Public (Público)

PROTEÇÃO DA BT

Norma de Manipulação de Dados e Classificação de Informações do Terceiro

Norma: 4.0 **Proprietário:** BT Security

Esta norma define os controlos básicos de segurança para os nossos terceiros que armazenarão, tratarão ou acederão a informações da BT.

Aplica-se a todos os terceiros que trabalham para ou em nome do Grupo BT, incluindo Openreach, EE e PlusNet. Para simplificar, basta dizer "BT" no resto do documento.

Introdução

A BT classifica os dados e as informações em categorias, com base nos danos que possam resultar da perda ou divulgação não autorizada. Aquando da sua criação, todos os dados e informações são avaliados para determinar a categoria de classificação apropriada.

Os dados e informações terão de ser retidos durante um período adequado para atender aos requisitos legais, regulamentares e comerciais, sendo que no final deste período são eliminados com segurança. Qualquer equipamento que armazene dados também terá de ser eliminado no final da sua vida útil. A eliminação do equipamento terá de ser realizada da forma mais adequada para o ambiente.

Esta norma define os requisitos para classificação, rotulagem, manuseamento / tratamento, retenção e eliminação de ativos de informação e dados da BT.

Definição de termos:

Período	Explicação
terá de	Esta palavra, ou os termos "NECESSÁRIO" ou "DEVERÁ", significa que a definição é um requisito absoluto
não poderá	Esta expressão, ou a expressão "NÃO DEVERÁ", significa que a definição é uma proibição absoluta
poderá	Esta palavra, ou o adjetivo "OPCIONAL", significa que um item é verdadeiramente opcional
deverá	Esta palavra, ou o adjetivo "RECOMENDADO", significa que, em certas situações, há um motivo válido para ignorar um item específico, mas as implicações serão totalmente entendidas e cuidadosamente avaliadas antes de escolher uma opção diferente.
não deverá	Esta expressão ou a expressão "NÃO RECOMENDADO" significa que serão feitos todos os esforços para atender aos requisitos de um controlo, mas nem sempre será possível evitar que a ação seja descrita em todos os casos.Quando um controlo não puder ser respeitado, as implicações serão avaliadas e totalmente entendidas.
BT	Este termo significa o Grupo BT, incluindo Openreach, EE e Plusnet. Para simplificar, basta dizer "BT" no resto do documento.

Âmbito

Esta norma aplica-se a todos os dados e informações da BT em todos os formatos. Isto inclui todo o papel, documentos eletrónicos, multimédia (fotos, vídeo, WebEx, etc.), informações verbais (conversas telefónicas / correio de voz) e de dados mantidas nos sistemas, aplicações ou equipamentos com capacidade de armazenamento, tratamento ou transmissão de dados. O âmbito desta norma abrange a classificação, rotulagem, manuseamento / tratamento, retenção e eliminação de informações.

O que está incluído neste documento?

1. Descrição Internal (Geral) da classificação de informações.

Nem todas as informações que serão mantidas ou tratadas por si como terceiro em relação à BT terão o mesmo valor ou sensibilidade. Será da responsabilidade da BT classificar as informações no âmbito do serviço que fornecerá para garantir que o nível correto de proteção é aplicado às informações e que tais informações são tratadas de forma eficiente e segura.

O esquema de classificação da BT possui as quatro categorias abaixo:

- Public (Público)
- Internal (Geral)
- Confidential (Confidencial)
- Highly Confidential (Altamente Confidential)

Se não foi informado sobre a classificação das informações que está a manipular, entre em contacto com a sua parte interessada da BT ou com o responsável pelas compras.

2. Níveis de classificação BT.

Public (Público)

Informações que foram especificamente aprovadas para publicação Internal (Geral). Não há requisitos especiais de manuseamento associados às informações desta classificação

Alguns exemplos são: Detalhes dos nossos produtos e serviços, informações publicadas no site externo da BT, boletins de imprensa, livros brancos, materiais publicitários.

Internal (Geral)

Informações cuja divulgação não autorizada, principalmente fora da BT, seria inadequada. Não considerado como sendo do interesse da BT a sua divulgação ao domínio Public (Público). Estas informações poderão estar limitadas a equipas ou funções específicas da empresa.

Nota: Quando acedida e/ou armazenada por um terceiro, a classificação de manipulação muda para "Confidential (Confidencial)"

Alguns exemplos são: Informações de funcionários e negócios na intranet, maioria das políticas, normas, processos e procedimentos da BT, maioria da documentação relacionada com o projeto e maioria das atas para reuniões

Confidential (Confidential (Confidencial))

A divulgação não autorizada destas informações, mesmo dentro da organização, poderá causar danos significativos para os interesses da BT. Estas informações estão reservadas para indivíduos autorizados a desempenhar uma necessidade comercial específica como parte da sua função e só podem ser partilhadas com os mesmos. O dano poderá resultar em perda financeira, perda de rentabilidade ou oportunidade, constrangimento, perda de reputação ou uma sanção legal ou regulamentar contra a BT. As informações pessoais, a propriedade intelectual e as informações sobre cartões de pagamento são classificadas como "Confidenciais".
As informações confidenciais têm requisitos de manipulação específicos que terão de ser respeitados.

Alguns exemplos são: Informações pessoais sobre o nosso pessoal, terceiros ou clientes (incluindo pagamentos financeiros relacionados), como: Contratos de funcionários, dados de desempenho, inquéritos CARE, identificador de serviço pessoal (ID de serviço, identificador de banda larga, identificador PSTN). Alguma documentação de projeto relacionada com infraestruturas ou projetos críticos, diagramas de rede, contratos com fornecedores do terceiro. Dados de registo do sistema; dados de vendas e marketing (alterações às tarifas antes do lançamento, desempenho financeiro antes da publicação nos mercados); planos de negócios locais; dados de risco; registos de dados de

Highly Confidential (Altamente Confidential)

A divulgação destas informações provavelmente afetará negativamente a consecução dos principais objetivos de negócios. Estas informações são excecionalmente sensíveis em termos da sua capacidade para causar danos graves caso sejam reveladas. As informações altamente confidenciais estão limitadas a um pequeno número de indivíduos. Terá de haver uma negação absoluta do acesso a pessoas não autorizadas. Os requisitos de manuseamento são mais rigorosos que os de manipulação de informações confidenciais. Esta classificação é a mais restritiva devido aos danos muito graves que poderão ocorrer. Poderá ser-lhe solicitado que assine um contrato de não divulgação (CND) ou uma "lista de

Alguns exemplos são: Palavras-passe de computador, um registo de riscos de segurança, certas informações pessoais sensíveis, como informações de cartões de pagamento, número nacional de seguro e detalhes do passaporte. Informações confidenciais de RH que possam alienar um número significativo de funcionários, planos estratégicos de negócios, estratégia competitiva, novos produtos estratégicos e novas políticas de marketing, avaliações de parceiros, concorrentes ou contratantes muito sensíveis, utilização da Internet, número de conta do cliente, relatórios ou descobertas de auditoria que contenham detalhes de deficiências / vulnerabilidades graves nas práticas ou processos da BT, informações que possam afetar o preço das nossas ações, incluindo atas do conselho, informações confidenciais sobre preços, informações relacionadas com fusões e aquisições, eventos de segurança, chaves de

detentores de informações privilegiadas", caso lide com estas informações.

3. Requisitos de manuseamento e tratamento.

Nota: Quando não especificamente mencionado, não há requisitos especiais de manuseamento associados às informações com um nível de classificação "Public (Público)".

3.1 Manuseamento de voz e multimédia.

Referência	O que pretende fazer com as informações	Classificação	Requisitos de manuseamento
HSMS10	Quero publicar informações nas redes sociais / profissionais	Public (Público)	Poderá publicar em qualquer grupo como, por exemplo, Splash ou Yammer. Não poderá fazer contribuições para sites nem publicar declarações online que possam ser razoavelmente atribuídas como pontos de vista da BT.
		Internal (Geral) / Confidential (Confidencial)	Não permitido.
		Highly Confidential (Altamente Confidential)	Não permitido
HSMS20	Quero discutir com ou apresentar alguém através de mensagens instantâneas internas usando, por exemplo, o Microsoft Lync	Internal (Geral) / Confidential (Confidencial)	Poderá usar Internal/BT Live Meeting, Webex, Webjoin e Skype for Business. Verifique se selecionou e confirmou que possui as pessoas corretas antes de discutir um tópico específico e tenha em mente que o seguinte não pode ser divulgado: · **Quaisquer informações do cartão de pagamento.** · **Dados pessoais** · **Dados bancários.** · **PIN ou qualquer outra palavra-passe.**
		Highly Confidential (Altamente Confidential)	Não permitido.
HSM30	Quero discutir com alguém através de ferramenta de conversação externa ao vivo. por exemplo, num site de suporte a fornecedores, como a Cisco	Public (Público)	As conversas terão de se limitar a "informações públicas" disponíveis gratuitamente no nosso site externo da BT
		Internal (Geral) / Confidential (Confidencial)	Só é permitido depois de verificar que a pessoa ou as pessoas com quem está a conversar têm "necessidade de saber" antes de revelar quaisquer informações confidenciais de uma ou várias pessoas, e o seguinte não poderá ser divulgado:

			· **Quaisquer informações do cartão de pagamento.** · **Dados pessoais** · **Dados bancários.** · **PIN ou qualquer outra palavra-passe.**
		Highly Confidential (Altamente Confidential)	Não permitido.
HSM40	Quero discutir com alguém por telefone / pessoalmente	Internal (Geral) / Confidential (Confidencial)	Terá de verificar se a identidade da pessoa com quem está a falar tem uma "necessidade de saber" antes de discutir quaisquer informações confidenciais (incluindo conversas na loja e centrais de atendimento). Se aplicável, terá de estar em vigor um CND antes do início da conversa. Certifique-se de que a conversa não pode ser ouvida por pessoas que não necessitam de tomar conhecimento da mesma. Não poderá deixar estas informações nos sistemas de correio de voz.
		Highly Confidential (Altamente Confidential)	Como "Confidential (Confidencial)". Reduza as informações "altamente confidenciais" ao mínimo absoluto.
HSM50	Quero enviar texto para todas as partes (internamente e externamente)	Public (Público)	O conteúdo da mensagem terá de se limitar a "informações públicas" disponíveis gratuitamente no nosso site externo da BT.
		Internal (Geral) / Confidential (Confidencial)	O conteúdo da mensagem está limitado à "necessidade de conhecer" e as seguintes informações não poderão ser divulgadas: · **Quaisquer informações do cartão de pagamento.** · **Dados bancários.** · **PIN ou qualquer outra palavra-passe.** · **Quaisquer informações pessoais.**
		Highly Confidential (Altamente Confidential)	Não permitido.

3.2 Manuseamento de documentos em papel.

Referência	O que pretende fazer com as informações	Classificação	Requisitos de manuseamento
HPD10	Quero armazenar, copiar, imprimir ou trabalhar com informações impressas no escritório.	Internal (Geral) / Confidential (Confidencial)	As informações da BT não deverão ser usadas em cópia impressa, a menos que tal faça especificamente parte do âmbito do trabalho ou seja aprovado pelas partes interessadas da BT; assim sendo, aplica-se o seguinte: Terão de ser protegidas contra uma divulgação acidental. Terão de ser apagadas quando não estiverem em utilização e, no fim do expediente, armazenadas numa área restrita a funcionários autorizados como, por exemplo, um cacifo, uma gaveta trancada ou uma sala de entrada restrita. Use uma impressora controlada por acesso, uma impressora ligada a um PC ou uma impressora numa sala de acesso controlado e verifique se está a enviar o documento para a impressora correta. Terá de usar a função de impressão segura para recuperar o material impresso na impressora, a menos que garanta a recolha imediata.
		Highly Confidential (Altamente Confidential)	Não permitido
HPD20	Quero imprimir enquanto estiver num edifício da BT	Internal (Geral) / Confidential (Confidencial)	Verifique se está a enviar o documento para a impressora certa e não deixe documentos na bandeja de impressão. Use uma impressora controlada por acesso, uma impressora ligada a um PC ou uma impressora numa sala de acesso controlado.
		Highly Confidential (Altamente Confidential)	Como "Internal (Geral) / Confidential (Confidencial)"

HPD30	Quero copiar ou imprimir informações que não estejam nas nossas instalações do terceiro ou em minha casa (por exemplo, em instalações de subcontratantes, num hotel, etc.)	Internal (Geral) / Confidential (Confidencial)	Não permitido.
		Highly Confidential (Altamente Confidential)	Não permitido.
HPD40	Desejo transportar informações impressas para fora de um escritório da BT, de instalações do terceiro ou de uma loja	Internal (Geral) / Confidential (Confidencial)	**Não poderá remover os dados do cliente e/ou pagamento da BT dos escritórios, instalações ou lojas do terceiro.** Outros tipos de informações também não poderão ser removidos, a menos que tal faça especificamente parte do âmbito do trabalho ou tenha sido aprovado pela parte interessada da BT; assim sendo, aplica-se o seguinte: Terá de lidar com o dever de diligência. Terá de se proteger contra comprometimentos acidentais; por exemplo, levar numa pasta ou bolsa opaca. Não poderá deixar as informações sem vigilância. Em caso de perda, terá de criar um incidente de segurança e notificar a sua parte interessada da BT o mais rápido possível.
		Highly Confidential (Altamente Confidential)	Não permitido

HPD50	Quero partilhar ou enviar informações em papel para partes internas.	Internal (Geral) / Confidential (Confidencial)	As informações da BT não deverão ser usadas em cópia impressa, a menos que tal faça especificamente parte do âmbito do trabalho ou seja aprovado pelas partes interessadas da BT; então, aplica-se o seguinte: Terá de colocar o documento num envelope de utilização interna ou num envelope sem janelas e entregá-lo em mão ou por correio usando o sistema de correio Internal (Geral). Não poderá ser enviado para partes internas domésticas. Não indique o nível de classificação no envelope externo. Se as informações estiverem cobertas por "privilégio legal", siga as suas diretrizes de privilégio legal Se se perderem, terá de levantar um incidente de segurança e avisar a parte interessada da BT assim que possível.
		Highly Confidential (Altamente Confidential)	Não permitido
HPD60	Quero partilhar ou enviar informações em cópia impressa a partes externas	Internal (Geral) / Confidential (Confidencial)	Não permitido
		Highly Confidential (Altamente Confidential)	Não permitido
HPD70	Quero enviar um fax	Internal (Geral) / Confidential (Confidencial)	Terá de enviar a página de cabeçalho com uma página de teste e entrar em contacto com o destinatário para confirmar a receção antes de enviar o conteúdo por fax. Se as informações estiverem cobertas por "privilégio legal", siga as suas diretrizes de privilégio legal.
		Highly Confidential (Altamente Confidential)	Não permitido

HPD80	Quero eliminar informações impressas	Internal (Geral) / Confidential (Confidencial)	Terá de verificar se as informações não precisam de ser retidas por razões legais ou regulamentares. O documento terá de ser triturado no mínimo de acordo com a norma P4 DIN66399 usando um triturador de corte cruzado (isto inclui informações do cartão de pagamento). Nunca coloque num caixote do lixo normal.
		Highly Confidential (Altamente Confidential)	Não deverá possuir esta classificação de informações em cópia impressa; no entanto, se a possuir, aplica-se o indicado em seguida. Terá de verificar se as informações não precisam de ser retidas por razões legais ou regulamentares. O documento terá de ser triturado no mínimo de acordo com a norma P4 DIN66399 usando um triturador de corte cruzado (isto inclui informações do cartão de pagamento) ou poderá ser incinerado em conformidade com a BS EN15713: 2009. Nunca coloque num caixote do lixo normal. **Nota: Certas informações poderão exigir que o material seja triturado no local por um terceiro certificado externo. Neste caso, terá de obter um certificado de destruição junto do terceiro.**

3.3 Manuseamento de documentos eletrónicos.

Referência	O que pretende fazer com as informações	Classificação	Requisitos de manuseamento
HED10	Quero armazenar informações eletrónicas no meu computador portátil / PC fornecido pela empresa	Todos os dados da BT	As cópias de trabalho só poderão ser mantidas no seu computador portátil de trabalho se este tiver encriptação de disco total, por exemplo, através de um produto como o Bitlocker. Este converte as informações em código ilegível que não poderá ser decifrado facilmente por pessoas não autorizadas. Os documentos concluídos terão de ser armazenados com segurança e as cópias de trabalho removidas do computador portátil.
HED20	Quero armazenar os meus documentos no sistema de gestão de documentos, por exemplo, no SharePoint ou numa unidade de rede	Internal (Geral) / Confidential (Confidencial)	Restrinja quem poderá editar o site e os documentos apenas às pessoas com aprovação. O sistema de gestão de documentos / proprietário ou administrador da unidade de rede terá de: - Usar níveis e grupos de autorização para configurar o controlo de acesso baseado na função. Estes terão de ser configurados para não mais do que o nível mínimo necessário para que as pessoas façam o seu trabalho. - Rever os controlos de acesso todos os anos. - Documentar o processo para designar pessoas para funções. - As funções e pessoas designadas terão de ser revistas em intervalos regulares, de preferência trimestralmente. **NOTA: os sistemas de gestão de documentos ou unidades de rede não poderão ser usados para armazenar informações de cartões de pagamento**

		Highly Confidential (Altamente Confidential)	Como "Internal (Geral) / Confidential (Confidencial)" e: Os documentos terão de ser encriptados antes do carregamento para o sistema de gestão de documentos. Também deverá definir uma data em que o acesso ao seu documento será revogado. **NOTA: os sistemas de gestão de documentos ou unidades de rede não poderão ser usados para armazenar informações de cartões de pagamento**
HED30	Desejo armazenar informações eletrónicas na nuvem ou em Serviços de Internet (quando não exista um contrato comercial para hospedar informações da BT), como Google docs, Github, Drop Box, Pastebin, Facebook, etc.	Todos os dados da BT	Não permitido.
HED40	Quero armazenar suportes eletrónicos ou amovíveis (por exemplo, uma pendrive)	Todos os dados da BT	Permitido apenas se tiver uma necessidade empresarial autorizada de transportar informações da BT para fora do escritório, mas todos os dispositivos ou informações terão de ser encriptados. Em caso de perda, terá de criar um incidente de segurança e notificar a parte interessada da BT o mais rápido possível. **NOTA: os suportes amovíveis não poderão ser usados para armazenar informações de cartões de pagamento**
HED50	Quero armazenar documentos ou informações eletrónicas no meu computador portátil ou dispositivo pessoal.	Todos os dados da BT	Não permitido.
HED60	Quero enviar documentos eletrónicos para o meu endereço de e-mail pessoal	Todos os dados da BT	Não permitido.

HED70	Quero encaminhar automaticamente para um endereço de e-mail externo	Todos os dados da BT	Não permitido.
HED80	Quero partilhar ou enviar documentos eletrónicos para partes internas	Internal (Geral) / Confidential (Confidencial)	Só deverá partilhar informações internas / confidenciais da BT com partes internas quando estas precisarem de as conhecer para desempenharem a sua função e: · Deixe claro que o e-mail contém informações internas / confidenciais da BT. · Use as definições de sensibilidade para assinalar o e-mail como Confidential (Confidencial). · Defina as permissões para "Não encaminhar". **NOTA: As informações de cartões de pagamento nunca deverão ser mantidas num PC, mas, caso tal seja necessário - incluindo o envio por e-mail - terão de estar sempre encriptadas.**
		Highly Confidential (Altamente Confidential)	Só deverá partilhar informações altamente confidenciais da BT com partes internas quando estas precisarem de as conhecer para desempenharem a sua função e: · Deixar claro que o e-mail contém informações altamente confidenciais da BT. · Use as definições de sensibilidade para assinalar o e-mail como Highly Confidential (Altamente Confidential). · Defina idealmente as permissões para "Não encaminhar" · Use o E-mail seguro para enviar (se não estiver disponível, terá de encriptar as informações). **NOTA: As informações de cartões de pagamento nunca deverão ser mantidas num PC, mas, caso tal seja necessário - incluindo o envio por e-mail - terão de estar sempre encriptadas.**

HED90	Quero partilhar ou enviar documentos eletrónicos para uma parte externa	Todos os dados da BT	Só terá de efetuar o envio ou partilha com uma parte externa quando houver uma necessidade comercial aprovada ou outra justificação, como um CND. · A partilha ou o envio só terão de ser efetuados para uma parte externa com base na necessidade de saber quando exista uma necessidade comercial, contratual ou legislativa aprovada e com a aprovação da parte interessada da BT. - Verifique se todos os documentos ou e-mails mostram o nível de classificação dos dados. · Terá de garantir que a parte externa conhece o nível de classificação do documento e está ciente dos requisitos de proteção. · Terá de encriptar as informações · Terá de confirmar que está a enviar para o endereço de e-mail correto. - Continua a ter de respeitar as diretrizes de privilégio legal, se aplicável.
HED91	Desejo enviar um e-mail a um grande grupo de funcionários da BT (mais de 100), (por exemplo, para inquéritos, formação, benefícios)	Internal (Geral) / Confidential (Confidencial)	Terá de respeitar o nosso guia do terceiro sobre o envio instruções por e-mail
		Highly Confidential (Altamente Confidential)	Não permitido
HED100	Quero transferir internamente um documento ou informações da BT sem utilizar e-mail, Skype / Lync for Business ou suportes amovíveis (por exemplo, porque o ficheiro é muito grande)	Todos os dados da BT	Poderá usar um recurso de transferência de ficheiros da Internet aprovado para utilização pela sua própria Política de Segurança. Terá de encriptar o documento na origem antes de fazer o carregamento.

HED110	Quero transferir externamente um documento ou informações da BT sem utilizar e-mail, Skype / Lync for Business ou suportes amovíveis (por exemplo, porque o ficheiro é muito grande)	Internal (Geral) / Confidential (Confidencial)	Só terá de efetuar o envio ou partilha com uma parte externa quando houver uma necessidade comercial aprovada ou outra justificação, como um CND. · Só terá de partilhar ou enviar para uma parte externa com base na necessidade de conhecer onde existe uma necessidade comercial, contratual ou legislativa aprovada e com a aprovação do autor ou do proprietário do documento. · Os dados terão de ser protegidos enquanto estiverem no ambiente externo para evitar perda de Confidential (Confidencial)idade, integridade ou disponibilidade. · Terá de encriptar as informações antes de serem enviadas ou ao longo da ligação entre o seu ambiente e o ambiente externo. - Verifique se todos os documentos mostram o nível de classificação de dados. · Confirme que está a enviar para o destinatário correto. · Use um protocolo de transferência de rede padrão, como FTP.

		Highly Confidential (Altamente Confidential)	Só terá de efetuar o envio ou partilha com uma parte externa quando houver uma necessidade comercial aprovada ou outra justificação, como um CND. · A partilha ou o envio só terão de ser efetuados para uma parte externa com base na necessidade de saber quando exista uma necessidade comercial, contratual ou legislativa aprovada e com a aprovação da parte interessada da BT. · Terá de usar a encriptação de ponta a ponta para proteger os dados da origem (o seu sistema) ao destino (sistema externo) e estáticos quando estiver no sistema do terceiro, de acordo com os requisitosda Secção Norma do terceiro 11. - Verifique se todos os documentos mostram o nível de classificação de dados. · Confirme que está a enviar para o destinatário correto. · Use um protocolo de transferência de rede padrão, como FTP.
HED120	Quero fazer uma cópia de segurança dos meus documentos eletrónicos	Todos os dados da BT	· Só deverá armazenar documentos da BT em locais como unidades de rede ou sistemas de gestão de documentos aprovados para utilização pela sua própria equipa do INFOSEC. (Se a única opção for usar suportes amovíveis, o dispositivo terá de ser encriptado) · Todo o conteúdo terá de ser encriptado ou protegido por palavra-passe.
HED130	Quero eliminar documentos eletrónicos	Todos os dados da BT	Os documentos mantidos no SharePoint e nas unidades de rede terão de ser eliminados usando a função de eliminação padrão do

			Windows. Os caixotes do lixo para reciclar terão de ser esvaziados pelo menos uma vez por semana. (Isto não se aplica aos ambientes Citrix como, por exemplo, back-office de retalho e centros de atendimento no estrangeiro, pois nestes casos a gestão e feita automaticamente). Os e-mails terão de ser eliminados quando já não forem necessários.
HED140	Pretendo eliminar ou reutilizar equipamentos de TI que contenham informações da BT confidenciais / altamente confidenciais como, por exemplo, peças, equipamentos do terceiro, cópias de segurança, peças de servidor enviadas para reparação	Todos os dados da BT	Poderão ser utilizados serviços de trituração para muitos tipos de suportes e hardware como, por exemplo, disco rígido, fita magnética, microficha, CD / DVD, placas de circuito, telefonia móvel Terá de guardar um registo do equipamento destruído. Poderão ser utilizados serviços de eliminação de dados para equipamentos a reutilizar. Terá de registar um equipamento em que os dados tenham sido apagados e obter um certificado de eliminação de dados. Sempre que o equipamento tiver contido dados do governo do Reino Unido, **TERÁ DE** usar-se o Blanco, pois este é o único produto certificado.
HED150	Quero eliminar os dados do sistema e da aplicação	Todos os dados da BT	Os dados terão de ser apagados a um nível que não permita a sua recuperação.De preferência, usando o método baseado em softwareData Erasure (às vezes denominado de limpeza de dados, eliminação de dados ou destruição de dados) para substituir os dados. As cópia de seguranças que precisem de ser retidas para efeitos legais e

			regulamentares não deverão ter uma utilização diária.

3.4 Sistema de manuseamento e dados de aplicações (dados eletrónicos).

Os dados eletrónicos incluem todos os dados e informações mantidos em sistemas ou aplicações geridos pelo departamento de Tecnologia ou por unidades de negócio individuais como, por exemplo, armazenamento de dados ou sistema de faturação.
Os extratos de dados de uma aplicação ou sistema recebidos por uma pessoa terão de ser tratados como um documento eletrónico (consulte a Secção 6.3).

Referência	O que pretende fazer com os dados e informações	Classificação	Requisitos de manuseamento
HSADE	Desejo armazenar e tratar dados e informações eletrónicas da BT num centro de dados (incluindo terceiros e nuvem)	Todas as informações da BT	Terá de seguir os controlos na norma do terceiro Se os dados incluírem informações de cartões de pagamento, estas terão de ser mantidas de acordo com os requisitos do PCI DSS. Se os dados incluírem dados de contas bancárias, por serem especialmente sensíveis,também serão aplicados os seguintes controlos. 1. As contas bancárias terão de ter tokens para indivíduos (contas bancárias pessoais de clientes e funcionários). 2. Ao exibir os detalhes reais de uma conta bancária a um agente como parte de um processo comercial (por exemplo, para verificar a conta correta a cobrar ou ao comunicar com um cliente, por exemplo por e-mail ou fatura), só terá de mostrar os últimos quatro dígitos da conta bancária (ou seja, dados da conta bancária mascarada). 3. Se for necessário aceder à conta bancária completa (por exemplo, para ativar uma solicitação de crédito ou

			débito de um banco), será necessário remover os tokens dos dados bancários ou estes deverão ser desencriptados e depois enviados para o banco usando um mecanismo de transporte encriptado. Imediatamente após a utilização, os dados bancários não encriptados ou sem token terão de ser eliminados em segurança.
HSAD1	Desejo armazenar e tratar dados e informações eletrónicos da BT num sistema ou numa aplicação do terceiro	Todos os dados	· Todas as informações confidenciais / altamente confidenciais e pessoais terão de ser encriptadas. · Informações de cartões de pagamento - terão de ser encriptadas de acordo com os requisitos do PCI DSS.
HSAD2	Desejo enviar dados e informações eletrónicos dentro de uma rede do terceiro ou externamente	Todos os dados da BT	O material terá de ter a aprovação das partes interessadas da BT para ser libertado. Os terceiros terão de ter um CND ou contrato adequado em vigor. A transferência de dados terá de ser encriptada. Quando tenham de ser enviadas informações confidenciais / altamente confidenciais, incluindo dados pessoais, para fora da sua rede para um terceiro, terá de ser implementado um "Contrato de Tratamento de Dados".

4. Retenção de informações.

O terceiroterá de ter uma "Política de Retenção de Dados" que apoie este "Programa de Retenção de Informações" específico, na qual os períodos de retenção deverão estar definidos para que as informações da BT sejam retidas. (O período de retenção deverá durar o tempo necessário para a execução do Contrato, após o qual deverá ser retido por um máximo de dois anos, a menos que tenha sido acordado um período de retenção diferente entre a BT e o terceiro ou qualquer lei aplicável tenha uma exigência diferente.)

Informações da BT - em qualquer forma, digitalmente ou em registos e não-registos físicos, como todas as cópias de trabalho, rascunhos, notas informais, e-mails indesejados ou outras formas de armazenamento (por exemplo, microfichas / microfilmes, películas fotográficas, cassetes de vídeo ou áudio).

5. Eliminação de equipamentos.

Qualquer equipamento que possa armazenar dados, incluindo componentes informáticos, terá de ser tratado como um ativo de informação. Exemplos de "Ativos de informação" poderão ser encontrados no Glossárioabaixo.
Todo o equipamento terá de ser eliminado no final da sua vida útil. Exemplos de fim de vida são os seguintes:

- Está com falhas
- Foi retirado (retirado do serviço ou desnecessário)
- Foi usado num julgamento ou prova de conceito

5.1 Requisitos de eliminação do terceiro.

Isto aplica-se a:

- Qualquer agência subcontratada ou do terceiro.
- Qualquer terceiro que execute serviços de manutenção em equipamentos da BT onde os ativos de informação possam ser removidos e substituídos como parte de tal serviço.
- Qualquer terceiro que forneça serviços terceirizados à BT quando estiverem dados da BT presentes nos equipamentos ou ficheiros do terceiro.
- Qualquer agência de eliminação de resíduos que elimine equipamentos da BT.

Referência	O que pretende fazer com os dados e informações	Classificação	Requisitos de manuseamento
EDR10	Quero eliminar equipamentos com dados da BT.	Todos os dados da BT	Unidades de disco rígido (HDD) - desintegração, incineração ou limpeza através de padrão de múltiplas passagens
			Unidade de Estado Sólido (SSD) - Limpeza através de padrão de múltiplas, desintegração
			CD-R / DVD-R, CD-RW / DVD-RW, BD-R, BD-RE, BD-RE - Abrasão, desintegração, incineração
			Fita magnética - Desmagnetização, desintegração, incineração
			Unidades de disco flash e USB - desmagnetização, desintegração e limpeza através de padrão de múltiplas passagens
			SIMS - corte em várias partes (através do contacto de metal) para que se tornem ilegíveis.

6. Requisitos de auditoria.

6.1 Requisitos de auditoria de eliminação de dados e informações

Terão de ser mantidos registos completos de retenção e eliminação de dados que forneçam uma pista de auditoria, evidências e rastreamento. Isto terá de incluir:

- Prova de destruição e/ou eliminação (incluindo data de realização e método usado)
- Registos de auditoria do sistema para eliminação.
- Certificados de eliminação de dados.
- Quem realizou a eliminação (incluindo quaisquer parceiros de eliminação / terceiros ou contratantes)?
- Terá de ser gerado um relatório de destruição e verificação para confirmar o sucesso ou a falha de qualquer processo de destruição / eliminação. (ou seja, um processo de substituição terá de fornecer um relatório a indicar todos os setores que não puderam ser apagados).

6.2 Requisitos de auditoria de eliminação de equipamentos

Terá de ser fornecida uma pista de auditoria para os seguintes tipos de equipamento:

- Suporte amovível.
- Unidades de disco.
- Fitas de cópia de segurança.
- Componentes informáticos (Ver glossário).

Terão de existir registos completos para fornecer uma pista de auditoria para incluir como mínimo:

- O nome da aplicação ou serviço que utilizou este equipamento.
- Tipo de equipamento como, por exemplo, computador de secretária, computador portátil, servidor, fita, router, etc.
- Número de discos rígidos que o equipamento contém (se aplicável).
- Equipamento identificado pelo número de série.
- Componentes do equipamento identificados pelo número de série.
- Rastreamento completo de ativos de todos os equipamentos e partes de componentes durante todo o ciclo de vida útil do equipamento.
- Prova de destruição e/ou eliminação (incluindo data de realização e método usado)
- Detalhes de quem realizou a eliminação (incluindo quaisquer parceiros de eliminação / terceiros / contratantes para eliminação de resíduos).
- Terá de ser gerado um relatório de destruição e verificação para confirmar o sucesso ou falha de qualquer processo de reciclagem / sanitização ou destruição. Por exemplo, um processo de substituição terá de fornecer um relatório a indicar todos os setores que não puderam ser apagados. Estes relatórios deverão incluir a capacidade, a marca, o modelo e o número de série dos suportes.

7. Glossário.

Período	Explicação
Terceiros	Qualquer empresa envolvida no tratamento de dados / informações da BT e no manuseamento de equipamentos da BT terá de respeitar esta norma. Isto inclui: · Qualquer agência terceirizada ou subcontratada · Qualquer terceiro que realize serviços de manutenção em equipamentos da BT, onde os ativos de informação possam ser removidos e substituídos como parte de tal serviço · Qualquer terceiro que forneça serviços terceirizados à BT, onde os dados da BT residam em equipamentos ou ficheiros do terceiro · Qualquer agência de eliminação de resíduos que elimine equipamentos da BT
AES	Norma de encriptação avançada
Chaves assimétricas	A criptografia assimétrica, também conhecida como encriptação de chave pública, usa chaves públicas e privadas para encriptar e desencriptar dados. As chaves são simplesmente números grandes que foram emparelhados, mas que não são idênticos (assimétricos). Uma chave no par poderá ser partilhada com todos; esta é denominada de chave pública.
Dados BT	Todos os dados pertencentes à BT ou licenciados pela mesma para operar como uma sociedade anónima no Reino Unido ou numa das suas subsidiárias globais.
CDP	Ponto de distribuição da lista de revogação de certificados
CESG	O grupo de segurança de comunicações eletrónicas do governo do Reino Unido.
componentes informáticos	Controladores de disco rígido, controladores de unidade de CD-ROM, controladores de unidade de DVD, placas de interface Ethernet, controladores de ecrã de computador e impressoras de rede.
CRL	Lista de revogação de certificado
cliente	Uma pessoa ou organização que obtenha, tenha obtido ou a BT ou as suas marcas considerem que seja provável que obtenha produtos ou receba ofertas de produtos ou serviços.
dados do cliente	Quaisquer dados pertencentes a clientes das marcas operadas pela BT.
dados	Palavras, números, datas, imagens, som, etc. sem contexto.
eliminação de dados	A eliminação de dados é a destruição de todos os dados e informações não são classificados como um registo permanente.
ciclo de vida dos dados	O ciclo de vida dos dados abrange a forma como os dados são recolhidos, armazenados, manipulados, tratados, transmitidos e destruídos.

período de retenção de dados	Este é o período (que poderá ser permanente) em que um tipo de dados ou informações é mantido / armazenado antes de poder ser destruído ou eliminado. Durante este período, estes dados poderão ser arquivados se permanecerem acessíveis até ao final do período de retenção de dados.
DEK	chave de encriptação de dados
dados eletrónicos	Dados eletrónicos são definidos como todos os dados e informações mantidos em sistemas ou aplicações geridos pelo departamento de Tecnologia ou por unidades de negócio individuais como, por exemplo, armazenamento de dados ou sistema de faturação.
Chaves de curva elíptica	Criptografia de curva elíptica. A criptografia de curva elíptica (ECC) é uma abordagem da criptografia de chave pública baseada na estrutura algébrica das curvas elípticas sobre campos finitos. A ECC requer chaves menores em comparação com a criptografia não-CE (com base em campos simples de Galois) para fornecer segurança equivalente
encriptação	Conversão de dados num código secreto para que a leitura não possa ser efetuada por uma pessoa não autorizada.
Entropia	Uma medida da aleatoriedade dos dados; a chave de 128 bits poderá ter um máximo de 128 bits de entropia ou um mínimo de 1.
GCM	Mensagens na nuvem do Google
HSMs	Módulos de segurança de hardware
registo inativo	Um registo poderá ter um estado ativo ou inativo. Quando um registo ativo expira ou já não é necessário: por exemplo, quando um cliente sai da BT, o registo do cliente torna-se inativo e quando um funcionário deixa a BT, o seu registo de RH fica inativo.
informações	Um conjunto de palavras, números, datas, imagens, sons, etc., inseridos no contexto, por exemplo, para lhes dar significado.
ativo de informação	Qualquer equipamento que possa armazenar dados é definido como um "ativo de informação". Alguns exemplos incluem o seguinte: Unidades de disco (estado sólido e magnéticas), suportes amovíveis (por exemplo, disquetes, USBs, DVDs, CDs, cartões de memória interna, cartões flash e cartões SD), fitas de cópia de segurança, cartões SIM para telemóvel. Componentes informáticos como, por exemplo, controladores de disco rígido, controladores de unidade de CD-ROM, controladores de unidade de DVD, placas de interface Ethernet, controladores de ecrã de computador e impressoras de rede.
sistemas de informação	Um conjunto de hardware, software, dados, pessoas e procedimentos que trabalham juntos para produzir informações de qualidade.
KEK	chave de encriptação
CND	Acordo de Confidential (Confidencial)idade
NIST	National Institute of Standard and Technology (Instituto Nacional de Normas e Tecnologia)

Nonce	Um número aleatório gerado e usado apenas uma vez durante uma troca criptográfica, Internal (Geral)mente para autenticação.
não registos	Duplicados de originais e cópias de trabalho. Documentos Internal (Geral)s relacionados com questões não comerciais. Rascunhos de cartas, relatórios, folhas de cálculo e notas informais. Livros, manuais e outros materiais impressos obtidos de fontes externas à BT para material de referência. Spam e lixo eletrónico.
OCSP	Protocolo de estado de certificado online
escritório	Relacionado com qualquer loja da BT como, por exemplo, loja de retalho, central de atendimento, sede, site de comutação.
informações de cartões de pagamento	São informações relacionadas com uma conta usada pelo titular do cartão para efetuar pagamentos a um comerciante - os exemplos incluem, mas não apenas, o número da conta de pagamento (PAN), a data de validade e o CVV. Isto é regido pelo regulamento PCI / DSS.
dados pessoais	Informações relacionadas com qualquer indivíduo - incluindo, sem limitação, nome completo, data de nascimento, endereço, número de telefone, incluindo clientes e qualquer pessoa que trabalhe na BT.
PRNG	Geradores de números pseudoaleatórios
registos	Documentos mantidos como evidência de transações comerciais, decisões, atividades e e-mails da BT ou como resultado de obrigações legais. Isto também inclui dados e informações mantidos em sistemas ou aplicações, pois também contêm evidências de transações comerciais, produtos e serviços de EE.
RSA	Uma tecnologia de encriptação de chave pública desenvolvida pela RSA Data Security, Inc. O acrónimo significa Rivest, Shamir e Adelman
Salted hashes	Na criptografia, um salt é um dado aleatório usado como uma entrada adicional para uma função unidirecional que faz hash numa palavra-passe ou expressão secreta. Para obter mais informações, consulte o anexo c.
Chaves simétricas	Os algoritmos de chave simétrica são algoritmos para criptografia que usam as mesmas chaves criptográficas para encriptação de texto sem formatação e desencriptação de texto encriptado.
política de retenção ao nível do sistema	Uma diretiva no nível do sistema indica durante quanto tempo um sistema retém os dados para respeitar os planos de retenção de dados da empresa
TPM	Trusted Platform Module (Módulo de Plataforma Fiável)

8. Alterar histórico.

N.º da versão	Data	Alteração feita por	Breves detalhes da mudança
Rascunho 4.0	05/08/2018	Karen Tanner	Rascunho para substituir a atual versão 3
Edição 4.0	07/11/2019	Karen Tanner	Revisto e assinado

N.º da versão	Data	Alteração feita por	Breves detalhes da mudança

9. Aprovação de documento.

Nome	Função	Data
Ian Morton	Proprietário do documento versão BT	07/11/2019

10. Conformidade.

Apreciamos a grande maioria dos atos do terceiro profissionalmente e em consonância com os valores da BT, mas se se comportar de forma inconsistente em relação a esta norma ou qualquer outra política ou norma, poderemos rescindir os acordos que temos consigo relativos aos seus serviços.

11. Propriedade e Confidential (Confidencial)idade.

Este documento não poderá ser partilhado com terceiros sem o consentimento por escrito da BT. Esta norma e qualquer documentação associada permanecem propriedade da BT e terão de ser devolvidas se solicitado