

Especificação de Classificação e Manipulação de Informação de Terceiros

Introdução

Nem todas as informações têm o mesmo valor ou sensibilidade e classificá-las ajuda-nos a perceber como devem ser protegidas; demonstra o nosso compromisso com essa proteção e ajuda-nos a lidar com ela de modo eficiente.

Temos quatro níveis de classificação:

- Pública
- Interna
- Confidencial
- Estritamente confidencial

O quadro abaixo fornece orientações sobre os tipos de informações que se enquadrarão em cada uma dessas quatro categorias.

Por defeito, qualquer Informação BT será classificada como Confidencial, salvo indicação em contrário.

Se não tiver a certeza de qual a categoria em que a informação se enquadra, entre em contacto com o seu Contacto de Segurança BT.

Classificação	Descrição geral	Exemplos
Pública - Cat 1	A informação pública é informação disponível tanto para as pessoas de dentro como de fora da BT.	<ul style="list-style-type: none"> • Campanhas de publicidade. • Comunicações genéricas já em domínio público (por exemplo, declarações de RP, artigos públicos sobre a BT) • Informações comerciais disponíveis publicamente, como preços ou ofertas publicados.
Interna - Cat 2	<p>Informação BT disponível para pessoas da BT e outras pessoas que tenham acesso à rede de informações da BT e quando esse acesso resulte num risco comercial mínimo para a BT.</p> <p>As informações internas podem incluir informações sujeitas a obrigações gerais de confidencialidade (por exemplo, emails de expediente geral, relatórios ou documentos contratuais), desde que essas informações não sejam suficientemente sensíveis comercialmente para exigirem as proteções mais exigentes descritas abaixo.</p>	<ul style="list-style-type: none"> • Boletins internos como a BT News • Artigos FixIt • Emails gerais não sensíveis (por exemplo, sem informações comerciais ou dados pessoais limitados, conforme detalhado na coluna à esquerda contida no corpo do email)
Confidencial - Cat 3	A informação Confidencial é informação que deve estar limitada a um público específico e quando a divulgação não autorizada da informação pode prejudicar a reputação da BT ou quando a sua divulgação seria potencialmente prejudicial para as pessoas a quem a informação diga respeito (por exemplo, a maioria dos dados pessoais)	<ul style="list-style-type: none"> • Dados de registo do sistema; • Dados comercialmente sensíveis de vendas e marketing; • Planos de negócios locais; • A maioria dos dados pessoais; e • Dados de risco. • Todos os Dados Pessoais (conforme definidos na Condição intitulada

	<p>sobre funcionários ou clientes). O princípio de "necessidade de saber" (<i>need-to-know</i>) deve ser aplicado à informação Confidencial.</p> <p>Recolha de múltiplos documentos Confidenciais</p> <p>Se tiver uma série de documentos "Confidenciais" num local, a classificação pode precisar de ser elevada e isso pode levar a uma nova classificação de documentos individuais como "Estritamente confidencial" ou exigir medidas de segurança adicionais para proteger a localização se:</p> <ul style="list-style-type: none"> • Juntos, poderiam causar danos excepcionais à BT se fossem divulgados; ou • Quando usados com outras combinações de elementos de dados, poderiam ser um alvo atraente. 	<p>"Proteção de Informação"), a menos que classificados como Estritamente confidenciais, abaixo.</p>
<p>Estritamente confidencial - Cat 4</p>	<p>A informação ou dados estritamente confidenciais têm uma circulação definida e mais reduzida em número; o princípio de "necessidade de saber" é rigorosamente aplicado (deve saber quem tem cópias e quem tem acesso). A divulgação não autorizada pode causar danos excepcionais à BT. Deve considerar cuidadosamente se a informação está como estritamente confidencial, porque isso requer os controlos de segurança mais rigorosos.</p>	<ul style="list-style-type: none"> • Dados de conta bancária • Os dados de autenticação devem ser tratados como estritamente confidenciais. • Palavras-passe de computador e palavras-passe devem ser armazenadas e protegidas de acordo com as Especificações de Encriptação da BT • Dados contabilísticos financeiros sob embargo até a publicação do relatório anual • Planos de negócios estratégicos, estratégia competitiva, novos produtos estratégicos e novas políticas de marketing • Avaliações muito sensíveis de concorrentes, parceiros ou contratadas • Informação de RH sensível que possa afastar um número significativo de funcionários • Detalhes dos principais planos de aquisição, aliança, desinvestimento e fusão • Detalhes sobre vulnerabilidades de rede significativas • Códigos de segurança de cliente, códigos de encriptação mestres, cálculos-chave, transações, contas ou detalhes de auditoria, detalhes de códigos de segurança de cliente, códigos de encriptação mestres, cálculos-chave, transações, conta ou auditoria • Relatórios de auditoria ou conclusões que contenham graves

Como devo lidar com os dados?

A informação deve ser tratada de acordo com o nível de classificação, para ser devidamente protegida, quer seja num computador, ao viajar através de uma rede, escrita ou verbal.

Temos regras para lidar com dados e informações.

- **Faladas e multimédia**, por exemplo, falar, redes sociais, mensagens de texto, skype
- **Documentos em papel**, por exemplo, impressão, publicação, eliminação
- **Documentos eletrónicos**, por exemplo, guardar, enviar por email, transferir, apagar
- **Em aplicações ou sistemas**, por exemplo, Centros de Dados

Também temos diretrizes separadas sobre o nível e tipo de encriptação que esperamos que seja usada para proteger a informação (o nosso "Padrão de Encriptação").

Lidar com dados falados e multimédia

Ref. ^a	O que deseja fazer?	Classificação	Requisitos de manipulação	Motivo
HSM10	Quero publicar informação em redes sociais/sites de rede - por exemplo, conta pessoal do Twitter	Pública	Não deve contribuir para sites ou publicar declarações online que possam ser razoavelmente atribuídas como opiniões da BT ou que sejam difamatórias para a BT e possam causar danos à marca e reputação da BT.	A divulgação não autorizada de informações ou comentários pessoais pode lesar a nossa marca
		Interna	Não permitido	
		Confidencial	Não permitido	
		Estritamente confidencial	Não permitido	
HSM20	Quero discutir ou apresentar qualquer coisa através de conferência ou mensagem internas	Interna	Pode usar Live Meeting, WebEx, Webjoin e Lync/Skype for Business	Os dados internos podem ser vistos por pessoas convidadas para a reunião
		Confidencial	Pode usar Live Meeting, WebEx, Webjoin e Lync/Skype for Business	Os dados IC podem ser vistos por pessoas convidadas para a reunião
		Estritamente confidencial	<ul style="list-style-type: none"> • Pode usar o Lync/Skype for Business hospedado na BT • Tem de verificar quem está na conferência • Tem de bloquear a reunião por conferência para que ninguém mais possa participar 	Lync/Skype for Business encriptados de acordo com os dados abaixo de Padrão de Encriptação
HSM30	Quero discutir alguma coisa através de chat externo ao vivo, por exemplo, num site de assistência de fornecedor, como a Cisco	Pública	As conversas têm de ser restringidas "informação pública" que esteja livremente disponível no nosso site	Para evitar a divulgação não autorizada de informação
		Interna	Não permitido	
		Confidencial	Não permitido	
		Estritamente confidencial	Não permitido	

DOCUMENTO PÚBLICO

HSM40	Quero discutir alguma coisa através de cara a cara/telefonema	Interna	Certifique-se de que a conversa não pode ser ouvida por qualquer pessoa que não trabalhe na ou para a BT	Para evitar a divulgação não autorizada de informação
		Confidencial	Como "Interna" e <ul style="list-style-type: none"> • Verifique a identidade da pessoa com quem vai falar e confirme que tem "necessidade de saber" antes de discutir qualquer coisa confidencial • Assegure-se de que haja um contrato em vigor com terceiros relevantes antes de iniciar a conversa, se aplicável (NB. Antes de atribuir ou subcontratar a totalidade ou qualquer parte do contrato a um terceiro, deve obter o consentimento prévio por escrito da BT) • Assegure-se de que a conversa não pode ser ouvida • Não deixe informação "Confidencial" nos sistemas de correio de voz 	Para proteger informação confidencial e certificar-se de que está restrita a quem precisa de saber
		Estritamente confidencial	Como "Confidencial" e <ul style="list-style-type: none"> • Mantenha a informação "Estritamente confidencial" ao mínimo absoluto 	
HSM50	Quero enviar uma mensagem/conteúdo por SMS/MMS para todas as partes (internas e externas)	Pública	O conteúdo da mensagem deve ser restrito a "Informação pública" disponível no nosso site	Para evitar a divulgação não autorizada de informação
		Interna	Sem requisitos de tratamento especiais	
		Confidencial	Certifique-se de que a mensagem só seja enviada para aqueles que precisam de saber e o seguinte não deve ser divulgado: <ul style="list-style-type: none"> • Informações de cartão de pagamento • Dados bancários • Detalhes da palavra-passe 	Esses 3 elementos são estritamente confidenciais
		Estritamente confidencial	Não permitido	

Manipulação de documentos em papel

Ref. ^a	O que deseja fazer?	Classificação	Requisitos de manipulação	Motivo
HPD10	Quero trabalhar em informações impressas em	Interna	Deve aplicar a política de limpar a mesa quando estiver afastado dela	Para impedir divulgação accidental
		Confidencial	Como "Interna" e	

DOCUMENTO PÚBLICO

	instalações de terceiros ou em casa		<ul style="list-style-type: none"> Quando não estiver a trabalhar nos documentos, coloque fora de visão e tranque. 	
		Estritamente confidencial	Como "Confidencial" e	
HPD20	Quero imprimir	Interna	<ul style="list-style-type: none"> Verifique se está a enviar para a impressora certa Não deixe documentos na bandeja de impressão 	Para impedir divulgação acidental
		Confidencial	Como "Interna" e <ul style="list-style-type: none"> Use uma impressora de acesso controlado, uma impressora ligada a um PC ou uma impressora numa sala com acesso controlado 	
		Estritamente confidencial	Como "Confidencial" e	
HPD30	Quero usar uma impressora que não esteja num Edifício de Fornecedor ou em minha casa (por exemplo, em instalações de terceiros, num hotel etc.)	Interna	Normalmente, isso não é permitido porque as impressoras possuem memórias e os dados podem ser recuperados delas. Use o seu senso comum - quer realmente que outras pessoas vejam esta informação?	Dados e informações podem ser recuperados da memória de uma impressora
		Confidencial	Não permitido	
		Estritamente confidencial	Não permitido	
HPD40	Quero levar informações impressas para fora do meu local de trabalho	Interna	Levar numa pasta ou saco opaco	Para proteger contra a divulgação acidental
		Confidencial	Como "Interna" e <ul style="list-style-type: none"> Não deve remover os dados de cliente e/ou dados de pagamento dos escritórios do Fornecedor 	
		Estritamente confidencial	Como "Confidencial" e	
HPD50	Quero partilhar ou enviar informação impressa para pessoas internas	Interna	<ul style="list-style-type: none"> Coloque num envelope e use o correio interno. 	Protege contra a observação acidental
		Confidencial	<ul style="list-style-type: none"> Não marque como que "Confidencial" no exterior do envelope. Se a informação estiver coberta por "privilégio legal", procure orientação da sua equipa legal. 	Impede que observadores casuais tomem conhecimento de que o conteúdo é Confidencial. Envio contra-assinatura fornece prova de envio, entrega contra-assinatura e confirmação online da entrega do objeto
		Estritamente confidencial	<ul style="list-style-type: none"> Use 2 envelopes e envie usando um entrega com "seguimento" Não marque o envelope externo com "Estritamente confidencial" 	Impede que observadores casuais tomem conhecimento de que o conteúdo é estritamente confidencial. Envio

DOCUMENTO PÚBLICO

			<ul style="list-style-type: none"> • Obtenha a permissão do proprietário do documento para partilhar a cópia impressa • De preferência, partilhe em mão com indivíduos autorizados designados • Associe cópias a indivíduos por meio de marca de água com um nome ou número (se disponível) • Em caso de extravio, tem de relatar um incidente de segurança 	contra-assinatura fornece prova de envio, entrega contra-assinatura e confirmação online da entrega do objeto
HPD60	Quero partilhar ou enviar cópias impressas para pessoas externas	Interna Confidencial Estritamente confidencial	Certifique-se de ter um contrato em vigor conforme HSM40 com terceiros relevantes. Depois, os controlos são os mesmos que para partilhar com pessoas internas	Veja HPD50
HPD70	Quero enviar um fax	Interna	Deve certificar-se de que uma página de cabeçalho de fax esteja incluída antes da(s) página(s) de conteúdo	Para impedir divulgação acidental
		Confidencial	<ul style="list-style-type: none"> • Deve enviar uma página de cabeçalho com uma página de teste e, em seguida, entrar em contacto com o destinatário para confirmar a receção, antes de enviar o conteúdo por fax • Se a informação estiver coberta por "privilégio legal", procure orientação da sua equipa legal. 	Para evitar que pessoas não autorizadas recebam informações
		Estritamente confidencial	Não permitido	
HPD80	Quero eliminar informação impressa	Interna	Tem de <ul style="list-style-type: none"> • usar triturador de papel ou • colocar num cesto de documentos que não possa ser retirado facilmente 	Os cestos de lixo e/ou de reciclagem gerais não são formas seguras de eliminação
		Confidencial	Deve destruir até ao mínimo de tamanho de partícula <160MM ² e partículas regulares de faixa com <2MM, por exemplo, 2X15 mm.	Para proteger a informação "Confidencial" de divulgação
		Estritamente confidencial	Deve destruir até ao mínimo de tamanho de partícula <160MM ² e partículas regulares de faixa com <2MM, por exemplo, 2X15 mm, usando uma trituradora de corte transversal	Para proteger a informação "Estritamente confidencial" de divulgação

Manipulação de documentos eletrónicos

Ref. ^a	O que deseja fazer?	Classificação	Requisitos de manipulação	Motivo
HED10	Quero armazenar informação eletrónica no meu portátil/PC de trabalho	Interna	Encriptação de disco completa usada de acordo com o Padrão de Encriptação abaixo.	Isto converte a informação em código ilegível que não pode ser

DOCUMENTO PÚBLICO

				decifrado facilmente por pessoas não autorizadas.
		Confidencial	Encriptação de disco completa usada de acordo com o Padrão de Encriptação abaixo.	
		Estritamente confidencial	Encriptação de disco completa usada de acordo com o Padrão de Encriptação abaixo.	
HED20	Quero armazenar os meus documentos em SharePoint ou noutra sistema de gestão de documentos que NÃO seja hospedado na nuvem ou com serviços da Internet	Interna	<ul style="list-style-type: none"> Use níveis de permissão e grupos para configurar o controlo de acesso baseado em função. Estes devem ser definidos para não mais do que o mínimo para que as pessoas cumpram as suas tarefas Reveja os controlos de acesso todos os anos 	Restringe o acesso e/ou a edição àqueles que precisam de saber
		Confidencial	Como "Interna" e <ul style="list-style-type: none"> Documentar o processo de atribuição de pessoas a funções. As funções e as pessoas que lhes são atribuídas devem ser revistos a cada 90 dias Os documentos devem ser encriptados de acordo com o Padrão de Encriptação abaixo 	
		Estritamente confidencial	Como "Interna" e <ul style="list-style-type: none"> Documentar o processo de atribuição de pessoas a funções. As funções e as pessoas que lhes são atribuídas devem ser revistos a cada 90 dias Os documentos devem ser encriptados de acordo com o Padrão de Encriptação abaixo 	
HED30	Quero armazenar informação eletrónica na nuvem ou com serviços da Internet, como o Google docs, GitHub, btcloud.bt.com, Drobbox, Pastebin, Facebook etc.	Interna	Não permitido.	Os serviços de Internet aumentam o risco de acesso não autorizado a informações
		Confidencial	Não permitido.	
		Estritamente confidencial	Não permitido.	
HED40	Quero armazenar informação eletrónica em meios removíveis como, por exemplo, um cartão de memória.	Interna	<ul style="list-style-type: none"> Os dispositivos USB devem ser encriptados de acordo com o Padrão de Encriptação abaixo <p>Em nenhuma circunstância os dados pessoais podem ser armazenados nesses dispositivos, a menos que estejam encriptados de acordo com o Padrão de Encriptação abaixo.</p>	Os meios removíveis podem ser perdidos ou roubados com mais facilidade do que um computador inteiro e, portanto, o risco de pessoas não autorizadas acederem aos dados é maior. Para proteger a informação, esta

DOCUMENTO PÚBLICO

				deve ser convertida em código ilegível que não possa ser decifrado facilmente por pessoas não autorizadas
		Confidencial	Como "Interna"	
		Estritamente confidencial	Como "Interna"	
HED50	Quero armazenar documentos eletrónicos ou informações da BT no meu portátil ou dispositivo pessoal	Interna	Não permitido	Pessoas não autorizadas podem aceder aos dados da BT, especialmente se o dispositivo for perdido, roubado, descartado por troca com um modelo mais novo.
		Confidencial	Não permitido	
		Estritamente confidencial	Não permitido	
HED60	Quero enviar documentos eletrónicos ou informação para o meu endereço de email pessoal	Interna	Não permitido	Para evitar a divulgação a pessoas não autorizadas
		Confidencial	Não permitido	
		Estritamente confidencial	Não permitido	
HED70	Quero encaminhar automaticamente para um endereço de email	Interna	Não permitido	Os dados podem ser acedidos por pessoas não autorizadas se a conta de email, o ISP ou a ligação à Internet estiverem comprometidos
		Confidencial	Não permitido	
		Estritamente confidencial	Não permitido	
HED80	Quero partilhar <i>internamente</i> ou enviar informações eletrónicas por email	Interna	Sem requisitos especiais	
		Confidencial	<ul style="list-style-type: none"> Tornar claro que o email é "Confidencial" Use as configurações de sensibilidade para marcar o email como "Confidencial" Idealmente, defina as permissões para "Não reencaminhar" Se a informação estiver coberta por "privilégio legal", procure orientação da sua equipa legal. 	Para manter o controlo sobre informação confidencial
		Estritamente confidencial	Como "Confidencial", mais <ul style="list-style-type: none"> Use email seguro para enviar Se o email seguro não for possível, terá de encriptar o ficheiro antes de o enviar, conforme o Padrão de Encriptação abaixo Defina as permissões para "Não reencaminhar" 	Para proteger a informação durante o trânsito através das redes

DOCUMENTO PÚBLICO

HED90	Quero partilhar externamente ou enviar informação eletrónica por email	Interna	Só pode enviar para uma pessoa externa se tiver um contrato em vigor, conforme HSM40	Para manter o controlo sobre informação confidencial
		Confidencial	Como "Interna" e <ul style="list-style-type: none"> • Encriptar de acordo com o Padrão de Encriptação abaixo • Confirme que está a enviar para o endereço de email correto • Se a informação estiver coberta por "privilégio legal", procure orientação da sua equipa legal. 	
		Estritamente confidencial	Como "Confidencial" e	
HED120	Quero fazer cópia de segurança de documentos eletrónicos da BT	Interna	<ul style="list-style-type: none"> • Tem de armazenar os seus documentos nas unidades de rede do Fornecedor ou no sistema de gestão de documentos do Fornecedor, conforme HED030. • O documento de cópia de segurança deve ser protegido ao mesmo nível que na unidade de rede, SharePoint. • Se usar meios removíveis, o dispositivo deve ser encriptado usando o Padrão de Encriptação abaixo. 	As cópias de segurança têm de ter o mesmo nível de classificação e de proteção que os dados originais
		Confidencial	Como "Interna" e <ul style="list-style-type: none"> • Encriptar o documento de acordo com o Padrão de Encriptação abaixo antes de fazer a cópia de segurança 	
		Estritamente confidencial	Como "Confidencial" e	

Manuseamento de dados de sistema e de aplicação

Ref. ^a	O que deseja fazer?	Classificação	Requisitos de manipulação	Motivo
HSADE	Quero armazenar e processar dados e informação eletrónicos mantidos num centro de dados ou em um servidor de sistema	Interna	Não há requisitos especiais se estiver em conformidade com todos os requisitos aplicáveis acima para armazenamento de dados para esta classificação.	
		Confidencial	Tem de seguir os requisitos de armazenamento de dados do terceiro externo http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	
		Estritamente confidencial	<p>Como "Confidencial", mais</p> <p>Para proteger os dados de conta bancária, é especialmente sensível que sejam aplicados os seguintes controlos. Estes têm precedência sobre quaisquer outros controlos aplicáveis nesta especificação de segurança.</p> <ol style="list-style-type: none"> 1. As contas bancárias devem ser referenciadas a pessoas físicas (contas bancárias pessoais de clientes e funcionários da BT), o que exclui os dados de conta bancária da própria BT e os dados bancários das várias entidades jurídicas da BT. 2. Se uma aplicação só detém contas bancárias empresariais, então o terceiro pode avaliar (com base em tempo, custo, recursos, número de contas e número de utilizadores com acesso à aplicação, etc.) se a BT aceitará inicialmente uma solução baseada em encriptação. <p>Se uma solução baseada em encriptação for acordada, a BT examinará depois a decisão quando todas as contas bancárias estiverem protegidas para determinar se isso é adequado para o futuro. Isso será influenciado pelos níveis de ameaça e pelo apetite pelo risco do negócio como um todo.</p> <ol style="list-style-type: none"> 3. Ao exibir os dados reais de conta bancária a um agente como parte de um processo de negócio (por exemplo, para verificar se temos a conta correta para faturação ou quando se comunica com um cliente, por exemplo, por email ou numa fatura), devemos apenas mostrar os últimos 4 dígitos da conta bancária (ou seja, dados de conta bancária mascarados). 4. Se houver necessidade de aceder à conta bancária completa (por exemplo, para permitir um pedido de crédito ou débito de um banco), os dados do banco devem ser des-referenciados ou des-encriptados e depois passados para o banco usando um mecanismo de transporte encriptado compatível com a política de segurança da BT. Imediatamente após o uso, os dados bancários des-encriptados ou des-referenciados devem ser eliminados de forma segura. 	

Padrões de Encriptação

Controlos gerais de encriptação.

Ref. ^a	Controlo	Motivo
C1.10	Têm de ser usadas as bibliotecas de encriptação atuais	As bibliotecas de encriptação são atualizadas regularmente. Além de atualizar pacotes de software em linha com os pacotes de encriptação de orientação do fornecedor, os pacotes de encriptação devem ser revistos e atualizados regularmente.
C1.20	Use somente conjuntos de cifras padrão da indústria aprovados para encriptação. Por exemplo, para TLS SSLv2	Cifras não aprovadas podem introduzir vulnerabilidades
C1.30	A versão mais recente de TLS deve ser usada para novas implantações. SSL V1,2 & 3 não deve ser usado	Versões anteriores, até e incluindo TLS1.0 já não são consideradas seguras
C1.40	Tem de ser ativada privacidade perfeita de encaminhamento (Perfect Forward Privacy)	Os algoritmos de perfeito segredo de encaminhamento impedem que as mensagens capturadas sejam descriptadas, mesmo que a chave privada de autenticação seja comprometida no futuro
C1.50	Os certificados autoassinados não devem ser usados	Os certificados autoassinados negam o benefício da autenticação de ponto final e também diminuem significativamente a capacidade de um indivíduo para detetar um ataque de homem-pelo-meio.
C1.60 GTS2.370	Uma autoridade de certificação padrão do setor deve ser usada para gestão de certificados. Por exemplo, verisign	Para manter um inventário dos certificados emitidos para vulnerabilidades e caducidade de certificado
C1.70	As palavras-passe devem ser protegidas usando uma função matemática unidirecional não reversível (por exemplo, algoritmo de hashing) com um fator aleatório exclusivo (Salt) por palavra-passe. NB. SALT é um dado aleatório que é usado como uma entrada adicional para uma função unidirecional que faz o "hash" de uma palavra-passe ou frase de passe.	Os ficheiros de palavras-passe armazenados podem ser extraídos e, como tal, todas as entradas devem ser protegidas para evitar a recuperação de palavras-passe em texto legível
C1.80	As palavras-passe protegidas conforme C1.70 devem ser armazenadas afastadas dos ficheiros de configuração de um sistema e ter o controlo de acesso implementado de modo a que apenas utilizadores com os privilégios apropriados possam ler ou copiar o conteúdo.	Nunca deve ser possível recuperar palavras-passe protegidas por atravessamento de diretórios, caminho SNMP, despejo de configuração ou outro mecanismo que possa permitir tentativas de cracking offline.

Implementação técnica de encriptação

Protocolos SSL/TLS	
Pode usar	Não usar
TLSv1.3 (tbc - Disponível em OpenSSL após 5 de abril).	SSLv3.0
TLSv1.2	SSLv2.0
TLSv1.1	
TLS v1.0 *	

* TLSv1.0 já está em fim de vida e pode ser abandonado a qualquer momento devido a problemas conhecidos. Por motivos de conformidade (por exemplo, PCI-DSS), protocolos como TLSv1.0 e TLSv1.1, podem ter de ser desligados. Todos os desenvolvedores devem estar prontos para desativar esses protocolos por configuração.

Tamanhos de chave			

DOCUMENTO PÚBLICO

	Simétrica	Assimétrica	Curva elíptica
Brownfield	≥ 112 bits	2048 bits	≥ 224 bits
Greenfield	≥ 128 bits	≥ 3072 bits	≥ 384 bits

Troca de chaves	
Pode usar	Não Usar
ECDHE (Ephemeral (temp key) Diffie-Hellman Key Exchange (chaves não baseadas em certificados))	kRSA (RSA Key Exchange)
	kDHr (Diffie-Hellman Key Exchange with RSA key)
	kDHd (Diffie-Hellman Key Exchange with DSA key)
	kSRP (Secure Remote Password (SRP) Key Exchange)
	kADH (Anonymous Diffie-Hellman key exchange)
	kPSK (Pre-shared Key Exchange)

A segurança perfeita de encaminhamento deve ser baseada em valores do grupo Diffie-Hellman configurados localmente ou gerados que incluam números-primos "seguros".

Parâmetros de Diffie Hellman

Parâmetros de Diffie Hellman	
Pode usar	Não Usar
Grupo Diffie-Hellman de 3072 bits (melhor - deve ser gerado localmente).	Os valores padrão do servidor (gere o seu próprio localmente)
Grupo Diffie-Hellman de 2048 bits (próximo de fim de vida - deve ser gerado localmente).	

Autenticação	
Pode usar	Não Usar
aRSA (autenticação RSA)	aNULL (sem autenticação)
aECDSA (Autenticação de Algoritmo de Assinatura Digital de Curva Elíptica)	aDSS (Autenticação DSS)
	aECDH (Curva Elíptica Diffie-Hellman)
	aDH (Diffie-Hellman)
	aDSA (Algoritmo de Assinatura Digital)
	aPSK (Chave pré-partilhada)
	aSRP (Palavra-passe Remota Segura)

Cifra/Encriptação	
Pode usar	Não Usar
AES 256 GCM (Rijndael (Advanced Encryption Standard) - Galois Counter Mode)	eNULL (sem encriptação)
AES 128 GCM (Rijndael (Advanced Encryption Standard) - Galois Counter Mode)	DES (encriptação DES)
CHACHA20/POLY1305 (256)	3DES (encriptação 3DES)
AES 256 CCM (Rijndael (Advanced Encryption Standard) - (Counter Mode with CBC-Mac)	RC4 (encriptação RC4)
AES 128 CCM (Rijndael (Advanced Encryption Standard) - (Counter Mode with CBC-Mac)	RC2 (encriptação RC2)
AES 256 CBC (Rijndael Cipher Block Chaining) - próximo de fim de vida.	IDEA (encriptação IDEA)

DOCUMENTO PÚBLICO

AES 128 CBC (Rijndael Cipher Block Chaining) - próximo de fim de vida.	Seed (criptação Seed)
	Camellia (criptação Camellia)
	ARIA (criptação ARIA)

MAC Digest Algorithm	
Pode usar	Não Usar
AEAD (Authenticated Encryption Additional Data)	MD5 (MD5 função Hash)
SHA512 (SHA2 family - SHA512 Hash function)	SHA1 (SHA1 função Hash)
SHA384 (SHA2 family - SHA384 Hash function)	SHA (alias para SHA1)
SHA256 (SHA2 family - SHA256 Hash function)	