PODER JUDICIÁRIO

JUSTIÇA FEDERAL

CONSELHO DA JUSTIÇA FEDERAL

PORTARIA Nº CJF-POR-2015/00103 de 6 de março de 2015

Dispõe sobre a aprovação do documento acessório comum "Política de Auditoria de Segurança da Informação", 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 CJF 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 primeiro e segundo graus, da Resolução CJF 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,

RESOLVE:

Art. 1º Aprovar o documento acessório comum "Política de Auditoria de Segurança da Informação", o qual estabelece, na forma do Anexo, as diretrizes para o programa, para o processo e para os projetos de auditoria de segurança da informação no Conselho e na 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 Auditoria de Segurança da Informação

1 Objetivo

Estabelecer diretrizes para o programa, para o processo e para os projetos de auditoria de segurança da informação no Conselho e na Justiça Federal de primeiro e segundo graus.

2 Considerações iniciais

A auditoria de segurança da informação – objeto deste documento acessório comum da Política de Segurança da Informação do Conselho e da Justiça Federal de primeiro e segundo graus – está limitada ao escopo das ações de segurança da informação, as quais compreendem as medidas de proteção dos ativos de informação, independentemente do meio ou da tecnologia utilizados.

A auditoria de segurança da informação objetiva informar às partes interessadas (*stakeholders*, cf. Item 5.6 desta política) o nível corrente da segurança da informação nesses órgãos e indicar eventuais falhas e deficiências.

3 Documentos de referência

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.

Resolução CNJ n. 171, de 1º de março de 2013, que dispõe sobre as normas técnicas de auditoria, inspeção administrativa e fiscalização nas unidades jurisdicionais vinculadas ao Conselho Nacional de Justiça.

Norma ISO/IEC 19011:2011, *Guidelines for auditing management systems*.

Norma ABNT NBR ISO/IEC 27005:2008, Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

Norma Complementar 11/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, do Departamento de Segurança da Informação e das Comunicações do Gabinete de

Segurança Institucional da Presidência da República - DSIC, *DIRETRIZES PARA AVALIAÇÃO DE CONFORMIDADE NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES*.

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

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

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.

Auditoria de segurança da informação – atividade estruturada para examinar criteriosamente a situação dos controles que se aplicam à segurança da informação, especialmente por meio da análise de objetos e respectivos pontos de controle.

Autenticidade – propriedade que garante ter sido a informação produzida, expedida, modificada ou destruída por determinada pessoa física ou por determinado sistema, órgão ou entidade.

Avaliação de conformidade em segurança da informação – exame sistemático comparativo do grau de atendimento dos requisitos relativos à segurança da informação com a legislação específica.

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

Confidencialidade – propriedade que garante não estar a informação disponível ou não ser revelada a pessoa física, sistema, órgão ou entidade não autorizados nem credenciados.

Conformidade – cumprimento da legislação, das normas e dos procedimentos relacionados à segurança da informação.

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

Entregáveis – artefatos e outros produtos resultantes do processo de auditoria (por exemplo: relatórios).

Gestão de riscos de segurança da informação – conjunto de processos que permitem identificar ou implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

Integridade – propriedade que garante não ter sido a informação modificada ou destruída de maneira não autorizada ou acidental.

Objeto de auditoria – objeto a ser examinado e selecionado em função do contexto e do propósito da auditoria (por exemplo: confidencialidade).

Ponto de controle – definido para cada objeto de auditoria, caracteriza situações específicas que podem ser relacionadas a produtos, processos, procedimentos, eventos ou a qualquer outro item observável e relevante para uma auditoria de segurança da informação (por exemplo: para o objeto de auditoria "confidencialidade", poderia constituir ponto de controle o uso de criptografia).

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 uma ou mais ameaças, com impacto negativo no negócio da organização.

Verificação de conformidade em segurança da informação – procedimento que faz parte da avaliação de conformidade e visa identificar o cumprimento da legislação, das normas e dos métodos relacionados à segurança da informação da organização.

Vulnerabilidade – conjunto de fatores internos ou causa potencial de incidente indesejado que podem resultar em risco para um sistema ou organização (podem ser evitados por uma ação interna de segurança da informação).

5 Princípios e diretrizes

5.1 As diretrizes gerais da auditoria de segurança da informação deverão considerar, no mínimo e prioritariamente: os objetivos estratégicos; os ativos de informação e os processos críticos de negócio; os riscos a que os ativos e os processos estão sujeitos, determinados por análise de risco nos termos da Política de Gestão de Riscos de Segurança da Informação do Conselho e da Justiça Federal de primeiro e segundo graus; os requisitos legais e a estrutura da Justiça Federal, além de estar alinhadas à Política de Segurança da Informação do Conselho e da Justiça Federal de primeiro e segundo graus.

5.2 A auditoria de segurança da informação é considerada um processo de negócio crítico da Justiça Federal, que deve ser contínuo, cujos resultados devem ser aplicados na gestão, na implementação e na operação de segurança da informação.

5.3 A auditoria de segurança da informação é independente da auditoria de tecnologia da informação.

5.4 A auditoria de segurança da informação deverá ser implementada como programa, desdobrado em um ou mais projetos, nos termos do Item 6 desta política.

5.5 Do ponto de vista de sua natureza, a auditoria de segurança da informação, no Conselho e na Justiça Federal de primeiro e segundo graus, classifica-se em:

5.5.1 Auditoria de conformidade: verifica se os controles de segurança da informação aplicados aos ativos de informação estão adequados à legislação e às normas aplicáveis ao Conselho e à Justiça Federal de primeiro e segundo graus.

5.5.2 Auditoria de gestão: verifica se as ações de gestão de segurança da informação estão de acordo com a estratégia e a Política de Segurança da Informação do Conselho e da Justiça Federal de primeiro e segundo graus.

5.5.3 Auditoria operacional: verifica se os controles de segurança da informação foram implementados de forma eficiente, eficaz

e econômica pelas unidades responsáveis do Conselho e da Justiça Federal de primeiro e segundo graus.

5.6 Considera-se como principal interessada (*stakeholder*) de um programa de auditoria de segurança da informação a alta administração de cada órgão da Justiça Federal.

5.6.1 Cabe às unidades de controle interno encaminhar o resultado da auditoria ao conhecimento da alta administração.

5.6.2 A alta administração do órgão, o Comitê de Resposta a Incidentes de Segurança da Informação da Justiça Federal - CRI-Jus ou as Comissões Locais de Resposta a Incidentes de Segurança da Informação - CLRIs poderão, motivadamente, solicitar a realização de auditorias de segurança da informação, que somente poderão ser realizadas com a coordenação do respectivo órgão de controle interno.

5.7 Quando, em auditoria operacional, for necessária a coleta de evidências que implicar a possibilidade de interrupção de serviço do órgão auditado, esta deverá ser autorizada pela alta administração.

5.8 Em obediência ao princípio da segregação de funções, será vedado a qualquer auditor intervir, a qualquer pretexto, na gestão, na implementação e na operação de segurança da informação do órgão auditado. Reciprocamente, os responsáveis pelas citadas atividades não poderão intervir no programa e nos projetos de auditoria. No entanto, é permitida a cooperação mútua.

5.9 Os achados das auditorias de segurança da informação servirão como insumo para a gestão de riscos de segurança da informação. As diretrizes do processo de gestão de riscos de segurança da informação deverão considerar, prioritariamente, os objetivos estratégicos, os processos de negócio, os requisitos legais e a estrutura dos órgãos da Justiça Federal, além de estar alinhadas à Política de Segurança da Informação do Conselho e da Justiça Federal de primeiro e segundo graus.

6 Programa, projetos e processo de auditoria

6.1 O programa, os projetos e o processo de auditoria de segurança da informação deverão seguir as diretrizes da Resolução CNJ n. 171, de 1º de março de 2013.

6.2 Norma específica da Secretaria de Controle Interno do Conselho da Justiça Federal estabelecerá as fases do processo de auditoria de segurança da informação.

7 Responsabilidades

7.1 Cabe à alta administração de cada órgão da Justiça Federal aprovar as diretrizes gerais de auditoria de segurança da informação complementares a esta política.

7.2 Cabe às unidades de controle interno definir o programa e os projetos de auditoria de segurança da informação, observada, entre outras, a respectiva Política de Segurança da Informação.

7.3 Cabe à alta administração do órgão aprovar as diretrizes gerais e o processo de gestão de riscos de segurança da informação, observada, entre outras, a respectiva Política de Segurança da Informação.

7.4 Cabe às unidades de controle interno da Justiça Federal coordenar a auditoria de segurança da informação nos seus respectivos órgãos.