Anexo 5: Requisitos de seguridad de alojamiento de datos

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

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

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

- Desde dónde accedieron al activo, por ejemplo: la dirección IP; y
- Cuándo, por ejemplo: registro de tiempo.
- Todo acceso físico y lógico debe quedar registrado en archivos de registro que se conserven durante un año (como mínimo);
- En caso de una infracción en la que los datos de BT se vean comprometidos, robados o modificados, debe establecerse un proceso para garantizar que se notifique a BT dentro de un período razonable de tiempo, con el suficiente nivel de detalle;

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

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