Sumário

Histórico					
Versão	Elaborado por	Data	Revisado por	Data	Principais Alterações
1.0	Edenilton Soares - ejsoares	17.05.2021	Maria das Graças - mgsmfernandes		

Objetivo

Prover aos membros da equipe de infraestrutura um framework para avaliar o nível de requerimentos de segurança que deve ser utilizado e guiar a equipe de segurança operacional na seleção destes requisitos para sua implementação, garantindo assim uma maior segurança.

Introdução

A implementação de uma metodologia que possa auxiliar no desenvolvimento seguro é um dos principais pontos dentro de um processo de segurança. Os requisitos apresentados neste documento foram definidos com base nas especificações propostas pelo Open Web Application Security Project® (OWASP) e Center For Internet Security (CIS).

Níveis de Implementação

O documento apresenta três níveis de verificação que devem ser observados durante o processo de configuração do serviço. Cada um dos níveis aqui apresentados tem sua particularidade e profundidade.

Nível 1 - Segurança Mínima Necessária	Nível 2 - Padrão para web	Nível 3 - Alto Valor, Garantia, Segurança e Resiliência
Para níveis baixos de garantia de segurança. Apresenta o nível mínimo de segurança esperado para qualquer aplicação web.	Para aplicações que contêm dados sensíveis. É o nível recomendado para a maioria das aplicações.	Para as aplicações mais críticas, que requerem o mais alto nível de confiança.

Nível 1 - Segurança mínima

Para se adequar a este nível, a aplicação não deve possuir vulnerabilidades de fácil descoberta e exploração, bem como as listadas no TOP 10 da OWASP ou mesmo em outras listas de vulnerabilidades similares classificadas como críticos e altos.

O nível 1 é considerado o mínimo de segurança para qualquer aplicação, no entanto, se os dados que devem ser protegidos por sua aplicação são críticos, raramente somente o Nível 1 trará o nível de proteção recomendado de segurança.

Nível 2 – Segurança Recomendada

Um serviço atinge o nível 2 se tiver resiliência suficiente contra a maioria dos riscos associados a ataques através de recursos externos. Portanto, deve ser utilizado como o nível padrão de segurança. Este nível, que é apropriado para aplicações que tratam dados sensíveis, garante que os controles de segurança existem, funcionam e são utilizados dentro da aplicação.

Ameaças a aplicações neste nível serão tipicamente feitas por atacantes habilidosos e motivados, focando em alvos específicos, utilizando ferramentas e técnicas efetivas para o descobrimento e exploração de fraquezas dentro de aplicações.

Características da Aplicação
Armazena, transmite ou processa dados pessoais, confidenciais ou sensíveis de funcionários, parceiros de negócio, terceiros ou prestadores de serviço
Aplicações cuja integridade é crítica.

Nível 3 – Segurança Alto valor, garantia e resiliência

Este nível é o mais alto e é normalmente reservado para serviços que requerem níveis significativos de verificações de segurança, como em situações de infraestrutura crítica, quando realizam processos críticos para o negócio ou funções sensíveis, quando é necessária a garantia da sua integridade para o funcionamento do negócio, ou seja, nível de segurança 3 é exigido em cenários onde uma falha pode provocar um impacto significativo nas operações da organização.

Características da Aplicação
Aplicações que executam funções críticas, onde a falha pode afetar significativamente as operações. Ex: uma aplicação interna que seja utilizada por várias outras, Sefaz Identity, Portal de Assinaturas, etc Aplicações que manipulam informações sigilosas ou que realizam processos críticos para o negócio ou funções sensíveis. Ex.: manipulação de informações sujeitas ao sigilo fiscal.

Seleção dos Requisitos de Segurança

Para o processo de seleção dos requisitos de segurança ser eficiente, deve-se aplicar uma avaliação mista, levando em consideração os ativos que devem ser protegidos e os riscos mapeados.

O anexo 1 apresenta uma lista de requisitos de segurança propostos, divididos nos três níveis de segurança. Além disso, os requisitos propostos nos anexos, não deverão ser tratados como únicos. Caso seja notada a necessidade de adição de um requisito, o mesmo pode e deve ser adicionado à sua respectiva tabela dentro do respectivo anexo.

A partir destes anexos, o PO irá gerar a Lista de Requisitos de Segurança, que será passada para a fase de sprint de desenvolvimento. Para gerar esta Lista de Requisitos de Segurança do Projeto, considere utilizar ferramentas, Kanban boards, Scrum ou tabelas que facilitarão na seleção e acompanhamento da implementação dos requisitos.

Anexo 1 – Requisitos de Segurança para Configuração

Este anexo apresenta os controles que devem ser avaliados, e caso atendam às necessidades de segurança da solução, devem ser aplicados. Esta lista de requisitos foi baseada primordialmente no CIS (Center For Internet Security) que apresenta uma lista das técnicas de boas práticas que deveriam ser incluídas em toda configuração inicial de recursos com finalidade de desenvolvimento de software.

1. Requisitos de Configuração Windows

1.1. Configuração WebServer

#	Descrição	1	2	3	CWE
1.1.1.	Recomenda-se que as mensagens de erro da Web do servidor de aplicação e do framework estejam configuradas para fornecer respostas personalizadas e acionáveis pelo usuário para eliminar quaisquer divulgações de segurança não intencionais. As informações confidenciais podem ser valiosas por si mesmas (como uma senha) ou podem ser úteis para lançar outros ataques mais sérios.	✓			209
1.1.2.	Recomenda-se que os modos de depuração da Web, servidor de aplicação e do framework esteja desativado na produção para eliminar recursos de debug, consoles de desenvolvedor e divulgações de segurança não intencionais. CIS: IIS.10 – Pag 46	✓			497
1.1.3.	Recomenda-se que a "navegação no diretório" esteja desativada. Garantir que a navegação no diretório esteja desabilitada pode reduzir a probabilidade de divulgação de conteúdo confidencial que é inadvertidamente acessível via IIS. CIS: IIS.10 – Pag 14	✓			
1.1.4.	Recomenda-se que a “identidade do pool de aplicativos” esteja configurada para todos os pools. As identidades do pool de aplicativos são os usuários/autoridades reais que executarão o processo de trabalho - w3wp.exe. Atribuir a autoridade de usuário correta ajudará a garantir que os aplicativos possam funcionar corretamente, sem conceder permissões excessivamente permissivas no sistema. Se estiver usando um usuário personalizado do Windows, como uma conta de serviço dedicada, esse usuário precisará ser um membro do grupo IIS_IUSRS. O grupo IIS_IUSRS tem acesso a todos os recursos de arquivo e sistema necessários para que uma conta, quando adicionada a esse grupo, possa agir como uma identidade de pool de aplicativos. CIS: IIS.10 – Pag 16				

1.1.5.	Recomenda-se que o 'pools de aplicativos exclusivos' estejam definidos para sites. Ao definir sites para serem executados em pools de aplicativos exclusivos, os aplicativos que consomem muitos recursos podem ser atribuídos a seus próprios pools de aplicativos, o que pode melhorar o desempenho do servidor e do aplicativo. O isolamento de aplicativos ajuda a reduzir o risco potencial de um aplicativo ter permissão para acessar os recursos de outro aplicativo. Também é recomendável interromper qualquer pool de aplicativos que não esteja em uso ou que tenha sido criado por uma instalação como .Net 4.0. CIS: IIS.10 – Pag 20				
1.1.6.	Recomenda-se que o Header Server seja removido. O cabeçalho do servidor pode especificar a tecnologia subjacente usada por um aplicativo. Embora essa não seja a única maneira de imprimir as impressões digitais de um site por meio dos cabeçalhos de resposta, ela o torna mais difícil e evita alguns invasores em potencial. A diretiva de remoção do cabeçalho do servidor é um novo recurso no IIS 10 que pode ajudar a mitigar esse risco CIS: IIS.10 – Pag 68	✓			

1.2. Configuração de Autenticação e Autorização

1.2.1.	Recomenda-se que 'regra de autorização global' esteja definida para restringir o acesso. Configurar uma regra de autorização global que restringe o acesso garantirá a herança das configurações na hierarquia dos diretórios da web; se esse conteúdo for copiado em outro lugar, as regras de autorização fluem com ele. Isso garantirá que o acesso ao conteúdo atual e futuro seja concedido apenas aos responsáveis apropriados, reduzindo o risco de acesso acidental ou não autorizado. CIS: IIS.10 – Pag 25				
1.2.2.	Recomenda-se que o acesso aos recursos confidenciais do site ocorra de forma autenticada. A configuração da autenticação ajudará a reduzir o risco de usuários não autorizados acessarem dados e / ou serviços e, em alguns casos, reduzir o dano potencial que pode ser causado a um sistema. CIS: IIS.10 – Pag 28	✓			

1.2.3.	Recomenda-se que a autenticação de formulários exija SSL A exigência de SSL para autenticação de formulários protegerá a confidencialidade das credenciais durante o processo de login, ajudando a mitigar o risco de roubo de informações do usuário. CIS: IIS.10 – Pag 32	✓			
1.2.4.	Recomenda-se que a autenticação de formulários esteja configurada para o uso de cookies. O uso de cookies para gerenciar o estado da sessão pode ajudar a reduzir o risco de tentativas de sequestro de sessão, evitando que o ASP.NET precise mover as informações da sessão para a URL. Mover identificadores de informações de sessão para a URL pode fazer com que IDs de sessão apareçam em logs de proxy, histórico de navegação e sejam acessíveis para scripts de cliente por meio de document.location. CIS: IIS.10 – Pag 34	✓			
1.2.5.	Recomenda-se que o “modo de proteção de cookie” esteja configurado para autenticação de formulários. Ao criptografar e validar o cookie, a confidencialidade e integridade dos dados dentro do cookie são garantidas. Isso ajuda a mitigar o risco de ataques, como sequestro de sessão e falsificação de identidade. CIS: IIS.10 – Pag 36	✓			
1.2.6.	Recomenda-se que a segurança da camada de transporte “autenticação básica” esteja configurada. As credenciais enviadas em texto não criptografado podem ser facilmente interceptadas por código malicioso ou por pessoas. Reforçar o uso do Transport Layer Security ajudará a reduzir as chances de credenciais sequestradas. CIS: IIS.10 – Pag 38	✓			
1.2.7.	Recomenda-se que as informações sensíveis (senhas e tokens) não estejam armazenadas em texto claro em arquivos de configuração. Informações sensíveis sempre devem ser protegidas para reduzir o risco vazamento. Por razões de segurança, é recomendado que informações sensíveis não sejam armazenadas em nenhum arquivo de configuração do IIS.Isso removerá todas as referências a usuários armazenados nos arquivos de configuração. CIS: IIS.10 – Pag 42	✓			

1.3. Configuração do ASP.NET

1.3.1.	Recomenda-se que a configuração “Deployment Method Retail” esteja habilitada. Usar a opção destinada especificamente para servidores IIS de produção eliminará o risco de vazamentos de informações vitais de aplicativos e sistemas que poderiam ocorrer se o rastreamento ou depuração fossem deixados habilitados ou customErrors fossem desligados. CIS: IIS.10 – Pag 44				
1.3.2.	Recomenda-se que os erros detalhados no HTTP do IIS sejam ocultos da exibição remota. As informações contidas em mensagens de erro personalizadas podem fornecer pistas sobre como os aplicativos funcionam, abrindo vetores de ataque desnecessários. Garantir que erros personalizados nunca sejam exibidos remotamente pode ajudar a mitigar o risco de pessoas mal-intencionadas obterem informações sobre como o aplicativo funciona. CIS: IIS.10 – Pag 50	✓			
1.3.3.	Recomenda-se que o rastreamento de pilha do APS.NET não esteja habilitado. As informações contidas em mensagens de erro personalizadas podem fornecer pistas sobre como os aplicativos funcionam, abrindo vetores de ataque desnecessários. Garantir que erros personalizados nunca sejam exibidos remotamente pode ajudar a mitigar o risco de pessoas mal-intencionadas obterem informações sobre como o aplicativo funciona. CIS: IIS.10 – Pag 52				
1.3.4.	Recomenda-se que o modo “HTTPCookie” esteja configurado para o estado da sessão. Os cookies que foram configurados corretamente ajudam a mitigar o risco de ataques, como tentativas de sequestro de sessão, evitando que o ASP.NET mova as informações da sessão para a URL; mover as informações da sessão no URI faz com que os IDs da sessão apareçam nos logs do proxy e são acessíveis ao script do cliente por meio de document.location. CIS: IIS.10 – Pag 55	✓			

1.3.5.	Recomenda-se que 'cookies' estejam configurados com o atributo HttpOnly O atributo httpOnlyCookies do nó httpCookies determina se o IIS definirá o sinalizador HttpOnly nos cookies HTTP que definir. O sinalizador HttpOnly indica ao agente do usuário que o cookie não deve ser acessível por script do lado do cliente (ou seja, document.cookie). Recomenda-se que o atributo httpOnlyCookies seja definido como verdadeiro. Definir o valor do atributo httpOnlyCookies do elemento httpCookies como true adicionará o sinalizador HttpOnly a todos os cookies definidos pelo aplicativo. Todas as versões modernas de navegadores reconhecem o atributo HttpOnly; versões mais antigas irão tratá-las como cookies normais ou simplesmente ignorá-las completamente. CIS: IIS.10 – Pag 57	✓			
1.3.6.	Recomenda-se que o método de validação MachineKey - .Net 3.5, esteja configurado. Definir a propriedade de validação como AES fornecerá proteção de confidencialidade e integridade ao viewstate. AES é o algoritmo de criptografia mais forte compatível com a propriedade de validação. Definir a propriedade de validação para SHA1 fornecerá proteção de integridade para o viewstate. SHA1 é o algoritmo de hash mais forte compatível com a propriedade de validação. CIS: IIS.10 – Pag 59				
1.3.7.	Recomenda-se que o método de validação MachineKey - .Net 4.5, esteja configurado O elemento machineKey do ASP.NET web.config especifica o algoritmo e as chaves que o ASP.NET usará para criptografia. O recurso Machine Key pode ser gerenciado para especificar configurações de hash e criptografia para serviços de aplicativo, como estado de exibição, autenticação de formulários, associação e funções e identificação anônima. CIS: IIS.10 – Pag 61				
1.3.8.	Recomenda-se que o nível de confiança global do .NET esteja configurado. O CAS determina as permissões concedidas ao aplicativo no servidor. Definir um nível mínimo de confiança compatível com os aplicativos limitará o dano potencial que um aplicativo comprometido pode causar a um sistema. CIS: IIS.10 – Pag 63				

1.4. Solicitação de Filtragem e Módulos de Restrição

1.4.1.	Recomenda-se que 'maxAllowedContentLength' esteja configurado. O filtro de solicitação maxAllowedContentLength é o tamanho máximo da solicitação http, medido em bytes, que pode ser enviado de um cliente para o servidor. Definir um valor apropriado que foi testado para o filtro maxAllowedContentLength reduzirá o impacto que uma solicitação anormalmente grande teria no IIS e/ou nos aplicativos da web. Isso ajuda a garantir a disponibilidade de conteúdo e serviços da web e também pode ajudar a mitigar o risco de ataques do tipo buffer overflow em componentes não gerenciados. CIS: IIS.10 – Pag 70	✓			
1.4.2.	Recomenda-se que seja colocado um limite no comprimento do URL utilizando o “filtro de solicitação maxURL”. O atributo maxURL da propriedade <requestLimits> é o comprimento máximo (em bytes) em que uma URL solicitada pode ter (excluindo a string de consulta) para que o IIS aceite. Com um Filtro de Solicitações configurado corretamente, limitando a quantidade de dados aceitos na URL, as chances de comportamentos indesejados do aplicativo afetarem a disponibilidade de conteúdo e serviços são reduzidas. CIS: IIS.10 – Pag 73				
1.4.3.	Recomenda-se que o 'filtro de solicitação MaxQueryString' esteja configurado. Com um Filtro de Solicitações configurado corretamente, limitando a quantidade de dados aceitos na URL, as chances de comportamentos indesejados do aplicativo afetarem a disponibilidade de conteúdo e serviços são reduzidas. CIS: IIS.10 – Pag 75				

1.4.4.	Recomenda-se que caracteres não ASCII em URLs não sejam permitidos Este recurso é usado para permitir ou rejeitar todas as solicitações ao IIS que contenham caracteres não ASCII. Ao usar este recurso, a Filtragem de Solicitações negará a solicitação se caracteres de bit alto estiverem presentes na URL. Esse recurso pode ajudar na defesa contra ataques de canonização, reduzindo a superfície de ataque potencial de servidores, sites e / ou aplicativos. CIS: IIS.10 – Pag 77	✓			
1.4.5.	Recomenda-se que solicitações duplamente codificadas sejam rejeitadas. Este recurso de filtro de solicitação evita ataques que dependem de solicitações com codificação dupla e se aplica se um invasor enviar uma solicitação com codificação dupla ao IIS. Quando o filtro de solicitações com codificação dupla é habilitado, o IIS passa por um processo de duas iterações para normalizar a solicitação. Se a primeira normalização for diferente da segunda, a solicitação será rejeitada e o código de erro será registrado como 404.11. Esse recurso ajudará a evitar ataques que dependem de URLs criados para conter solicitações com codificação dupla. CIS: IIS.10 – Pag 79	✓			
1.4.6.	Recomenda-se que o “Método de rastreamento de HTTP” esteja desativado. O método HTTP TRACE retorna o conteúdo das solicitações HTTP do cliente no corpo da entidade da resposta TRACE. Os invasores podem aproveitar esse comportamento para acessar informações confidenciais, como dados de autenticação ou cookies, contidos nos cabeçalhos HTTP da solicitação. Os invasores podem abusar da funcionalidade HTTP TRACE para obter acesso a informações em cabeçalhos HTTP, como cookies e dados de autenticação. Este risco pode ser mitigado não permitindo o verbo TRACE. CIS: IIS.10 – Pag 81	✓			

1.4.7.	Recomenda-se que as extensões de arquivo não listadas não sejam permitidas. O FileExtensions Request Filter permite que os administradores definam extensões específicas que seus servidores da Web. A proibição de todas as extensões de arquivo, exceto as necessárias, pode reduzir muito a superfície de ataque de aplicativos e servidores. CIS: IIS.10 – Pag 83	✓			

1.5. Restrições de IP

1.5.1.	Recomenda-se que a restrição de endereço IP dinâmico esteja ativada. O recurso de restrições de endereço IP dinâmico do IIS pode ser usado para impedir ataques DDOS. A filtragem de endereço IP dinâmica permite que os administradores configurem o servidor para bloquear o acesso de IPs que excedam o número especificado de solicitações ou frequência de solicitações. Certifique-se de receber a página Proibido assim que o bloqueio for aplicado. CIS: IIS.10 – Pag 92	✓			

1.6. Configuração registro de LOG IIS

1.6.1.	Recomenda-se que o local do log da Web padrão do IIS seja movido locais diferentes. O IIS registrará informações relativamente detalhadas em cada solicitação. Esses logs são geralmente o primeiro item analisado em uma resposta de segurança e podem ser os mais valiosos. Usuários mal-intencionados estão cientes disso e frequentemente tentarão remover evidências de suas atividades. Portanto, é recomendável que o local padrão dos arquivos de log do IIS seja alterado para uma unidade restrita, não pertencente ao sistema. Mover o log do IIS para uma unidade restrita que não seja do sistema ajudará a reduzir o risco de os logs serem alterados, removidos ou perdidos de forma mal-intencionada no caso de falha (s) da unidade do sistema. Mover os armazenamentos de arquivos de log para uma unidade que não seja do sistema ou partição separada de onde os aplicativos da Web são executados e / ou o conteúdo é exibido é o preferido. Além disso, as permissões de NTFS no nível da pasta devem ser definidas da forma mais restritiva possível; Administradores e SYSTEM são tipicamente os únicos responsáveis pelo acesso. CIS: IIS.10 – Pag 94	✓			
1.6.2.	Recomenda-se que o log avançado do IIS esteja habilitado. O Registro Avançado do IIS é um módulo que fornece flexibilidade para registrar solicitações e dados do cliente. Ele fornece controles que permitem às empresas especificar quais campos são importantes, adicionar facilmente campos adicionais e fornecer políticas relativas à substituição do arquivo de log e filtragem de solicitações Muitos dos campos disponíveis no Registro Avançado podem fornecer dados e detalhes extensos em tempo real que não poderiam ser obtidos de outra forma. Desenvolvedores e profissionais de segurança podem usar essas informações para identificar e corrigir vulnerabilidades de aplicativos / padrões de ataque. CIS: IIS.10 – Pag 96	✓			
1.6.3.	Recomenda-se que “ETW Logging” esteja ativado. O IIS libera as informações de log para o disco, portanto, antes do IIS, os administradores não têm acesso às informações de log em tempo real. Arquivos de log baseados em texto também podem ser difíceis e demorados para processar, ao habilitar o ETW, os administradores têm acesso ao uso de ferramentas de consulta padrão para visualizar informações de registro em tempo real. CIS: IIS.10 – Pag 98				

1.7. Solicitações de FTP

1.7.1.	Recomenda-se que as solicitações de FTP sejam criptografadas. Usando SSL, a transmissão FTP é criptografada e protegida ponto a ponto e todo o tráfego FTP, bem como credenciais, são protegidos contra interceptação. CIS: IIS.10 – Pag 100	✓			
1.7.2.	Recomenda-se que as restrições de tentativas de login do FTP estejam ativadas. O IIS introduziu um recurso de segurança de rede integrado para bloquear automaticamente ataques de FTP de força bruta. Isso pode ser usado para evitar que um cliente mal-intencionado tente um ataque de força bruta em uma conta descoberta, como a conta do administrador local. Ataques de FTP de força bruta bem-sucedidos podem permitir que um usuário não autorizado faça alterações nos dados que não deveriam ser feitas. Isso pode permitir que um usuário não autorizado modifique o código do site, carregando software malicioso ou até mesmo alterando a funcionalidade de itens como pagamentos online. CIS: IIS.10 – Pag 102	✓			

1.8. Criptografia de Transporte

1.8.1.	Recomenda-se que a implementação do cabeçalho HSTS esteja definida. HTTP Strict Transport Security (HSTS) é um padrão simples e com amplo suporte para proteger o cliente, garantindo que seus navegadores sempre se conectem a um site por HTTPS. Quando um navegador sabe que um domínio ativou o HSTS, ele faz duas coisas: 1. Sempre usa uma conexão ”https://”, mesmo ao clicar em um link “http://” ou depois de digitar um domínio na barra de localização sem especificar um protocolo. 2. Remove a capacidade de os usuários clicarem em avisos sobre certificados inválidos. CIS: IIS.10 – Pag 106	✓			
1.8.2.	Recomenda-se que o SSLv2 esteja desativado. Desativar protocolos fracos ajudará a garantir a confidencialidade e integridade dos dados em trânsito. CIS: IIS.10 – Pag 109	✓			

1.8.3.	Recomenda-se que o SSLv3 esteja desativado. Desativar protocolos fracos ajudará a garantir a confidencialidade e integridade dos dados em trânsito. CIS: IIS.10 – Pag 112	✓			
1.8.4.	Recomenda-se que o TLS 1.0 esteja desativado. Desativar protocolos fracos ajudará a garantir a confidencialidade e integridade dos dados em trânsito. CIS: IIS.10 – Pag 115	✓			
1.8.5.	Recomenda-se que o TLS 1.1 esteja desativado O TLS 1.1 é necessário para compatibilidade com versões anteriores. Certifique-se de testar totalmente seu aplicativo para garantir que a compatibilidade com versões anteriores não seja necessária. Desativar protocolos fracos ajudará a garantir a confidencialidade e integridade dos dados em trânsito CIS: IIS.10 – Pag 118	✓			
1.8.6.	Recomenda-se que o TLS 1.2 esteja ativado TLS 1.2 é o protocolo mais recente e maduro para proteger a confidencialidade e integridade do tráfego HTTP. A ativação deste protocolo ajudará a garantir a confidencialidade e integridade dos dados em trânsito. CIS: IIS.10 – Pag 121	✓			
1.8.7.	Recomenda-se desativar a cifra NULL devido não fornecer confidencialidade ou integridade de dados. Ao desativar a cifra NULL, há uma melhor chance de manter a confidencialidade e integridade dos dados. CIS: IIS.10 – Pag 123	✓			
1.8.8.	Recomenda-se que a cifra “DES” esteja desativada devido possuir uma chave simétrica fraca. Ao desabilitar o DES, há uma chance melhor de manter a confidencialidade e integridade dos dados. CIS: IIS.10 – Pag 125	✓			

1.8.9.	Recomenda-se que o RC4 seja desativado. A única cifra RC4 habilitada por padrão no Server 2012 e 2012 R2 é RC4 128/128. O uso de RC4 pode aumentar a capacidade do adversário de ler informações confidenciais enviadas por SSL / TLS CIS: IIS.10 – Pag 127	✓			
1.8.10.	Recomenda-se que o conjunto de cifras AES 256/256 esteja ativado. AES 256/256 é o pacote de criptografia mais recente e maduro para proteger a confidencialidade e integridade do tráfego HTTP. Ativar AES 256/256 é recomendado. Ativar essa cifra ajudará a garantir a confidencialidade e integridade dos dados em trânsito. CIS: IIS.10 – Pag 132	✓			
1.8.11.	Recomenda-se que o pedido do TLS esteja configurado Os clientes enviam uma lista de cifras que suportam em ordem de preferência para um servidor. O servidor então responde com o conjunto de criptografia que ele seleciona na lista de criptografia do cliente. Os pacotes de criptografia devem ser ordenados do mais forte para o mais fraco, a fim de garantir que a configuração mais segura seja usada para criptografia entre o servidor e o cliente. CIS: IIS.10 – Pag 134	✓			