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~~.

Dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2° graus. (Redação dada pela Resolução n. 687, de 15 de dezembro de 2020)

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

~~ANEXO I~~

(~~Resolução nº 006, de 07 de abril de 2008.~~)

Anexo I em vigor com a redação constante do Anexo I da Resolução n. 687, de 15 de julho de 2020

~~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.

ANEXO I

(Redação dada pela Resolução n. 687, de 15 de dezembro de 2020)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. APRESENTAÇÃO

Esta Política tem caráter estratégico e deve ser atendida por todos os níveis hierárquicos, visando sua eficácia na proteção das informações.

Cada órgão deverá complementar o disposto nesta Política bem como regulamentar localmente os temas afetos à Segurança da Informação nos documentos acessórios de sua responsabilidade, relacionados no Anexo II, sempre de maneira harmônica com os princípios e diretrizes aqui estabelecidos.

2. OBJETIVO

Esta Política destina-se a estabelecer as diretrizes e os princípios da Segurança da Informação com o objetivo de nortear a implementação de medidas de proteção que deverão ser aplicadas às informações que têm valor, independentemente de seu suporte material ou tecnológico (ativo de informação), com vistas ao resguardo da missão, da visão, dos objetivos estratégicos e da imagem dos órgãos.

3. ESCOPO

O escopo desta Política de Segurança da Informação abrange o Conselho e a Justiça Federal de 1° e 2º graus.

4. PÚBLICO–ALVO

Esta Política de Segurança da Informação, assim como os documentos que a compõem, se aplica a todos aqueles que tenham contato com informação protegida por esta política, como por exemplo: os agentes públicos dos órgãos participantes, estagiários, aprendizes, clientes, parceiros e contratados.

5. REFERÊNCIAS LEGAIS E NORMATIVAS

Legislação

Lei n. 11.419, de 19 de dezembro de 2006 – Dispõe sobre a informatização do processo judicial; altera a Lei n. 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.

Lei n. 12.527, de 18 de novembro de 2011 – Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências.

Decreto n. 3.505, de 13 de junho de 2000, da Presidência da República – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Decreto n. 7.845, de 14 de novembro de 2012, da Presidência da República – Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Lei n. 13.709 de 14 de agosto de 2018, da Presidência da República - Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Normas Brasileiras e Internacionais

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

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação.

ABNT NBR ISO/IEC 27004:2017 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Monitoramento, medição, análise e avaliação.

ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

ABNT NBR ISO/IEC 27014:2013 – Tecnologia da Informação – Técnicas de Segurança – Governança de segurança da informação.

ABNT NBR ISO 15999-1:2007 – Gestão de continuidade de negócios – Parte 1: Código de prática.

COBIT 5 – Modelo Corporativo para Governança e Gestão de TI da Organização.

Norma Complementar n. 03/IN01/DSIC/GSIPR – Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos da Administração Pública Federal, e demais Normas Complementares, produzidas pelo Departamento de Segurança da Informação e das Comunicações – Gabinete de Segurança Institucional da Presidência da República.

Normas e Resoluções dos Órgãos Superiores do Poder Judiciário

Resolução CNJ n. 211, de 15 de dezembro de 2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

Diretrizes para a Gestão da Segurança da Informação no Âmbito do Poder Judiciário, do Conselho Nacional de Justiça.

Plano Estratégico da Justiça Federal – PEJF e Plano Estratégico de Tecnologia da Informação – PETI-JUS 2015/2020.

Determinações do Tribunal de Contas da União

Acórdão n. 3.117, de 12 de novembro de 2014.

Manual de Boas Práticas de Segurança da Informação, disponível em http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf.

6. DEFINIÇÕES

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

Alta Administração – unidades organizacionais com poderes deliberativos ou normativos no âmbito da organização.

Ameaça – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Ativo – qualquer coisa que represente valor para uma instituição. A informação é considerada um ativo.

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

Controle – forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Comitê Gestor de Estratégia da Justiça Federal - COGEST – Criado pela RESOLUÇÃO CJF n. 668, de 9 de novembro de 2020.

ETIR – abreviação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Denominação tradicionalmente atribuída a grupos

de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia.

Gestão estratégica – forma de acrescentar novos elementos de reflexão e ação sistemática e continuada, a fim de avaliar a situação, elaborar projetos de mudanças estratégicas, acompanhar e gerenciar os passos de sua implementação.

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

Gestor de segurança da informação – é responsável por fazer o planejamento e coordenar as ações de segurança da informação no âmbito de um Órgão da Justiça Federal.

Informação – dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Norma – documento estabelecido por consenso e aprovado por um organismo reconhecido que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou para seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto.

Procedimento – conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim (por exemplo, como instalar um microcomputador).

Risco – probabilidade da ocorrência de um evento que tenha impacto na segurança da informação.

Vulnerabilidade – fragilidade, ou fraqueza, de um ativo ou grupo de ativos que possa ser explorada por uma ameaça.

7. PRINCÍPIOS

7.1. Tratar a informação como um ativo essencial para o Conselho da Justiça Federal e para a Justiça Federal e, em consequência, proporcionar-lhe as seguintes **garantias fundamentais**:

7.1.1. **Confidencialidade** – A informação deve ser conhecida somente por quem dela efetivamente necessite e possua os direitos e privilégios adequados para fazê-lo.

7.1.2. **Disponibilidade** – A informação deve estar disponível, durante o período adequado e no momento oportuno, para quem tem acesso autorizado a mesma.

7.1.3. **Integridade** – A informação deve ser protegida contra qualquer alteração e/ou destruição indevida, acidental ou propositada.

7.1.4. **Autenticidade** – A informação é proveniente da fonte anunciada e não foi alvo de mutações ao longo de um processo.

7.2. Tais garantias devem ser implementadas por meio de ações ou controles, que devem fazer parte de um processo de Gestão de Segurança da Informação baseado nas seguintes premissas:

7.2.1. Independência do suporte em que se ache o ativo de informação;

7.2.2. Interdisciplinaridade;

7.2.3. Necessidade de proteção da organização;

7.2.4. Definição clara de responsabilidades e de atribuições;

7.2.5. Consideração do ciclo de vida da informação;

7.2.6. O comprometimento da Segurança da Informação pode impactar na atividade finalística da Justiça Federal ou na exposição de autoridades;

7.2.7. Gestão dos Riscos de Segurança da Informação;

7.2.8. Gestão da Continuidade de Negócios.

7.3. A Política de Segurança da Informação, aqui estabelecida, é de caráter estratégico e formaliza os princípios que regem a Segurança da Informação.

7.4. Controles ou ações específicas para a implementação dos princípios desta Política, e respectivos detalhes, serão disciplinados em Documentos Acessórios, que, por seu escopo, se classificam em:

7.4.1. Nacionais, ou comuns, de origem do CSI-Jus e aplicáveis ao CJF e a toda a Justiça Federal;

7.4.2. Regionais ou locais, produzidos pelas CLSIs e aplicáveis aos TRFs, Seções Judiciárias e demais Órgãos das Regiões.

7.5. Os Documentos Acessórios devem ser definidos e padronizados em um Documento Acessório do tipo Norma.

7.6. O Anexo II, Lista de Referência de Documentos Acessórios, define o conjunto mínimo de documentos requeridos para cada escopo.

8. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

8.1. A Governança da Segurança da Informação possui os seguintes objetivos:

8.1.1. Alinhar os objetivos e estratégias de segurança da informação com os objetivos e estratégias de negócio, observando a conformidade com as leis, normativos aplicáveis (resoluções do CNJ e CJF), determinações e recomendações dos órgãos de controle;

8.1.2. Agregar valor para a Justiça Federal e para a sociedade em geral;

8.1.3. Garantir que os riscos da informação estejam sendo adequadamente endereçados por meio de uma abordagem de gestão de riscos, apoiada por sistemas de controles internos.

8.2. O Comitê Gestor de Estratégia da Justiça Federal - COGEST é responsável por garantir que a abordagem dos órgãos para a segurança da informação seja eficiente, transparente, aceitável e alinhada com os objetivos e estratégias de negócio, considerando o interesse da coletividade.

8.3. Os resultados desejados a partir da implementação eficaz da governança da segurança da informação incluem:

8.3.1. Definição de objetivos corporativos estratégicos para a gestão de segurança da informação;

8.3.2. Visibilidade do COGEST sobre a situação da segurança da informação na Justiça Federal;

8.3.3. Uma abordagem ágil para a tomada de decisões sobre os riscos da informação;

8.3.4. Investimentos eficientes e eficazes em segurança da informação;

8.3.5. Conformidade com requisitos legais, normativos e regulamentares.

8.4. Os seguintes princípios basilares são fundamentais para a governança de segurança da informação:

8.4.1. A segurança da informação é objetivo de toda a organização e depende da atuação de todos e cada unidade deve entender sua responsabilidade para a proteção das informações;

8.4.2. As decisões devem ser baseadas na gestão adequada dos riscos, sendo necessária a definição do apetite ao risco dos órgãos participantes;

8.4.3. Uma estratégia de investimento em segurança da informação, tanto de curto como de médio prazo, deve ser estabelecida visando atender às necessidades atuais e emergentes;

8.4.4. As políticas e práticas de segurança da informação devem atender à legislação, às regulamentações obrigatórias e os requisitos de negócio;

8.4.5. Promover um ambiente positivo de segurança da informação, com a implantação de programas de educação, treinamento e conscientização em segurança;

8.4.6. Analisar criticamente o desempenho de segurança da informação em relação aos resultados de negócios através de um programa de medição de desempenho para monitoramento, auditoria e melhoria.

8.5. O COGEST deve aprovar o Planejamento Estratégico de Segurança da Informação da Justiça Federal – PESI, alinhado e na mesma periodicidade

que o da Estratégia da Justiça Federal. e submetê-lo à apreciação do plenário do CJF.

8.6. O COGEST, apoiado pelo CSI-Jus, é responsável pelos seguintes processos com o objetivo de verificar se os objetivos de governança de segurança da informação foram atingidos:

8.6.1. Avaliação: averiguar o atingimento atual e previstos dos objetivos de segurança e determinar eventuais ajustes para o atingimento dos objetivos estratégicos.

8.6.2. Direção: direcionar os objetivos e estratégias de segurança que precisam ser implementados, priorizando recursos e atividades.

8.6.3. Monitoração: avaliar a eficácia das atividades de gestão de segurança da informação com o objetivo de verificar o atingimento dos objetivos estratégicos definidos.

8.6.4. Comunicação: processo bidirecional em que o corpo diretivo e órgãos externos, ou em última instância com a própria sociedade, trocam informações sobre a segurança.

9. GESTÃO DE SEGURANÇA DA INFORMAÇÃO

9.1. A gestão da Segurança da Informação é responsável pelas ações de planejamento, desenvolvimento, execução e monitoramento de segurança da informação necessárias para a efetividade das direções definidas pela governança.

9.2. O Comitê de Segurança da Informação da Justiça Federal – CSI-Jus é o responsável pela gestão de segurança da informação em âmbito nacional, normatizando esta Política e promovendo a aplicação das estratégias de segurança da informação.

9.3. As Comissões Locais de Segurança da Informação – CLSI, existentes no CJF e em cada TRF, são as responsáveis pela gestão de segurança da informação em âmbito local, em conformidade com as definições do CSIJus, normatizando os temas que sejam de sua alçada e promovendo a aplicação das estratégias de segurança da informação.

9.4. É competência do Comitê de Segurança da Informação da Justiça Federal – CSI-Jus:

9.4.1. Propor meios para o alcance da estratégia de segurança da informação;

9.4.2. Promover a atualização da Política de Segurança da Informação;

9.4.3. Elaborar e revisar os Documentos Acessórios Nacionais e submeter ao Conselho da Justiça Federal;

9.4.4. Apoiar o CJF nas questões relacionadas à gestão da Segurança da Informação, podendo solicitar a assistência da CRI-Jus e/ou de especialistas externos, quando necessário e sob a condição de confidencialidade;

9.4.5. Manter intercâmbio com as Comissões Locais de Segurança da Informação, promovendo inclusive ações preventivas e educativas de segurança da informação;

9.4.6. Recomendar ao Sistema de Controle Interno da Justiça Federal a realização de auditorias extraordinárias em segurança da informação no CJF e nos órgãos da Justiça Federal;

9.4.7. Acompanhar a evolução do conhecimento em segurança da informação visando a melhoria contínua da gestão de segurança de segurança da informação;

9.4.8. Propor programas destinados à formação e ao aprimoramento das equipes especializadas em todos os campos da segurança da informação;

9.4.9. Monitorar o desempenho e avaliar os resultados com o objetivo de verificar se as diretrizes de segurança da informação estão sendo aplicadas nos Órgãos da Justiça Federal;

9.4.10. Promover o processo de Avaliação de Maturidade da Segurança da Informação;

9.4.11. Propor alterações em seu Regimento Interno.

9.5. O Comitê de Segurança da Informação da Justiça Federal – CSI-Jus deve ser composto por:

9.5.1. Representante do Comitê Gestor de Planejamento Estratégico da Justiça Federal – COGEST, que atua como coordenador;

9.5.2. Representante do Sistema de Tecnologia da Informação da Justiça Federal – SIJUS;

9.5.3. Representante do Comitê de Gestão Documental e Memória da Justiça Federal – COGED;

9.5.4. Representante do CJF e um de cada TRF, preferencialmente da área de segurança da informação ou com conhecimento em segurança da informação;

9.5.5. Para cada integrante deverá ser indicado suplente;

9.5.6. Todos os membros do CSI-Jus devem receber qualificação em gestão de segurança da informação.

9.6. É competência das Comissões Locais de Segurança da Informação – CLSI:

9.6.1. Elaborar e revisar os Documentos Acessórios Locais e submeter à presidência do órgão;

9.6.2. Apoiar a presidência do órgão nas questões locais relacionadas à Segurança da Informação, podendo solicitar a assistência do CSI-Jus e/ou de especialistas externos, quando necessários e sob a condição de confidencialidade;

9.6.3. Manter intercâmbio com as Comissões Locais de Segurança da Informação, promovendo inclusive ações preventivas e educativas de segurança da informação;

9.6.4. Definir a metodologia de análise e avaliação de riscos;

9.6.5. Definir a tolerância do órgão ao risco, por meio da definição de quais categorias de risco devem ser tratadas e quais são toleradas;

9.6.6. Promover a aplicação local dos Documentos Acessórios Nacionais;

9.6.7. Disciplinar demais temas relativos à segurança da informação que não tenham sido objeto dos documentos acessórios à esta Política;

9.6.8. Monitorar o desempenho e os resultados locais da gestão de segurança da informação;

9.6.9 Promover o intercâmbio com a unidade responsável pela gestão do acesso à informação do órgão com vistas a dar suporte quanto à segurança e proteção à informação, sem prejuízos ao cumprimento da legislação aplicável.

9.7. As Comissões Locais de Segurança da Informação – CLSI devem ter composição multidisciplinar, ou seja, composta por integrantes das áreas de negócio, como por exemplo, Presidência, Corregedoria, Judiciária, Gestão de Pessoas, Segurança, etc, contando inclusive com representantes da Justiça Federal de 1º Grau, e ser definidas de acordo com as necessidades locais, sendo obrigatória a representação dos gestores de segurança da informação.

9.7.1. Todos os membros da CLSI devem receber qualificação em gestão de segurança da informação.

9.8. A Gestão da Segurança da Informação é considerada atividade estratégica dos Órgãos da Justiça Federal, devendo ser exercida privativamente por servidores do quadro.

10. UNIDADES DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

10.1. A estrutura organizacional do CJF e de cada um dos Tribunais Regionais Federais deverá conter uma unidade de gestão de segurança da informação, com atribuição exclusiva, vinculada à Alta Administração, composta por no mínimo 2 (dois) servidores, sendo vedada a subordinação às áreas operacionais, tais como infraestrutura de TI e desenvolvimento de sistemas.

10.2. Os membros da unidade de gestão de segurança da informação devem receber qualificação em gestão de segurança da informação.

10.3. Compete à unidade de Gestão de Segurança da Informação:

10.3.1. Promover as ações de segurança da informação voltadas para dar efetividade à Política de Segurança da Informação;

10.3.2. Coordenar as ações de análise, avaliação e tratamento de riscos de segurança da informação a serem executadas pelas áreas operacionais;

10.3.3. Elaborar 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;

10.3.4. Propor à unidade de educação corporativa cronograma de ações de capacitação e de conscientização voltadas ao Órgão, de acordo com as características de cada público destinatário, priorizando, sempre que possível, a capacitação na modalidade EAD;

10.3.5. Cooperar com a CLRI do órgão para o tratamento de incidentes de segurança da informação.

11. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

11.1. A gestão de incidentes busca desenvolver a capacidade de gerenciar os eventos e incidentes que afetem a segurança da informação e dos ativos de informação da Justiça Federal.

11.2. A gestão de incidentes requer a definição de processos e planos de ação voltados tanto para a prevenção quanto para a reação em caso de ocorrência de eventos que comprometam a segurança da informação.

11.3. O processo de gestão de incidentes deve prever a preparação, o monitoramento proativo de vulnerabilidades, a aplicação de proteções para o ambiente tecnológico, bem como, na ocorrência de incidente, detecção, triagem e resposta.

11.4. O Comitê de Resposta a Incidentes de Segurança da Informação da Justiça Federal – CRI-Jus deve ser composto por um representante da Comissão Local de Resposta a Incidentes de Segurança da Informação de cada TRF e do CJF.

11.4.1. Todos os membros do CRI-Jus devem receber qualificação em tratamento de incidentes.

11.5. É competência do Comitê de Resposta a Incidentes de Segurança da Informação da Justiça Federal – CRI-Jus:

11.5.1. Ser a ETIR responsável pela coordenação nacional no tratamento e resposta dos incidentes de segurança da informação em sistemas computacionais da Justiça Federal;

11.5.2. Coordenar ações de resposta a incidentes de segurança da informação relacionados à tecnologia da informação que atinjam mais de um dos órgãos ou que afetem infraestrutura crítica para a Justiça Federal;

11.5.3. Consolidar registros e estatísticas de incidentes de segurança da informação na Justiça Federal;

11.5.4. Definir o processo e as diretrizes para o gerenciamento dos incidentes, incluindo fluxo de processos, indicadores, medidas, métricas e modelo de maturidade;

11.5.5. Manter estreito intercambio com as Comissões Locais de Resposta a Incidentes – CLRI;

11.5.6. Manter estreito intercâmbio, inclusive com a assinatura de acordos de cooperação, com os centros de resposta a incidentes de coordenação nacional, tais como o CAIS/RNP, o CTIR.GOV e o CERT.BR;

11.5.7. Auxiliar o CSI-Jus na produção de Documentos Acessórios Nacionais relativos a Resposta a Incidentes e propor o processo para a Gestão de Incidentes de Segurança da Informação na Justiça Federal;

11.5.8. Definir e propor alterações em seu Regimento Interno;

11.5.9. Solicitar a assistência de especialistas externos, sob a condição de confidencialidade, que possam contribuir para a resposta aos incidentes de segurança da informação de maior complexidade;

11.5.10. Acompanhar a evolução do conhecimento na resposta a incidentes de segurança da informação.

11.6. As Comissões Locais de Resposta a Incidentes de Segurança da Informação – CLRI devem ter composição multidisciplinar e serem definidas de acordo com as necessidades locais, sendo obrigatória a representação dos gestores de segurança de TI e de Seções Judiciárias da Região nas comissões dos TRFs.

11.6.1. Todos os membros da CLRI devem receber qualificação em tratamento de incidentes;

11.6.2 A CLRI deve ter constante colaboração das áreas de TIC nas ações proativas e reativas sob sua competência.

11.7. É competência das Comissões Locais de Resposta a Incidentes:

11.7.1. Atuar como uma ETIR responsável pela gestão local de incidentes de segurança da informação em sistemas computacionais;

11.7.2. Dar tratamento a incidentes que atinjam o órgão a que se acham vinculados, manter seu registro e estatística;

11.7.3. Escalar incidentes que atinjam outros órgãos ou instituições, da Justiça Federal ou externos, segundo critérios definidos em norma específica.

11.7.4. Notificar o CRI-Jus todos os incidentes que ocorrem em sua jurisdição para fins de registro, estatística e apoio;

11.7.5. Solicitar a assistência de especialistas externos, sob a condição de confidencialidade, que possam contribuir para a resposta aos incidentes de segurança da informação de maior complexidade;

11.7.6. Manter intercâmbio com as demais Comissões Locais de Resposta a Incidentes;

11.7.7. Utilizar e propor melhorias aos processos e diretrizes para o gerenciamento dos incidentes, incluindo fluxo de processos, indicadores, medidas, métricas e modelo de maturidade estabelecido pelo CRI-Jus.

12. GESTÃO DE ATIVOS DE INFORMAÇÃO

12.1. A gestão de ativos tem por objetivo alcançar e manter a proteção adequada dos ativos do órgão, com vistas a aplicar os controles de segurança adequados conforme a criticidade do ativo para a continuidade do negócio ou a classificação da informação.

12.2. Cada órgão deve identificar claramente todos os seus ativos bem como manter e estruturar um inventário de ativos de informação críticos, tendo em vista a Gestão de Riscos de Segurança da Informação e a Gestão de Continuidade de Negócios nos termos dos Documentos Acessórios Nacionais que as regulamentam.

12.3. O inventário deve documentar e classificar a importância do ativo para o negócio, o impacto para atividades finalísticas em caso de comprometimento e a estratégia que permita a recuperação do ativo em caso de desastre.

12.4. Todos os ativos críticos devem ter um proprietário formalmente designado.

12.5. O proprietário dos ativos de informação é a parte interessada do órgão ou entidade, ou indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

12.6. O proprietário é responsável por:

12.6.1. Assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificadas;

12.6.2. Definir e periodicamente analisar criticamente as classificações e as exigências de segurança da informação para os ativos de informação;

12.6.3. Identificar os riscos e comunicar as exigências de segurança da informação para os ativos sob sua responsabilidade aos custodiantes e usuários;

12.6.4. Implementar controles internos a fim de verificar se as exigências estão sendo cumpridas.

12.7. O proprietário do ativo pode delegar formalmente as tarefas de rotina a um custodiante que cuida do ativo no dia-a-dia, porém a responsabilidade permanece do proprietário.

12.8. O custodiante dos ativos de informação é qualquer indivíduo ou estrutura que tenha a responsabilidade formal de proteger um ou mais ativos de informação. É responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação informadas pelo proprietário dos ativos de informação.

12.9. As regras para uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação devem ser identificadas, documentadas e implementadas.

12.10. Os usuários que têm acesso aos ativos do órgão devem estar conscientes dos requisitos de segurança da informação, associados à informação e aos recursos de processamento da informação.

12.11. A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada, segundo Norma de Classificação de Ativos de Informação.

12.12. O proprietário do ativo de informação deve ser responsável por sua classificação.

13. AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

13.1. A Auditoria em Segurança da Informação é uma atividade devidamente 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. Para tanto, é preciso verificar que os controles estejam de acordo com as normas e políticas de segurança estabelecidas para esses ativos, bem como se o que está em operação alcança os objetivos de segurança.

13.2. Compete ao Sistema de Controle Interno da Justiça Federal a Auditoria de Segurança da Informação, nos termos do Documento Acessório Nacional que a regulamenta.

14. DISPOSIÇÕES FINAIS

14.1. Compete ao CJF designar os membros do Comitê de Segurança da Informação da Justiça Federal (CSI-Jus) e do Comitê de Resposta a Incidentes de Segurança da Justiça Federal (CRI-Jus), e aprovar esta Política de Segurança da Informação, os documentos acessórios nacionais, e promover sua aplicação.

14.2. Compete ao CJF e aos Tribunais Regionais Federais:

14.2.1. Indicar os seus representantes que comporão o CSI-Jus e o CRIJus;

14.2.2. Assegurar a existência e regulamentar suas CLSIs e as CLRIs;

14.2.3. Assegurar a existência de unidade de gestão de segurança da informação;

14.2.4. Cumprir e fazer cumprir esta Política de Segurança da Informação e respectivos documentos acessórios nacionais;

14.2.5. Aprovar e cumprir, os documentos acessórios de sua competência, listados no Anexo II.

14.3. As áreas de Segurança orgânica ou institucional (Resolução n. 176/2013 – CNJ) devem cooperar com a CRI-Jus e as CLRIs no tratamento dos incidentes de segurança da informação que envolvam aspectos de segurança física e ambiental, e reportá-los à CSI-Jus e às CLSIs, conforme a escala da ocorrência.

14.4. A Política de Segurança da Informação deve ser amplamente divulgada por todos os meios, sendo considerada um documento de relevante interesse público.

Autenticado eletronicamente por **Ministro HUMBERTO EUSTÁQUIO SOARES MARTINS**, **Presidente**, em 16/12/2020, às 10:43, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0180655** e o código CRC **B59C0023**.

ANEXO II

(Incluído pela Resolução n. 687, de 15 de dezembro de 2020)

LISTA DE REFERÊNCIA DE DOCUMENTOS ACESSÓRIOS

1. DOCUMENTOS ACESSÓRIOS NACIONAIS

1.1. Padrão para Criação de Documentos.

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

1.2. Norma de Auditoria de Segurança da Informação.

Estabelece diretrizes para o programa, para o processo e para os projetos de auditoria de segurança da informação, objetivando informar às partes interessadas o nível corrente da segurança da informação nesses órgãos e indicar eventuais falhas e deficiências.

1.3. Norma de Gestão de Risco de Segurança da Informação.

Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação, 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.

1.4. Norma de Segurança para Aquisição, Desenvolvimento e Manutenção de Sistemas.

Estabelece 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 1º e 2º graus.

1.5. Norma de Classificação de Informações.

Estabelece diretrizes para a identificação, classificação e tratamento da informação visando à proteção da informação conforme o seu valor, sensibilidade ou criticidade.

1.6. Norma Permanente de Conscientização e Treinamento.

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 dessa política.

1.7. Norma de Gestão de Continuidade de Negócios.

Estabelece diretrizes para a Gestão de Continuidade de Negócios em Segurança da Informação, minimizando os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades críticas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

1.8. Norma de Sanitização e Descarte de Mídias.

Estabelece procedimentos formais para o descarte seguro de mídias e a efetiva eliminação da informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados, com o devido registro histórico e documental do descarte.

1.9. Norma de Gestão de Incidentes de Segurança da Informação.

Estabelece diretrizes para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre vulnerabilidades e eventos de segurança da informação.

1.10. Norma de Padrões Criptográficos.

Regulamenta os padrões de hardware e os algoritmos e parâmetros criptográficos a serem utilizados pelos Órgãos da Justiça Federal, para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

1.11. Norma de Proteção de Dados Pessoais.

Estabelece as diretrizes para o tratamento de dados pessoais visando à adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

1.12. Norma de Penalidades.

Estabelece penalidades aos usuários que violarem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de segurança da informação.

1.13. Norma de Monitoração e Acompanhamento da Evolução da Segurança da Informação.

Estabelece o processo de monitoramento contínuo, bem como o projeto das reais necessidades e atividades de monitoramento, para o alcance da maturidade de Segurança da Informação da Justiça Federal.

1.14 Norma de Classificação de Ativos de Informação.

Estabelece as diretrizes para a identificação e classificação dos ativos de informação com base no valor que possuam para o órgão tendo em vista a criticidade do ativo para a continuidade do negócio ou a classificação da informação.

2. DOCUMENTOS ACESSÓRIOS LOCAIS / REGIONAIS

2.1. Norma de Segurança de Acesso Físico e Ambiental.

Estabelece as regras necessárias ao controle de acesso físico às instalações envolvidas na guarda das informações, para prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização. Aborda também os aspectos relacionados com a monitoração do ambiente, incluindo climatização e proteção elétrica.

2.2. Norma de Controle de Acesso Lógico.

Estabelece procedimentos de acesso lógico aos ativos de informação em todos os seus níveis, de forma a limitar o acesso à informação e aos recursos de processamento da informação.

2.3. Norma de Utilização de Recursos de TI.

Estabelece as regras de segurança da informação no uso dos recursos de TI.

Autenticado eletronicamente por **Ministro HUMBERTO EUSTÁQUIO SOARES MARTINS**, **Presidente**, em 16/12/2020, às 10:43, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0180658** e o código CRC **63D5E329**.
