cualquier equipo de BT alojado en instalaciones de terceros) y garantizar que se realice como mínimo una prueba anual para comprobar que dicho inventario esté actualizado y sea completo y preciso.

7.2. 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, carácter crítico 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.

8. Acceso a los sistemas de BT

8.1 El tercero debe cumplir todas las instrucciones pertinentes que se le faciliten con respecto al acceso y uso de los sistemas de BT.

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

8.3 El tercero garantizará que la identificación de usuario, contraseñas, PINs, tokens y el acceso a los recursos de conferencias son miembros individuales del personal del tercero y no se comparten. Los detalles se deben guardar en forma segura y separada del dispositivo empleado para acceder. Si una contraseña la conoce otra persona, debe cambiarse inmediatamente.

Conectividad entre sistemas

8.4 La vinculación entre dominios con los sistemas de BT no está permitida salvo que esté específicamente aprobado y autorizado por BT.

8.5 El tercero debe hacer todo lo posible para garantizar que no entren virus o códigos maliciosos (como se entienden generalmente las expresiones en la industria informática) en los sistemas de BT.

8.6 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 establecidos en la **Sección 11 Criptografía**.

8.7 Además, el tercero procurará que los sistemas y la infraestructura utilizados estén contenidos en una red lógica específica. Esta red solo debe constar de los sistemas específicos para la prestación de un recurso seguro de tratamiento de datos de clientes.

9. Seguridad física en 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 debe incluir 1 o más de lo siguiente:
- 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 (a producir 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 del control ambiental, mantenimiento de alarmas y servicio de limpieza.

9.3 Las áreas seguras en las instalaciones de terceros utilizadas para prestar el servicio (por ej., salas de comunicaciones de redes) se separarán 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 esas áreas debe ser auditado regularmente y debe hacerse una evaluación de la nueva autorización de derechos de acceso como mínimo una vez al año.

9.4 El tercero debe contar con sistemas de seguridad de CCTV en lugares donde se almacene o gestione información de BT.

9.5 Las grabaciones de los CCTV deben guardarse durante un mínimo de 20 días. Ese periodo podría ampliarse en las siguientes situaciones:

- Si existen pruebas de vídeo de los CCTV, deben guardarse para una investigación penal o de un incidente; o
- Si se especifica como requerimiento necesario para cumplir con la legislación

9.6 Todas las grabaciones y grabadoras de los CCTV deben ubicarse en lugares seguros para evitar la manipulación, eliminación o visualización «casual» de las pantallas de CCTV asociadas y el acceso a las grabaciones debe controlarse y limitarse solo a las personas autorizadas.

9.7 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 la 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, acondicionamiento de aire y detección de agua.
- Prevención de daños por agua, localización de depósitos de agua, tuberías, etc. dentro de las instalaciones.

9.8 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 relevantes dispongan de dicho acceso.

9.9 El tercero debe asegurar la prohibición de fotografiar y/o capturar imágenes de la información de BT. Si existe una necesidad empresarial de capturar esas imágenes, deberá obtenerse la confirmación por escrito de la Parte interesada de BT.

Provisión del entorno de alojamiento para los equipos de BT.

9.10 Si el tercero provee un área de acceso seguro en sus instalaciones para el alojamiento de los equipos de BT o de los clientes de BT, deberá:

- Suministrar 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 del tercero relevante.
- Implementar un proceso de gestión de claves seguro.

9.11 BT suministrará 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).

10.Protección y clasificación de los datos.

10.1 El tercero debe contar con un marco o sistema de clasificación y gestión de la información consolidado y uniforme (alineado con las buenas prácticas de la industria/requisitos de BT) 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 puede emplearse para ningún fin distinto de aquel para el que se haya suministrado.
- La información de BT debe ser gestionada de acuerdo con el Estándar de clasificación de la información y gestión de datos para terceros.

11. Criptografía.

11.1 El tercero debe garantizar que si existe un nivel de riesgo que exige encriptación, dichos datos se encriptarán convenientemente (en tránsito y cuando no se estén trasmitiendo) y que si se utilizan claves criptográficas, estas estarán diseñadas y se aplicarán para cumplir los requisitos de seguridad especificados en el estándar NIST FIPS 140-2 dentro del nivel 2 o superior.

11.2 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.

11.3 Si el NIST anuncia que un criptoalgoritmo ya no es seguro, no deberá utilizarse en nuevos despliegues. Los despliegues existentes deben revisar el uso continuado de criptoalgoritmos obsoletos y proporcionar un plan de migración para abandonarlos en beneficio de otros más seguros.

11.4 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.

11.5 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 segmentación no están permitidos: MD2, MD4, MD5 y SHA-1.

11.6 Gestión de claves - Creación y uso

- Deben crearse claves de sesión y *nonces* utilizando un generador de números pseudoaleatorios seguro. Debe alimentarse con como mínimo tantos bits de entropía o imprevisibilidad de un mensaje, como el número de bits de seguridad efectivos proporcionados por el algoritmo que utilizará la clave.
- Está prohibido tomar una clave más corta de 64 bits y combinarla de forma no criptográfica con la misma clave de 64 bits para obtener 128 bits.
- Todos los bits de la clave deben ser utilizados por el algoritmo
- El relleno u otros bits utilizados por el algoritmo no se tendrán en cuenta a la hora de determinar la longitud de la clave

11.7 Gestión de claves - Aleatoriedad

- Debe emplearse una fuente de datos aleatorios robusta al producir las claves de sesión que se vayan a usar en las partes simétricas de la criptografía híbrida o para producir sales o vectores de inicialización.
- Pueden utilizarse generadores de números pseudoaleatorios (PRNG) pero, para ser considerados seguros, los PRNG no deben permitir a los atacantes:
  - Adivinar el resultado futuro del generador si tiene conocimiento de los resultados anteriores
  - Calcular los estados anteriores del generador si tiene conocimiento de su estado actual
  - Distinguir el resultado del PRNG de la verdadera aleatoriedad. (El uso del rand() no está permitido.

11.8 Gestión de claves - Intercambio de claves

- Las claves de sesión generadas para ser utilizadas con un algoritmo simétrico deben intercambiarse empleando un protocolo de intercambio de claves seguro

11.9 Gestión de claves - Almacenamiento de claves

- Si se utilizan claves para proteger los datos en reposo, la clave de encriptación de datos (DEK) debe protegerse empleando una clave de encriptación de claves (KEK) que debe estar almacenada en un servidor independiente o en un módulo de plataforma de confianza (TPM).
- Si la KEK se almacena en un servidor independiente, debe protegerse durante la transmisión al servidor que albergue los datos.

11.10 Gestión de claves - Rotación de claves (regeneración)

- Debe ser posible regenerar las claves de acuerdo con las buenas prácticas de la industria en momentos clave.
- Debe ser posible reencriptar los datos que se vayan a proteger con la clave regenerada.
- Debe ser posible llevar a cabo la regeneración *ad hoc* de claves y reencriptar los datos si se sospecha que la clave de encriptación original se ha visto comprometida.
- En el caso de AES GCM, la probabilidad de que la función de encriptación autenticada llegue a invocarse con el mismo IV y la misma clave en dos (o más) conjuntos de datos de entrada diferentes no debe ser superior a 232

11.11 Gestión de claves - Módulos de seguridad de hardware (HSM)

- Las claves criptográficas deben cargarse en un HSM utilizando tarjetas inteligentes.

- Las tarjetas inteligentes deben requerir un PIN para permitir el acceso.
- Los PIN deben elegirse de acuerdo con la política de control de acceso.
- Los PIN y las tarjetas inteligentes deben guardarse en una caja fuerte revisada por su equipo de Infosec.
- No debe ser posible extraer claves criptográficas de un HSM.
- Los HSM deben destruir las claves criptográficas almacenadas si se produce un intento de abrir la caja fuerte.
- En el caso de los HSM que contengan claves altamente sensibles, los PIN y las tarjetas inteligentes usados para protegerlos deben ser configurados y almacenados solamente por miembros del personal de seguridad tecnológica.
- Si el HSM se va a utilizar para proteger datos altamente sensibles, debe exigirse un quórum mínimo de 2 tarjetas inteligentes y sus PIN asociados para realizar cambios en el HSM. Los miembros del quórum deben verificarse en el nivel de cribado mejorado.

11.12 Certificados digitales

- Los certificados deben tener la serie de atributos Punto de distribución de lista de revocación de certificados (CDP).
- Debe usarse el Protocolo de estado de certificados online (OCSP) o la Lista de revocación de certificados (CRL) para determinar el estado de los mismos.
- Los responsables de los certificados deben comprobar la validez y vencimiento de los certificados para garantizar que los eventos de vencimiento previstos no provoquen un fallo del sistema.
- Los consumidores de los certificados (clientes) deben comprobar la validez y vencimiento de los certificados para garantizar que los eventos de vencimiento previstos no provoquen un fallo del sistema.
- La vida útil de los certificados debe establecerse de acuerdo con el objetivo de los mismos.
- La vida útil de los certificados debe determinarse antes de su emisión.
- Uso de identidad estándar (cliente, servidor) 1024 no permitido

11.13 Datos en tránsito

- La encriptación de datos en tránsito suele llevarse a cabo utilizando la encriptación de trasporte o carga útil (mensaje o campo selectivo). Los mecanismos de encriptación de transporte incluyen entre otros:
- Seguridad de capa de transporte (TLS)
- Tunelación segura (IPSec)
- Secure Shell (SSH)
- Para la encriptación del transporte, el componente simétrico debe cumplir la sección 12.14 de este estándar.
- Los protocolos de seguridad del transporte deben configurarse para evitar la negociación de algoritmos más débiles y/o longitudes de clave menores cuando ambos puntos son compatibles con la opción más robusta.
- El protocolo SSL no debe utilizarse si existe un número de vulnerabilidades conocidas dirigidas en este protocolo.
- Los vectores de inicialización de los cifradores de flujo y AES en modo CBC no deben ser predecibles.
- El IV/*nonce* en AES GCM debe cumplir el siguiente requisito de «exclusividad»:
  - El cumplimiento de este requisito es crucial para la seguridad de GCM
  - Los protocolos de seguridad del transporte deben configurarse (es decir, uso de bits de dirección) para evitar ataques de texto sin cifrar conocidos desde mensajes conocidos devueltos, por ejemplo «nada que declarar».

- La verificación de identidad mutua debe realizarse durante la configuración del transporte.
- En el caso de datos de longitud corta sensibles que requieran encriptación de carga útil (claves de encriptación, contraseñas, información de tarjetas de pago), debe utilizarse la encriptación asimétrica empleando como mínimo las longitudes de clave mínimas y los algoritmos que se detallan en este documento.
- Los datos de gestión del sistema deben encriptarse en tránsito.
- Las siguientes opciones TLS no están permitidas: TLS v1.0, TLS v1.2, v6.0, TLS v6.1 y SSL (cualquier versión)
- Las siguientes opciones SSH (SFTP) no están permitidas: SSH v1
- Las siguientes opciones IPSec no están permitidas: IKE Versión 1

11.14 Datos en reposo

- Los datos en reposo incluyen datos almacenados en archivos, bases de datos, ubicaciones temporales y de intercambio y en cualquier dispositivo, incluyendo entre otros, PC, ordenadores portátiles y otros dispositivos portátiles, servidores, cintas, SAN, USB, CD, DVD, disquetes y otras soluciones de almacenamiento extraíbles.
- Los datos definidos con el nivel de confidenciales o superior almacenados en una memoria no volátil de cualquier dispositivo deben encriptarse.
- La información de tarjetas de pago almacenada en cualquier dispositivo en una memoria no volátil debe encriptarse.
- Si se almacenan datos simétricos protegidos por una clave asimétrica, la clave asimétrica debe ofrecer una resistencia equivalente, medida en bits de seguridad, a la de la propia clave simétrica.
- La documentación del sistema debe identificar la clasificación de datos y los volúmenes almacenados por el sistema.
- Las claves empleadas para la desencriptación no deben almacenarse ni incluirse en una copia de seguridad junto con los datos que desencriptan. El software debe haberse probado completamente antes de desplegarse en los sistemas de producción.

12. Prevención de la fuga de datos.

12.1 El tercero debe tener un marco establecido y coherente que asegure que la protección contra la fuga de datos inapropiada está implementada garantizando que la protección incluye (entre otros) los siguientes vectores:

- Correo electrónico
- Internet/Pasarela web (incluyendo almacenamiento online y webmail)
- Puertos/dispositivos de almacenamiento portátiles USB, ópticos y de otro tipo, etc.
- Informática móvil y BYOD
- Servicios de acceso remoto
- mecanismos de intercambio de archivos y redes sociales

NOTA Los soportes extraíbles/dispositivos portátiles deben deshabilitarse por defecto y solo se habilitarán por motivos empresariales legítimos. Todos los datos almacenados en soportes extraíbles o dispositivos portátiles deben encriptarse en función del riesgo. 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. Ver Estándar de clasificación de la información y gestión de datos de terceros para obtener más información acerca de la gestión de soportes extraíbles.

13. PCI DSS

13.1 El tercero debe garantizar que si trabaja con datos de tarjetas de pago, cumplirá como corresponda los DSS de PCI.

14.Computación en la nube/online.

14.1. 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 datos no públicos almacenados en la nube sea aprobado y se someta a los controles apropiados equivalentes a la última versión de la Cloud Security Alliance, Cloud Controls Matrix (CCM) .

14.2. Los acuerdos de nivel de servicio (internos o externalizados) de infraestructuras y redes deben documentar con claridad los controles de seguridad, la capacidad y los niveles de servicio así como los requisitos empresariales o del cliente

14.3. 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 personas no autorizadas (por ej., otros clientes de la nube) accedan a la información de BT y a los servicios utilizados por BT.

15. Redes sociales

15.1. El tercero debe contar con un marco 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 sus clientes
- Usar los logotipos de la organización o los clientes sin permiso previo
- Exponer información no pública de la organización o el cliente sin autorización previa
- Publicar opiniones acerca de la organización o sus clientes que pueda interpretarse razonablemente como un comentario oficial de la organización o de sus clientes
- No debe revelar ninguna información de BT etiquetada como «Confidencial» o «Altamente confidencial».

16.Configuración de sistemas.

16.1. El tercero debe contar con un marco consolidado y uniforme para garantizar que los sistemas estén correctamente configurados (tanto los sistemas de terceros como los que se suministren a BT), incluyendo los siguientes componentes:

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

17. Desarrollo de software seguro.

17.1. El tercero debe garantizar que los entornos productivos y no productivos estén debidamente controlados garantizando la presencia de los siguientes componentes:

- 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 deberes entre el desarrollo productivo y no productivo

17.2. El tercero debe contar con un marco de desarrollo de sistemas consolidado y uniforme para evitar las vulnerabilidades de seguridad y las violaciones de la 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 la producción

17.3. Si se precisa un custodio para proteger a todas las partes de elementos propios o de terceros (es decir, propiedad intelectual/código fuente, etc.), el tercero deberá contar con un marco consolidado y uniforme que incluya los siguientes componentes:

- 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 otro material hasta que se cumplan las condiciones de publicación
- Condiciones de publicación apropiadas
- Actualizaciones continuas, pagos apropiados y revisiones del contrato de custodia.

18. Protección antimalware.

18.1. El tercero debe garantizar que se aplique la última protección antimalware a todos los activos informáticos para evitar perturbar el 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.

19. Gestión de vulnerabilidades.

19.1. 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.

19.2. El marco de gestión de vulnerabilidades del tercero debe garantizar que se comprueben de manera rutinaria los siguientes elementos para detectar posibles eventos de ciberseguridad

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

19.3. 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 desde fuentes internas y externas (como 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.

19.4. El tercero debe garantizar que se apliquen a los sistemas/activos/redes/aplicaciones los últimos parches de seguridad de forma puntual que garanticen que:

- El tercero usa parches obtenidos de: distribuidores directos de sistemas y parches patentados que (i) estén 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 como procedente de una comunidad de soporte reconocida de software de código abierto.
- El tercero prueba todos los parches en sistemas que representan de forma precisa la configuración de los sistemas de producción objetivo antes de desplegar el parche en los sistemas de producción y que se comprueba el correcto funcionamiento del servicio al que se aplica el parche después de cualquier actividad de parcheado.
- Monitorizar a todos los proveedores pertinentes y otras fuentes de información relevantes con respecto a alertas de vulnerabilidad.
- Si un sistema no puede parchearse, desplegar contramedidas apropiadas.

19.5. El tercero debe garantizar que, al menos una vez al año, se encargará una prueba de penetración/evaluación de la seguridad informática independiente para su infraestructura y aplicaciones informáticas empleadas para prestar servicios que incluya puntos de recuperación tras desastres para identificar vulnerabilidades que podrían explotarse para perpetrar violaciones de datos/servicios e impedir las violaciones 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.

19.6. El tercero debe asegurar que el acceso a los puertos de diagnóstico y gestión así como a herramientas de diagnóstico estén bajo controles seguros.

19.7. El tercero debe asegurar que el acceso a las herramientas de auditoría esté limitado al personal del

proveedor correspondiente y su uso monitorizado.

19.8. El tercero debe asegurar que los servidores que se usen 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 [por ej., en Internet]) sin los controles de seguridad apropiados.

20.Integridad de la red.

20.1. El tercero debe garantizar que se establezca y mantenga la integridad de la red garantizando el adecuado control de los siguientes componentes:

- 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 violaciones 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 con gestión de la identidad efectiva y la configuración del sistema operativo que debe protegerse y documentarse convenientemente;
- Deshabilitación (cuando se pueda) de servicios, aplicaciones y puertos que no se usen.
- Deshabilitación o eliminación de cuentas de invitados.
- Evitar relaciones de confianza entre servidores;
- Uso del principio de seguridad de buenas prácticas de «privilegio mínimo» para realizar una función;
- Garantizar 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.

20.2. La red del tercero debe 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 las violaciones, la identificación de las personas que obtuvieron acceso y la determinación de cómo lo obtuvieron.

21. Mitigación de las denegaciones de servicio.

21.1. 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).

22. Registro y monitorización continua de la seguridad.

22.1. El tercero debe garantizar que exista un marco de gestión de registros y auditoría consolidado y uniforme que garantice que los sistemas clave que incluyan aplicaciones se configuran para registrar eventos clave (incluyendo accesos privilegiados y actividad del personal) y dichos registros deberán conservarse durante un período mínimo de 12 meses. Como mínimo, el tercero debe garantizar que los registros (si procede) contengan los siguientes eventos:

- Puntos de inicio y parada del proceso registrado.
- Cambios en el tipo de eventos registrados tal y como exija el rastreado de auditoría (por ej., los parámetros de arranque y cualquier cambio en los mismos).
- Arranque y parada 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, sello de tiempo)

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

- Garantizar que los registros sean revisados por una función independiente al menos cada mes para detectar 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 con umbrales de alerta por incidentes establecidos y se actúa puntualmente según la gravedad de la alarma.

23. Formación y sensibilización.

23.1. 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 buenas prácticas en ciberseguridad y protección de datos personales en el plazo de un mes desde su incorporación y refresque los 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

23.2. El tercero debe garantizar que exista un componente de prueba para verificar que el usuario comprende la formación y sensibilización.

24. Derecho de inspección.

24.1. 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 al menos una vez al año (o inmediatamente después de un incidente).

24.2. El tercero será el responsable de los costes de remediar las debilidades de seguridad que identifique BT dentro de un calendario acordado por ambas Partes.

24.3. Si se produce un incidente grave, el tercero debe 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 los activos relevantes pertenecientes al tercero y para ayudar en la investigación, y el tercero no deberá retrasar ni retener de forma injustificada dicha solicitud.

25. Seguridad física - Instalaciones de BT.

25.1 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. BT podrá también 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 locales.

25.2 Si el personal del tercero ha recibido una tarjeta de acceso de BT, el tercero deberá notificar a BT inmediatamente y, en cualquier caso, en el plazo de 5 días laborables, cuando dicho personal ya no precise acceder a las instalaciones de BT.

25.3 Solo los servidores aprobados de BT, los PC Webtop y los dispositivos finales fiables 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 aprobado por BT a ningún dominio de BT sin la autorización previa y por escrito de BT.

25.4 Deberá cumplirse la protección física y las directrices de trabajo 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.

25.5 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

Además, el firmante autorizado del tercero y el personal del tercero deberán pasar controles pre-empleo mínimo L2.

26. Seguridad de la red – Red propia de BT.

26.1 El tercero deberá proporcionar al Contacto de seguridad de BT los nombres, direcciones (y otros datos que exija BT) de cada miembro del personal del tercero que pueda estar involucrado periódicamente en el despliegue, mantenimiento y/o gestión del servicio antes de iniciar dichas tareas de despliegue, mantenimiento y/o gestión.

26.2 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 (o a quien designe) y el equipo deberá asistir a las reuniones que puntualmente decida mantener el Contacto de seguridad de BT.

26.3 El tercero proporcionará al Contacto de seguridad de BT un programa (actualizado según se precise) de todos los componentes activos incluidos en el servicio y/o los servicios y sus fuentes respectivas.

26.4 El tercero proporcionará los datos del empleado que contactará con el equipo de gestión de vulnerabilidades (CERT) de BT en relación con las conversaciones sobre vulnerabilidades identificadas del tercero y BT en el servicio y/o servicios. El tercero proporcionará a BT información puntual sobre vulnerabilidades, y cumplirá (a coste del tercero) los requisitos razonables en relación con las vulnerabilidades que puedan ser notificadas ocasionalmente por el Contacto de seguridad de BT. El tercero informará a BT de cualquier vulnerabilidad con tiempo suficiente para permitir la aplicación o instalación de los controles de mitigación antes de que el tercero las haga públicas.

26.5 El tercero procurará que todos los componentes relacionados con la seguridad comprendidos en el Servicio, como los identificados por o para BT ocasionalmente, sean evaluados externamente a coste del tercero a satisfacción razonable de BT.

26.6 El tercero deberá proporcionar rápidamente, y en cualquier caso en un plazo de 7 días laborables, al Contacto de seguridad de BT los detalles completos de cualquier característica y/o funcionalidad en cualquier Servicio (o que esté planificada en la hoja de ruta de cualquier Servicio) que puntualmente:

- conozca el tercero; o
- el Contacto de seguridad de BT crea con cierta razonabilidad y por tanto informe al tercero que están diseñadas para, o podrían usarse para, la interceptación legal o cualquier otra interceptación del tráfico de telecomunicaciones. Esos detalles deben incluir toda la información que sea razonablemente necesaria para que el Contacto de seguridad de BT comprenda en profundidad la naturaleza, composición y medida de tales funciones y/o funcionalidades.

26.7 A fin de mantener el acceso a los sistemas y/o las redes de BT, el tercero deberá notificar de inmediato a BT de cualquier cambio en su método de acceso a través de los cortafuegos, incluyendo la provisión de traducciones de direcciones de redes.

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

26.9 El tercero procurará que la funcionalidad IPv6 incluida en los sistemas operativos esté deshabilitada en los *hosts* (por ejemplo, en los dispositivos o servidores del usuario final) que se conectan a la red de BT y los dominios deberán ser deshabilitados cuando no se necesiten.

26.10 El personal del tercero que cree, desarrolle o facilite soporte a los activos de red o redes de BT procurará que todo el personal del tercero disponga de controles pre-empleo L2. Algunos roles identificados por el Contacto de seguridad de BT requerirán controles pre-empleo L3. En los casos en que el tercero no tenga la capacidad de autorizar directamente los niveles de seguridad de los miembros del personal del tercero como parte de los controles pre-empleo L3, BT le asistirá para obtener la autorización pero a coste del tercero.

26.11 El tercero deberá mantener el hardware y el software según las especificaciones del fabricante.

26.12 El tercero no usará soportes extraíbles (discos, unidades de disco USB, etc.) destinados al soporte y mantenimiento para ningún otro propósito.

27. Glosario.

Término	Definición
autenticación de doble factor	A veces se conoce como verificación en dos pasos o autenticación de doble factor y se trata de un proceso de seguridad en el que el usuario facilita dos factores de autenticación diferentes que se autoverifican para proteger mejor tanto las credenciales del usuario como los recursos a los que el usuario puede tener acceso.
Tercero	Personas que trabajan para nosotros, pero que no son empleados de BT
AES	Advanced Encryption Standard (AES), es una especificación para encriptar datos electrónicos creado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos en 2001.
ASG	Grupo de soporte de aplicaciones
Grupo BT	Grupo BT se refiere a todas las CFU y CU del Grupo BT, incluyendo entre otros, Openreach, EE y Plusnet; en el resto de este documento, se referirá como «BT» salvo indicación contraria.
Parte interesada de BT	El empleado de BT que tiene la responsabilidad del trabajo que ha sido encargado al tercero.
CCTV	significa televisión por circuito cerrado.
DBA	Administrador de bases de datos
DC	Centro de datos
Defensa en profundidad	Es un enfoque en ciberseguridad en el que una serie de mecanismos de defensa se disponen por capas para proteger datos e información de valor. Si un mecanismo falla, otro entra en acción inmediatamente para frustrar un ataque.
DR	Recuperación tras desastres
GCM	El Galois/Counter Mode es un modo de operación de los cifradores de bloque criptográficos de clave simétrica que ha sido ampliamente adoptado debido a su rendimiento
HDD	Unidad de disco duro
HMG	El Gobierno de su Majestad - Son los organismos gubernamentales del Reino Unido
ISMS	Sistema de gestión de la seguridad de la información. Se trata de un marco de políticas y procedimientos que incluyen todos los controles legales, físicos y técnicos involucrados en los procesos de gestión de riesgos de la información de una organización.
ISO 27001	Es una especificación de norma industrial para un sistema de gestión de la seguridad de la información (ISMS).
ISO 27017	Código de prácticas para los controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube
ISO 7816	Es una norma internacional relativa a las tarjetas de identificación electrónicas con contactos, especialmente las tarjetas inteligentes, gestionadas conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).
NAS	dispositivo de almacenamiento individual que opera en archivos de datos.
NIST	El Instituto Nacional de Normas y Tecnología es un laboratorio de ciencias físicas y un organismo no regulador del Departamento de Comercio de los Estados Unidos.
PCI DSS	El estándar de seguridad de los datos del sector de las tarjetas de pago (PCI DSS) es un estándar de seguridad de la información para las organizaciones que gestionan tarjetas de crédito de marca de las principales redes de tarjetas.

Cuentas privilegiadas	Un usuario privilegiado es alguien que tiene acceso administrativo a sistemas críticos
RSA	(Rivest–Shamir–Adleman) es uno de los primeros criptosistemas de clave pública y es ampliamente utilizado para la transmisión segura de datos.
SAN	red local de múltiples dispositivos que operan en bloques de discos
SSD	Unidad de estado sólido

28.Historial de cambios.

N.º de versión	Fecha	Autor de los cambios	Breve descripción del cambio
0.1	30/10/2017	Mark Tilston	Borrador inicial para rastrear y actualizar contenidos
0.2	10/04/2019	Tim Hunt	Transferido a nuevo formato
1.0	01/05/2019	Ian Morton	Presentado a Asuntos
1.1	01/10/2019	Karen Tanner	Controles adicionales añadidos como parte de la optimización de los requisitos de seguridad de BT

29.Aprobación de documentos

Puesto	Fecha
Mark Tilston	06/11/2019

30.Cumplimiento

Somos conscientes de que la mayoría de los empleados de BT actúan de forma profesional y de acuerdo con los valores de la empresa pero en caso de comportamiento no conforme a este estándar, BT podrá emprender acciones disciplinarias en función de la legislación y normativa local.

Para todo lo demás, en caso de comportamiento incoherente con este estándar, podremos rescindir nuestros acuerdos con usted para la prestación de sus servicios.

31.Enlaces útiles e información

Para el personal de BT:

En este enlace puede revisar todas las Políticas y estándares de BT .

Revisamos todas nuestras políticas y estándares al menos anualmente. Para acceder a nuestro programa de revisiones, puede hacer clic aquí.

Para informar de un «incidente de seguridad», puede escribir a: Centro de control de seguridad

Si necesita más información u orientación acerca de este estándar o cualquier otra política de seguridad, contacte con security.policy@bt.com

Para terceros:

En este enlace puede ver todos los Estándares y otras condiciones de seguridad relevantes.

32. Responsabilidad y confidencialidad

Este documento no debe ser compartido con ningún tercero sin la autorización previa por escrito de BT.
Este estándar y cualquier documentación asociada siguen siendo propiedad de BT y deben devolverse si así se solicita.

Este documento está clasificado como «Interno», pero si lo descarga un tercero deberá gestionarse como «Confidencial».