Requisitos para el alojamiento externo de datos de terceros

Deben cumplirse las siguientes condiciones cuando los datos de BT sean

- Alojados en un entorno externo (No Centro de Datos BT)
- Transferidos entre el Centro de Datos (DC) (No Centro de datos BT)
- Transferidos entre el Centro de Datos y centros de *backup (copias de seguridad)*. (No Centro de Datos BT)

Se aplica a todos los datos 'Confidenciales' de BT (IC), datos 'Estrictamente confidenciales de BT' (ISC) y datos Personales de BT. Ver la Clasificación de información de terceros y la Especificación para el tratamiento de datos http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm para las definiciones. Hay previstos controles adicionales para los Datos personales sensibles.

Ref.	Control	Razón
EDH20	Si el alojamiento externo se ve comprometido y los datos de BT son robados o modificados, debe establecerse un proceso para garantizar que BT sea notificada según conste en el contrato, con el nivel suficiente de detalle según los Requisitos mínimos de seguridad de BT y la condición denominada "Protección de datos personales" en la que se procesan datos personales.	Para garantizar que BT sea rápidamente conocedora de un potencial incidente/robo de datos.
EDH30	El Centro de Datos debe contar con un certificado ISO 27001 válido para la gestión de seguridad (o certificaciones que demuestren controles equivalentes, sustentados por informes de auditores independientes).	ISO27001 demuestra que existe un marco de control de buenas prácticas para la gestión del riesgo de la información.
EDH60	El tratamiento de las claves criptográficas debe cumplir los requisitos del Estándar de Criptografía en la Clasificación de información de terceros y la Especificación para el tratamiento de datos.	Buenas prácticas criptográficas.
EDH70	El acceso lógico del usuario a efectos de Administración debe estar basado en roles y usar la autenticación de doble factor estándar de la industria, por ej. tokens de contraseñas de un solo uso o certificados emitidos por las autoridades de certificación raíz reconocidas que se pueden encontrar en - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Un control de acceso deficiente podría dar lugar al acceso no autorizado.
EDH90	La administración de aplicaciones o datos alojados externamente debe tener lugar a través de una conexión segura (encriptada) y usar autenticación de doble factor según EDH70.	Para asegurar que el acceso remoto sea tan seguro como el acceso local.
EDH100	Cualquier acceso directo remoto a los datos cuando los datos de BT se encuentran en tránsito o en reposo deberá realizarse desde el mismo país que el Centro de Datos o en un país o territorio que garantice un nivel adecuado de protección de los datos de BT. El almacenamiento externo debe realizarse en el mismo país que el Centro de Datos o en un país o territorio que garantice un nivel adecuado de protección de los datos de BT.	Para minimizar el riesgo de que no se cumplan las leyes nacionales de protección de datos o que se procesen datos confidenciales en regiones de interés para BT.
EDH110	Cualquier acceso (físico o lógico) a efectos de control de cambios o investigación/solución de fallos debe ir acompañado por una solicitud de cambio o un ticket de fallo. Dicho acceso solo se concederá durante el período de la modificación/fallo y se eliminará posteriormente.	Para minimizar el riesgo de que se efectúen cambios no autorizados.

EDH130	El almacenamiento de datos en forma de copias de seguridad debe estar encriptado a nivel de medios, por ej., cintas, discos, etc., según el estándar de Encriptación de Clasificación de información de terceros y las Especificaciones para el tratamiento de datos. http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Proteger los datos de BT y minimizar el riesgo de no cumplir con las leyes de protección de datos nacionales.