Conselho da Justiça Federal

RESOLUÇÃO Nº 006, DE 07 DE ABRIL DE 2008

Dispõe sobre a implantação da Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

O PRESIDENTE DO CONSELHO DA JUSTIÇA FEDERAL, no uso de suas atribuições legais e considerando a necessidade de estruturar, elaborar, manter e administrar uma Política de Segurança para a utilização dos ativos e recursos de informática dos órgãos, bem como o decidido no Processo nº 2008161107, em sessão realizada no dia 04 de abril de 2008, resolve:

Art. 1º As diretrizes e regulamentações relativas à segurança da informação que tratam de práticas seguras de gestão, aproveitamento, processamento, armazenamento, transmissão e recuperação de toda informação produzida no Conselho e na Justiça Federal de primeiro e segundo graus regem-se por esta Resolução.

Art. 2º A fim de conferir plena efetividade à segurança da informação, cada órgão responsável pela implantação da Política de Segurança da Informação deverá elaborar documentos próprios e diferenciados, conforme orientações contidas no Anexo I desta Resolução.

Art. 3º Os sistemas de informações do Conselho e da Justiça Federal de primeiro e segundo graus deverão ser adaptados ao disposto nesta Resolução no período máximo de dois anos, contados a partir de sua publicação.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

Ministro HUMBERTO GOMES DE BARROS
Presidente

Publicada no Diário Oficial da União
Em 22/04/2008 Seção 1 pág. 136

Conselho da Justiça Federal

ANEXO I
(Resolução nº 006, de 07 de abril de 2008.)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. APRESENTAÇÃO

Esta política norteará a implementação de medidas de proteção que deverão ser aplicadas a toda e qualquer informação, independentemente de onde ela se encontre, com vistas ao resguardo da imagem e dos objetivos institucionais dos participantes.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que seu maior patrimônio, a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

2. ESCOPO

O escopo desta Política de Segurança da Informação abrange todos os Tribunais Regionais Federais, suas seções e subseções, Conselho da Justiça Federal e demais participantes.

3. PÚBLICO ALVO

Esta Política de Segurança da Informação, assim como os documentos que a compõem, se aplica aos agentes públicos dos órgãos participantes e ainda a estagiários, aprendizes, clientes e parceiros.

4. RESPONSÁVEIS PELA POLÍTICA DE SEGURANÇA E SUAS ATRIBUIÇÕES

4.1. Conselho da Justiça Federal

Ao CJF cabe:

- criar e regulamentar o Comitê de Segurança da Informação da Justiça (CSI-Jus) e o Comitê de Resposta a Incidentes da Justiça (CRI-Jus);
- aprovar e regulamentar administrativamente esta Política de Segurança da Informação e sua aplicação.

4.2. Órgãos Participantes

Compete aos órgãos participantes:

- criar e definir a composição da Comissão Local de Segurança da Informação e da Comissão Local de Resposta a Incidentes;
- aprovar e regulamentar, administrativamente, os documentos acessórios da Política de Segurança da Informação, dentro do âmbito de seu órgão.

4.3. Sistema de Tecnologia da Informação e Comunicação da Justiça Federal - SIJUS

Compete ao SIJUS:

- recomendar as providências necessárias a cada órgão, para a implementação das práticas de segurança da informação;
- definir as competências, atribuições e composição do Centro de Resposta a Incidentes de Segurança da Informação da Justiça (CRI-Jus) e do Comitê de Segurança da Informação da Justiça (CSI-Jus).

4.4. Área de TI & C dos Órgãos Participantes

- Deve gerenciar a implementação e o cumprimento das práticas propostas na política de segurança da informação no escopo de seu órgão;
- Deve indicar os componentes da área de TI & C para o Centro Local de Resposta a Incidentes de Segurança.

4.5. Agentes Públicos, Estagiários e Aprendizes

Devem cumprir o disposto nesta política de segurança da informação.

4.6. Clientes e Parceiros

Devem cumprir o disposto nesta política de segurança da informação em relação a recursos compartilhados com os participantes.

5. AGENTES RESPONSÁVEIS PELA POLÍTICA DE SEGURANÇA E SUAS ATRIBUIÇÕES

5.1. Comitê de Segurança da Informação da Justiça – CSI-Jus

O CSI-Jus será composto por no mínimo um titular e um suplente, provenientes da Área de Segurança da Informação de cada TRF e CJF por indicação de seus dirigentes; todo e qualquer membro do CSI-Jus deve, preferencialmente, receber qualificação em gestão de segurança da informação.

Compete ao CSI-Jus:

- manter, em conjunto com as áreas de TI & C de cada órgão, ações preventivas e educativas de segurança da informação;
- manter atualizada a política de segurança da informação e seus documentos acessórios, de acordo com a periodicidade determinada em cada documento;
- dar ciência aos responsáveis pelas áreas de TI & C de todas as modificações e ajustes propostos nos documentos da política de segurança da informação, mediante relatórios periódicos;
- manter estreito intercâmbio com as Comissões Locais de Segurança da Informação;
- sugerir convite ou contratação de profissionais externos à Justiça, de relevante importância na área de segurança da informação, para auxílio em questões que assim o exijam, sob a condição de confidencialidade;
- definir e manter atualizadas as métricas de segurança da informação, incluindo as necessárias ao trabalho do CRI-Jus;
- propor ações de treinamento e atualização necessárias;
- coordenar as atividades e analisar os resultados do CRI-Jus em caráter consultivo.

5.2. Comitê de Resposta a Incidentes de Segurança da Justiça – CRI-Jus

O CRI-Jus deve ser composto por no mínimo um titular e um suplente, provenientes da Área de Segurança da Informação de cada TRF e CJF por indicação de seus dirigentes; todo e qualquer membro do CRI-Jus e dos comitês de resposta a incidentes locais deve receber completa qualificação em tratamento de incidentes.

Compete ao CRI-Jus:

- manter, em conjunto com as áreas de TI & C de cada órgão, ações preventivas e educativas de segurança;
- dar resposta a qualquer incidente de segurança relevante no âmbito dos órgãos participantes, em conjunto com as Comissões Locais de Resposta a Incidentes e as áreas de TI & C de cada órgão;
- dar ciência aos responsáveis pelas áreas de TI & C de todos os incidentes relevantes tratados pelo comitê, mediante relatórios periódicos, além de manter o registro estatístico e pericial dos incidentes;
- manter estreito intercâmbio com outros comitês ou centros de resposta a incidentes de segurança;
- sugerir convite ou contratação de profissionais externos à Justiça, de relevante importância na área de segurança da informação, para auxílio em questões que assim o exijam, sob a condição de confidencialidade;
- auxiliar na implementação e revisão da Política de Segurança.

5.3. Comissão Local de Segurança da Informação – CLSI

A CLSI deve ser presidida pelo dirigente do órgão ou seu representante, e composta por, no mínimo, um membro da Área de Segurança da Informação, um membro da área administrativa, um membro da área judiciária e um membro da área jurídica, sob a chefia da Área de Segurança da Informação para questões técnicas.

Cabe ao CLSI:

- manter ações preventivas e educativas de segurança;
- manter atualizados os documentos acessórios da política de segurança de sua competência, de acordo com a periodicidade determinada em cada um;
- dar ciência ao Comitê de Segurança da Informação da Justiça - CSI-Jus, de todas as modificações e ajustes propostos nos documentos da política de segurança de sua competência, por meio de relatórios periódicos, além de manter atualizados os dados estatísticos e indicadores de ambas as estruturas;
- utilizar as métricas de segurança da informação definidas pelo CSI-Jus;
- propor ações de treinamento e atualização necessárias;
- coordenar as atividades e analisar os resultados do CLRI.

5.4. Comissão Local de Resposta a Incidentes de Segurança da Informação – CLRI

A CLRI deve ser chefiada por um membro da Área de Segurança da Informação e composta por, no mínimo, um membro da Área de Segurança da Informação e um membro da Área de Informática, sob a coordenação da CLSI para questões jurídicas e administrativas; todos os membros do CLRI devem receber completa qualificação em tratamento de incidentes.

Compete à CLRI:

- manter, em conjunto com a CLSI, ações preventivas e educativas de segurança;
- dar resposta a qualquer incidente de segurança no âmbito de seu órgão, dando ciência à CRI-Jus e à área de TI & C;
- classificar os incidentes de segurança de acordo com as métricas definidas pelo CSI-Jus, solicitando auxílio ao CRI-Jus sempre que o evento atingir os parâmetros de relevância definidos;
- dar ciência aos responsáveis pelas áreas de TI & C de todos os incidentes relevantes tratados pela comissão, através de relatórios periódicos, além de manter o registro estatístico e pericial dos incidentes;
- manter estreito intercâmbio com o CRI-Jus e com os outros CLRIs;
- auxiliar na implementação e revisão dos documentos acessórios da Política de Segurança da Informação de sua alçada.

6. DIRETRIZES

A Política define as Diretrizes para a Segurança da Informação dos participantes, visando preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações, descrevendo a conduta considerada adequada para o tratamento da informação em todo o seu ciclo de vida (criação, manuseio, armazenamento, transporte e descarte).

Esta Política de Segurança da Informação, assim como os demais documentos acessórios que a compõe e leis que regulamentam as atividades de cada participante, são aplicáveis e devem ser obedecidos por todos os Agentes Públicos, sendo responsabilidade de cada um o seu cumprimento.

Devem ser estabelecidas normas e responsabilidades pela gestão e operação dos ativos de processamento das informações.

Um processo de gestão de risco deve ser implementado, com o objetivo de minimizar os riscos associados à informação, para o direcionamento das medidas de segurança necessárias.

Um processo de gestão da continuidade do negócio deve ser implementado, visando reduzir, para um nível aceitável, a interrupção causada por desastres ou falhas nos recursos que suportam os processos de informação da instituição.

Os Agentes Públicos integrantes dos participantes devem ser capacitados na política de segurança da informação e no uso correto dos ativos disponibilizados, de forma a minimizar possíveis riscos de segurança, bem como estar conscientes de suas responsabilidades.

Comissões de Segurança da Informação devem ser implementadas, fornecendo o suporte às ações institucionais estratégicas, priorizando e conduzindo a elaboração e manutenção de uma política de segurança da informação coesa, que possa ser gradualmente efetivada e sirva como referência a questões de segurança da informação.

Recomenda-se que as Comissões tenham representatividade intersetorial, promovendo as ações de segurança por meio do comprometimento apropriado da Alta Administração dos participantes.

Incidentes que afetam a segurança das informações, assim como o descumprimento desta política de segurança da informação, devem ser reportados à Comissão Local de Resposta a Incidentes, cuja abrangência abarque o local da ocorrência, para as devidas providências legais e administrativas, sendo que a comissão local deve repassar as informações

para a Comissão de Resposta a Incidentes da Justiça Federal de acordo com a gravidade do incidente ocorrido.

O cumprimento da política de segurança da informação deve ser periodicamente revisado pelas Comissões de Segurança da Informação e auditado pela área de qualidade dos participantes.

Uma estrutura organizacional responsável pela Gestão da Segurança da Informação nos participantes deve ser criada e implementada.

O cumprimento da política de segurança da informação dos participantes será avaliado periodicamente, de acordo com os critérios sugeridos e homologados pela Comissão de Segurança da Informação da Justiça – CSI-Jus.

Os diversos níveis gerenciais dos participantes devem zelar pelo cumprimento da política de segurança da informação no âmbito de sua competência.

Toda e qualquer informação criada, armazenada, manutenida ou descartada pelos participantes é considerada seu patrimônio e deve ser protegida conforme estabelecido na política de segurança da informação.

Para acesso às informações dos órgãos participantes, que não sejam de domínio público, é necessário o aceite de um termo de responsabilidade, por parte dos Agentes Públicos.

7. OBJETIVOS

Proteger as informações dos participantes, bem como seus ativos computacionais.

Permitir a integração dos participantes, por meio da adoção de critérios conhecidos e previamente acordados de medição dos riscos e ameaças envolvidos no processo.

Permitir a integração com parceiros externos, garantindo a integridade das informações e sistemas computacionais dos participantes.

Garantir o grau de autenticidade, disponibilidade, confidencialidade e integridade exigidos pelos participantes e seus clientes.

Possibilitar a adoção de uma Política de Gestão de Riscos pelos participantes.

8. DISPOSIÇÕES GERAIS

8.1. Dos Aspectos da Segurança

A abordagem da segurança da informação é feita sob o critério de segurança física, segurança lógica e humana, conforme delimitado a seguir:

- Segurança Física - refere-se à segurança dos ativos computacionais, instalações prediais e documentos em meio físico. Também engloba o controle de acesso às instalações dos participantes, por meio de recomendações;
- Segurança Lógica - refere-se a toda e qualquer informação em meio digital, seja em equipamentos servidores, em tráfego pela rede, por correio eletrônico ou armazenado nas estações de trabalho dos usuários;
- Segurança de Recursos Humanos - refere-se à educação e conscientização dos integrantes de cada participante sobre a responsabilidade de cada um para com a segurança de informação, por meio de recomendações e ações educativas.

8.2. Dos Guias e Procedimentos

Para que esta política tenha êxito em sua aplicação, é necessário que todos os procedimentos operacionais estejam devidamente documentados, tarefa que deverá ser executada de forma única ou específica, conforme o caso, pelos participantes.

Para confecção destes documentos, utilizar-se-ão como base os documentos acessórios, quando os mesmos não estiverem detalhados o suficiente para permitir a execução direta dos procedimentos recomendados ou quando houver particularidades nas instalações dos participantes.

Em nenhum caso os guias poderão se contrapor às orientações desta política ou dos documentos acessórios, sendo sempre baseados e subordinados aos mesmos.

9. DOCUMENTOS ACESSÓRIOS

São os documentos onde ficam contidas as orientações e melhores práticas para as diversas disciplinas abordadas por esta política, seguindo as especificidades de cada participante, quando necessário.

Tem como característica e função principais a descrição de regras e procedimentos que materializem as diretrizes da política de segurança, sempre respeitando os limites impostos por ela e passando por aprovação junto aos participantes afetados.

A criação e manutenção dos documentos acessórios serão feitas segundo os critérios expostos no documento "Padrão para Criação de Documentos", que é o primeiro documento acessório desta política.

Todos os documentos deverão possuir prazo de revisão sugerido explícito em seu bojo, de forma a garantir uma periodicidade mínima de atualização.

9.1. Documentos Acessórios Comuns

Os documentos acessórios comuns descrevem as metodologias e as melhores práticas a serem adotadas por todos os participantes, de maneira uniforme, garantindo uma base comum para as ações de segurança da informação.

9.1.1. Padrão para Criação de Documentos

Descreve as regras para criação dos demais documentos acessórios desta política.

9.1.2. Política de Auditoria de Segurança da Informação

Visa a garantir, em intervalos planejados, dentro da área de TI & C, uma rotina de verificação dos seguintes aspectos relacionados à política de segurança da informação:

- atender os requisitos das normas ISO IEC17799 e 27001 e a legislação ou regulamentação pertinenentes;
- atender os requisitos de segurança de informação identificados;
- verificar se os objetivos estão mantidos e implementados de forma eficaz;
- verificar se foram executados conforme esperado.

Toda a Política de Segurança de Informação deve ser planejada levando-se em consideração a situação e a importância dos processos da área de TI, bem como os resultados das auditorias anteriores.

Todos os relatórios deverão ser entregues única e exclusivamente ao titular da área de informática, ao titular da área de segurança de informação e ao representante legal do órgão participante auditado.

9.1.3. Política de Gestão de Risco

Tem como objetivo a identificação, análise, avaliação e tratamento dos riscos, e, se for o caso, a devida comunicação aos órgãos participantes; definir os objetivos em termos de tolerância a riscos, bem como desenvolver critérios para aceitação dos riscos e identificar os níveis aceitáveis de risco.

9.1.4. Política de Segurança para Aquisição, Desenvolvimento e Manutenção de Sistemas

Define as melhores práticas e os parâmetros a serem avaliados para aquisição, desenvolvimento e manutenção de sistemas informatizados no âmbito dos participantes, bem como dos sistemas que troquem dados com suas respectivas áreas de TI & C.

Também descreve os procedimentos para avaliações periódicas de sistemas em produção.

9.1.5. Metodologia de Avaliação de Efetividade da Implementação da Política de Segurança

Define a metodologia necessária para o acompanhamento das ações descritas nesta política e em seus documentos acessórios, de forma a permitir a identificação dos ajustes necessários.

Define também os indicadores que serão utilizados como parâmetros de controle da aplicação da política para todos os participantes, de forma unificada, garantindo um índice único de avaliação da efetividade das ações executadas.

9.2. Documentos Acessórios Diferenciados até o nível de Região

Os documentos acessórios aqui definidos descrevem as metodologias e melhores práticas a serem adotadas de forma individualizada, devendo ser elaborados de acordo com as especificidades de cada um dos participantes, sendo que, no caso dos Tribunais Regionais Federais, serão elaborados pela 2ª Instância, servindo como balizadores para suas seções e subseções.

9.2.1. Política de Segurança de Acesso Físico

Esta política, mandatória para as áreas de TI & C, e recomendação para as demais áreas da instituição, tem como objetivo descrever as orientações e melhores práticas necessárias ao controle de acesso físico às instalações envolvidas na guarda das informações de cada participante.

9.2.2. Política Permanente de Conscientização e Treinamento

Esta política define as ações educativas necessárias à sua manutenção e à redução dos riscos associados ao fator humano, abrangendo todo o público alvo previsto no escopo desta política.

9.2.3. Penalidades

Documento que define as penalidades para cada tipo de infração a esta política.

9.3. Documentos Acessórios Diferenciados até o nível de Seção Judiciária

Os documentos acessórios aqui definidos descrevem as metodologias e melhores práticas a serem adotadas de forma individualizada, devendo ser elaborados de acordo com as especificidades de cada um dos participantes, sendo que, neste caso, serão elaborados por todos os participantes, excluindo-se as subseções judiciárias, que utilizarão os documentos gerados por suas respectivas seções judiciárias.

9.3.1. Política de Controle de Acesso Lógico

Nesta política são estabelecidos procedimentos de acesso lógico aos ativos de informação em todos os seus níveis, de forma a possibilitar não só o controle de acesso à rede como também o controle de acesso aos dados internos de caráter sensível ou confidencial.

Os seguintes pontos são abordados por este documento:

- rede local;
- confiança entre sites distintos;
- acesso via Rede Virtual Privada (VPN);
- acesso via linha discada;
- acesso via redes sem fio;
- telefonia IP externa;
- novos serviços de interesse dos órgãos participantes;
- mensageria externa;
- mensageria corporativa;
- mensageria instantânea;
- acesso à Internet;
- acesso à Intranet;
- acesso a Extranets;
- transferências de arquivos;
- novos serviços que venham a ser incorporados.

9.3.2. Política de Utilização de Recursos de TI

Esta política estabelece as regras de segurança de informação no uso dos recursos de TI no âmbito dos órgãos participantes, na forma a seguir:

- meios de impressão;
- meios de armazenamento de dados;
- computação móvel;
- estações de trabalho;
- quarentena para dispositivos suspeitos;
- novos recursos de TI que venham a ser disponibilizados.

9.3.3. Política de Classificação de Informações

Como estabelecido no texto da apresentação, é necessário que a informação, patrimônio basilar para a atividade-fim da Justiça, "tenha o grau de autenticidade, disponibilidade, confidencialidade e integridade exigidos".

No entanto, diferentes itens desse acervo possuem diversos níveis de criticidade e de sensibilidade para dos participantes; algumas informações podem ser tornadas públicas, como endereços dos Fóruns, e outras devem receber um alto grau de preservação e de sigilo, a exemplo dos processos em segredo de Justiça. Esse fato deve ser levado em consideração na hora de estabelecer-se uma política de segurança da informação.

A Norma NBR ISO/IEC 17799:2005, em seu Item 7.2, dá uma explicação clara: "Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.".

A política de classificação da informação deve ser definida em parceria com profissionais das áreas envolvidas com o negócio de cada participante, indicados por seu dirigente.

9.3.4. Plano de Continuidade de Negócios

O PCN é constituído por uma série de procedimentos e medidas que têm por objetivo minimizar as perdas decorrentes de um desastre, ou seja, de um evento de grandes proporções em termos de impacto. Esses procedimentos e medidas visam à preservação da integridade física das pessoas, a redução dos prejuízos causados por desastres e a continuidade operacional dos processos da instituição que foram identificados como críticos.

Os seguintes aspectos são abordados neste documento:

- definição de criticidade de processos e recursos;
- continuidade de negócios;
- diretrizes para implementação do PCN;
- estrutura do PCN;
- testes do PCN;
- manutenção da PCN;
- reavaliação do PCN;
- planos de salvamento e recuperação;
- gestão de meios de armazenamento;
- alta-disponibilidade e redundância;
- site backup;
- demais documentos pertinentes à continuidade das atividades dos órgãos envolvidos.

10. DOCUMENTOS ANEXOS

Os documentos anexos são aqueles que auxiliam na aplicação da política de segurança, sem, no entanto, fazer parte dela.

10.1. Termos de Responsabilidade

- Termo de Responsabilidade de Agente Público;
- Termo de Responsabilidade de Administrador de TI;
- Termo de Responsabilidade de Técnico de Atendimento.

10.2. Legislação e Normas Técnicas

- Norma ABNT ISO/IEC 17799:2005 e ABNT ISO/IEC 27001:2006 e/ou normas que as sucederem;

- Decreto Nº 3.505, de 13 de junho de 2000;
- Decreto Nº 3.587, de 5 de setembro de 2000; e
- Decreto Nº 4.553, de 27 de dezembro de 2002.

10.3. Documentos Diversos

- Dicionário de Referência para os termos técnicos utilizados;
- Demais documentos que não componham a política de segurança, mas que sejam úteis a sua aplicação, desde que não descumpram nenhum de seus dispositivos, salvo em casos expressos em lei.

****