

# Relacionamento entre Sentenças e Riscos de Segurança

Favor indicar a qual risco de segurança do OWASP Top 10 cada sentença está associada. Mais de um opção pode ser selecionada (Ex: Uma sentença pode estar associada a dois riscos diferentes).

Desde já, obrigado por contribuir para a melhoria da segurança do software brasileiro.

Para quaisquer outras dúvidas, faça contato com [rnpelat@gmail.com](mailto:rnpelat@gmail.com).

- 1. O PHPUnit se integra bem com a maioria das IDEs para desenvolvimento PHP tais como Eclipse, NetBeans, ZendStudio, etc., além de ser uma ferramenta facilmente utilizável por linha de comando.**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código

- 2. Todas as páginas e recursos requerem autenticação exceto aquelas que especificamente devem ser públicas.**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

- 3. O uso da senha de acesso ao sistema eletrônico é de inteira e exclusiva responsabilidade do licitante, incluindo qualquer transação efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao (...), promotor da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)

- 4. Serviços de Analise de Suporte Banco de Dados nível II: formação superior concluída na área de tecnologia da informação, experiência comprovada por atestado e/ou treinamento certificado de no mínimo 5 (cinco) anos em analise de suporte em administração de banco de dados Oracle, MySQL ou Postgre, linguagem PL/SQL e SQL Standard e certificação fornecida pelo fabricante.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

- 5. Aplicação protege adequadamente as variáveis e recursos compartilhados contra acesso concorrente inapropriado.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos

**6. Exemplo de Query Binds pelo PHP @param string \$strUsuarioNome \* @param string \$strSenha \* @return integer \*/ function exemploDeAcessoBanco( \$strUsuarioNome, \$strSenha ) { \$strUsuarioNome = (string)\$strUsuarioNome; \$strSenha = (string)\$strSenha; \$objBanco = new PDO('pgsql:dbname=database'); \$objComando = \$objBanco->prepare( " SELECT co\_usuario FROM usuario WHERE no\_usuario = :usuario AND ds\_senha = :senha" ); \$objComando->bindParam(':usuario', \$strUsuarioNome ); \$objComando->bindParam(':senha', md5( \$strSenha ) ); \$objResultado = \$objComando->execute(); return (integer)\$objResultado->co\_usuario; } ?>", import java.util.List; import javax.management.Query; import javax.persistence.EntityManager; import javax.persistence.Query;import org.apache.commons.lang.StringUtils;\* \* Exemplo de Query Binds para JPA abstract class exemploQueryBinds { (...) public List<Usuario> getUsuarioPeloNome(String strNome) { String strConsulta = ""+ "SELECT "+ " u "+ " FROM"+ " Usuario u " + " WHERE " + " LOWER( Usuario.strNome ) = :nomeUsuario"; Query objComando = getEntityManager().createQuery(strConsulta).**

*Check all that apply.*

- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)

**7. Identificação da sessão é alterada ou cancelada no logout.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis

**8. Comprovada, de no mínimo 6 (seis) anos como programador JAVA especificadamente em projetos de desenvolvimento e manutenção de sistemas; Experiência em desenvolvimento de sistemas baseado no processo unificado (UP) ou similar; Experiência em leitura de modelos UML; Conhecimento da técnica de desenvolvimento XP; Conhecimentos HTML, CSS e Java Script; Conhecimentos de SQL; Conhecimento na plataforma Jcompany; Conhecimento na elaboração de testes unitários.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código

**9. Todas as funções criptográficas usadas para proteger segredos do usuário da aplicação são implementadas no lado servidor.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos

**10. Os documentos apresentados nesta licitação deverão: a) estar em nome da licitante, com um único número de CNPJ; b) estar no prazo de validade estabelecido pelo órgão expedidor; c) ser apresentados em original, em publicação da imprensa oficial ou em cópia autenticada por cartório, por pregoeiro ou por servidor da (...).**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso

**11. Todos os módulos criptográficos falham de forma segura (princípio do fail safe).**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis

**12. Um único controle de validação de entrada é usado pela aplicação para cada tipo de dado que é aceito.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)

**13. Deve-se utilizar parâmetros sempre que um valor for passado à query***Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**14. Alguns Componentes: Autenticação, Lista de Controle de Acesso( ACL ), Cache, Configuração, Mail, Session, Internacionalização.***Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**15. Todas as funções de gerenciamento de contas são no mínimo tão resistentes a ataques quanto o mecanismo primário de autenticação.***Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso

**16. Todos os códigos que implementam ou usam controles de acesso não são afetados por qualquer código malicioso.***Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)

**17. Todos os controles de validação de entrada não são afetados por qualquer código malicioso.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código

**18. Aplicação não registra dados sensíveis específicos da aplicação que poderiam ajudar um atacante, incluindo identificadores de sessão do usuário e informações pessoais ou sensíveis.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)

**19. Todas as falhas na validação de entradas resultam na rejeição ou sanitização da entrada.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso

**20. Mesmas regras de controle de acesso aplicadas pela camada de apresentação são executadas no lado servidor.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código

**21. Identificação da sessão é alterada no login.***Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**22. Os Webservices devem ser utilizados mediante autenticação com usuário e senha, utilizando o perfil "UsernameToken" definido na especificação WS-Security e autenticação segura por meio do protocolo HTTPS.***Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)

**23. Todos os códigos que implementam ou usam controles de autenticação não são afetados por qualquer código malicioso.***Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso

**24. Controles de codificação/escape de saídas codificam todos os caracteres desconhecidos para garantir segurança ao interpretador***Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso

25. **Todos os documentos exigidos no presente instrumento convocatório poderão ser apresentados em original, por qualquer processo de cópia autenticada por tabelião, ou publicação em órgão da imprensa oficial**

*Check all that apply.*

- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos

26. **Todos os formulários que contenham informações sensíveis têm desabilitado o cache do lado do cliente, incluindo recursos de auto completar.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A3 – Cross-Site Scripting (XSS)

27. **Produção Instalação própria (...) Sistema Web Linux/Windows, Java SQL Server, I"MER Código Sigla Sistema Nome Sistema (...) Gerenciar toda a sistemática de avaliação para progressão funcional dos servidores (...)**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos

28. **Toda resposta HTTP contém um cabeçalho do tipo de conteúdo (content type header) especificando um conjunto seguro de caracteres (por exemplo, UTF-8).**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso

29. **Existe um padrão único de implementação do TLS, usado pela aplicação, que é configurado para operar de maneira aprovada\*. Veja <http://csrc.nist.gov/groups/STM/cmvp/documents/fips1402/FIPS1402IG.pdf>.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código

30. **Possui automatização de lógicas de pesquisa QBE (Query by Example).**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso

31. **Usuários podem acessar somente os dados para os quais eles possuem autorização específica.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

32. **Aplicação gera um token aleatório como parte de todos os links e formulários associados com transações ou no acesso a informações sensíveis, e se a aplicação verifica a presença desse token com o valor adequado para o usuário atual no processamento dessas requisições.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso

**33. Usuários podem acessar somente arquivos para os quais eles possuem autorização específica.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso

**34. Desenvolvedor/Engenheiro de SW Perfil a) Curso superior completo na área de informática; b) Experiência comprovada em programação Java para Web e ambientes corporativos; Pelo menos 1/3 da equipe de desenvolvedores deverá possuir Certificação Java Programmer; c) Experiência na utilização de linguagens de consulta a banco de dados (SQL e PL/SQL); d) Conhecimento de Programação Java utilizando Web Services, XML.**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis

**35. Os documentos exigidos neste edital poderão ser apresentados no original, por cópia autenticada por tabelião, ou publicação em órgão da imprensa oficial, ou cópia acompanhada do original para conferência pelo Pregoeiro.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso

**36. O acesso a estas informações deve ser protegido por senha e conexão segura ou outro método equivalente.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código

**37. Tokens de sessões autenticadas são suficientemente longos e randômicos para resistir aos ataques que são típicos das ameaças no ambiente implantado.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código

**38. A partir do horário previsto no Edital, a sessão pública na internet será aberta por comando do Pregoeiro**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso

**39. Identificação da sessão é alterada na re-autenticação.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso

**40. Os documentos e anexos exigidos, quando remetidos via fax, deverão ser apresentados em original ou por cópia autenticada, nos prazos estabelecidos no Edital.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código

**41. Outras Funcionalidades:** Em qualquer momento durante a execução da sessão pública, o Pregoeiro pode: Reabrir uma Fase: A razão será registrada no chat e, após o comando do Pregoeiro, automaticamente, o sistema o direcionará para a fase .

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**42. Todos os dados não confiáveis que são saídas para interpretadores SQL, usam interfaces parametrizadas, instruções preparadas ou realizam o escape apropriado.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos

**43. Controles de acesso falham de forma segura (princípio do fail safe).**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A1 – Injeção de código

**44. Uma arquitetura de alto nível para a aplicação foi definida.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso

**45. Usuários podem acessar somente serviços para os quais eles possuem autorização específica.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos

**46. Módulo de Fiscalização Sistema de Capacitação e Administração de Brigada Sistema Nacional de Informações sobre Fogo (...) Sistema de comunicação de acidentes ambientais com informações espaciais (...) Sala de Comando Controle e Comunicação da (...) Portal Nacional dos Planos de emergência individual e planos de ação de emergência licenciados (...) Sistema Informatizado de Licenciamento do Transporte Interestadual de Cargas Perigosas.**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código

**47. Todas as credenciais de autenticação para acesso a serviços externos à aplicação são cifradas e armazenadas em um local protegido (não dentro do código-fonte).**

*Check all that apply.*

- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

48. **Empresa criadora da plataforma Java. HTML Session HTTP/IDE Java Java EE Login MVC Query RAD SGBD Stored Procedure SQL SOA Sun DOCUMENTO DE ARQUITETURA DE REFERÊNCIA DE SOFTWARE (...) DIRETORIA DE INFORMÁTICA GERÊNCIA DE TECNOLOGIA UNIDADE DE INOVAÇÃO E ARQUITETURA DE TI WAP W3C Sigla para Wireless Application Protocol: Protocolo para Aplicações sem Fio.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código

49. **Lógica de tratamento de erros nos controles de segurança nega o acesso por padrão.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código

50. **Deverão ser empregadas tecnologias como GED/ECM, certificação digital, computação móvel, CBS Computação Baseada em Servidor, Data Warehouse, Workflow, arquitetura orientada a serviços, dentre outras.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código

**51. Possibilitar uma seleção estadual (...) WEB/PHP/PostGreSQL/Informativo Eletrônico Inscrição (...) PRÓCONSELHO Divulgar os boletins de serviço das Secretarias e Subsecretarias (...) WEB WEB/ASP ASP/SQLServer 2000 SQL. Provê o cadastro de cursos que fazem parte do Programa Nacional (...) Catálogo de Sistemas Versão 1.0 de 24/06/2010 Sigla do Sistema Nome do Sistema (...) CONSELHO (...) OBJETIVO Plataforma Linguagem SGBD (...) Integração SBA x SGB alinhado a política do Governo Federal (...).**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código

**52. Aplicação aceita somente um conjunto definido de métodos de requisição HTTP, tais como GET e POST.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código

**53. Um caminho pode ser construído a partir de uma CA confiável para cada certificado de servidor Transport Layer Security (TLS), e se cada certificado de servidor é válido.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)

- 54. Todos os atributos de dados e usuários e informações de política usados pelos controles de acesso não podem ser manipulados pelos usuários finais a menos que especificamente autorizado.**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

- 55. A Contratada deverá prover a Contratante de informação detalhada da execução dos serviços, por intermédio de ferramenta, em tempo real, protegida por senha e conexão segura.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso

- 56. Os documentos necessários à habilitação poderão ser apresentados no seu original, ou por cópia autenticada em Cartório de Notas ou por servidor público competente, ou publicação em órgão da imprensa oficial ou, ainda, por cópias acompanhadas dos originais para conferência pelo Pregoeiro.**

*Check all that apply.*

- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso

- 57. Todos os controles de autenticação (incluindo bibliotecas que chamam serviços de autenticação externa) tem uma implementação centralizada.**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

58. **Todos os dados não confiáveis que são saídas para HTML (incluindo elementos HTML, valores de dados javascript, blocos CSS, atributos URI) realizam o escape apropriado para o contexto da aplicação.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código
- A3 – Cross-Site Scripting (XSS)

59. **Caso sejam detectadas falhas nos produtos que estão em processo de homologação, mesmo após a vigência contratual, a CONTRATADA deverá providenciar as devidas correções em até 72 horas, sem ônus para a CONTRATANTE e, no caso de falhas no ambiente de produção, imediatamente.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código

60. **Todas as informações sensíveis em cache ou as cópias temporárias enviadas ao cliente são protegidas contra acesso não autorizado, ou se elas são removidas /invalidadas após serem acessadas por um usuário autorizado (por exemplo, os cabeçalhos no-cache e no-store Cache-Control são definidos).**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso

61. **Todos os componentes que não são parte da aplicação, mas que a aplicação depende para operar, estão identificados**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)

**62. Oferece ainda como ferramenta o Profiler (permite a verificação das queries executadas no banco durante um período)**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos

**63. Usuários podem acessar somente funções protegidas para as quais eles possuem autorização específica**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso

**64. Todos os códigos que implementam ou usam controles de gerenciamento de sessões não são afetados por qualquer código malicioso.**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis

**65. Os documentos poderão ser apresentados em original, cópia autenticada por Cartório ou cópia simples, para autenticação por membro da Comissão de Licitação, neste caso acompanhado dos originais, não sendo aceitos fac-símiles (fax).**

*Check all that apply.*

- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**66. Todos os dados não confiáveis que são incluídos em parâmetros de comandos do sistema operacional realizam o escape apropriado.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso

**67. Os comandos feitos pela persistência devem ser coerentes ao comando que o Banco de Dados é capaz de interpretar.**

*Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso
- A1 – Injeção de código

**68. Lista de dados sensíveis processados pela aplicação é identificada, e que existe uma política explícita de como o acesso a esses dados deve ser controlado e quando estes dados devem ser cifrados (tanto em repouso quanto em trânsito). Verificar se esta política é devidamente aplicada.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso

**69. Todos os códigos que implementam ou usam tratamento de erros e controles de logs não são afetados por qualquer código malicioso.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis

**70. Todos os controles de autenticação falham de forma segura (princípio do fail safe).***Check all that apply.*

- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos

**71. Usuários podem acessar somente URLs para as quais eles possuem autorização específica.***Check all that apply.*

- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso

**72. Todos os dados sensíveis são enviados para o servidor no corpo da mensagem HTTP (parâmetros URL nunca são usados para enviar dados sensíveis).***Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)

**73. Todas as decisões de autenticação são registradas (logs).***Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código

74. A CONTRATADA contratada do Lote 02 deverá prover o CONTRATANTE de informação detalhada da execução dos serviços, por meio de ferramenta, em tempo real, protegida por senha

*Check all that apply.*

- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

75. A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha privativa do licitante e subsequente encaminhamento da Proposta de Preços (...)

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código

76. Um número máximo de tentativas de autenticação for excedido, a conta é bloqueada por um período de tempo suficiente para deter os ataques de força bruta.

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- A7 – Falta de Função para Controle do Nível de Acesso

77. Implementação padrão do gerenciamento de sessões do framework é utilizada pela aplicação.

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A3 – Cross-Site Scripting (XSS)
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**78. Limitações de entrada e de acesso impostas pelo negócio na aplicação (tais como limites de transações diárias ou sequenciamento de tarefas) não podem ser burladas.**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A3 – Cross-Site Scripting (XSS)
- A1 – Injeção de código

**79. Interfaces do controle de segurança são simples o suficiente para que os desenvolvedores as utilizem corretamente.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**80. Cookies que contêm os tokens/identificadores de sessões autenticadas têm seu domínio e caminho definidos para um valor adequadamente restritivo para o site.**

*Check all that apply.*

- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão

**81. Assegurar, nos casos de desastres naturais, acidentes, falhas de equipamentos, falhas de segurança, perda de serviços e ações intencionais, que por ventura possam ocorrer em seu ambiente, a continuidade da prestação dos serviços, por meio da execução de planos de contingência, visando à recuperação das operações a tempo de não causar paralisação dos serviços prestados à CONTRATANTE.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- Não se Relaciona com Nenhum desses Riscos
- A7 – Falta de Função para Controle do Nível de Acesso

**82. Acesso a qualquer segredo master é protegido de acesso não autorizado (Um segredo master é uma credencial da aplicação armazenada em texto claro no disco que é usada para proteger o acesso às informações de configuração de segurança).**

*Check all that apply.*

- Não se Relaciona com Nenhum desses Riscos
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código

**83. Todas as decisões de controle de acesso são registradas (logs), inclusive as decisões de falha de acesso.**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos
- A1 – Injeção de código

84. **Lista de acrônimos em uso no texto APF ASP CASE CFPS CGSI CMMI COBIT CPM CSM CSS DTDIE EGTI E-MAG (...) E-PING HTML IFFPUG ISO ITIL MPS.BR NBR NESMA Análise de Pontos de Função; Active Server Pages; ComputerAided Software Engineering; Certified Function Point Specialist; Coordenação-Geral de Sistemas de Informação; Capability Maturity Model Integration; Control Objectives For Information and Related Technology ; Counter Practices Manual; Certified Scrum Máster; Cascade Style Sheet; (...) Estratégia Geral de Tecnologia da Informação; Modelo de Acessibilidade de Governo Eletrônico; (...) Padrões de Interoperabilidade de Governo Eletrônico; Hyper Text Markup Language; Instituição de Ensino Superior; International Function Point Users Group; (...) International Organization for Standardization ; Information Technology Infrastructure Library; (...) Melhoria de Processos do Software Brasileiro; Norma da Associação Brasileira de Normas Técnicas (ABNT); Netherlands Software Metrics Association; NMA O&M OS PDTI PF PHP PMBOK PMI PMP RE SAEB SCBCD SCDJWS SCJD SCJP SCWCD SEFTI SICAF (...) SQL TCU TI TIC UML UP VB XML XSL ZCE Nota Mensal de Avaliação; Organização e Métodos; Ordem de Serviço; Plano Diretor de Tecnologia da Informação; Ponto de Função; Hypertext Preprocessor; Project Management Body of Knowledge; Project Management Institute; Project Management Professional; Relação de Empregados; (...) Sun Certified Business Component Developer; Sun Certified Developer For Java Web Services; Sun Certified Java Developer; Sun Certified Java Programmer; Sun Certified Web Component Developer; Secretaria de Fiscalização de Tecnologia da Informação; Sistema Integrado de Cadastro de Fornecedores;(...); Structured Query Language; (...) Tecnologias da Informação e Comunicação; Unified Modeling Language; Unified Process; Visual Basic; Extensible Markup Language; Extensible Stylesheet Language; Zend Certified Engineer.**

*Check all that apply.*

- A1 – Injeção de código
- A6 – Exposição de Dados Sensíveis
- A3 – Cross-Site Scripting (XSS)
- A7 – Falta de Função para Controle do Nível de Acesso
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- Não se Relaciona com Nenhum desses Riscos

85. **As principais ferramentas são o Management Studio (visualizador de objetos e processador de queries) e o Query Analyzer (processador de queries).**

*Check all that apply.*

- A3 – Cross-Site Scripting (XSS)
- Não se Relaciona com Nenhum desses Riscos
- A6 – Exposição de Dados Sensíveis
- A2 – Quebra de Autenticação e Gerenciamento de Sessão
- A1 – Injeção de código
- A7 – Falta de Função para Controle do Nível de Acesso

**86. A participação dos interessados, no dia e hora fixados no preâmbulo deste Edital, dar-se-á por meio de digitação da senha privativa do licitante e subsequente encaminhamento da proposta de preços com valores expressos na moeda oficial do Brasil, exclusivamente por meio eletrônico.**

*Check all that apply.*

- A2 – Quebra de Autenticação e Gerenciamento de Sessão
  - A3 – Cross-Site Scripting (XSS)
  - A1 – Injeção de código
  - A7 – Falta de Função para Controle do Nível de Acesso
  - Não se Relaciona com Nenhum desses Riscos
  - A6 – Exposição de Dados Sensíveis
-