

# 8 responses

[View all responses](#)
[Publish analytics](#)

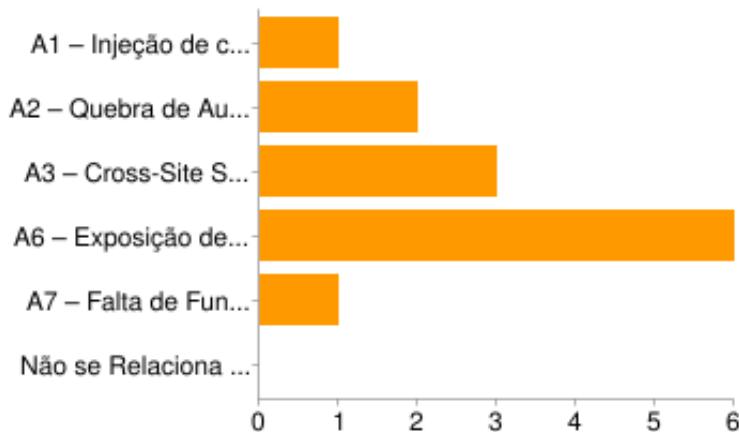
## Summary

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	60%
Não se Relaciona com Nenhum desses Riscos	<b>2</b>	40%

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



A1 – Injeção de código	<b>1</b>	16.7%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	33.3%
A3 – Cross-Site Scripting (XSS)	<b>3</b>	50%
A6 – Exposição de Dados Sensíveis	<b>6</b>	100%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	16.7%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	80%

**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.**



A1 – Injeção de código	<b>3</b>	60%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>5</b>	100%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

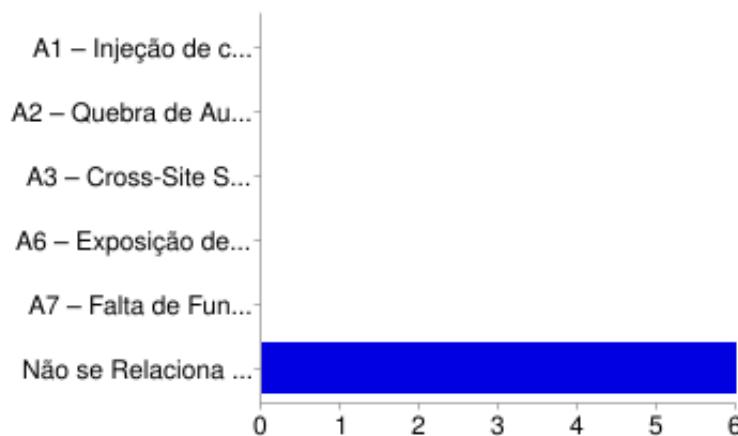
**Todos os atributos de dados e usuários e informações de política usados pelos controles de acesso não podem ser manipulados pelos usuários finais a menos que especificamente autorizado.**



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%

A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>5</b>	100%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>6</b>	100%

**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**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	33.3%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%

A6 – Exposição de Dados Sensíveis	<b>1</b>	16.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>3</b>	50%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>5</b>	100%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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 .**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%

A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	100%

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



A1 – Injeção de código	<b>3</b>	50%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	33.3%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	33.3%
A6 – Exposição de Dados Sensíveis	<b>3</b>	50%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	33.3%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	16.7%

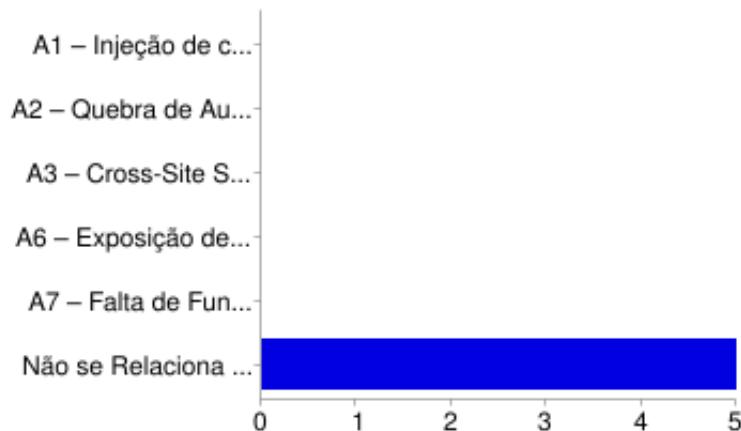
**Cookies que contêm os tokens/identificadores de sessões autenticadas têm seu domínio e caminho definidos para um valor adequadamente restritivo para o site.**



A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>5</b>	83.3%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	66.7%
A6 – Exposição de Dados Sensíveis	<b>3</b>	50%

A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	50%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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 (...).**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	100%

**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**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%

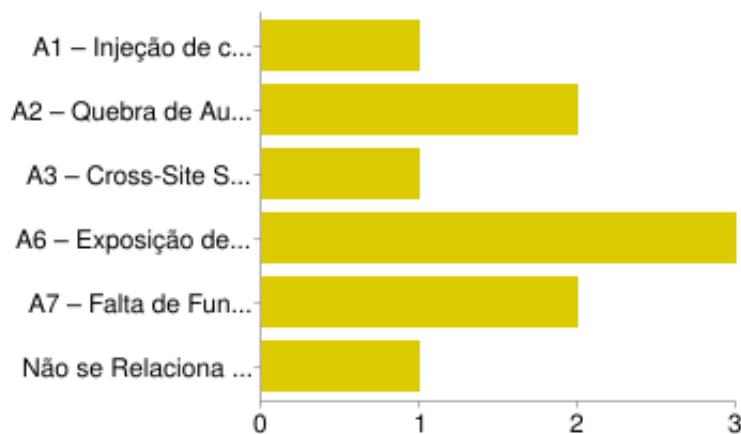
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	100%

**Deve-se utilizar parâmetros sempre que um valor for passado à query**



A1 – Injeção de código	<b>5</b>	100%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

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



A1 – Injeção de código	0	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	0	0%
A3 – Cross-Site Scripting (XSS)	0	0%
A6 – Exposição de Dados Sensíveis	0	0%
A7 – Falta de Função para Controle do Nível de Acesso	0	0%
Não se Relaciona com Nenhum desses Riscos	5	100%

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



A1 – Injeção de código	2	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	5	100%
A3 – Cross-Site Scripting (XSS)	2	40%
A6 – Exposição de Dados Sensíveis	2	40%
A7 – Falta de Função para Controle do Nível de Acesso	2	40%
Não se Relaciona com Nenhum desses Riscos	0	0%

**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.**



A1 – Injeção de código	<b>1</b>	16.7%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>5</b>	83.3%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	16.7%
A6 – Exposição de Dados Sensíveis	<b>4</b>	66.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	50%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>4</b>	80%
A7 – Falta de Função para Controle do Nível de Acesso	<b>5</b>	100%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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.**



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	80%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	80%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	60%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



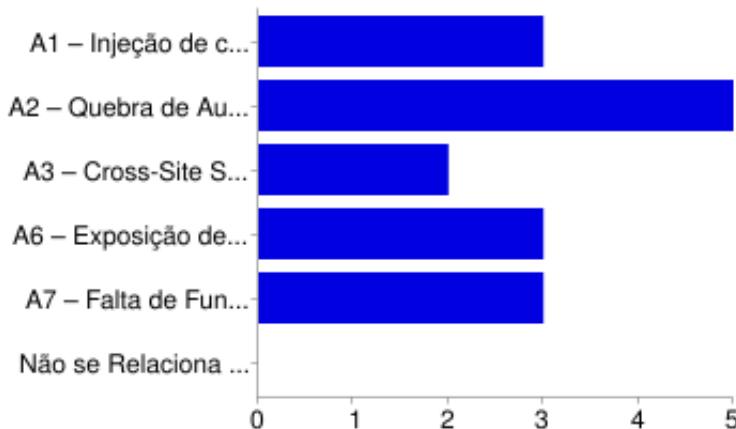
A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	50%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	33.3%
A6 – Exposição de Dados Sensíveis	<b>3</b>	50%
A7 – Falta de Função para Controle do Nível de Acesso	<b>5</b>	83.3%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

## Uma arquitetura de alto nível para a aplicação foi definida.



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>6</b>	100%

## Todos os controles de autenticação falham de forma segura (princípio do fail safe).



A1 – Injeção de código	<b>3</b>	50%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>5</b>	83.3%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	33.3%
A6 – Exposição de Dados Sensíveis	<b>3</b>	50%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	50%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**Lista de acrônimos em uso no texto APF ASP CASE CFPS CGSI CMMI COBIT CPM CSM CSS DTDIE EGTI E-MAG (...) E-PING HTML IFPUG 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.**



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	80%

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



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>5</b>	100%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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.**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>6</b>	100%

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



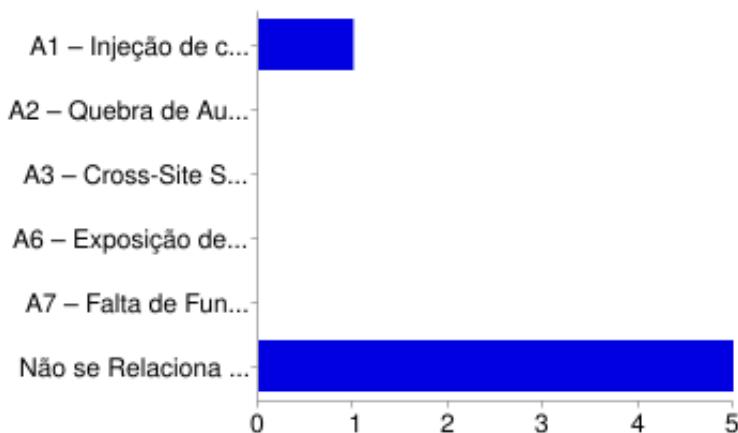
A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	80%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	80%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>4</b>	80%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>1</b>	16.7%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	83.3%

**Usuários podem acessar somente URLs para as quais eles possuem autorização específica.**



A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	33.3%
A3 – Cross-Site Scripting (XSS)	<b>3</b>	50%
A6 – Exposição de Dados Sensíveis	<b>2</b>	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	<b>5</b>	83.3%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>3</b>	42.9%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	57.1%
A3 – Cross-Site Scripting (XSS)	<b>3</b>	42.9%
A6 – Exposição de Dados Sensíveis	<b>5</b>	71.4%
A7 – Falta de Função para Controle do Nível de Acesso	<b>7</b>	100%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>4</b>	80%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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.**



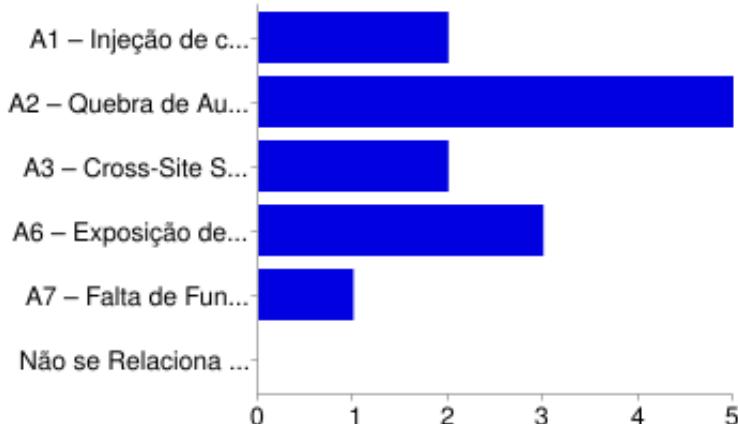
A1 – Injeção de código	<b>1</b>	16.7%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	16.7%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	16.7%
A6 – Exposição de Dados Sensíveis	<b>1</b>	16.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	16.7%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	83.3%

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



A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	16.7%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	16.7%
A6 – Exposição de Dados Sensíveis	<b>2</b>	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	33.3%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	66.7%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>5</b>	100%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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.**



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

**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.**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	100%

**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).

```



A1 – Injeção de código	<b>4</b>	80%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	80%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

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



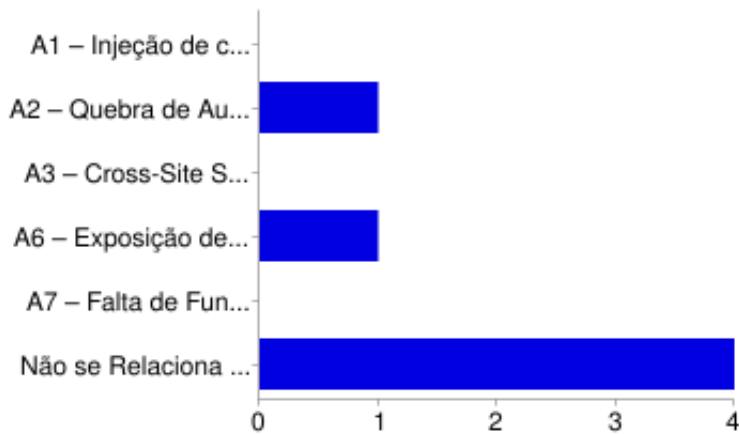
A1 – Injeção de código	<b>2</b>	28.6%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	57.1%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	14.3%
A6 – Exposição de Dados Sensíveis	<b>6</b>	85.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>6</b>	85.7%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	100%

**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.**



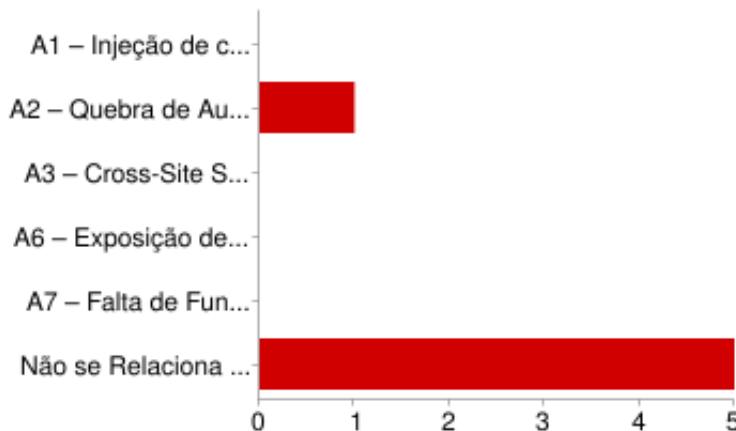
A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	16.7%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>1</b>	16.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	66.7%

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



A1 – Injeção de código	<b>5</b>	83.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	50%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	66.7%
A6 – Exposição de Dados Sensíveis	<b>2</b>	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	33.3%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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.**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	16.7%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	83.3%

**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.**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	100%

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



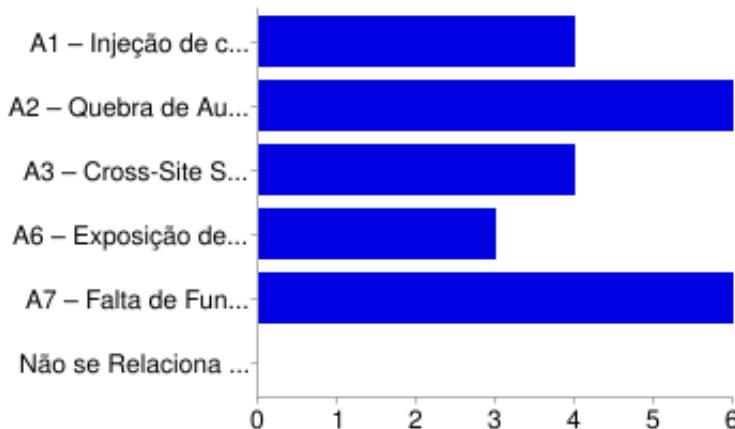
A1 – Injeção de código	<b>6</b>	100%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	33.3%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	33.3%
A6 – Exposição de Dados Sensíveis	<b>2</b>	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	33.3%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>5</b>	100%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>4</b>	57.1%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>6</b>	85.7%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	57.1%
A6 – Exposição de Dados Sensíveis	<b>3</b>	42.9%
A7 – Falta de Função para Controle do Nível de Acesso	<b>6</b>	85.7%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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).**



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>5</b>	100%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	60%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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.**



A1 – Injeção de código	1	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	1	20%
A3 – Cross-Site Scripting (XSS)	0	0%
A6 – Exposição de Dados Sensíveis	1	20%
A7 – Falta de Função para Controle do Nível de Acesso	0	0%
Não se Relaciona com Nenhum desses Riscos	4	80%

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



A1 – Injeção de código	1	14.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	2	28.6%
A3 – Cross-Site Scripting (XSS)	1	14.3%
A6 – Exposição de Dados Sensíveis	1	14.3%
A7 – Falta de Função para Controle do Nível de Acesso	1	14.3%
Não se Relaciona com Nenhum desses Riscos	5	71.4%

**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> ).**



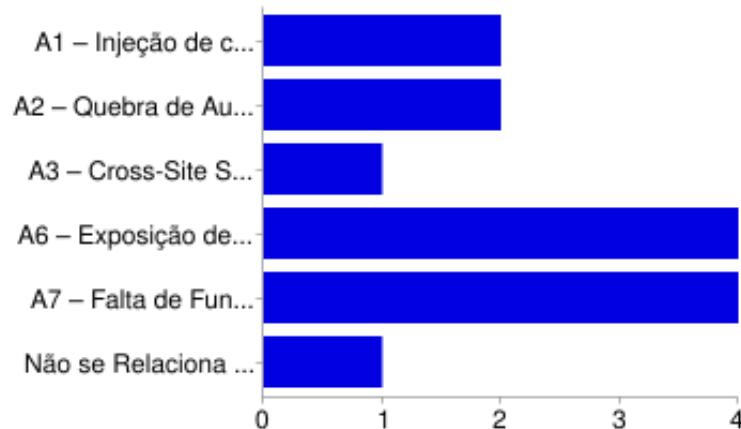
A1 – Injeção de código	<b>2</b>	28.6%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	57.1%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	28.6%
A6 – Exposição de Dados Sensíveis	<b>5</b>	71.4%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	14.3%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	14.3%

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



A1 – Injeção de código	<b>5</b>	83.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	50%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	66.7%
A6 – Exposição de Dados Sensíveis	<b>2</b>	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	<b>4</b>	66.7%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>4</b>	80%
A7 – Falta de Função para Controle do Nível de Acesso	<b>4</b>	80%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>5</b>	100%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**Controles de codificação/escape de saídas codificam todos os caracteres desconhecidos para garantir segurança ao interpretador**



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>3</b>	60%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

**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.



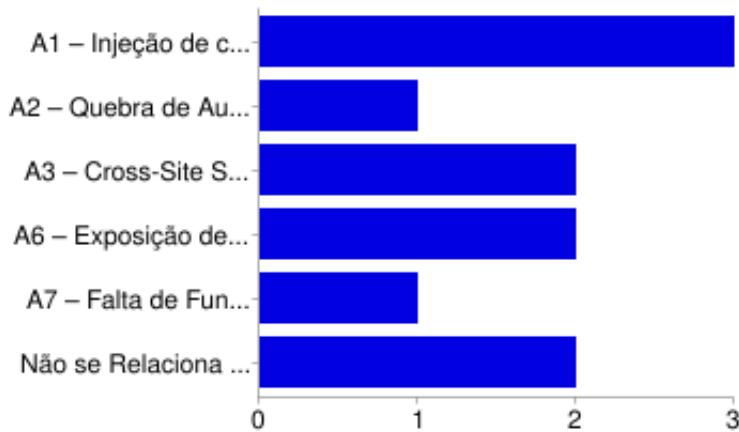
A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>4</b>	80%

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



A1 – Injeção de código	<b>6</b>	100%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	66.7%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	66.7%
A6 – Exposição de Dados Sensíveis	<b>3</b>	50%
A7 – Falta de Função para Controle do Nível de Acesso	<b>5</b>	83.3%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>3</b>	60%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>2</b>	40%

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



A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	66.7%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	33.3%
A6 – Exposição de Dados Sensíveis	<b>3</b>	50%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	50%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	16.7%

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



A1 – Injeção de código	<b>2</b>	28.6%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	42.9%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	57.1%
A6 – Exposição de Dados Sensíveis	<b>4</b>	57.1%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	42.9%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	14.3%

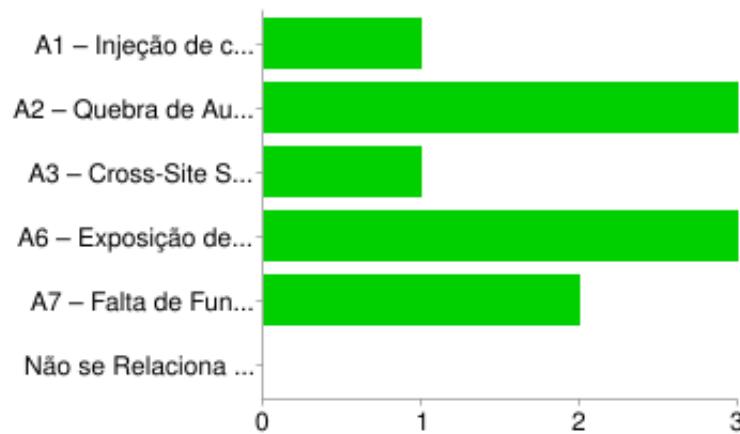
**Desenvolvedor/Engenheiro de SW Perfil a) Curso superior completo na área de informática; b) Experiência comprovada em programação Java para Web e ambientes corporativos; Pelo menos 1/3 da equipe de desenvolvedores deverá possuir Certificação Java Programmer; c) Experiência na utilização de linguagens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



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	100%

**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.**



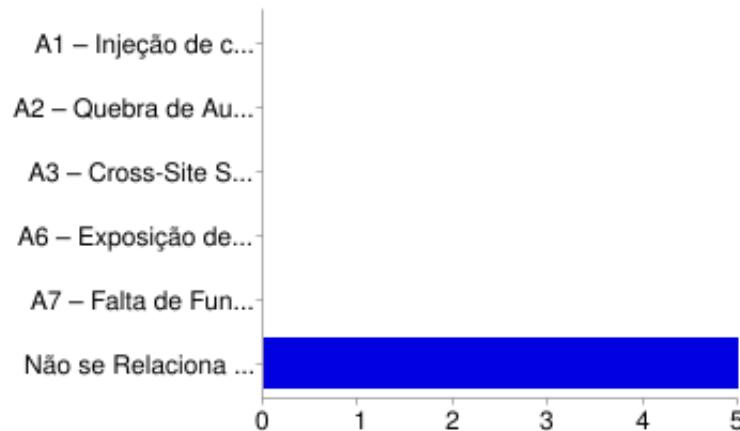
A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>4</b>	80%
A6 – Exposição de Dados Sensíveis	<b>1</b>	20%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

**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.**



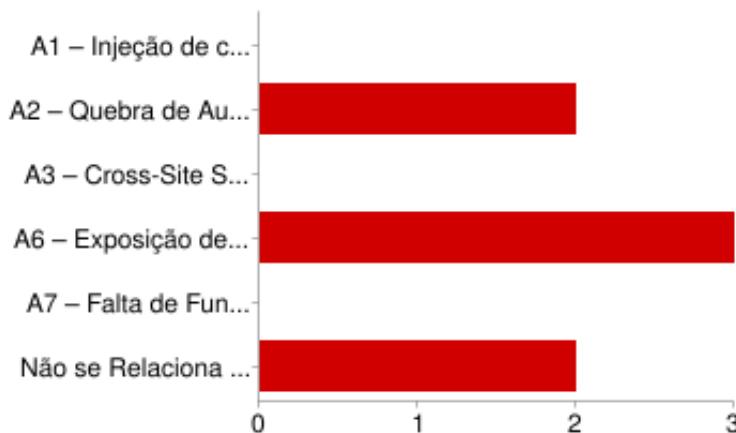
A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>5</b>	100%

**Identificação da sessão é alterada no login.**



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	80%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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.**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>2</b>	40%

**Alguns Componentes: Autenticação, Lista de Controle de Acesso( ACL ), Cache, Configuração, Mail, Session, Internacionalização.**



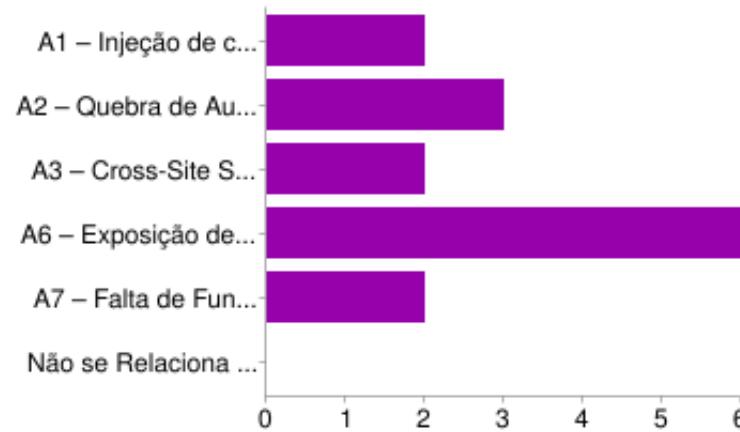
A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>5</b>	83.3%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	16.7%
A6 – Exposição de Dados Sensíveis	<b>4</b>	66.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>4</b>	66.7%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	16.7%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>3</b>	60%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	60%
Não se Relaciona com Nenhum desses Riscos	<b>2</b>	40%

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



A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	50%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	33.3%
A6 – Exposição de Dados Sensíveis	<b>6</b>	100%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	33.3%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**Todas as decisões de autenticação são registradas (logs).**



A1 – Injeção de código	<b>1</b>	16.7%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	66.7%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	33.3%
A6 – Exposição de Dados Sensíveis	<b>2</b>	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	16.7%
Não se Relaciona com Nenhum desses Riscos	<b>2</b>	33.3%

**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.**



A1 – Injeção de código	<b>1</b>	16.7%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	66.7%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	16.7%
A6 – Exposição de Dados Sensíveis	<b>4</b>	66.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	33.3%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	16.7%

**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).**



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>4</b>	80%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

**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.**



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>4</b>	80%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>1</b>	20%

**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.**



A1 – Injeção de código	<b>3</b>	60%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>1</b>	20%
A3 – Cross-Site Scripting (XSS)	<b>3</b>	60%
A6 – Exposição de Dados Sensíveis	<b>2</b>	40%
A7 – Falta de Função para Controle do Nível de Acesso	<b>1</b>	20%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

**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).**



A1 – Injeção de código	<b>1</b>	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	40%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	20%
A6 – Exposição de Dados Sensíveis	<b>5</b>	100%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>2</b>	40%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>3</b>	60%
A3 – Cross-Site Scripting (XSS)	<b>2</b>	40%
A6 – Exposição de Dados Sensíveis	<b>4</b>	80%
A7 – Falta de Função para Controle do Nível de Acesso	<b>2</b>	40%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>4</b>	66.7%
A3 – Cross-Site Scripting (XSS)	<b>3</b>	50%
A6 – Exposição de Dados Sensíveis	<b>1</b>	16.7%
A7 – Falta de Função para Controle do Nível de Acesso	<b>5</b>	83.3%
Não se Relaciona com Nenhum desses Riscos	<b>0</b>	0%

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



A1 – Injeção de código	<b>2</b>	33.3%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>2</b>	33.3%
A3 – Cross-Site Scripting (XSS)	<b>1</b>	16.7%
A6 – Exposição de Dados Sensíveis	<b>2</b>	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	<b>3</b>	50%
Não se Relaciona com Nenhum desses Riscos	<b>2</b>	33.3%

**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.**



A1 – Injeção de código	<b>0</b>	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	<b>0</b>	0%
A3 – Cross-Site Scripting (XSS)	<b>0</b>	0%
A6 – Exposição de Dados Sensíveis	<b>0</b>	0%
A7 – Falta de Função para Controle do Nível de Acesso	<b>0</b>	0%
Não se Relaciona com Nenhum desses Riscos	<b>7</b>	100%

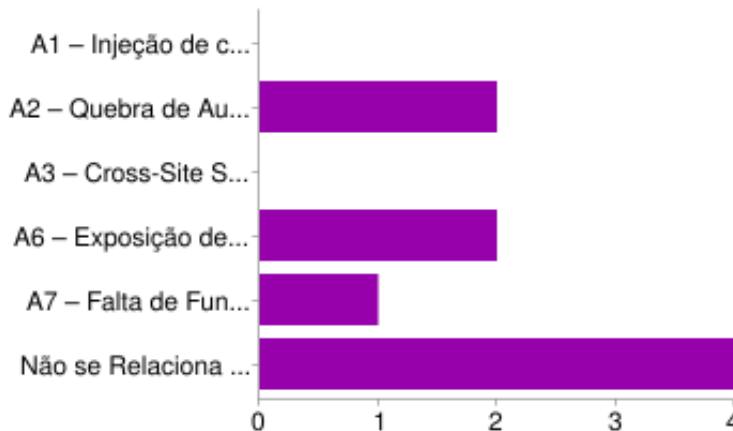
**Possibilitar uma seleção estadual (...) WEB/PHP/PostGreSQL/Informativo Eletrônico Inscrição (...) PRÓCONSELHO Divulgar os boletins de serviço das Secretarias e Subsecretarias (...) WEB WEB/ASP ASP/SQLServer 2000**

**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 (...).**



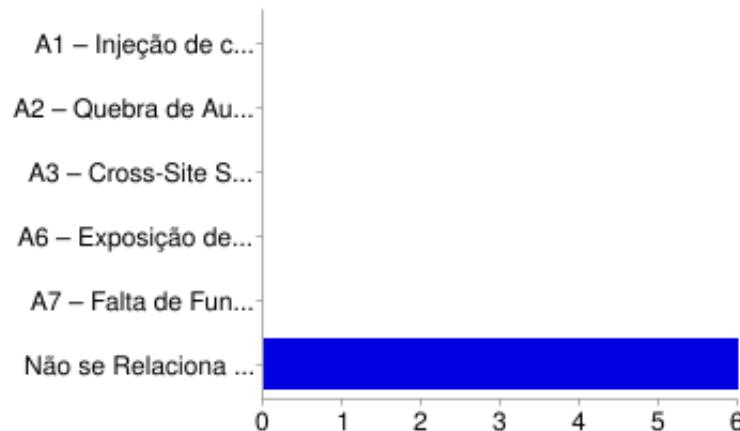
A1 – Injeção de código	1	20%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	0	0%
A3 – Cross-Site Scripting (XSS)	1	20%
A6 – Exposição de Dados Sensíveis	0	0%
A7 – Falta de Função para Controle do Nível de Acesso	0	0%
Não se Relaciona com Nenhum desses Riscos	4	80%

**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.**



A1 – Injeção de código	0	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	2	33.3%
A3 – Cross-Site Scripting (XSS)	0	0%
A6 – Exposição de Dados Sensíveis	2	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	1	16.7%
Não se Relaciona com Nenhum desses Riscos	4	66.7%

**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).**



A1 – Injeção de código	0	0%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	0	0%
A3 – Cross-Site Scripting (XSS)	0	0%
A6 – Exposição de Dados Sensíveis	0	0%
A7 – Falta de Função para Controle do Nível de Acesso	0	0%
Não se Relaciona com Nenhum desses Riscos	6	100%

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



A1 – Injeção de código	1	16.7%
A2 – Quebra de Autenticação e Gerenciamento de Sessão	4	66.7%
A3 – Cross-Site Scripting (XSS)	1	16.7%
A6 – Exposição de Dados Sensíveis	2	33.3%
A7 – Falta de Função para Controle do Nível de Acesso	2	33.3%
Não se Relaciona com Nenhum desses Riscos	2	33.3%

## Number of daily responses

