

Anexo 1 - Classificação das informações

Introdução

Dentro da BT todo dado ou informação possui um proprietário de negócios BT responsável por sua classificação.

Os dados e informações devem ser protegidos por todos os usuários que vierem a ter contato com os mesmos. Como usuários de informações da BT, vocês são responsáveis por manter a conformidade com os controles de classificação de segurança contidos neste documento e quaisquer requisitos de projeto específicos especificados pela BT. Vocês só devem utilizar o documento ou o dado para sua finalidade prevista e é preciso ter aprovação do proprietário dos dados caso desejem permitir que mais pessoas tenham acesso a ele.

Caso recebam informações da BT que ainda não tenham sido classificadas, vocês deve entrar em contato com o remetente ou com seu gerente BT para confirmar a classificação, caso contrário, entre em contato com a Segurança BT, de acordo com as Exigências de Segurança, Anexo 3.

Nota: Caso tenham acesso à rede de área local Greenside da BT (LAN) ou precisem criar documentos para a BT que incluam informações da mesma, é preciso consultar a Política de Segurança 4, caso contrário será aplicado o que segue

Classificação das informações

Existem 4 classificações de informações:

- Públicas
- Internas
- Confidenciais
- Estritamente confidenciais

Públicas

Informações públicas não precisam ser controladas, ou destinam-se ao consumo público.

Internas

Informações internas são disponibilizadas aos funcionários da BT e a outras pessoas que tenham acesso à rede de informações da BT e quando este acesso resulta em baixo risco empresarial para a BT.

Confidenciais

Informações confidenciais possuem uma audiência específica: o princípio do "é preciso ter conhecimento" (controles de acesso) é rigorosamente aplicado. A divulgação não autorizada de informações confidenciais pode afetar a reputação da BT ou pode prejudicar pessoas.

Por exemplo:

- Informações pessoais relacionadas a indivíduos, sejam eles funcionários da BT, terceiros ou clientes;
- Dados de registro do sistema;

- Dados de vendas e marketing;
- Planos de negócios local;
- Dados de risco;
- Senhas;
- Informações legalmente confidenciais.

Conjunto de diversos documentos Confidenciais

Caso tenha um conjunto de diversos documentos Confidenciais em um único local, a classificação pode precisar ser atualizada e isso pode levar à reclassificação de documentos individuais como sendo Estritamente confidencial ou à adição de medidas de segurança para proteger o local, se:

- Juntos, caso vazem informações sobre estes documentos, possam vir causar danos excepcionais à BT;
- Quando usados com outras combinações de dados, ex. nome e endereço e/ou quando houver diversos registros de dados bancários em um sistema, estes dados possam vir a ser um alvo atrativo.

Caso tenha dúvidas com relação às informações que têm em mãos, fale com seu contato junto à BT.

Estritamente confidenciais

Informações ou dados Estritamente confidenciais têm uma circulação definida e de número reduzido; o princípio “é preciso ter conhecimento” é rigorosamente aplicado (você deve saber quem tem cópias e quem tem acesso). A divulgação não autorizada pode causar danos excepcionais à BT. Você deve analisar cuidadosamente se uma informação deve ser considerada Estritamente confidencial, uma vez que ela exige os mais rigorosos controles de segurança.

Controles de segurança

Conceitos definidos:

Criptografia

Requisitos mínimos:

- Use a criptografia AES 256 bits.
- As chaves simétricas devem ter um comprimento mínimo de 256 bits.
- As chaves assimétricas (ex. RSA) devem ter um comprimento de chave de pelo menos 2048 bits.
- Use apenas cifras criptografadas conhecidas e confiáveis.
- Não use certificados auto assinados.

Senha/Frase secreta – (para criptografia)

Deve ser de fácil adivinhação (ex. o mais aleatório possível, não deve estar relacionada à identificação, aos usuários, à identidade, data, etc.) e não pode ser encontrada em dicionários de senhas comumente usadas. No entanto, elas devem ter pelo menos:-

- 8 caracteres.
- Dois dos itens a seguir
 - Não alfanuméricos, ex. (!, £, ", \$, %, ^, &, *, (,), -, _ , +, =, :, ` , @, ~, #, ?, <, >,)
 - Número decimal: (0... 9)
 - Letra maiúscula: (A... Z)
- Chaves confidenciais devem ser protegidas por uma frase secreta usando uma mistura de caracteres alfanuméricos e símbolos, conforme definido acima.

Nota: Para evitar dúvidas, qualquer exigência contratual específica de um cliente contida no contrato do cliente que exija um nível mais alto de segurança prevalecerá sobre os controles a seguir.

	Controles de segurança	Internas	Confidenciais	Estritamente confidenciais
1	Legislação nacional de proteção de dados - Dados pessoais e confidenciais	Não devem ser tratados como internos. Proteja os registros individuais como sendo Confidenciais.	Proteja os registros individuais como sendo Confidenciais.	Proteja os registros em massa como sendo Estritamente confidenciais

PÚBLICO

2	Controle de distribuição e rastreamento de circulação de documentos comerciais (Word, Excel, etc.)	Não é necessário o controle e rastreamento. Coloque a marcação "INTERNO BT" em todas as páginas ou "INTERNO OPENREACH" caso ele só deva ser compartilhado no Openreach.	Coloque "CONFIDENCIAL" em todas as páginas do documento e não deixe de seguir o "princípio é preciso ter conhecimento" , e considere usar uma lista de distribuição . É necessário criptografar conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.	Coloque a frase "ESTRITAMENTE CONFIDENCIAL" em todas as páginas do documento. Inclua uma lista de distribuição dentro do documento. O proprietário deve se certificar de que o "princípio do é preciso ter conhecimento" está sendo seguido. É preciso criptografar antes de armazenar utilizando um software em conformidade com os termos definidos "Criptografar" e "Senha/Frase secreta" acima quando os dados não estiverem armazenados em um PC/Laptop da BT com disco rígido criptografado, ex. mídia removível. O mesmo se aplica quando os dados forem enviados por e-mail a alguém, seja da BT ou não.
3	Armazenamento seguro em um laptop e PC	É preciso ter um armazenamento seguro, ex. PGP, WinZip 9	Criptografia de todo o disco, conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.	Criptografia de todo o disco, conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.
4	Armazenamento seguro no servidor e em bases de dados (fixas - disco/fita)	Não é preciso ter um armazenamento seguro caso esteja em conformidade com todas as exigências segurança físicas, caso contrário, o armazenamento seguro é necessário, ex. PGP, WinZip 9	As informações da BT precisam ser criptografadas conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.	As informações da BT precisam ser criptografadas conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.

PÚBLICO

5	Armazenamento seguro em Blackberry, Windows Mobile, outros PDAs, tablets (iPads, etc.), telefones celulares e MP3 players	É proibido armazenar informações internas nestes dispositivos, a não ser que o dispositivo seja fornecido pela BT ou que uma concessão seja aprovada pela Segurança da BT. Estes dispositivos não devem ser configurados para que tenham acesso às contas de e-mail da BT.com (é permitido apenas o acesso ao e-mail da bt.com através do webmail).	É proibido armazenar informações Confidenciais nestes dispositivos, a não ser que o dispositivo seja fornecido pela BT ou que uma concessão seja aprovada pela Segurança da BT. Estes dispositivos não devem ser configurados para que tenham acesso às contas de e-mail da BT.com (é permitido apenas o acesso ao e-mail da bt.com através do webmail).	É proibido armazenar informações Estritamente confidenciais nestes dispositivos.
6	Armazenamento seguro em: Mídias removíveis como cartões de memória, memória flash, CD/DVD, discos rígidos USB, cartões digitais seguros, disquetes e outros dispositivos similares.	As informações da BT precisam ser criptografadas quando armazenadas nestes dispositivos, conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.	As informações da BT precisam ser criptografadas quando armazenadas nestes dispositivos, conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.	É proibido armazenar informações Estritamente confidenciais nestes dispositivos.
7	Armazenamento na Web/on-line ou em qualquer instalação de armazenamento da internet	Proibido	Proibido	Proibido
8	Colaboração Web externa	Qualquer plataforma MS LiveMeeting ou Webjoin	Proibido	Proibido

PÚBLICO

9	Enviar via e-mail	Criptografia não obrigatória.	Criptografado para destinatários (quando o destinatário não for um e-mail bt.com), conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.	É necessário criptografar, conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.
10	Reencaminhamento automático de e-mail:	Proibido	Proibido	Proibido
11	Transmissão em rede	Criptografia não obrigatória.	Criptografado para transmissões internas e externas, conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.	Criptografado para transmissões internas e externas, conforme os termos definidos "Criptografar" e "Senha/Frase secreta" acima.
12	Transferência de arquivo	Use transferência segura de arquivos, ex. SFTP, XFB.	Use transferência segura de arquivos, ex. SFTP, XFB.	Use transferência segura de arquivos, ex. SFTP, XFB.
13	Remoção/Exclusão de dados	Utilize as capacidades de exclusão de aplicativo ou de sistema operacional.	Higienize os dados sobrescrevendo todos os setores com cadeias binárias aleatórias ao menos uma vez com o uso de um produto de software, ex. Blanco HMG Edition ou Blanco Versão 5 se estiver usando dispositivos de estado sólido.	Higienize os dados sobrescrevendo todos os setores com cadeias binárias aleatórias ao menos uma vez com o uso de um produto de software, ex. Blanco HMG Edition ou Blanco Versão 5 se estiver usando dispositivos de estado sólido.
14	Descarte ou reutilização de um equipamento de TI (contendo informações da BT) Inclusive, mas não limitado a: - Descarte de peças; - Destruição de equipamentos de fornecedores;	Use uma solução de remoção de software testada e que possa ser verificada que produza um certificado de verificação da remoção. Qualquer equipamento que não consiga realizar a remoção deve ser destruído e uma certificação formal deve ser fornecida/recebida com pelo menos um registro do número	Os discos (ou outra mídia de armazenamento, inclusive, mas não restrita a flash compacto, dispositivo de estado sólido) devem ser higienizados ao sobrescrever todos os setores com cadeias binárias aleatórias ao menos uma vez com o uso de um produto de software, ex. Blanco HMG Edition ou Blanco Versão 5 se estiver usando dispositivos de estado sólido.	Os discos (ou outra mídia de armazenamento, inclusive, mas não restrita a flash compacto, dispositivo de estado sólido) devem ser higienizados ao sobrescrever todos os setores com cadeias binárias aleatórias ao menos uma vez com o uso de um produto de software, ex. Blanco HMG Edition ou Blanco Versão 5 se estiver usando dispositivos de estado sólido.

PÚBLICO

	- Requisitos de destruição para backups; - Peças do servidor devolvidas ao fabricante para reparo.	de série do equipamento como prova do descarte. A solução acima não pode ser usada com um Disco de Estado Sólido (SSD), que deve ser destruído e deve receber ou fornecer uma certificação formal. Consulte a BS EN 17513 para mais informações.	Caso não seja possível realizar a higienização ou a mesma não seja apropriada, o disco (ou outra mídia de armazenamento, inclusive, mas não restrita a flash compacto, dispositivo de estado sólido) deve ser destruído com a utilização de um dispositivo de destruição de disco. Um certificado formal deve ser produzido para comprovar a remoção ou destruição.	Caso não seja possível realizar a higienização ou a mesma não seja apropriada, o disco (ou outra mídia de armazenamento, inclusive, mas não restrita a flash compacto, dispositivo de estado sólido) deve ser destruído com a utilização de um dispositivo de destruição de disco. Um certificado formal deve ser produzido para comprovar a remoção ou destruição.
15	Impressão	Utilize uma impressora conectada ao PC ou presente na impressora da rede enquanto estiver imprimindo.	Utilize uma impressora controlada por PIN, conectada ao PC ou uma impressora em uma sala com controle de acesso. Verifique para qual impressora seu documento foi encaminhado e não deixe documentos na bandeja de impressão.	Utilize uma impressora controlada por PIN, conectada ao PC ou uma impressora em uma sala com controle de acesso. Tenha cuidado ao imprimir documentos. Verifique para qual impressora seu documento foi encaminhado e não deixe documentos na bandeja de impressão.
16	Serviços postais/de entrega entre a BT e o fornecedor	Envelope simples	Utilize envelopes duplos, envie ao remetente apenas por carta registrada e não marque o primeiro envelope como "Confidencial".	Utilize envelopes duplos, envie ao remetente apenas por carta registrada e não marque o primeiro envelope como "Estritamente confidencial".
17	Divulgação externa	Busque a aprovação do contato de segurança da BT. Consulte o anexo 3.	Busque a aprovação do contato de segurança da BT. Consulte o anexo 3.	Busque a aprovação do contato de segurança da BT. Consulte o anexo 3.

PÚBLICO

18	Utilizado em treinamento, desenvolvimento ou testes	Deve ser anonimizado pela BT e deve estar em conformidade com o guia BP001 de melhores práticas de anonimização de dados da BT.	Deve ser anonimizado pela BT e deve estar em conformidade com o guia BP001 de melhores práticas de anonimização de dados da BT.	Proibido
19	Descarte de papéis	Triturado com a utilização de trituradores de corte transversal.	Triturado com a utilização de trituradores de corte transversal.	Triturado com a utilização de trituradores de corte transversal para papéis de 4 x 15mm.
20	Espaços públicos	Não fale sobre Informações Internas em público.	Não fale sobre Informações Confidenciais em público. Não trabalhe em documentos em espaços públicos em que você possa se descuidar.	Não fale sobre Informações Estritamente Confidenciais em público. Não trabalhe em documentos em espaços públicos.