Anexo 2: Clasificación de la información

Introducción

Dentro de BT todos los datos y la información tienen un responsable de negocio que se encarga de clasificar los documentos o los datos.

Todos los usuarios que entran en contacto con los datos y la información deben protegerlos. Como usuario de la información de BT, usted es responsable de asimilar los controles de clasificación de seguridad de este documento y los requisitos del proyecto concreto especificados por BT. Solo debe utilizar el documento o los datos para su propósito original y obtener la aprobación del propietario de los datos si desea permitir que más personas accedan a ellos.

Si usted recibe información de BT que no se haya clasificado debe comunicarse con el remitente o su gerente de BT para confirmar la clasificación, en caso contrario, póngase en contacto con seguridad de BT como indica el Anexo 3 de los Requisitos de seguridad.

Nota: Si usted tiene acceso a la red de área local (LAN) BT Greenside o se le exige que cree documentos para BT que incluyan cualquier información de BT, entonces usted necesita hacer referencia a la Política de seguridad 4, de lo contrario se le aplicará lo siguiente:

Clasificaciones de la información

Hay 4 clasificaciones de la información:

- Pública
- Interna
- Confidencial
- Estrictamente confidencial

Pública
La información pública no requiere controles o se destina al consumo público.

Interna
La información interna está disponible para personal de BT y otras personas que tengan acceso a la red de información de BT, suponiéndole dicho acceso algo de riesgo empresarial a BT.

Confidencial
La información confidencial tiene un público concreto: se impone estrictamente el principio de la necesidad de saber (controles de acceso). La divulgación no autorizada de información confidencial puede afectar a la reputación de BT o ser perjudicial para las personas.

Algunos ejemplos son:

- Información personal acerca de individuos, ya sea personal de BT, terceros o clientes;
- Datos de registro del sistema;
- Datos de ventas y comercialización;

- Planes de negocios locales;
- Datos de riesgo;
- Contraseñas;
- Información que es legalmente confidencial.

Colección de varios documentos confidenciales
Si tiene una colección de documentos confidenciales en una sola ubicación, es posible que la clasificación necesite actualizarse, lo que puede dar lugar a la reclasificación de documentos individuales como "estrictamente confidenciales" o requerir medidas adicionales de seguridad para garantizar la ubicación si:

- Juntos pudieran causar un daño excepcional a BT en caso de filtración;
- Cuando se utilizan con otras combinaciones de datos individuales, como nombre y dirección, y/o existen numerosos registros bancarios detallados en un sistema, pueden resultar un objetivo atractivo.

Si le preocupa la información que está en su posesión, hable con su contacto de BT.

Estrictamente confidencial
La información o los datos estrictamente confidenciales tienen una circulación definida y pequeña en número; se impone estrictamente el principio de la necesidad de saber (usted debe saber quién tiene copias y quién tiene acceso). La divulgación no autorizada podría causar daños excepcionales a BT. Hay que considerar cuidadosamente si la información es estrictamente confidencial ya que esta requiere los controles de seguridad más rigurosos.

Controles de seguridad

Términos definidos:

<u>Cifrado</u>
<u>Requisitos mínimos:</u>
- Utilice cifrado AES de 256 bits.
- Las claves simétricas deben tener una longitud mínima de clave de 256 bits.
- Las claves asimétricas (por ejemplo, RSA) deben tener una longitud de clave de al menos 2048 bits.
- Utilice solo códigos criptográficos conocidos y de confianza.
- No use certificados autofirmados.

Contraseña/frase de acceso (para el cifrado)

No debe ser fácilmente predecible (es decir, debe ser lo más aleatoria posible, sin relación con el ID de usuario, los usuarios, la identidad, la fecha, etc.) y no ser detectable usando diccionarios de contraseñas comúnmente utilizadas. Sin embargo, deben tener como mínimo:-
- Al menos 8 caracteres de longitud.
- Contener al menos dos de los siguientes elementos:
  - Elementos no alfanuméricos, p. ej: !, £,", $, %,^, &,*, (,), -,_, +, =, :, `, @, ~, #, ?, <, >
  - Números decimales: (0... 9)
  - Letras mayúsculas: (A... Z)
- Las claves privadas deben protegerse con una frase de acceso que utilice una mezcla de caracteres alfanuméricos y símbolos, tal como se ha definido arriba.

<u>Nota: Para evitar dudas, los requisitos contractuales específicos del cliente contenidos en un contrato de cliente que requieran un mayor nivel de seguridad tendrán prioridad sobre los siguientes controles.</u>

	Controles de seguridad	Interna	Confidencial	Estrictamente confidencial
1	**Legislación nacional sobre protección de datos: datos personales y datos personales sensibles**	No deben ser tratados como información interna. Proteja los registros individuales como confidenciales.	Proteja los registros individuales como confidenciales.	Proteja los registros individuales como estrictamente confidenciales.

2	**Seguimiento de los movimientos y control de la distribución de la documentación empresarial (Word, Excel, etc.)**	No son necesarios el control ni el seguimiento. Ponga la marca "**BT INTERNO**" en cada página, o "**OPENREACH INTERNO**" si es solo para compartir en Openreach.	Ponga "**CONFIDENCIAL**" en cada página del documento, asegúrese de seguir el "**principio de la necesidad de saber**" y considere el uso de una **lista de distribución.** Se requiere cifrado según los términos "Cifrado" y "Contraseña/frase de acceso" definidos anteriormente.	Ponga "ESTRICTAMENTE CONFIDENCIAL" en cada página del documento. Incluya una **lista de distribución** de personas dentro del documento. El propietario debe asegurarse de seguir el "**principio de la necesidad de saber**". Se requiere cifrado antes del almacenamiento utilizando software que respete los términos de "Cifrado" y "Contraseña/frase de acceso" definidos anteriormente cuando los datos no se almacenan en un PC o portátil suministrado por BT con disco duro cifrado, es decir, soportes extraíbles. Lo mismo se aplica cuando lo envía por correo electrónico a cualquier persona, de BT o ajena a BT.
3	**Almacenamiento seguro en ordenador portátil y PC**	Se requiere almacenamiento seguro, por ej. con PGP, WinZip 9.	Cifrado de disco completo según los términos definidos de "Cifrado" y "Contraseña/frase de acceso" anteriormente.	Cifrado de disco completo según los términos definidos de "Cifrado" y "Contraseña/frase de acceso" anteriormente.
4	**Almacenamiento seguro en servidor y bases de datos (fijo - disco o cinta)**	No se requiere almacenamiento seguro si cumplen todos los requisitos seguro físicos de lo contrario se exige el almacenamiento seguro, por ej. con PGP, WinZip 9	La información de BT debe cifrarse tal como se define en los términos "Cifrado" y "Contraseña/frase de acceso" mencionados anteriormente.	La información de BT debe cifrarse tal como se define en los términos "Cifrado" y "Contraseña/frase de acceso" mencionados anteriormente.

5	**Almacenamiento seguro en Blackberry, Windows Mobile, dispositivos PDA, tabletas (iPads, etc.), teléfonos móviles y reproductores de MP3**	Está prohibido almacenar información interna en estos dispositivos a menos que el dispositivo lo suministre BT o sea una concesión aprobada por seguridad de BT. Estos dispositivos no deben configurarse para acceder a cuentas de correo electrónico BT.com (se permite el acceso al correo electrónico bt.com a través de webmail).	Está prohibido almacenar información confidencial en estos dispositivos a menos que el dispositivo lo suministre BT o sea una concesión aprobada por seguridad de BT. Estos dispositivos no deben configurarse para acceder a cuentas de correo electrónico BT.com (se permite el acceso al correo electrónico bt.com a través de webmail).	Está prohibido almacenar ISC en estos dispositivos.
6	**Almacenamiento seguro en:** **Soportes extraíbles como tarjetas de memoria, memoria flash, CD/DVD, discos duros USB, tarjetas digitales seguras, disquetes y otros dispositivos similares.**	La información de BT debe cifrarse cuando se almacene en dichos dispositivos tal como se define en los términos "Cifrado" y "Contraseña/frase de acceso" mencionados anteriormente.	La información de BT debe cifrarse cuando se almacene en dichos dispositivos tal como se define en los términos "Cifrado" y "Contraseña/frase de acceso" mencionados anteriormente.	Está prohibido almacenar ISC en estos dispositivos.
7	**Almacenamiento web/en línea o en cualquier instalación de almacenamiento de Internet**	Prohibido	Prohibido	Prohibido
8	**Colaboración web externa**	Cualquier plataforma MS LiveMeeting o Webjoin	Prohibido	Prohibido
9	**Envío mediante correo electrónico**	No se requiere cifrado.	Cifrado para los destinatarios (cuando el destino no es una dirección de correo electrónico de bt.com) según	Se requiere cifrado según los términos "Cifrado" y

			los términos "Cifrado" y "Contraseña/frase de acceso" definidos anteriormente.	"Contraseña/frase de acceso" definidos anteriormente.
10	**Reenvío automático de correo electrónico**	Prohibido	Prohibido	Prohibido
11	**Transmisión de red**	No se requiere cifrado.	Cifrado para la transmisión externa e interna, según los términos "Cifrado" y "Contraseña/frase de acceso" definidos anteriormente.	Cifrado para la transmisión externa e interna, según los términos "Cifrado" y "Contraseña/frase de acceso" definidos anteriormente.
12	**Transferencia de archivos**	Utilice la transferencia segura de archivos, como SFTP, XFB.	Utilice la transferencia segura de archivos, como SFTP, XFB.	Utilice la transferencia segura de archivos, como SFTP, XFB.
13	**Borrado/eliminación de datos**	Use las funcionalidades de eliminación de la aplicación o del sistema operativo.	Borre físicamente los datos sobreescribiendo todos los sectores al menos una vez con cadenas binarias aleatorias utilizando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD.	Borre físicamente los datos sobreescribiendo todos los sectores al menos una vez con cadenas binarias aleatorias utilizando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD.
14	**Eliminación o reutilización de equipos informáticos (con información de BT)** **Incluye, entre otros:** **- La eliminación de piezas** **- La destrucción de equipos del proveedor** **- Los requisitos de destrucción de copias de seguridad** **- Piezas del servidor que enviaron de vuelta al**	Utilice una solución de borrado de software verificable y probada en la que se emita un certificado formal para verificar el borrado. Cualquier equipo que no pueda borrarse debe ser destruido, debiendo recibirse/facilitarse una certificación formal con al menos un registro del número de serie del equipo como prueba del borrado.	Los discos (u otros soportes de almacenamiento, incluidos, entre otros, tarjetas compact flash, dispositivos SSD) se deben borrar sobreescribiendo todos los sectores con cadenas binarias aleatorias, al menos una vez, usando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD. Si no se puede conseguir el borrado o este no es correcto, entonces el disco	Los discos (u otros soportes de almacenamiento, incluidos, entre otros, tarjetas compact flash, dispositivos SSD) se deben borrar sobreescribiendo todos los sectores con cadenas binarias aleatorias, al menos una vez, usando un producto de software como, por ejemplo: Blancco HMG, o Blancco versión 5 si se emplean dispositivos SSD. Si no se puede conseguir el borrado o este no es correcto, entonces el

	fabricante para su reparación	La solución anterior no puede utilizarse con unidades de estado sólido (SSD) que deben destruirse y recibir/facilitar una certificación formal. Consulte BS EN 17513 para obtener más información.	(u otros soportes de almacenamiento, incluidos, entre otros, tarjetas compact flash, dispositivos SSD) deben destruirse con una funcionalidad de destrucción de discos. Debe emitirse un certificado formal para verificar el borrado o la destrucción.	disco (u otros soportes de almacenamiento, incluidos, entre otros, tarjetas compact flash, dispositivos SSD) deben destruirse con una funcionalidad de destrucción de discos. Debe emitirse un certificado formal para verificar el borrado o la destrucción.
15	**Impresión**	Utilice una impresora conectada al PC o esté presente junto a la impresora de red, mientras dura la impresión.	Utilice una impresora controlada con un PIN, una impresora conectada al PC o una impresora situada en una sala de acceso controlado. Compruebe cuál es la impresora que va a utilizar y no deje documentos en la bandeja de impresión.	Utilice una impresora controlada con un PIN, una impresora conectada al PC o una impresora situada en una sala de acceso controlado. Tenga cuidado cuando esté imprimiendo. Compruebe cuál es la impresora que va a utilizar y no deje documentos en la bandeja de impresión.
16	**Servicios postales/de mensajería entre BT y el proveedor**	Un único sobre.	Utilice sobres dobles y envíe por correo certificado solo al destinatario; no escriba "Confidencial" en el primer sobre.	Utilice sobres dobles y envíe por correo certificado solo al destinatario; no escriba "Estrictamente confidencial" en el primer sobre.
17	**Divulgación externa**	Busque la autoridad del contacto de seguridad de BT. Consulte el Anexo 3.	Busque la autoridad del contacto de seguridad de BT. Consulte el Anexo 3.	Busque la autoridad del contacto de seguridad de BT. Consulte el Anexo 3.
18	**Utilizado en formación, desarrollo o pruebas**	BT debe anonimizarlo respetando la guía BP001 de prácticas recomendadas para anonimizar datos de BT.	BT debe anonimizarlo respetando la guía BP001 de prácticas recomendadas para anonimizar datos de BT.	Prohibido

19	**Eliminación de papel**	Cortado con trituradoras de corte transversal.	Cortado con trituradoras de corte transversal.	Cortado con trituradoras de corte transversal a 4 x 15 mm.
20	**Zonas públicas**	No hable sobre información interna en público.	No hable sobre información confidencial en público. No trabaje con documentos en espacios públicos donde se le pueda espiar.	No hable sobre información estrictamente confidencial en público. No trabaje con documentos en espacios públicos.