PODER JUDICIÁRIO

JUSTIÇA FEDERAL

CONSELHO DA JUSTIÇA FEDERAL

PORTARIA Nº CJF-POR-2015/00104 de 6 de março de 2015

Dispõe sobre a aprovação do documento acessório comum "Política de Segurança para Desenvolvimento, Aquisição e Manutenção de Sistemas", de que trata a Resolução n. 6, de 2008.

O PRESIDENTE DO CONSELHO DA JUSTIÇA FEDERAL, usando de suas atribuições legais, tendo em vista o decidido no Processo n. CF-ADM-2012/00325 e considerando os termos da Resolução n. 6, de 7 de abril de 2008, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus, da Resolução n. 240, de 22 de abril de 2013, que dispõe sobre a aprovação do regimento interno do Comitê de Segurança da Informação da Justiça Federal - CSI-Jus e da Portaria da Presidência n. 239, de 10 de junho de 2014, que altera a composição do Comitê de Segurança da Informação da Justiça Federal - CSI-Jus.

RESOLVE:

Art. 1º Aprovar o documento acessório comum "Política de Segurança para Desenvolvimento, Aquisição e Manutenção de Sistemas", o qual estabelece, na forma do Anexo, princípios e diretrizes de segurança da informação para a validação dos sistemas desenvolvidos, mantidos, adquiridos ou em produção no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

MINISTRO FRANCISCO FALCÃO

ANEXO

Política de Segurança para Desenvolvimento, Aquisição e Manutenção de Sistemas

1 Objetivo

Estabelecer princípios e diretrizes de segurança da informação para a validação dos sistemas desenvolvidos, mantidos, adquiridos ou em produção no âmbito do Conselho da Justiça Federal e da Justiça Federal de primeiro e segundo graus.

2 Considerações iniciais

A política de segurança para a aquisição, o desenvolvimento e a manutenção de sistemas – objeto deste documento acessório comum da Política de Segurança da Informação da Justiça Federal – está limitada ao escopo das ações de segurança da informação, as quais compreendem as medidas de proteção dos ativos de informação e das informações digitais, independentemente do meio ou da tecnologia utilizados.

Essa política deverá ser observada na contratação ou implementação de soluções de TI que envolvam o desenvolvimento, a manutenção ou a aquisição de sistemas, independentemente de quem os tenha desenvolvido ou adaptado e são aplicáveis, no que couber, àqueles que tenham sido adquiridos prontos (“de prateleira”), assim como aos sistemas em produção.

3 Documentos de referência

Lei n. 12.682/2012 – Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.

Resolução CNJ n. 90/2009 – Dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário

Resolução CJF n. 6, de 7 de abril de 2008, que estabelece a Política de Segurança da Informação do Conselho e da Justiça Federal de primeiro e segundo graus.

Norma ABNT NBR ISO/IEC 27001:2013, Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.

Norma ABNT NBR ISO/IEC 27002:2013, Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

Norma ISO/IEC 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*.

Norma ISO/IEC 15408-3:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*.

FIPS 199 e 200, do *National Institute of Standards and Technology - NIST*.

Application Security Principles, da *Open Web Application Project - OWASP*. Disponível em: <https://www.owasp.org/index.php/Category:Principle>. Acesso em: 25 de agosto de 2014.

Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário Brasileiro – MoReq-Jus.

Norma Complementar 16/IN01/DSIC/GSIPR, de 21 de novembro de 2012, do Departamento de Segurança da Informação e das Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC, Diretrizes para Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal.

4 Conceitos e definições

Para os efeitos desta política, são estabelecidos os seguintes conceitos e definições:

Ameaça – conjunto de fatores externos ou causa potencial de incidente indesejado que podem resultar em dano para um sistema ou organização.

Análise/avaliação de riscos – processo completo de análise e avaliação de riscos.

Análise de riscos – uso sistemático de informações para identificar fontes e para estimar o risco.

Análise dinâmica – tipo de teste que verifica o comportamento externo do *software* em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o *software* em execução. Um exemplo são os chamados testes de penetração.

Análise estática – tipo de teste de *software* que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários.

Ativos de informação – meios de armazenamento, transmissão e processamento, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Avaliação de conformidade em segurança da informação – exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação com as legislações específicas.

Avaliação de riscos – processo para comparar o risco estimado com critérios predefinidos para determinar a importância do risco.

Confidencialidade – propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizados e credenciados.

Controles de segurança – medidas adotadas para evitar ou diminuir a probabilidade de exploração de uma vulnerabilidade. Exemplos de controles de segurança são: a criptografia, as funções de *hash*, a validação de entrada, o balanceamento de carga, as trilhas de auditoria, o controle de acesso, a expiração de sessão, os *backups* etc.

Criptografia – a disciplina que incorpora os princípios, meios e métodos para a transformação de dados com a finalidade de ocultar o conteúdo semântico e prevenir a utilização não autorizada ou a modificação não detectada.

Criticidade – propriedade de que a redução ou perda de funcionalidade de um determinado ativo cause impacto ao negócio de acordo com sua gravidade.

Disponibilidade – propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

Integridade – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Modelo positivo de segurança – modelo no qual se define o que é permitido explicitamente, rejeitando o restante.

Recuperação segura em caso de falha – modelo no qual a falha no processamento de um controle de segurança resulte no mesmo caminho que seria executado no caso de uma vedação emitida por tal controle.

Requisitos de segurança – conjunto de necessidades de segurança que o sistema deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais, não funcionais e legais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais etc.), dentre outros. Os aspectos não funcionais descrevem procedimentos necessários para que o sistema permaneça executando as funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados e o registro de *logs* de auditoria com informações suficientes para análise forense.

Riscos de segurança da informação – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto desses ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

Segurança da informação – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações.

Sistema de informação – conjunto de recursos, meios e procedimentos que junta, armazena, processa e disponibiliza informação relevante para uma organização de modo a torná-la acessível e útil para quem a deseje e possa utilizar.

Trilha de auditoria – um registro mostrando quem acessou um sistema de informação e quais operações o usuário executou em um determinado período.

Vulnerabilidade – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou

organização, os quais podem ser evitados por uma ação interna de segurança da informação.

5 Princípios e diretrizes

Para o desenvolvimento, a manutenção, a aquisição ou o funcionamento de sistemas de informação no Conselho da Justiça Federal e na Justiça Federal de primeiro e segundo graus, independentemente das metodologias ou das tecnologias utilizadas, devem-se observar os seguintes princípios e diretrizes:

5.1 Identificar, definir, validar e documentar, na fase inicial de qualquer demanda, os requisitos de segurança, disponibilidade a que os sistemas deverão atender.

5.2 Usar um modelo positivo de segurança, definido no contexto da aplicação e dos ativos envolvidos, baseado na classificação da informação e conhecimentos dos processos de negócio envolvidos.

5.3 Implementar controle de acesso baseado em papéis ou perfis de usuários, preferencialmente por meio de componentes isolados.

5.4 Implementar controles de segurança necessários para proteger os ativos de informação e informações digitais, de acordo com a sua criticidade.

5.4.1 Usar controles de segurança como componentes, de forma que sejam catalogados e reutilizados em outros sistemas.

5.4.2 É recomendado que esses componentes sejam baseados nos controles definidos nas Normas Brasileiras Certificadoras pela ISO, órgão responsável por padronizar produtos (bens) e serviços de TI - NBR ISO/IEC 27001 e 27002.

5.5 Implementar os controles de segurança em múltiplas camadas da arquitetura do sistema, de acordo com a criticidade das informações tratadas.

5.6 Construir o sistema de forma que suas mensagens de erro não revelem detalhes de sua estrutura interna ou a configuração do ambiente.

5.7 Verificar o atendimento dos requisitos de segurança do *software*, por meio de análise estática e/ou análise dinâmica, preferencialmente na fase de construção.

5.8 Identificar e corrigir as vulnerabilidades encontradas anteriormente à entrada de qualquer sistema em produção, segundo um critério de prioridade e de aceitação do risco.

5.9 Sanitizar todo sistema desenvolvido, quando da passagem para o ambiente de produção, da seguinte forma:

5.9.1 Devem ser removidos arquivos desnecessários para o funcionamento do sistema, informações sigilosas nos comentários de código e contas criadas para teste.

5.9.2 Não implementar parâmetros de configuração dentro do código. Usar arquivos externos de configuração, adequadamente protegidos contra acesso e alteração indevidos.

5.10 A execução de configurações que afetem o comportamento da aplicação do ponto de vista da segurança da informação deve ser feita em conjunto entre os responsáveis pelo desenvolvimento do sistema e pela administração da infraestrutura.

5.11 Utilizar o princípio do mínimo privilégio, observada a legislação pertinente.

5.12 Recuperar-se de modo seguro em caso de falha.

5.13 Registrar em *logs* todos os eventos relevantes para o negócio e para a segurança da informação, com o armazenamento de informações suficientes para investigação e análise forense.

5.13.1 Os logs que permitam a construção de uma trilha de auditoria deverão ser protegidos de forma consistente com o contexto da aplicação e dos processos de negócios envolvidos.

5.14 Utilizar controles de segurança da informação específicos para os sistemas, independentemente de quaisquer proteções utilizadas na infraestrutura subjacente.

5.15 As bases e massas de dados utilizadas para teste e validação de sistemas deverão ser anonimizadas caso contenham dados classificados como sigilosos, conforme a legislação.

5.16 Não permitir acesso ao ambiente de produção por pessoal estranho às unidades envolvidas na manutenção de infraestrutura, salvo em situações devidamente justificadas e documentadas e com acompanhamento contínuo e presencial.

5.17 Observar que, em caso de contratação de serviço para desenvolvimento ou manutenção de *software*, o código-fonte deve ser custodiado de modo seguro pelo órgão.

5.18 Definir as regras para transferência do conhecimento sobre o *software* desenvolvido de modo a permitir a sua manutenção, de forma independente, por parte dos órgãos da Justiça Federal.

5.19 Estabelecer acordos de licenciamento, propriedade dos códigos e direitos de propriedade intelectual condizentes com o interesse da Justiça Federal, de forma a adquirir a titularidade do *software* ou para apenas exercer o direito de uso.

5.20 Instaurar meios que visem o controle da qualidade e precisão do trabalho efetuado de forma a garantir que os requisitos de segurança sejam atendidos.

5.21 Sistemas que possuam a necessidade de controle de acesso ou lidem com dados sigilosos deverão utilizar criptografia para a transmissão de dados.

5.22 Definir a execução de testes pela contratada e homologação pela Justiça Federal, antes da instalação do *software* obtido no ambiente de produção.

5.22.1 Devem ser realizadas tanto a análise estática quanto a análise dinâmica do *software* desenvolvido por terceiros.

5.23 Definir regras, estabelecer responsabilidades e procedimentos operacionais quanto à liberação de acesso aos recursos tecnológicos e ao ambiente físico ou lógico de cada órgão da Justiça Federal.

5.24 Na fase do ciclo de vida do sistema em que são levantados os requisitos, as necessidades, o estabelecimento de relação com o negócio ou o levantamento de custos, deverão ser desenvolvidas as seguintes atividades de segurança:

5.24.1 Avaliação preliminar de impactos e categorização do sistema conforme a tabela do subitem 5.30;

5.24.2 Definição dos requisitos de segurança.

5.25 Na fase do ciclo de vida do sistema em que são especificados e analisados os requisitos, o custo/benefício ou elaborado o plano de gerenciamento de riscos, deverão ser desenvolvidas as seguintes atividades de segurança:

5.25.1 Análise de riscos;

5.25.2 Definição dos controles de segurança da informação que serão implementados.

5.26 Na fase do ciclo de vida em que o sistema é construído, deverá ser desenvolvida a seguinte atividade de segurança:

5.26.1 Desenvolvimento e teste dos controles de segurança da informação.

5.27 Na fase do ciclo de vida em que o sistema é implantado, deverá ser desenvolvida a seguinte atividade de segurança:

5.27.1 Monitorar e avaliar a segurança da informação, podendo utilizar a norma ISO/IEC 15408 como referência.

5.28 Na fase de manutenção do sistema, deverá ser desenvolvida a seguinte atividade de segurança:

5.28.1 Gerenciamento e revalidação dos controles de segurança da informação.

5.29 A avaliação de impacto potencial deverá ser realizada com base na tabela do FIPS 199 (NIST, 2004):

Objetivos de Segurança	Impacto Potencial		
	Baixo	**Médio**	**Alto**
Confidencialidade Restrições quanto ao acesso e à divulgação das informações, incluindo meios de proteger informações de privacidade e direitos de propriedade pessoais.	A divulgação não autorizada da informação poderia causar efeitos prejudiciais limitados nas operações e nos ativos organizacionais ou individuais.	A divulgação não autorizada da informação poderia causar sérios efeitos prejudiciais nas operações e nos ativos organizacionais ou individuais.	A divulgação não autorizada da informação poderia causar efeitos prejudiciais severos ou catastróficos nas operações e nos ativos organizacionais ou individuais.
Integridade Proteção contra modificação ou destruição indevida das informações.	A modificação ou a destruição não autorizada da informação poderia causar efeitos prejudiciais limitados nas operações e nos ativos organizacionais ou individuais.	A modificação ou a destruição não autorizada da informação poderia causar sérios efeitos prejudiciais nas operações e nos ativos organizacionais ou individuais.	A modificação ou a destruição não autorizada da informação poderia causar efeitos prejudiciais severos ou catastróficos nas operações e nos ativos organizacionais ou individuais.
Disponibilidade Garantia de uso e de acesso confiável e em tempo à informação.	A interrupção do uso ou acesso à informação ou a um sistema poderia causar efeitos prejudiciais limitados nas operações e nos ativos organizacionais ou individuais.	A interrupção do uso ou acesso à informação ou a um sistema poderia causar sérios efeitos prejudiciais nas operações e nos ativos organizacionais ou individuais.	A interrupção do uso ou acesso à informação ou a um sistema poderia causar efeitos prejudiciais severos ou catastróficos nas operações e nos ativos organizacionais ou individuais.

6 Responsabilidades

6.1 Os envolvidos no processo de desenvolvimento, manutenção e aquisição de sistemas no Conselho da Justiça Federal e na Justiça

Federal de primeiro e segundo graus deverão receber treinamento em segurança de *software*.

6.2 O cumprimento desta política deve ser observado na elaboração de contratos de desenvolvimento, manutenção ou aquisição de sistemas.

6.2.1 Nas condições contratuais de suporte para o sistema, devem ser previstas as correções de vulnerabilidades que venham a ser identificadas na solução contratada.

6.3 As CLSIs poderão estabelecer normas internas com o objetivo de complementar o estabelecido nesta política.