ANEXO 9 - Contrato 6097-00

PADRÕES DE SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS PROCERGS

Este anexo tem o objetivo de descrever os padrões mínimos de segurança a serem observados no desenvolvimento e na manutenção de sistemas mantidos pela PROCERGS.

1. O desenvolvimento de software na PROCERGS deve estar aderente à Política de Segurança da Informação e Cibernética, bem como com as demais normas e diretrizes que venham a ser instituídas sobre o tema.

Essas diretrizes incluem, dentre outras determinações, o uso de repositórios oficiais, a segregação adequada de ambientes para desenvolvimento, o uso seguro de credenciais, bem como práticas relacionadas ao controle de acesso, proteção de dados e governança do código-fonte.

2. Riscos de Segurança em Aplicações Web

Os sistemas desenvolvidos para a PROCERGS e seus clientes devem adotar medidas rigorosas de prevenção contra riscos de segurança em aplicações Web, tendo como referência a compilação elaborada pelo projeto OWASP (*Open Worldwide Application Security Project*), que identifica as dez principais categorias de riscos de segurança conhecidas como OWASP Top 10 (https://owasp.org/Top10/2025).

Ressalta-se que os riscos de segurança em aplicações Web não se limitam exclusivamente aos itens descritos no OWASP Top 10, devendo as equipes adotarem uma abordagem abrangente e contínua de segurança ao longo de todo o ciclo de vida do software.

A seguir, apresenta-se o OWASP Top 10 – 2025, com descrições resumidas para fins de orientação e prevenção:

2.1. A01:2025 - *Broken Access Control* (Quebra de Controle de Acesso): Falhas de controle de acesso ocorrem quando usuários conseguem executar ações ou acessar dados além do que deveria ser permitido. Geralmente decorrem de regras de autorização ausentes ou insuficientes no servidor, validações inconsistentes ou políticas de acesso mal definidas.

2.2. A02:2025 - *Security Misconfiguration* (Configuração Incorreta de Segurança): Inclui configurações inseguras, permissões mal implementadas, serviços expostos desnecessariamente e funcionalidades habilitadas sem necessidade, especialmente em ambientes com múltiplas camadas de configuração (aplicação, infraestrutura e componentes integrados).

2.3. A03:2025 - *Software Supply Chain Failures* (Falhas na Cadeia de Suprimentos de Software):
Envolve riscos relacionados a dependências e componentes de terceiros, softwares e canais de distribuição desatualizados e falha no controle dos componentes utilizados, podendo resultar na introdução de código malicioso, adulteração de artefatos ou exploração de bibliotecas vulneráveis e processos de build inseguros.

2.4. A04:2025 - *Cryptographic Failures* (Falhas Criptográficas):
Refere-se ao uso inadequado de mecanismos criptográficos para proteção de dados em trânsito e em repouso, incluindo a escolha incorreta de algoritmos ou parâmetros, gerenciamento inadequado de chaves criptográficas e configurações inseguras.

2.5. A05:2025 - *Injection* (Injeção):
Ocorre quando entradas de usuário não confiáveis são enviadas a uma aplicação ou banco de dados, por exemplo, e interpretadas como comandos, consultas ou instruções pelo sistema. Abrange ataques como SQL *Injection*, injeção de comandos, templates, entre outros, podendo resultar em acesso indevido, alteração de dados ou execução não autorizada.

2.6. A06:2025 - *Insecure Design* (Design Inseguro):
Refere-se a falhas originadas na definição de requisitos e decisões de arquitetura, como a ausência de modelagem de ameaças e de requisitos de segurança, tornando o sistema vulnerável por concepção.

2.7. A07:2025 - *Authentication Failures* (Falhas de Autenticação):
Inclui problemas relacionados a mecanismos de login, recuperação de conta, gerenciamento de sessões e tokens, bem como falhas em proteções contra abuso, podendo permitir uso indevido de credenciais, sequestro de sessão e acesso não autorizado.

2.8. A08:2025 - *Software or Data Integrity Failures* (Falhas de Integridade de Software ou Dados):
Ocorre quando o sistema não valida adequadamente a origem e integridade de código, atualizações, bibliotecas, artefatos, dados ou mensagens, permitindo adulteração de componentes, inserção de conteúdo malicioso e quebra de limites de confiança.

2.9. A09:2025 - *Security Logging and Alerting Failures* (Falhas de Registro e Alerta de Segurança):
Falhas de registro e alerta acontecem quando logs são insuficientes, inconsistentes ou não acionáveis, ou quando não existem mecanismos de alerta capazes de gerar resposta adequada a eventos relevantes. Isso reduz a capacidade de detectar incidentes, investigar eventos e responder a ameaças em tempo hábil.

2.10. A10:2025 - Mishandling of Exceptional Conditions (Tratamento Inadequado de Condições Excepcionais):
Esta categoria trata do tratamento inadequado de erros e condições anormais, incluindo falhas como comportamento do tipo fail-open, erros lógicos e exposição de informações sensíveis em mensagens de erro, além de comportamentos inesperados que podem ser explorados em cenários de exceção.

3. Checklist de Validação de Segurança no Desenvolvimento Web

Este checklist apresenta controles essenciais de segurança para aplicações web, não sendo uma lista exaustiva e devendo ser complementado por outras boas práticas conforme o contexto.

3.1. Validação de entrada de dados
Validar, filtrar e limitar tipo, formato, tamanho e faixa de valores de todos os dados de entrada, independentemente da origem (usuário, APIs, arquivos ou outros sistemas).

3.2. Tratamento de warnings e erros de build
Atentar para warnings e mensagens do processo de build, tratando-os como potenciais falhas de segurança. Sempre que possível, configurar o build para falhar em warnings críticos.

3.3. Simplicidade e clareza de código
Manter o código simples, legível e modular, reduzindo a superfície de ataque e facilitando revisões, auditorias e manutenção.

3.4. Negar por padrão (Deny by default)
Adotar o princípio de negar o acesso por padrão para páginas, funcionalidades, APIs, botões e campos, liberando apenas o que for explicitamente autorizado.

3.5. Princípio do menor privilégio
Garantir que usuários, serviços, processos e integrações possuam apenas os privilégios mínimos necessários para executar suas funções.

3.6. Sanitização e minimização de dados em integrações
Sanitizar, validar e minimizar os dados enviados para outros sistemas, evitando o compartilhamento de informações desnecessárias ou sensíveis.

3.7. Funções intrinsecamente seguras
Implementar validações e controles de segurança o mais próximo possível da lógica crítica, evitando depender exclusivamente de validações externas.

3.8. Tratamento adequado de erros e exceções
Verificar e tratar corretamente códigos de erro, exceções e retornos inesperados, evitando falhas silenciosas, estados inconsistentes ou vazamento de informações internas.

3.9. Uso correto de tipos e limites
Atentar para limites de tipos, conversões e castings, prevenindo erros como overflows, underflows e falhas lógicas que possam gerar vulnerabilidades.

3.10. Documentação do código e decisões de segurança
Documentar o código, incluindo decisões relevantes de segurança, validações críticas e comportamentos esperados, facilitando manutenção e auditorias.

3.11. Conformidade com a especificação
Garantir que a implementação siga fielmente os requisitos funcionais e de segurança definidos na especificação e nos requisitos do sistema.

3.12. Autenticação, autorização e sessão
Assegurar mecanismos adequados de autenticação e autorização, com proteção de sessão (expiração, invalidação, cookies seguros e proteção contra ataques de força bruta).

3.13. Gestão de senhas e credenciais
Nunca versionar senhas, tokens, chaves ou credenciais no código-fonte. Utilizar mecanismos seguros de armazenamento e rotação de credenciais.

3.14. Criptografia de dados sensíveis
Garantir o uso de criptografia forte para dados sensíveis em trânsito e em repouso, evitando algoritmos proprietários ou obsoletos.

3.15. Logs e monitoramento de segurança
Registrar eventos relevantes de segurança de forma adequada, garantindo que logs não exponham informações sensíveis.

3.16. Dependências e bibliotecas
Manter dependências atualizadas, remover bibliotecas não utilizadas e monitorar vulnerabilidades conhecidas em componentes de terceiros.

3.17. Testes e revisões de segurança
Realizar revisões de código focadas em segurança e, sempre que possível, utilizar testes automatizados e ferramentas de análise de vulnerabilidades.

4. Riscos de Segurança em Aplicações Mobile

Os sistemas mobile desenvolvidos para a PROCERGS e seus clientes devem adotar medidas rigorosas de prevenção contra riscos de segurança em aplicações mobile, tendo como referência a compilação elaborada pelo OWASP (*Open Worldwide Application Security Project*), que identifica as dez principais categorias de riscos conhecidas como OWASP Mobile Top 10 (https://owasp.org/www-project-mobile-top-10/).

Ressalta-se que os riscos de segurança em aplicações mobile não se limitam exclusivamente aos itens descritos no OWASP Mobile Top 10, devendo ser adotadas práticas abrangentes e contínuas de segurança ao longo de todo o ciclo de vida do aplicativo, desde o design até a distribuição e manutenção.

A seguir, apresenta-se o OWASP Mobile Top 10 – 2024, com descrições resumidas para fins de orientação e prevenção:

4.1. M1:2024 - *Improper Credential Usage* (Uso Inadequado de Credenciais)
O uso inadequado de credenciais em aplicativos móveis, como credenciais embutidas no código ou armazenadas de forma insegura, pode permitir que agentes de ameaça realizem ataques automatizados. Esses agentes podem localizar e explorar essas credenciais para obter acesso não autorizado a dados sensíveis, funcionalidades do aplicativo ou serviços de back-end.

4.2. M2:2024 - *Inadequate Supply Chain Security* (Segurança Inadequada da Cadeia de

Suprimentos)
Vulnerabilidades na cadeia de suprimentos de aplicativos móveis podem permitir a inserção de código malicioso durante o desenvolvimento, compilação ou distribuição do aplicativo. A exploração de bibliotecas de terceiros, SDKs ou fornecedores comprometidos pode resultar em roubo de dados, espionagem, negação de serviço ou controle total do aplicativo ou dispositivo.

4.3. M3:2024 - *Insecure Authentication/Authorization* (Autenticação/Autorização Insegura)
Falhas nos mecanismos de autenticação e autorização podem ser exploradas por agentes de ameaça para contornar controles de acesso ou obter privilégios indevidos. Esses ataques normalmente utilizam ferramentas automatizadas para explorar fragilidades em logins, tokens, sessões ou validações inadequadas de autorização.

4.4. M4:2024 - *Insufficient Input/Output Validation* (Validação Insuficiente de Entrada/Saída)
A validação e higienização insuficientes da entrada e saída de dados em aplicativos móveis pode expor o aplicativo a ataques como injeção de SQL, injeção de comandos e *cross-site scripting* (XSS). Essas vulnerabilidades podem resultar em acesso não autorizado a dados sensíveis, manipulação da lógica da aplicação e comprometimento de sistemas associados.

4.5. M5:2024 - *Insecure Communication* (Comunicação Insegura)
A comunicação insegura entre aplicativos móveis e servidores remotos pode permitir a interceptação e modificação de dados quando não há criptografia adequada ou quando são utilizados protocolos obsoletos. Atacantes podem atuar por meio de redes Wi-Fi comprometidas, dispositivos de rede não confiáveis ou malware presente no próprio dispositivo móvel.

4.6. M6:2024 - *Inadequate Privacy Controls* (Controles de Privacidade Inadequados)
A ausência de controles adequados de privacidade pode resultar na exposição indevida de informações de identificação, como dados pessoais, financeiros ou sensíveis. Essas informações podem ser utilizadas para fraude, uso indevido de dados, chantagem ou comprometimento da integridade, confidencialidade e disponibilidade das informações do usuário.

4.7. M7:2024 - *Insufficient Binary Protections* (Proteção Binária Insuficiente)
A falta de proteções adequadas nos binários de aplicativos móveis pode permitir a extração de senhas, chaves de API, lógica de negócio ou modelos de IA pré-treinados. Além disso, binários podem ser alterados para burlar controles de segurança, acessar recursos pagos ou distribuir versões maliciosas do aplicativo.

4.8. M8:2024 - *Security Misconfiguration* (Configuração de Segurança Incorreta)
Configurações incorretas de segurança, controle de acesso e permissões em aplicativos móveis podem expor funcionalidades e dados sensíveis, a acessos não autorizados. Essas falhas podem ser exploradas por atacantes com acesso físico ao dispositivo ou por aplicativos maliciosos executados no mesmo ambiente.

4.9. M9:2024 - *Insecure Data Storage* (Armazenamento de Dados Inseguro)

O armazenamento inseguro de dados em aplicativos móveis pode permitir que agentes maliciosos acessem informações sensíveis armazenadas localmente. Fragilidades como criptografia inadequada, uso incorreto de armazenamento local e proteção insuficiente de credenciais aumentam significativamente o risco de vazamento de dados.

4.10. M10:2024 - *Insufficient Cryptography* (Criptografia Insuficiente)

O uso de criptografia fraca, obsoleta ou mal implementada pode comprometer a confidencialidade, integridade e autenticidade das informações. Atacantes podem explorar essas falhas para descriptografar dados sensíveis, manipular informações ou realizar fraudes.

5. Checklist de validação de segurança no desenvolvimento mobile.

Este checklist reúne princípios básicos de segurança para aplicações móveis, não esgotando todas as diretrizes aplicáveis, que devem ser avaliadas conforme o contexto e os riscos.

5.1. Identificação e proteção de dados sensíveis em dispositivos móveis

Identificar dados sensíveis manipulados pela aplicação móvel e garantir sua proteção adequada, incluindo armazenamento seguro, criptografia e controle de acesso no dispositivo.

5.2. Gerenciamento seguro de credenciais no dispositivo

Armazenar e gerenciar credenciais de forma segura, evitando armazenamento em texto claro e utilizando mecanismos seguros fornecidos pelo sistema operacional (ex.: Keychain, Keystore).

5.3. Proteção de informações sensíveis em trânsito

Assegurar que todas as informações sensíveis transmitidas entre o aplicativo e serviços remotos sejam protegidas por canais seguros, utilizando criptografia forte e protocolos adequados.

5.4. Autenticação, autorização e gerenciamento de sessão

Implementar corretamente mecanismos de autenticação do usuário, autorização de acesso e gerenciamento de sessão, incluindo expiração, invalidação e proteção contra uso indevido.

5.5. Segurança das APIs e do back-end

Garantir que as APIs de back-end e a infraestrutura de servidores sejam devidamente protegidas, aplicando controles de autenticação, autorização, validação de entrada e proteção contra abusos.

5.6. Integração segura com serviços e aplicativos de terceiros

Assegurar que integrações com serviços e aplicativos de terceiros sejam realizadas de forma segura, minimizando dados compartilhados e avaliando riscos associados a dependências externas.

5.7. Consentimento para coleta e uso de dados do usuário
Coletar, armazenar e gerenciar o consentimento do usuário de forma clara, segura e rastreável, garantindo conformidade com requisitos legais e de privacidade.

5.8. Proteção contra acesso não autorizado a recursos pagos ou sensíveis
Implementar controles para impedir o acesso não autorizado a recursos do dispositivo ou serviços pagos, como carteira, SMS, chamadas telefônicas e outros recursos sensíveis.

5.9. Provisionamento e distribuição segura de aplicações móveis
Assegurar que o processo de build, assinatura, provisionamento e distribuição das aplicações móveis seja realizado de forma segura, prevenindo adulteração e distribuição não autorizada.

5.10. Tratamento seguro de erros em tempo de execução
Verificar e tratar cuidadosamente erros de interpretação de código e exceções em tempo de execução, evitando falhas inesperadas, comportamentos inseguros ou exposição de informações internas.

6. Referências:

1 - Política de Segurança da Informação e Cibernética da PROCERGS
2 - https://owasp.org/www-project-top-ten/
3 - https://owasp.org/Top10/2025
4 - https://owasp.org/www-project-mobile-top-10/
5 - https://owasp.org/www-project-mobile-security/