PODER JUDICIÁRIO

JUSTIÇA FEDERAL

CONSELHO DA JUSTIÇA FEDERAL

PORTARIA Nº CJF-POR-2014/00093 de 20 de fevereiro de 2014

Dispõe sobre a aprovação do Documento Acessório Comum "Política de Gestão de Riscos", de que trata a Resolução n. 006, de 2008.

O PRESIDENTE DO CONSELHO DA JUSTIÇA FEDERAL, usando de suas atribuições legais e considerando a Política de Segurança da Informação na Justiça Federal, aprovada pela Resolução n. 6, de 7 de abril de 2008, e o contido no Processo n. CF-ADM-2012/00325,

RESOLVE:

Art. 1º Aprovar o Documento Acessório Comum "Política de Gestão de Riscos", o qual estabelece, na forma dos Anexos, as diretrizes para o processo de gestão de riscos neste 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 FELIX FISCHER

Classif. documental	40.01.00.01

Publicado no Diário Oficial da União
Em 25/02/2014 Seção 1 pág. 146/147

Publicado também no Boletim Especial – 20/02/2014

ANEXO I

"Política de Gestão de Riscos"

1 Objetivo

Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação no Conselho e na Justiça Federal de primeiro e segundo graus, assegurando que os riscos a que estão sujeitos os ativos de informação sejam geridos com a utilização equilibrada de recursos financeiros, materiais, tecnológicos e humanos.

2 Considerações iniciais

Convém que o processo de Gestão de Riscos de Segurança da Informação esteja alinhado ao planejamento estratégico da organização e, também, ao processo maior de gestão de riscos corporativos, se este existir.

A Gestão de Riscos de Segurança da Informação – objeto deste documento acessório comum está limitada ao escopo das ações de segurança da informação, as quais se restringem às medidas de proteção dos ativos de informação, independentemente do meio ou da tecnologia utilizados.

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.

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

Norma ABNT NBR ISO/IEC 31000:2009, Gestão de riscos – Princípios e diretrizes.

Norma Complementar n. 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC, "GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES".

4 Conceitos e definições

Para os efeitos desta norma, 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.

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

Comunicação do risco – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

Estimativa de riscos – processo utilizado para atribuir valores à probabilidade e às consequências de um risco.

Evitar risco – forma de tratamento de risco na qual a alta administração decide não realizar a atividade para não se envolver em situação de risco ou para se retirar dela.

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.

Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco.

Reduzir risco – forma de tratamento de risco na qual a alta administração decide realizar determinada atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

Reter risco – forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.

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.

Transferir risco – forma de tratamento de risco na qual a alta administração decide realizar a atividade compartilhando com outra entidade o ônus associado a um risco.

Tratamento dos riscos – processo e implementação de ações de segurança da informação para evitar, reduzir, reter ou transferir um risco.

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 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.

5.2 O processo de Gestão de Riscos de Segurança da Informação deve ser contínuo e aplicado à implementação e à operação da Gestão de Segurança da Informação.

5.3 O processo de Gestão de Riscos de Segurança da Informação, a fim de fomentar a sua melhoria contínua, deve coadunar-se com o modelo denominado PDCA (*Plan-Do-Check-Act*).

5.4 A Gestão de Riscos de Segurança da Informação deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e a Gestão de Continuidade de Negócios.

5.5 As decisões relativas à Gestão de Riscos de Segurança da Informação deverão ser formalmente documentadas e comunicadas ao tomador de decisão e a outras partes interessadas.

6 Procedimentos

Nos itens abaixo, será apresentada abordagem sistemática do processo de Gestão de Riscos de Segurança da Informação com o objetivo de manter os riscos em níveis aceitáveis. Esse processo é composto pelas etapas de definições preliminares, análise/avaliação dos riscos, plano de tratamento dos riscos, aceitação dos riscos, implementação do plano de tratamento dos riscos, monitoração e análise crítica, melhoria do processo de Gestão de Riscos de Segurança da Informação e comunicação dos riscos, conforme apresentado no **Anexo II** desta norma.

6.1 **Definições preliminares:** nesta fase, deve-se realizar análise da organização visando estruturar o processo de Gestão de Riscos de Segurança da Informação, sendo consideradas as características do órgão e as restrições a que estão sujeitas. Essa análise inicial permitirá que os critérios e o enfoque da Gestão de Riscos de Segurança da Informação sejam os mais apropriados para o órgão, apoiando-o na definição do escopo e na adoção de uma metodologia. Nesse sentido, deverão se adotados estes procedimentos:

6.1.1 definir o escopo de aplicação da Gestão de Riscos de Segurança da Informação a fim de delimitar o âmbito de atuação. Esse escopo pode abranger o órgão como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação;

6.1.2 priorizar, no mínimo, a gestão dos riscos aos ativos de informação associados aos processos críticos do negócio definidos pela organização;

6.1.3 adotar metodologia de Gestão de Riscos de Segurança da Informação que atenda aos objetivos, às diretrizes gerais e ao escopo definido, contemplando, no mínimo, os critérios de

avaliação e de aceitação do risco definidos pela alta administração.

6.2 **Análise/avaliação dos riscos:** nesta fase, inicialmente serão identificados os riscos, considerando-se as ameaças e as vulnerabilidades associadas aos ativos de informação, para, em seguida, serem estimados os níveis de riscos, de modo que eles sejam avaliados e priorizados. Nesta etapa, é imprescindível:

6.2.1 realizar inventário e mapeamento dos ativos de informação no âmbito do escopo estabelecido;

6.2.2 identificar os riscos associados ao escopo definido, considerando:

a) as ameaças envolvidas;

b) as vulnerabilidades existentes nos ativos de informação;

c) as ações de segurança da informação já adotadas.

6.2.3 estimar os riscos levantados, levando em conta os valores ou níveis para a probabilidade e para a consequência dos riscos associados à perda de disponibilidade, integridade, confidencialidade e autenticidade dos ativos considerados;

6.2.4 avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos no item 6.3;

6.2.5 relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos.

6.3 **Plano de tratamento dos riscos:** nesta fase, serão determinadas as formas de tratamento dos riscos, considerando-se as opções de reduzir, evitar, transferir ou reter o risco, devendo ser observados:

a) a eficácia das ações de segurança da informação já existentes;

b) as restrições organizacionais, técnicas e estruturais;

c) os requisitos legais;

d) a análise do custo/benefício.

6.3.1 O Plano de Tratamento dos Riscos elaborado deverá relacionar, no mínimo, as ações de segurança da informação, os responsáveis, as prioridades e os prazos de execução necessários à sua implantação.

6.4 **Aceitação dos riscos:** verificar os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.

6.5 **Implementação do plano de tratamento dos riscos:** executar as ações de segurança da informação incluídas no plano de tratamento dos riscos aprovado.

6.6 **Monitoração e análise crítica:** detectar possíveis falhas nos resultados, monitorar os riscos, as ações de segurança da informação e verificar a eficácia do processo de Gestão de Riscos de Segurança da Informação. Esta etapa enfocará:

6.6.1 **processo de gestão**: monitorar e analisar criticamente o processo de Gestão de Riscos de Segurança da Informação de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às necessidades do órgão;

6.6.2 **risco**: manter os riscos monitorados e analisados criticamente, a fim de verificar, regularmente, no mínimo, as seguintes mudanças:

a) nos critérios de avaliação e aceitação dos riscos;

b) no ambiente;

c) nos ativos de informação;

d) nas ações de segurança da informação;

e) nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).

6.7 **Melhoria do processo de Gestão de Riscos de Segurança da Informação**: propor à alta administração do órgão a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica, executar as ações corretivas ou

preventivas aprovadas e assegurar que as melhorias atinjam os objetivos pretendidos.

6.8 **Comunicação do Risco:** cientificar formalmente a alta administração a respeito de todas as fases da gestão de riscos, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas.

7 Responsabilidades

7.1 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.

7.2 As Comissões Locais de Segurança da Informação – CLSIs, em conjunto com os gestores das áreas de negócio, são responsáveis pela coordenação da Gestão de Riscos de Segurança da Informação nos órgãos.

7.3 De acordo com as necessidades de cada órgão, as CLSIs poderão propor à alta administração gerentes de atividades, a quem serão conferidas, no mínimo, as seguintes atribuições:

7.3.1 análise/avaliação e tratamento dos riscos;

7.3.2 elaboração sistemática de relatórios para a CLSI, de cujo conteúdo constarão a análise sobre a aceitação dos resultados obtidos e a consequente proposição de ajustes e de medidas preventivas e proativas à alta administração.

ANEXO II

Processo de Gestão de Riscos de Segurança da Informação