Guia de Segurança em Aplicações Web

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 1.0

Brasília, abril de 2021

GUIA DE SEGURANÇA EM APLICAÇÕES WEB

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Caio Mario Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Luis Felipe Salin Monteiro

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Mauro Cesar Sobrinho

Diretor do Departamento de Governança de Dados e Informações

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Fábio Hitsuki Nitto

Luiz Henrique do Espírito Santo Andrade

Marcus Paulo Barbosa Vasconcelos

Tássio Correia da Silva

Equipe Revisora

Marcelo de Lima

Histórico de Versões

Data	Versão	Descrição	Autor
12/04/2021	1.0	Primeira versão do Guia de Segurança em Aplicações Web.	Equipe Técnica de Elaboração

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente guia buscar compartilhar e difundir as melhores práticas internacionais em matéria de segurança em aplicações web, algumas das quais não se encontram integralmente disponíveis em língua portuguesa. O documento é especialmente recomendado e dirigido aos órgãos e às entidades da administração pública federal brasileira para auxiliar o atendimento do Capítulo VII - da segurança e das boas práticas - da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), mas pode também ser aproveitado por outras instituições que busquem informações sobre o tema.

O guia é de autoria exclusiva da Secretaria de Governo Digital do Ministério da Economia, mas contém referências a publicações e a outros documentos técnicos, com destaque para aqueles do *Open Web Application Security Project* (OWASP)[1] e do *Center for Internet Security* (CIS)[2]. Muitas das referências foram traduzidas de forma livre pelos técnicos do governo brasileiro, com propósitos educativos e não comerciais e com o objetivo de democratizar e de ampliar o acesso a tais conhecimentos no país.

Ao proceder desse modo, a Secretaria de Governo Digital enfatiza que: a) não representa, tampouco se manifesta em nome do OWASP ou do CIS, e vice-versa; b) não é coautora das publicações internacionais abordadas; c) não assume nenhuma responsabilidade administrativa, técnica ou jurídica pelo uso ou pela interpretação inadequados, fragmentados ou parciais do presente guia; e d) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações do OWASP e do CIS em sua versão original, na língua inglesa, deverá consultar diretamente as fontes oficiais de informação ofertadas pelas referidas instituições.

Um agradecimento especial deve ser registrado ao OWASP e ao CIS pelas valiosas contribuições para a comunidade de segurança da informação.

1 https://owasp.org/
2 https://www.cisecurity.org/

INTRODUÇÃO

O guia de Segurança em Aplicações Web surge como complemento à série de guias operacionais[3] elaborados pela Secretaria de Governo Digital (SGD) da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, de modo a fomentar a adequação à proteção dos dados pessoais[4][5] e a aumentar a proteção de ambientes web da Administração Pública Federal.

O objetivo deste Guia é auxiliar aos profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação (*Security by Design*[6]). Para tanto, o Guia é inspirado nos documentos Melhores Práticas de Codificação Segura OWASP - Guia de Referência Rápida e *CIS Control*, versão 7.1. Porém, a consulta ao Guia não substitui a leitura dos documentos originais em busca de informações complementares. Ademais, é importante ressaltar que este guia não substitui normativos existentes na Administração Pública Federal que tratem do mesmo assunto.

É fundamental que a Instituição conheça e adeque seus processos de desenvolvimento e sustentação de Software ao previsto na Norma Complementar nº 16 DSIC/GSIPR, de 21/11/12, que trata de diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração.

Ao longo do guia, as diretrizes que o desenvolvimento seguro deve seguir são detalhadas e os respectivos requisitos de segurança que devem ser avaliados para cada diretriz são listados.

O documento será atualizado à medida que novos ajustes forem necessários para acompanhar o amadurecimento dos processos de segurança da informação e as novas tecnologias vigentes.

Ressalta-se que a instituição é livre para adequar todas as proposições deste guia a sua realidade. A abordagem oferece uma visão geral dos principais requisitos e orientações

[3] https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd

[4] Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 28 fev. 2021.

[5] Guia de Boas Práticas LGPD. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em 28 fev. 2021.

[6] *Security-by-Design* é uma abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas. Isso inclui a incorporação de especificações de segurança no projeto, avaliação de segurança contínua em cada fase e adesão às melhores práticas (Cyber Security Agency of Singapore, 2017).

relacionadas ao desenvolvimento seguro, e estas proposições não devem ser vistas como uma referência completa e suficiente para o tema, tampouco substituir a necessidade de a instituição compreender sua própria postura de risco institucional. A intenção principal deste documento é ajudar a instituição a seguir as boas práticas de segurança e concentrar seus esforços com base nos recursos de que dispõem e integrá-los ao processo de gestão de riscos pré-existente.

1 – Diretrizes gerais

Os Controles do CIS (*Center for Internet Security*, Inc.) são um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura por meio das melhores práticas para mitigar os tipos de ataques mais comuns. Os controles foram desenvolvidos por pessoas experientes e dos mais diversos setores da economia, incluindo saúde, manufatura, educação, governo, defesa e outros.

As medidas contidas nos controles do CIS auxiliam a detecção, a resposta e a mitigação de danos provocados por esses ataques. Para este Guia, que trata de segurança em aplicações, foram escolhidos os subcontroles do controle 18 (Controle de Aplicações) do CIS como diretriz para atingir as melhores práticas no desenvolvimento seguro. Tais subcontroles estão expostos abaixo:

1. Definir práticas seguras de codificação apropriadas para a linguagem de programação e o ambiente de desenvolvimento que está sendo utilizado na instituição;
2. Para o software desenvolvido internamente, garantir que a verificação explícita de erros seja realizada e documentada para todas as entradas de dados, abrangendo verificação de tamanho, tipo e intervalos de dados, formatos aceitáveis, entre outros;
3. Verificar se a versão de todo o software adquirido de fora da instituição ainda é compatível com o ambiente de desenvolvimento ou adequadamente reforçada com base nas recomendações de segurança do desenvolvedor;
4. Utilizar apenas componentes de terceiros aprovados e atualizados para os desenvolvimentos realizados pela instituição;
5. Utilizar apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados;
6. Garantir que todos os responsáveis pelo desenvolvimento de software estejam devidamente treinados para poder escrever código seguro para seu ambiente de desenvolvimento, de acordo com suas responsabilidades específicas no contexto da instituição onde atuam;

7. Aplicar ferramentas de análise estática e dinâmica para verificar se as práticas de codificação seguras estão sendo seguidas para os softwares desenvolvidos internamente e, quando for possível, para os softwares desenvolvidos e providos por terceiros.

8. Estabelecer um processo de aceitação e tratamento de informações sobre vulnerabilidades de softwares, incluindo mecanismos para que entidades externas contactem o grupo de segurança da instituição;

9. Manter ambientes separados para sistemas de produção e não produção. Os desenvolvedores não devem ter acesso não monitorado aos ambientes de produção.

10. Proteger as aplicações web implantando firewalls de aplicação web (*Web Application Firewalls - WAFs*) que inspecionam todo o tráfego que flui para a aplicação web em busca de ataques a aplicações comuns. Para aplicações que não são baseadas no acesso web, *firewalls* de aplicação específicos devem ser implantados se essas ferramentas estiverem disponíveis para o tipo de aplicação fornecida. Se o tráfego for criptografado, o dispositivo deve possuir a capacidade de descriptografar o tráfego antes da análise. Se nenhuma das opções for apropriada, um firewall de aplicação web baseado em host deve ser implantado.

11. Para aplicações que dependem de um banco de dados, utilizar modelos de configuração de proteção padronizado. Todos os sistemas que fazem parte de processos críticos de negócios também devem ser testados.

Reforça-se que as diretrizes têm como objetivo auxiliar a instituição a amadurecer as linhas de defesa de forma gradativa e não impedem que subcontroles de perfil mais avançado sejam implementados na instituição.

2 – Requisitos gerais

Este capítulo trata de requisitos gerais que compreendem a adoção de um processo de gerenciamento de ambiente e a adoção de mecanismos de proteção do perímetro da aplicação.

Os requisitos gerais visam reduzir a exposição dos ativos a vetores de ataque, e compreendem ações como, por exemplo: aplicação de *patches* de segurança e atualização de softwares que sustentam a aplicação; eliminação de protocolos, serviços ou portas nos servidores da aplicação que não sejam essenciais para seu funcionamento; limitação da exibição de informações sobre os ativos que sustentam a aplicação; e mitigação e bloqueio de requisições suspeitas direcionadas à aplicação de forma a impossibilitar a execução de ataques.

Requisito geral 1: Gerenciamento de ambiente

O trabalho da organização na segurança das aplicações não termina quando a aplicação se torna operacional. Novos recursos de segurança e *patches* são lançados regularmente para as várias tecnologias que sustentam a aplicação, até que se tornem obsoletas ou não tenham mais suporte.

Patches de segurança e novas versões são lançadas frequentemente para corrigir as vulnerabilidades que são descobertas ao longo dos ciclos de vida das tecnologias. Por isso, é essencial monitorar as vulnerabilidades das tecnologias utilizadas pela aplicação, aplicar *patches* ordenados e oportunos em todos os sistemas afetados, bem como utilizar versões seguras.

O gerenciamento de ambiente se concentra em manter o ambiente das aplicações seguro pela aplicação de *patches* e da atualização dos softwares que sustentam a aplicação, e por meio do uso de técnicas, configurações, ferramentas e melhores práticas para eliminar potenciais vetores de ataque *(hardening)*[7].

Para que a aplicação de *patches* e atualização dos softwares sejam realizadas de forma eficiente, a organização deve adotar um processo de gerenciamento para identificar os *patches* e atualizações necessárias, planejar essas atividades, documentá-las, executá-las e, por fim, mensurar todo o processo.

[7] https://owaspsamm.org/model/operations/environment-management/

Além disso, por meio do *hardening*, busca-se blindar os componentes que sustentam a aplicação, mitigar e corrigir vulnerabilidades, e reduzir a superfície de ataque dos componentes da aplicação.

Requisito geral 2: Proteção do perímetro da aplicação

O perímetro da aplicação consiste na fronteira entre a rede interna da instituição e a Internet – ou outra rede externa.

O perímetro da aplicação inclui: roteadores de borda, Firewalls, sistemas de prevenção e detecção de intrusões (IPS e IDS), e redes de perímetro, como as zonas desmilitarizadas (ZDM).

A proteção do perímetro da aplicação consiste na aplicação de controles e regras para o tráfego que flui entre a fronteira da rede interna e externa. Esses controles de segurança visam bloquear o tráfego de rede suspeito ou malicioso, limitar o acesso às aplicações somente a endereços confiáveis e necessários, registrar informações sobre os pacotes de rede que atravessam a fronteira, de modo a identificar possíveis incidentes de segurança, impedindo-os ou reportando-os ao responsável pela segurança da aplicação. Redes de perímetro também podem ser utilizadas para separar a aplicação de outros serviços, e evitar que um potencial dano à eles possam comprometer a aplicação.

3 – Requisitos específicos

Este capítulo expõe 14 categorias de requisitos extraídos do guia de "Melhores Práticas de Codificação Segura OWASP". Tais categorias devem ser analisadas ao longo do ciclo de vida da aplicação. É importante salientar que a listagem abaixo não representa um conjunto de requisitos exaustivos:

Requisito 1: Validação dos dados de entrada

As vulnerabilidades baseadas nos dados de entrada podem surgir em qualquer funcionalidade de uma aplicação, e podem estar presentes em praticamente toda tecnologia de uso comum existente.

Uma grande variedade de ataques a aplicações web se origina ou envolve o envio de dados de entrada inesperados ou especialmente construídos para causar comportamentos

inesperados na aplicação. Sendo assim, toda entrada de dados em um sistema deve ser considerada, a princípio, não confiável.

Alguns mecanismos de defesa podem ser utilizados, conforme detalhamento disposto na tabela abaixo:

ID	Detalhamento do Controle de Segurança Crítico
1.1	Efetuar toda a validação dos dados em um sistema confiável – por exemplo, centralizar todo o processo no servidor.
1.2	Identificar todas as fontes de dados e classificá-las como sendo confiáveis ou não. Em seguida, validar os dados provenientes de fontes nas quais não se possa confiar (ex: base de dados, *stream* de arquivos etc.).
1.3	A rotina de validação de dados de entrada deve ser centralizada na aplicação.
1.4	Especificar conjunto de caracteres apropriado, como UTF-8, para todas as fontes de entrada de dados.
1.5	Codificar os dados para um conjunto de caracteres comuns antes da validação (*Canonicalize*).
1.6	Quando há falha de validação, a aplicação deve rejeitar os dados fornecidos.
1.7	Determinar se o sistema suporta conjuntos de caracteres estendidos UTF-8 e, em caso afirmativo, validar após efetuar a descodificação UTF-8.
1.8	Validar todos os dados provenientes dos clientes antes do processamento, incluindo todos os parâmetros, campos de formulário, conteúdo das URLs e cabeçalhos HTTP, como, por exemplo, os nomes e os valores dos *Cookies*. Certificar-se, também, de incluir mecanismos automáticos de *postback* nos blocos de código *JavaScript*, *Flash* ou qualquer outro código embutido.
1.9	Verificar se os valores de cabeçalho, tanto das requisições, como das respostas, contêm apenas caracteres ASCII.
1.10	Validar dados provenientes de redirecionamentos. Os atacantes podem incluir conteúdo malicioso diretamente para o alvo do mecanismo de redirecionamento, podendo assim contornar a lógica da aplicação e qualquer validação executada antes do redirecionamento.
1.11	Validar tipos de dados esperados.
1.12	Validar intervalo de dados.

1.13	Validar o tamanho dos dados.
1.14	Validar, sempre que possível, todos os dados de entrada através de um método baseado em "listas de permissões" (*whitelists*) que utilizem uma lista de caracteres ou expressões regulares para definirem os caracteres permitidos.
1.15	Se qualquer caractere potencialmente perigoso precisa ser permitido na entrada de dados da aplicação, certificar-se de que foram implementados controles adicionais como codificação dos dados de saída, *APIs* específicas que fornecem tarefas seguras e trilhas de auditoria no uso dos dados pela aplicação. A seguir, como exemplo de caracteres "potencialmente perigosos", temos: <, >, ", ', %, (,), &, +, \, \', \".
1.16	Se a rotina de validação padrão não abordar as seguintes entradas, então elas devem ser verificadas: a) Verificar bytes nulos (%00) b) Verificar se há caracteres de nova linha (%0d, %0a, \r, \n) c) Verificar se há caracteres "ponto-ponto barra" (../ ou ..\) que alteram caminhos. Nos casos de conjunto de caracteres que usem a extensão UTF-8, o sistema deve utilizar representações alternativas como: %c0%ae%c0%ae/. A canonicalização deve ser utilizada para resolver problemas de codificação dupla (*double encoding*) ou outras formas de ataques por ofuscação.

Requisito 2: Codificação de dados de saída

Com a diversidade de arquiteturas modernas de aplicações web, a realização da codificação de saída é muito importante. Pode ser difícil fornecer validação de entrada robusta em certos cenários. Portanto, o uso de APIs mais seguras com consultas parametrizadas, estruturas de modelagem com escape automático ou codificação de saída cuidadosamente escolhida é fundamental para a segurança da aplicação.

O propósito da codificação de saída é converter a entrada não confiável em uma forma segura, onde a entrada é exibida como dados para o usuário, sem executar uma codificação no navegador. A tabela a seguir detalha uma lista de subcontroles de codificação de saída.

ID	Detalhamento do Controle de Segurança Crítico
2.1	Efetuar toda a codificação dos dados em um sistema confiável - por exemplo, centralizar todo o processo no servidor.
2.2	Utilizar uma rotina padrão e testada para cada tipo de codificação de saída.
2.3	Realizar a codificação, baseada em contexto, de todos os dados enviados para o cliente que têm origem em um ambiente fora dos limites de confiança da aplicação. A codificação das entidades HTML é um exemplo, mas nem sempre funciona para todos os casos.
2.4	Codificar todos os caracteres, a menos que sejam conhecidos por serem seguros para o interpretador de destino.
2.5	Realizar o tratamento (sanitização), baseado em contexto, de todos os dados provenientes de fontes não confiáveis usados para construir consultas SQL, XML e LDAP.
2.6	Tratar todos os dados provenientes de fontes que não sejam confiáveis que gerem comandos para o sistema operacional.

Requisito 3: Autenticação e gerenciamento de credenciais

Um requisito necessário em praticamente toda aplicação é o acesso do usuário aos seus dados e às funcionalidades. Esse acesso é gerenciado normalmente por três mecanismos interrelacionados:

- Autenticação
- Gerenciamento de sessões (requisito 4)
- Controle de Acesso (requisito 5)

A autenticação é o processo que busca verificar a identidade digital de uma entidade de um sistema quando tal entidade requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo. Vide abaixo uma lista de subcontroles a serem considerados nessa hipótese:

ID	Detalhamento do Controle de Segurança Crítico
3.1	Requerer autenticação para todas as páginas e recursos, exceto para aqueles que são intencionalmente públicos.
3.2	Os controles de autenticação devem ser executados em um sistema confiável - por exemplo, centralizar todo o processo no servidor.
3.3	Sempre que possível, estabelecer e utilizar serviços de autenticação padronizados e testados.
3.4	Utilizar uma implementação centralizada para realizar os procedimentos de autenticação, disponibilizando bibliotecas que invoquem os serviços externos de autenticação.
3.5	Separar a lógica de autenticação do recurso que está a ser requisitado e usar redirecionadores dos controladores de autenticação centralizados.
3.6	Quando ocorrerem situações excepcionais nos controles de autenticação, executar procedimentos em caso de falha com o propósito de manter o sistema seguro.
3.7	Todas as funções administrativas e de gerenciamento de contas devem ser tão seguras quanto o mecanismo de autenticação principal.
3.8	Se a aplicação gerenciar um repositório de credenciais, esta deverá garantir que as senhas são armazenadas na base de dados somente sob a forma de resumo/hash da senha na forma de *one-way salted hashes* e que a tabela/arquivo que armazena as senhas e as próprias chaves são manipuladas apenas pela aplicação. Não utilizar algoritmos de *hash* reconhecidamente inseguros.
3.9	A geração dos resumos (*hash*) das senhas deve ser executada em um sistema confiável - por exemplo, centralizar o controle no servidor.
3.10	Validar os dados de autenticação somente no final de todas as entradas de dados, especialmente para as implementações de autenticação sequencial.
3.11	As mensagens de falha na autenticação não devem indicar qual parte dos dados de autenticação está incorreta. Por exemplo, em vez de exibir mensagens como “Nome de

	usuário incorreto" ou "Senha incorreta", utilize apenas mensagens como: "Usuário e/ou senha inválidos", para ambos os casos de erro. As respostas de erro devem ser idênticas nos dois casos.
3.12	Utilizar autenticação para conexão a sistemas externos que envolvam tráfego de informação sensível ou acesso às funções.
3.13	As credenciais de autenticação para acessar serviços externos à aplicação devem ser cifradas e armazenadas em um local protegido de um sistema confiável - por exemplo, no servidor da aplicação. Obs.: o código-fonte não é considerado um local seguro.
3.14	Utilizar apenas requisições *POST* para transmitir credenciais de autenticação.
3.15	Somente trafegar senhas (não temporárias) através de uma conexão protegida (SSL/TLS) ou no formato de dado cifrado, como no caso de envio de e-mail cifrado. Senhas temporárias enviadas por e-mail podem ser um caso de exceção aceitável.
3.16	Exigir que os requisitos de complexidade de senha estabelecidos pela política ou regulamento sejam cumpridos. As credenciais de autenticação devem resistir a ataques que, tipicamente, ameaçam o ambiente de produção. Um exemplo pode ser a exigência do uso simultâneo de caracteres alfabéticos, numéricos e/ou caracteres especiais.
3.17	Exigir que os requisitos de comprimento de senha estabelecidos pela política ou pelo regulamento sejam cumpridos. O uso de oito caracteres é o mais comum, porém usar 16 é mais recomendado. Considere, ainda, o uso de senhas que contenham várias palavras (uma frase).
3.18	A entrada da senha deve ser ocultada na tela do usuário. Em HTML, utilizar o campo do tipo "*password*".
3.19	Desativar a conta após um número pré-definido de tentativas inválidas de autenticação (e.g. cinco tentativas é o mais comum). A conta deve ser desativada por um período suficientemente longo para desencorajar a dedução das credenciais pelo método de força bruta, mas não tão longo ao ponto de permitir um ataque de negação de serviço.
3.20	Os processos de redefinição de senhas e operações de mudanças devem exigir os mesmos níveis de controle previstos para a criação de contas e autenticação.

3.21	Esquemas de pergunta/resposta (pré-definidos) usados para a redefinição da senha devem evitar ataques que lancem respostas aleatórias. Por exemplo, "livro favorito" é uma questão fraca, pois "A Bíblia" é uma resposta muito comum.
3.22	Se optar por usar redefinição de senha baseada em e-mail, envie um e-mail somente para o endereço pré-definido contendo um link ou uma senha de acesso temporário que permitam ao usuário redefinir a senha.
3.23	O tempo de validade das senhas e dos links temporários deve ser curto.
3.24	Exigir a mudança de senhas temporárias na próxima vez que o usuário realizar a autenticação no sistema.
3.25	Notificar o usuário quando a senha for reiniciada (*reset*).
3.26	Prevenir a reutilização de senhas.
3.27	As senhas devem ter, pelo menos, um dia de duração antes de poderem ser alteradas, a fim de evitar ataques de reutilização de senhas.
3.28	Garantir que a troca de senhas está em conformidade com os requisitos estabelecidos na política ou regulamento. Sistemas críticos podem exigir alterações mais frequentes nas credenciais de segurança. O tempo entre as trocas de senhas deve ser controlado administrativamente.
3.29	Desativar a funcionalidade de lembrar a senha nos campos de senha do navegador.
3.30	A data e a hora da última utilização (bem ou malsucedida) de uma conta de usuário devem ser comunicadas no próximo acesso ao sistema.
3.31	Realizar monitoramento para identificar ataques contra várias contas de usuários, utilizando a mesma senha. Esse padrão de ataque é utilizado para explorar o uso de senhas padrão.
3.32	Modificar todas as senhas que, por padrão, são definidas pelos fornecedores, bem como os identificadores de usuários (IDs), ou desativar as contas associadas.
3.33	Exigir nova autenticação dos usuários antes da realização de operações críticas.
3.34	Utilizar autenticação de múltiplos fatores (utilizando simultaneamente *token*, senha,

	biometria, etc.) para contas altamente sensíveis ou de alto valor transacional.
3.35	Caso utilize código de terceiros para realizar a autenticação, inspecione-o cuidadosamente para garantir que ele não é afetado por qualquer código malicioso.

Requisito 4: Gerenciamento de sessões

Praticamente toda sessão de usuário é implementada por meio de um token que identifica a sessão e que é concedido após o usuário se autenticar. A sessão, em si, é um conjunto de estruturas armazenadas no servidor, que mantém controle das interações do usuário com a aplicação.

A grande maioria dos ataques contra o gerenciamento de sessões de uma aplicação busca comprometer o token concedido a outros usuários. Se bem-sucedido, o autor do ataque pode se passar pelo usuário (vítima) como se fosse o usuário autenticado.

Os principais problemas surgem na forma como o token é criado – o que pode permitir a um atacante adivinhar o token de outros usuários - e na forma como os tokens são gerenciados - permitindo que um autor de ataque obtenha o token de outro usuário e, com base no envio de tal token, realize um ataque de personificação. Vide abaixo uma lista de subcontroles a serem considerados nessa hipótese:

ID	Detalhamento do Controle de Segurança Crítico
4.1	Utilizar controles de gerenciamento de sessão baseados no servidor ou em framework. A aplicação deve reconhecer apenas esses identificadores de sessão como válidos.
4.2	A criação dos identificadores de sessão deve ser sempre realizada em um sistema confiável - por exemplo, centralizado no servidor.
4.3	O controle de gestão de sessão deve usar algoritmos conhecidos, padronizados e bem testados que garantam a aleatoriedade dos identificadores de sessão.
4.4	Definir o domínio e o caminho para os cookies que contenham identificadores de sessão autenticados, para um valor devidamente restrito ao site.

4.5	A funcionalidade de saída (*logout*) deve encerrar completamente a sessão ou conexão associada.
4.6	A funcionalidade de saída (*logout*) deve estar disponível em todas as páginas que requerem autenticação.
4.7	Estabelecer um tempo de expiração da sessão que seja o mais curto possível, baseado no balanceamento dos riscos e requisitos funcionais do negócio. Na maioria dos casos, não deve ser maior que algumas horas.
4.8	Não permitir logins persistentes (sem prazo de expiração), e realizar o encerramento da sessão periodicamente, mesmo quando ela estiver ativa. Isso deve ser feito, especialmente, em aplicações que suportam várias conexões de rede ou que se conectam a sistemas críticos. O tempo de encerramento deve estar em sintonia com os requisitos do negócio e o usuário deve receber notificações suficientes para atenuar os impactos negativos dessa medida.
4.9	Se uma sessão estava estabelecida antes do login, ela deve ser encerrada para que uma nova seja estabelecida após o login.
4.10	Gerar um novo identificador de sessão quando houver uma nova autenticação.
4.11	Não permitir conexões simultâneas com o mesmo identificador de usuário.
4.12	Não expor os identificadores de sessão em URLs, mensagens de erro ou logs. Os identificadores de sessão devem apenas ser encontrados no cabeçalho do cookie HTTP. Por exemplo, não trafegar os identificadores de sessão sob a forma de parâmetros GET.
4.13	Proteger os dados de sessão do lado servidor contra acessos não autorizados por outros usuários do servidor, através da implementação de controles de acesso apropriados no servidor.

4.14	Gerar um novo identificador de sessão e desativar o antigo periodicamente. Isso pode mitigar certos cenários de ataques de sequestro de sessão (*session hijacking*), quando o identificador de sessão original for comprometido.
4.15	Gerar um novo identificador de sessão caso a segurança da conexão mude de HTTP para HTTPS, como pode ocorrer durante a autenticação. Internamente à aplicação, é recomendável utilizar HTTPS de forma constante em vez de alternar entre HTTP e HTTPS.
4.16	Utilizar mecanismos complementares ao mecanismo padrão de gerenciamento de sessões para operações sensíveis do lado servidor, como no caso de operações de gerenciamento de contas, através da utilização de tokens aleatórios ou parâmetros associados à sessão. Esse método pode ser usado para prevenir ataques do tipo *Cross Site Request Forgery* (CSRF).
4.17	Utilizar mecanismos complementares ao gerenciamento de sessões para operações altamente sensíveis ou críticas, utilizando tokens aleatórios ou parâmetros em cada requisição em vez de basear-se apenas na sessão.
4.18	Configurar o atributo "*secure*" para cookies transmitidos através de uma conexão TLS.
4.19	Configurar os cookies com o atributo "*HttpOnly*", a menos que seja explicitamente necessário ler ou definir os valores deles através de scripts do lado cliente da aplicação.

Requisito 5: Controle de acesso

Uma das principais etapas tratamento de acesso do usuário é averiguar se cada solicitação individual de acesso deve ser permitida ou negada. Se os mecanismos de validação de identidade estão funcionando corretamente, a aplicação reconhece se as requisições de acesso são válidas.

Uma aplicação pode suportar inúmeras funções de usuários, cada uma envolvendo diferentes combinações de privilégios específicos. Funções específicas podem implementar limites de transação e outras verificações, todas baseadas na identidade do usuário.

Devido à natureza complexa dos requisitos típicos de controle de acesso, tal função é uma fonte frequente de vulnerabilidades de segurança que permitem a um invasor obter acesso não autorizado a dados e funcionalidades.

Os desenvolvedores costumam fazer suposições erradas sobre como os usuários irão interagir com o aplicativo e frequentemente cometem erros ao dispensar verificações de controle de acesso de algum aplicativo. Analisar essas vulnerabilidades costuma ser trabalhoso, porque essencialmente as mesmas verificações precisam ser repetidas para cada funcionalidade da aplicação.

Devido à prevalência de falhas de controle de acesso, no entanto, esse esforço é uma atividade que pode fornecer benefícios indevidos a um autor de ataque a uma aplicação da web. Vide abaixo uma lista de subcontroles a serem considerados nessa hipótese.

ID	Detalhamento do Controle de Segurança Crítico
5.1	Utilizar apenas objetos do sistema que sejam confiáveis, como ocorre com os objetos de sessão do servidor, para realizar a tomada de decisão sobre a autorização de acesso.
5.2	Utilizar um único componente em toda a aplicação Web para realizar o processo de verificação de autorização de acesso. Isto inclui bibliotecas que invocam os serviços externos de autorização.
5.3	Quando ocorrer alguma falha no controle de acesso, ela deve ocorrer de modo seguro, sem que sejam repassados detalhes que possam facilitar ataques direcionados.
5.4	Negar todos os acessos, caso a aplicação não consiga ter acesso às informações contidas na configuração de segurança.
5.5	Garantir o controle de autorização em todas as requisições, inclusive em scripts do lado servidor, "*includes*" e requisições provenientes de tecnologias do lado cliente.
5.6	Isolar do código da aplicação os trechos de código que contêm lógica privilegiada.

5.7	Restringir o acesso aos arquivos e outros recursos, incluindo aqueles que estão fora do controle direto da aplicação, somente aos usuários autorizados.
5.8	Restringir o acesso às URLs protegidas somente aos usuários autorizados.
5.9	Restringir o acesso às funções protegidas somente aos usuários autorizados.
5.10	Restringir o acesso às referências diretas aos objetos somente aos usuários autorizados.
5.11	Restringir o acesso aos serviços somente aos usuários autorizados.
5.12	Restringir o acesso aos dados da aplicação somente aos usuários autorizados.
5.13	Restringir o acesso aos atributos e dados dos usuários, bem como informações das políticas usadas pelos mecanismos de controle de acesso.
5.14	Restringir o acesso às configurações de segurança relevantes apenas aos usuários autorizados.
5.15	As regras de controle de acesso representadas pela camada de apresentação devem coincidir com as regras presentes no lado servidor.
5.16	Se o estado dos dados deve ser armazenado no lado cliente, utilizar mecanismos de criptografia e verificação de integridade no lado servidor para detectar possíveis adulterações.
5.17	Garantir que os fluxos lógicos da aplicação obedecem às regras de negócio.
5.18	Limitar o número de transações que um único usuário ou dispositivo pode executar em determinado período de tempo. As transações por período de tempo devem estar acima das necessidades reais do negócio, mas abaixo o suficiente para impedir ataques automatizados.

5.19	Utilizar o campo "*referer*" do cabeçalho somente como forma de verificação suplementar. Ele não deve ser usado sozinho como forma de validação de autorização, pois pode ter o valor adulterado.
5.20	Se for permitida a existência de sessões autenticadas por longos períodos, fazer a revalidação periódica da autorização do usuário para garantir que os privilégios não foram modificados e, caso tenham sido, realizar o registro em log do usuário e exigir nova autenticação.
5.21	Implementar a auditoria das contas de usuário e assegurar a desativação de contas não utilizadas. Por exemplo, a conta deve ser desativada não mais do que 30 dias após a expiração da senha.
5.22	A aplicação deve dar suporte à desativação de contas e ao encerramento das sessões quando terminar a autorização do usuário - por exemplo, quando ocorrer alguma alteração dos dados do usuário, situação profissional, processos de negócio etc.
5.23	As contas de serviço ou contas de suporte a conexões provenientes ou destinadas a serviços externos devem possuir o menor privilégio possível.
5.24	Criar uma Política de Controle de Acesso para documentar as regras de negócio da aplicação, tipos de dados e critérios ou processos de autorização, para que os acessos possam ser devidamente concedidos e controlados. Isso inclui identificar requisitos de acessos - tanto para os dados, como para os recursos do sistema.
5.25	Configurar os cabeçalhos HTTP para o uso do C.O.R.S (*Cross-Origin Resource Sharing),* utilizado para permitir ou bloquear o acesso a conteúdo como AJAX, fontes em outros sites, de acordo com as regras de negócio da aplicação.

Requisito 6: Criptografia

As aplicações necessitam ser desenhadas com uma arquitetura de criptografia forte para proteger seus dados de acordo com sua classificação. Criptografar todas as informações pode ser inviável, mas não criptografar nenhum dado é um grande risco assumido. Um equilíbrio deve ser

buscado, normalmente durante a fase de desenho e projeto da aplicação. Desenhar e desenvolver a arquitetura de criptografia durante o desenvolvimento da aplicação, ou após a aplicação estar pronta, inevitavelmente irá custar muito mais que simplesmente construí-la de forma segura desde o início do desenvolvimento.

Alguns requisitos de alto nível devem ser observados:

- Os módulos de criptografia devem apresentar erros de maneira segura e ser tratados corretamente.
- Um gerador de número aleatórios seguro deve ser utilizado.
- O acesso às chaves de criptografia deve ser gerenciado de forma segura.

Ainda sobre criptografia, deve ser observado que o item 6.5, listado na tabela abaixo, deve ser implementado de forma atenta e crítica pelos gestores da área de tecnologia da informação. Isso porque o *Federal Information Processing Standard* (FIPS) 140-3 foi aprovado em 22 de março de 2019, tendo entrado em vigor em 22 de setembro de 2019[8], em substituição ao FIPS 140-2. Embora os respectivos certificados de validação do FIPS 104-3 ainda não tenham sido emitidos, há a expectativa de que isso ocorra em breve.

ID	Detalhamento do Controle de Segurança Crítico
6.1	Todas as funções de criptografia utilizadas para proteger dados sensíveis dos usuários da aplicação devem ser implantadas em um sistema confiável - neste caso, o servidor.
6.2	A senha mestra deve ser protegida contra acessos não autorizados.
6.3	Quando ocorrer alguma falha nos módulos de criptografia, permitir que ela ocorra de modo seguro.
6.4	Todos os números, nomes de arquivos, GUIDs e strings aleatórias devem ser gerados usando um módulo criptográfico com gerador de números aleatórios, somente se os valores aleatórios gerados forem impossíveis de serem deduzidos.

[8] https://www.nist.gov/news-events/news/2019/05/announcing-approval-and-issuance-fips-140-3-security-requirements

6.5	Os módulos de criptografia usados pela aplicação devem ser compatíveis com a FIPS 140-2 ou com um padrão equivalente (http://csrc.nist.gov/groups/STM/cmvp/validation.html).
6.6	Estabelecer e utilizar uma política e um processo que defina como é realizado o gerenciamento das chaves criptográficas.

Requisito 7: Tratamento de erros e logs

O principal objetivo do tratamento de erros e logs é fornecer informação útil para usuários, administradores e times de resposta a incidentes. Devem-se buscar logs de alta qualidade, com mais sinal do que ruído, de forma a evitar a criação de uma quantidade massiva de logs.

Logs com informação de qualidade normalmente possuem dados sensíveis e devem ser protegidos conforme a Norma Complementar nº 21 [9]IN01/DSIC/GSIPR, que trata de diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. Por geralmente possuírem informações bastante sensíveis, os logs também podem ser um alvo bem atraente para os atacantes.

É importante também garantir que a aplicação apresente erros de forma segura, e que esses erros não vazem informações desnecessariamente.

ID	Detalhamento do Controle de Segurança Crítico
7.1	Não expor informações sensíveis nas repostas de erros, inclusive detalhes de sistema, identificadores de sessão ou informação da conta do usuário.
7.2	Usar mecanismos de tratamento de erros que não mostrem informações de depuração (*debug*) ou informações da pilha de exceção.
7.3	Usar mensagens de erro genéricas e páginas de erro personalizadas.

[9]https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224

7.4	A aplicação deve tratar os erros sem se basear nas configurações do servidor.
7.5	A memória alocada deve ser liberada de modo apropriado quando ocorrerem condições de erro.
7.6	O tratamento de erros lógicos associados com os controles de segurança deve, por padrão, negar o acesso.
7.7	Todos os controles de log devem ser implementados em um sistema confiável, por exemplo, centralizar todo o processo no servidor.
7.8	Os controles de log devem dar suporte tanto para os casos de sucesso como os de falha relacionados com os eventos de segurança.
7.9	Garantir que os logs armazenam eventos importantes.
7.10	Garantir que as entradas de log que incluam dados nos quais não se confia não sejam executadas como código-fonte na interface de visualização de logs.
7.11	Restringir o acesso aos logs apenas para pessoal autorizado.
7.12	Utilizar uma rotina centralizada para realizar todas as operações de log.
7.13	Não armazenar informações sensíveis nos registros de logs, como detalhes desnecessários do sistema, identificadores de sessão e senhas.
7.15	Garantir o uso de algum mecanismo que conduza (ou facilite) o processo de análise de logs.
7.16	Registrar em log todas as falhas de validação de entrada de dados.
7.17	Registrar em log todas as tentativas de autenticação, especialmente as que falharam por algum motivo.
7.18	Registrar em log todas as falhas de controle de acesso.

7.19	Registrar em log todos os eventos suspeitos de adulteração, inclusive alterações inesperadas no estado dos dados.
7.20	Registrar em log as tentativas de conexão com tokens de sessão inválidos ou expirados.
7.21	Registrar em log todas as exceções lançadas pelo sistema.
7.22	Registrar em log todas as funções administrativas, inclusive as mudanças realizadas nas configurações de segurança.
7.23	Registrar em log todas as falhas de conexão TLS com o *backend*.
7.24	Registrar em log todas as falhas que ocorreram nos módulos de criptografia.
7.25	Utilizar uma função de hash criptográfica para validar a integridade dos registros de log.

Requisito 8: Proteção de dados

É necessário que a aplicação proteja os dados tratados por ela, de forma que o acesso às suas informações se restrinja ao mínimo necessário. Além disso, é importante adotar controles de segurança ao armazenar as informações para garantir que os dados necessários sejam criptografados e que informações temporárias ou registradas em cache sejam eliminadas quando não forem mais utilizadas.

É preciso também evitar que informações sensíveis sejam transportadas de forma insegura, e evitar que informações sensíveis sobre a aplicação estejam visíveis aos usuários finais.

ID	Detalhamento do Controle de Segurança Crítico
8.1	Implementar uma política de privilégio mínimo, restringindo aos usuários apenas às funcionalidades, dados e informações do sistema que são necessárias para executarem suas tarefas.

8.2	Proteger contra acesso não autorizado todas as cópias temporárias ou registradas em cache que contenham dados sensíveis e estejam armazenadas no servidor; excluir esses arquivos logo que não forem mais necessários.
8.3	Criptografar informações altamente sensíveis quando armazenadas – como dados de verificação de autenticação – mesmo que estejam no lado servidor, usando sempre algoritmos conhecidos, padronizados e bem testados. Consulte a seção que trata sobre "Práticas de Criptografia" para orientações adicionais.
8.4	Proteger o código-fonte presente no servidor para que não seja acessado por usuários não autorizados.
8.5	Não armazenar senhas, strings de conexão ou outras informações confidenciais em texto claro/legível ou em qualquer forma criptograficamente insegura no lado cliente. Isso é válido também quando há utilização de formatos inseguros, como *MS viewstate* ou código compilado que é executado no lado cliente.
8.6	Remover comentários do código de produção que podem ser acessados pelos usuários e podem revelar detalhes internos do sistema ou outras informações sensíveis.
8.7	Remover aplicações desnecessárias e documentação do sistema que possam revelar informações importantes para os autores de ataques.
8.8	Não incluir informações sensíveis nos parâmetros de requisição HTTP GET.
8.9	Desativar a funcionalidade de autocompletar nos formulários que contenham informações sensíveis, inclusive no formulário de autenticação.
8.10	Desativar a cache realizada no lado cliente das páginas que contenham informações sensíveis. O parâmetro "*Cache-Control: no-store*" pode ser usado em conjunto com o controle definido no cabeçalho HTTP "Pragma: no-cache", que é menos efetivo, porém compatível com HTTP/1.0[10].

[10] https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Headers/Pragma

8.11	A aplicação deve dar suporte à remoção de dados sensíveis quando estes não forem mais necessários - como, por exemplo, informação pessoal ou dados financeiros.
8.12	Implementar mecanismos de controle de acesso apropriados para dados sensíveis armazenados no servidor. Isto inclui dados em cache, arquivos temporários e dados que devem ser acessíveis somente por usuários específicos do sistema.
8.13	Prover mecanismos que garantam a anonimização[11] dos dados pessoais e dados pessoais sensíveis, conforme a Lei Geral de Proteção de Dados Pessoais brasileira.

Requisito 9: Segurança nas comunicações

Para transmissão de dados e informações, é ideal que se utilizem canais de comunicação seguros, o que pode ser implementado utilizando o protocolo TLS ou outra cifra forte. Devem-se utilizar de recomendações mais recentes de boas práticas de configuração para habilitar e ordenar os algoritmos e cifras preferenciais.

Algoritmos e cifras fracos, ou perto de serem considerados obsoletos, devem ser considerados somente em último caso. Algoritmos e cifras conhecidamente inseguros ou obsoletos não devem ser utilizados.

ID	Detalhamento do Controle de Segurança Crítico
9.1	Utilizar criptografia na transmissão de todas as informações sensíveis. Isto deve incluir TLS para proteger a conexão e deve ser complementado com criptografia de arquivos que contém dados sensíveis ou conexões que não usam o protocolo HTTP.
9.2	Os certificados TLS devem ser válidos, possuir o nome de domínio correto, não estar expirados e ser instalados com certificados intermediários, quando necessário.
9.3	Quando ocorrer alguma falha nas conexões TLS, o sistema não deve fornecer uma conexão insegura.

[11] Lei nº 13.709/2018, art. 6º, XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

9.4	Utilizar conexões TLS para todo o conteúdo que requerer acesso autenticado ou que contenha informação sensível.
9.5	Utilizar TLS para conexões com sistemas externos que envolvam funções ou informações sensíveis.
9.6	Utilizar um padrão único de implementação TLS configurado de modo apropriado.
9.7	Especificar a codificação dos caracteres para todas as conexões.
9.8	Filtrar os parâmetros que contenham informações sensíveis, provenientes do "*HTTP referer*", nos links para sites externos.

Requisito 10: Configuração do sistema

A configuração de uma aplicação recém-lançada deve ser segura o suficiente para estar publicada na Internet, o que significa uma configuração segura por padrão. É importante certificar que a aplicação possua:

• Um ambiente de construção seguro, repetível e automatizado;

• Biblioteca de terceiros reforçada, gerenciamento de dependência e configuração de forma que componentes desatualizados ou inseguros não sejam incluídos na aplicação;

• Uma configuração baseada no conceito *Security by Default* – a qual possui, por padrão, configurações seguras, de forma que a escolha por configurações menos rígidas de segurança seja uma escolha de administradores e usuários.

ID	Detalhamento do Controle de Segurança Crítico
10.1	Garantir que os servidores, *frameworks* e componentes do sistema estão executando a última versão aprovada.
10.2	Garantir que os servidores, *frameworks* e componentes do sistema possuem as atualizações mais recentes e seguras aplicadas para a versão em uso.

10.3	Desativar a listagem de diretórios.
10.4	Restringir, para o mínimo possível, os privilégios do servidor Web, dos processos e das contas de serviços.
10.5	Quando ocorrerem exceções no sistema, garantir que as falhas ocorram de modo seguro.
10.6	Remover todas as funcionalidades e arquivos desnecessários.
10.7	Remover código de teste ou qualquer funcionalidade desnecessária para o ambiente de produção, antes de instalar o sistema no servidor de produção.
10.8	Prevenir a divulgação da estrutura de diretórios, impedindo que robôs de busca façam indexação de arquivos sensíveis, através da configuração do arquivo "*robots.txt*". Os diretórios que não devem ser acessados por estes indexadores devem ser colocados em um diretório isolado. Assim, apenas é necessário negar o acesso ao diretório pai definido no arquivo "robots.txt", evitando ter que negar o acesso a cada diretório individualmente.
10.9	Definir quais métodos HTTP, GET ou POST a aplicação irá suportar, e se serão tratados de modo diferenciado nas diversas páginas da aplicação.
10.10	Desativar as extensões HTTP desnecessárias como, por exemplo, o *WebDAV*. Caso seja necessário o uso de alguma extensão HTTP com o propósito de suportar a manipulação de arquivos, utilize um mecanismo de autenticação conhecido, padronizado e bem testado.
10.11	Se o servidor processa tanto requisições HTTP 1.0 como HTTP 1.1, certificar-se de que ambos são configurados de modo semelhante ou assegure que qualquer diferença existente seja compreendida - como, por exemplo, o manuseio de métodos HTTP estendidos.

10.12	Remover informações desnecessárias presentes nos cabeçalhos de resposta HTTP e que podem estar relacionadas com o sistema operacional, versão do servidor web e *frameworks* de aplicação.
10.13	O armazenamento da configuração de segurança para a aplicação deve ser capaz de ser produzida de forma legível para dar suporte à auditoria.
10.14	Implementar um sistema de gestão de ativos para manter o registro dos componentes e programas.
10.15	Isolar o ambiente de desenvolvimento da rede de produção e conceder acesso somente para grupos de desenvolvimento e testes. É comum os ambientes de desenvolvimento serem configurados de modo menos seguro do que os ambientes de produção. Deste modo, os autores de ataques podem usar essa diferença para descobrir vulnerabilidades comuns ou encontrar formas de exploração.
10.16	Implementar um sistema de controle de mudanças para gerenciar e registrar as alterações no código, tanto de desenvolvimento, como dos sistemas em produção.
10.17	Rejeitar requisições que utilizem métodos (ou verbos) HTTP além do GET ou POST que não são utilizados pela aplicação (*Verb tempering attacks*), como, por exemplo, os verbos TRACE e OPTIONS e demais métodos.

Requisito 11: Segurança em Banco de Dados

A coleta e o tratamento de dados são tarefas fundamentais para que as organizações consigam, através de análises específicas, traçar metas e alcançar o objetivo final de atendimento aos usuários.

Desta forma, é fundamental que as organizações consigam garantir a proteção dos dados armazenados em banco de dados contra acessos indevidos, ações de hackers e incidentes técnicos.

ID	Detalhamento do Controle de Segurança Crítico
11.1	Usar consultas parametrizadas fortemente tipadas.
11.2	Utilizar validação de entrada e codificação de saída e assegurar a abordagem de meta caracteres. Se houver falha, o comando não deverá ser executado no banco de dados.
11.3	Certificar-se de que as variáveis são fortemente tipadas.
11.4	Realizar a codificação (*escaping*) de meta caracteres em instruções SQL.
11.5	A aplicação deve usar o menor nível possível de privilégios ao acessar o banco de dados.
11.6	Usar credenciais seguras para acessar o banco de dados.
11.7	Não incluir strings de conexão na aplicação. As strings de conexão devem estar em um arquivo de configuração separado, armazenado em um sistema confiável e as informações devem ser criptografadas.
11.8	Usar procedimentos armazenados (*stored procedures*) para abstrair o acesso aos dados e permitir a remoção de permissões das tabelas no banco de dados.
11.9	Encerrar a conexão assim que possível.
11.10	Remover ou modificar senhas-padrão de contas administrativas. Utilizar senhas robustas (pouco comuns ou difíceis de deduzir) ou implementar autenticação de múltiplos fatores. Desativar qualquer funcionalidade desnecessária no banco de dados, como "*stored procedures*" ou serviços não utilizados. Instalar o conjunto mínimo de componentes ou de opções necessárias (redução da superfície de ataque).
11.11	Eliminar o conteúdo desnecessário incluído por padrão pelo fornecedor como esquemas e bancos de dados de exemplo.

11.12	Desativar todas as contas criadas por padrão e que não sejam necessárias para suportar os requisitos de negócio.
11.13	A aplicação deve conectar-se ao banco de dados com diferentes credenciais de segurança para cada tipo de necessidade - como, por exemplo, usuário, somente leitura, convidado ou administrador.
11.14	O Banco de Dados deve ser hospedado em um servidor diferente (virtualizados ou não) dos demais serviços.
11.15	Instalar, tão logo quanto possível, *patches* e *hotfixes* de versões mais atuais validadas e homologadas.
11.16	Encriptar os Backups de modo a proteger o sigilo das informações em caso de perda ou extravio.

Requisito 12: Gerenciamento de Arquivos

É comum que as aplicações recebam arquivos do usuário. Porém, os arquivos fornecidos pelos usuários também são um vetor de ataque bastante utilizados por atacantes. Por meio do envio de arquivos maliciosos, por exemplo, é possível obter novas formas de interagir com o servidor e até executar códigos de forma remota.

Assim, é importante adotar um gerenciamento de arquivos que trate, manipule e armazene de forma segura os arquivos que possam ser manipulados pelos usuários.

ID	Detalhamento do Controle de Segurança Crítico
12.1	Não repassar dados fornecidos pelos usuários diretamente a uma função de inclusão dinâmica.
12.2	Solicitar autenticação antes de permitir que seja feito o carregamento de arquivos.
12.3	Limitar os tipos de arquivos que podem ser enviados para aceitar somente os necessários ao propósito do negócio.

12.4	Validar se os arquivos enviados são do tipo esperado, através da validação dos cabeçalhos, pois realizar a verificação apenas pela extensão é insuficiente.
12.5	Não salvar arquivos no mesmo diretório de contexto da aplicação Web. Os arquivos devem ser armazenados no servidor de conteúdos ou no banco de dados.
12.6	Prevenir ou restringir o carregamento de qualquer arquivo que possa ser interpretado ou executado pelo servidor Web.
12.7	Desativar privilégios de execução nos diretórios de armazenamento de arquivos.
12.8	Implantar o carregamento seguro nos ambientes UNIX por meio da montagem do diretório de destino como uma unidade lógica, usando o caminho associado ou o ambiente de "*chroot*".
12.9	Ao referenciar arquivos, usar uma lista de permissões (*whitelist*) de nomes e de tipos de arquivos permitidos. Realizar a validação do valor do parâmetro passado e, caso ele não corresponda ao que é esperado, rejeitar a entrada ou utilizar um valor padrão.
12.10	Não transmitir, sem nenhum tipo de tratamento, os dados informados pelo usuário a redirecionamentos dinâmicos. Se isso for necessário, o redirecionamento deverá aceitar apenas URLs relativas e validadas.
12.11	Não passar caminhos de diretórios ou de arquivos em requisições. Usar algum mecanismo de mapeamento desses recursos para índices definidos em uma lista pré-definida de caminhos.
12.12	Nunca enviar o caminho absoluto do arquivo para o lado cliente de uma aplicação ou para o usuário.
12.13	Certificar-se de que os arquivos da aplicação e os recursos estão definidos somente com o atributo de leitura.

12.14	Verificar os arquivos que os usuários submeterem através do mecanismo de carregamento em busca de vírus e *malwares*.
12.15	Limitar o tamanho máximo aceito para *uploads* de arquivos no servidor.

Requisito 13: Gerenciamento de memória

Informações sensíveis ou úteis a um atacante podem ser armazenadas ou acessadas na memória por meio de técnicas e funções que permitem esse acesso. Além disso, atacantes podem se utilizar da técnica de transbordamento de dados (*buffer overflow)* -na qual o programa, ao escrever dados em um buffer, ultrapassa o limite de tamanho do buffer, sobrescrevendo a memória adjacente – para acessar endereços de memória ou injetar códigos maliciosos.

Nesse contexto, é de suma importância que os desenvolvedores implementem técnicas e controles que garantam que a aplicação fará o gerenciamento e o uso adequado dos recursos de memória, visando com isso a evitar que processos legítimos sejam impactados por ações internas ou externas que possam comprometer o comportamento esperado do sistema ou degradar a performance da aplicação.

ID	Detalhamento do Controle de Segurança Crítico
13.1	Utilizar controle de entrada/saída para os dados que não sejam confiáveis.
13.2	Verificar se o *buffer* é tão grande quanto o especificado.
13.3	Ao usar funções que aceitem determinado número de bytes para realizar cópias, como *strncpy*(), estar ciente de que, se o tamanho do *buffer* de destino for igual ao tamanho do *buffer* de origem, ele não pode encerrar a sequência de caracteres com valor nulo (*null*).
13.4	Verificar os limites do *buffer* caso as chamadas à função sejam realizadas em ciclos e verificar se não há nenhum risco de ocorrer gravação de dados além do espaço reservado.

13.5	Truncar todas as strings de entrada para um tamanho razoável antes de passá-las para as funções de cópia e concatenação.
13.6	Na liberação de recursos alocados para objetos de conexão, identificadores de arquivo etc., não contar com o "*garbage collector*" e realizar a tarefa explicitamente.
13.7	Usar pilhas não executáveis, quando disponíveis.
13.8	Evitar o uso de funções reconhecidamente vulneráveis, como *printf(), strcat(), strcpy()* etc.
13.9	Liberar a memória alocada de modo apropriado após concluir a sub-rotina (função/método) e em todos os pontos de saída.

Requisito 14: Práticas Gerais de Codificação

Com o advento da metodologia de desenvolvimento "*DevOps*", os procedimentos de segurança, adotados outrora pela equipe de arquitetura de segurança, devem ser readequados para que a rotina de análise de segurança de aplicações seja introduzida nesse novo contexto de desenvolvimento ágil.

Os procedimentos de análise de segurança são vistos normalmente como inflexíveis e excessivamente assertivos pelos profissionais de desenvolvimento de aplicações, já que estes podem, em diversas oportunidades, argumentar que existem várias maneiras de resolver um problema. De fato, quando se aborda a arquitetura de softwares e aplicações, não existe solução única e simples para determinado problema.

É provável que uma função específica de uma aplicação web seja revisada continuamente ao longo de sua vida útil, mas a arquitetura geral raramente mudará e pode passar por evoluções graduais. O mesmo quadro acontece quando se fala de arquitetura de segurança. Ao desenvolver uma aplicação web com controles de segurança desde sua concepção, a organização interessada provavelmente irá poupar tempo e dinheiro, reduzindo as chances da ocorrência de incidentes de segurança.

ID	Detalhamento do Controle de Segurança Crítico
14.1	Para tarefas comuns, utilizar sempre código testado, gerenciado e aprovado, ao invés de criar código novo e não gerenciado.
14.2	Utilizar APIs que executem tarefas específicas para realizar operações do sistema operacional. Não permitir que a aplicação execute comandos diretamente no sistema operacional, especialmente através da utilização de "*shells*" de comando iniciadas pela aplicação.
14.3	Utilizar mecanismos de verificação de integridade por "*checksum*" ou "*hash*" para verificar a integridade do código interpretado, bibliotecas, arquivos executáveis e arquivos de configuração.
14.4	Utilizar mecanismos de bloqueio para evitar requisições simultâneas para a aplicação ou utilizar um mecanismo de sincronização para evitar condições de concorrência (*race conditions*).
14.5	Proteger as variáveis compartilhadas e os recursos contra acessos concorrentes inapropriados.
14.6	Instanciar explicitamente todas as variáveis e dados persistentes durante a declaração, ou antes da primeira utilização.
14.7	Quando a aplicação tiver que ser executada com privilégios elevados, aumentar os privilégios o mais tarde possível e revogá-los logo que seja possível.
14.8	Evitar erros de cálculo decorrentes da falta de entendimento da representação interna da linguagem de programação usada e de como é realizada a interação com os aspectos de cálculo numérico.
14.9	Prestar bastante atenção nas discrepâncias de tamanho de byte, precisão, distinções de sinal (*signed/unsigned*), truncamento, conversão e "*casting*" entre os tipos, cálculos que devolvam erros do tipo "*not-a-number*" e, também, como a linguagem de

	programação trata a representação interna de números muito grandes ou muito pequenos.
14.10	Não transferir diretamente dados fornecidos pelo usuário para qualquer função de execução dinâmica sem antes realizar o tratamento dos dados de modo adequado.
14.11	Restringir a geração e a alteração de código por parte dos usuários.
14.12	Revisar todas as aplicações secundárias, códigos e bibliotecas de terceiros para determinar a necessidade do negócio e validar as funcionalidades de segurança, uma vez que estas podem introduzir novas vulnerabilidades.
14.13	Implementar atualizações de modo seguro. Se a aplicação precisar realizar atualizações automáticas, utilizar mecanismos de assinatura digital para garantir a integridade do código e garantir que os clientes façam a verificação da assinatura após descarregarem as atualizações. Usar canais criptografados para transferir o código a partir do host do servidor.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013**: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2019**: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019**: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 31000:2018**: Gestão de Riscos — Diretrizes. Rio de Janeiro, 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 23 fev. 2021.

AUDITSCRITPS. CIS Controls Initial Assessment Tool, versão 7.1d. Disponível em: < https://www.auditscripts.com/download/4229/ >. Acesso: 28 fev. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. **Glossário de Segurança da Informação**. Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663 >. Acesso em: 23 fev. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa nº 01**, de 27 de maio de 2020. Brasília, DF, GSI/PR, 2020. Disponível em: < http://dsic.planalto.gov.br/assuntos/editoria-

c/documentos-pdf-1/instrucao-normativa-no-1-de-27-de-maio-de-2020-1.pdf >. Acesso em: 24 fev. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar nº 16** /IN01/DSIC/GSIPR - Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta, de 21 de novembro de 2012. Brasília, DF, GSI/PR, 2012. Disponível em: < https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=21/11/2012&jornal=1&pagina=1&totalArquivos=200 >. Acesso em: 02 mar. 2021.

CENTER INTERNET SECURITY. **CIS Controls**, versão 7.1. Abril de 2019. Disponível em: < https://learn.cisecurity.org/cis-controls-download >. Acesso em: 28 fev. 2021.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD.** Agosto de 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd >. Acesso em: 28 fev. 2021.

CYBER SECURITY AGENCY OF SINGAPORE (CSA). **Security-by-Design Framework Versão 1.0**. Singapura, 2017. Disponível em: < https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf >. Acesso em: 28 fev. 2021.

INTERNATIONAL STANDARD. **ISO/IEC 29100:2011**: Information technology — Security techniques — Privacy framework. Genebra, 2011.

INTERNATIONAL STANDARD. **ISO/IEC 29134:2017**: Information technology – Security techniques – Guidelines for privacy impact assessment. Genebra, 2017.

INTERNATIONAL STANDARD. **ISO/IEC 29151:2017**: Information technology — Security techniques — Code of practice for personally identifiable information protection. Genebra, 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica, versão 1.1, 2018. Disponível em: < https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf >. Acesso em: 28 fev. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity**, versão 1.1, 2018. Disponível em: < https://doi.org/10.6028/NIST.CSWP.04162018 >. Acesso em: 28 fev. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-53 revisão 5**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, 2020.

THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP). **Melhores práticas de Codificação Segura – Guia de Referência Rápida.** Versão 1.3. Disponível em: <https://owasp.org/images/b/b3/OWASP_SCP_v1.3_pt-BR.pdf>. Acesso em: 22 de mar. 2021.

THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP). **Software Assurance Maturity Model.** Versão 2. Disponível em: < https://owasp.org/www-project-samm/>. Acesso em: 22 de mar. 2021.