Política de Segurança da Informação – CGEE

(Atualizada em agosto de 2022)

1. Objetivos e princípios

1.1. A Política de Segurança da Informação (PSI) do CGEE tem como objetivo estabelecer as orientações, normas, ações e responsabilidades relativas à proteção da informação custodiada ou de propriedade do CGEE.

1.2. A PSI do CGEE busca atender aos princípios de segurança da informação e comunicação (confidencialidade, disponibilidade, integridade e autenticidade) da informação produzida, utilizada, armazenada ou comunicada pelo Centro.

1.3. A PSI do CGEE é regida pelos preceitos constitucionais, legislação brasileira vigente e pelas normas e regulamentos do Centro, e guiada pelos seguintes princípios:

1.3.1. Conhecimento:

Para garantir a confiança nos ativos de informação, em termos de confidencialidade, disponibilidade, integridade e autenticidade, todos os interessados e envolvidos devem ter ciência das normas e procedimentos de segurança da informação e comunicação vigentes.

1.3.2. Responsabilidade

As responsabilidades pela proteção de cada ativo constituinte do patrimônio informacional do CGEE, e pelo cumprimento de processos de segurança, devem ser claramente definidas.

1.3.3. Proporcionalidade

A complexidade e os custos dos controles de segurança da informação devem ser apropriados e proporcionais ao valor e à necessidade de confiança nos ativos de informação considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual.

1.3.4. Integração

Os controles e processos de segurança da informação devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de criar um sistema de segurança da informação coerente.

1.3.5. Liberdade

Os processos e controles de segurança da informação devem ser compatíveis com o legítimo uso e fluxo de informações, devendo ser observados o direito individual e coletivo das pessoas, o adequado uso dos bens institucionais e o direito de realização de auditorias.

2. Referências legais e normativas

2.1. As referências utilizadas para o estabelecimento da PSI do CGEE estão contidas no relatório do estudo "Princípios da Segurança da Informação. Brasília: CGEE, 2015."

3. Escopo e abrangência

3.1. A PSI do CGEE aplica-se ao corpo diretivo, funcionários, estagiários, e no relacionamento do Centro com agentes externos.

3.2. Trata da proteção aos ativos de informação do Centro nos aspectos físicos, tecnológicos e humanos, estabelecendo direitos e deveres para todos os atores envolvidos.

3.3. Aplica-se, na medida da necessidade, ao ciclo de vida da informação no Centro conforme requisitos estabelecidos por seu responsável ou proprietário.

3.4. Trata da gestão de continuidade das ações do Centro frente a incidentes de segurança relativos aos ativos de informação.

4. Diretrizes gerais

4.1. Estrutura

4.1.1. A PSI do CGEE é composta por este documento de diretrizes e complementada, na medida da necessidade, por normas (resoluções da presidência) e procedimentos.

4.1.2. Normas definirão, no plano tático, um conjunto determinado de ativos de informação e seus respectivos controles de segurança da informação.

4.1.3. Um procedimento define a instrumentação de uma norma no plano operacional, estabelecendo detalhadamente tarefas, ferramentas e responsabilidades operacionais para implementação dos controles de segurança da informação.

4.1.4. Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas nos normativos só devem ser realizadas após prévia e formal autorização do Núcleo de Segurança da Informação.

4.2. Gestão

4.2.1. Todo ativo de informação afeito a controles de segurança da informação deverá ter um responsável definido.

4.2.2. A normatização de segurança da informação será dirigida por demandas oriundas dos processos de trabalho do CGEE.

4.2.3. Os responsáveis por ativos de informação, em conjunto com o Núcleo de Segurança da Informação e demais interessados, definirão os controles de segurança da informação para os ativos de informação envolvidos nos processos de trabalho em foco, utilizando sempre que possível um método de gestão de riscos.

4.2.4. A partir dos requisitos de segurança da informação, novas normas e procedimentos poderão ser propostos.

4.2.5. Constitui requisito de segurança da informação obrigatório para qualquer ativo de informação, a sua classificação de sigilo da informação que deverá observar as definições contidas em norma específica.

4.2.6. A proteção ao patrimônio de informação custodiado ou de propriedade do CGEE será acompanhada pelo Comitê de Segurança da Informação que acionará os mecanismos previstos na PSI com objetivo de garantir os princípios de segurança da informação.

4.3. Continuidade do negócio

4.3.1. Planos de continuidade de negócio dispostos em instrumentos próprios terão por objetivos garantir níveis adequados de disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação utilizados pelo CGEE.

4.3.2. Constitui objetivo dos planos de continuidade de negócio evitar impactos no funcionamento do CGEE, ou minimizar esse impacto, nas ocorrências de incidentes de segurança da informação.

4.4. Propriedade intelectualAs informações produzidas por funcionários, colaboradores e prestadores de serviço no exercício de suas funções para o Centro, são patrimônio intelectual do CGEE e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o reconhecimento de autoria.

4.5. Ativos de Informação e Recursos de Tecnologia da Informação (TI)

4.5.1. Ativos de Informação: Qualquer informação que tenha valor para a Instituição, independentemente de onde essa informação esteja armazenada, ou o recurso de Tecnologia da Informação que a detém, armazena, processa ou transmite.

4.5.2. Recurso de TI: Os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios.

4.5.3. Os ativos de informação e recursos de TI de propriedade ou sob responsabilidade do CGEE devem ser utilizados somente para fins profissionais e de acordo com as orientações dos fornecedores e do Centro.

4.5.4. Inventário de Recursos de TI: O CGEE deve realizar inventário de hardwares e softwares que possuir, devendo a Coordenação de TIC indicar

as informações necessárias e ser a responsável pelo seu registro, armazenamento e atualização.

4.5.5. Catálogo dos Ativos de Informação: O CGEE deve catalogar os Ativos de Informação que possuir ou utilizar, devendo a Coordenadoria de TIC indicar as informações necessárias e ser responsável pelo seu registro, armazenamento e atualização.

4.6. Proteção de Dados Pessoais

4.6.1. O CGEE respeita a privacidade. Assim deve garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais. O CGEE deve avaliar as seguintes medidas de segurança da informação quanto à tratamento de dados pessoais:

4.6.1.1. Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente;

4.6.1.2. Adoção de medidas de segurança para proteger os dados pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito;

4.6.1.3. Elaboração de plano de análise e resposta às violações de dados pessoais;

4.6.1.4. Armazenamento de modo seguro, controlado e protegido, especialmente quanto se tratarem de dados pessoais sensíveis;

4.6.1.5. Processos de anonimização e pseudonimização, sempre que necessário;

4.6.1.6. Protocolos de criptografia na transmissão e armazenamento, quando verificado necessário;

4.6.1.7. Registro lógico das operações de tratamento de dados pessoais;

4.6.1.8. Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias;

4.6.1.9. Transferência aos Agentes de Tratamento de modo seguro e contratualmente previsto;

4.6.1.10. Mapeamento e manutenção de inventário de fluxos de dados pessoais;

4.6.1.11. Elaboração de relatórios de impacto à proteção de dados pessoais, quando necessário;

4.6.1.12. Gestão e tratamento adequado de incidentes que envolvam dados pessoais.

4.7. Gestão de riscos

4.7.1. A gestão de riscos relativo aos ativos de informação será disposto em instrumento próprio e terá por objetivo definir conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos de segurança da informação para o CGEE.

4.7.2. Constitui objetivo da gestão de riscos conferir razoável segurança quanto ao alcance dos princípios de segurança da informação no CGEE.

5. Penalidades

5.1. Ações que violem a política de segurança da informação, suas normas e procedimentos ou que quebrem os controles de segurança da informação serão devidamente apuradas e aos responsáveis serão aplicadas as sanções administrativas, civis e penais em vigor.

6. Papéis e responsabilidades

6.1. A governança em segurança da informação no CGEE envolve, minimamente, os seguintes atores e responsabilidades principais.

6.2. Conselho de Administração

6.2.1. Responsável pela aprovação e publicação da Política de segurança da informação.

6.3. Diretoria Colegiada

6.3.1. Responsável pela aprovação e publicação dos instrumentos normativos derivados.

6.4. Representante da Diretoria

6.4.1. Um integrante da Diretoria do CGEE, responsável pela orientação, supervisão e decisão relativa à Política de Segurança da Informação e seus instrumentos.

6.5. Comitê de segurança da informação (CSI)

6.5.1. Grupo de funcionários do CGEE, responsável pela gestão de segurança da informação do Centro.

6.6. Núcleo de segurança da informação (NSI)

6.6.1. Grupo de funcionários do Centro, responsável pela coordenação e execução das ações relativas à segurança da informação, e tratamento de incidentes de segurança da informação.

6.7. Encarregado pelo Tratamento de Dados Pessoais

6.7.1. Responsável por analisar e aprovar contratos que envolvam tratamento de dados pessoais, seguindo a legislação vigente e aplicável a cada situação em suas particularidades.

6.8. Responsável por ativo de informação

6.8.1. Funcionário do Centro, responsável por zelar pela segurança (ou, realizar a proteção) de ativo de informação em uso, ou armazenado, no CGEE.

6.9. Usuário

6.9.1. Qualquer pessoa que por força de vínculo com o CGEE tenha necessidade de acesso ou uso de recurso de TI ou ativo de informação custodiados ou de propriedade do Centro.

6.10. Usuário externo

6.10.1. Qualquer pessoa que tenha acesso à informação ou serviços disponibilizados por meio recursos de Tecnologia da Informação do CGEE, ou que acesse ou use as instalações físicas do Centro.

7. Aprovação e atualização da PSI

7.1. Os controles de segurança da informação devem ser planejados, aplicados, implementados e, periodicamente, avaliados de acordo com os objetivos institucionais e os riscos para o CGEE.

7.2. Alteração da PSI do CGEE ou de seus instrumentos derivados será realizada conforme as seguintes regras.

7.2.1. Para a PSI:

7.2.1.1. Ordinariamente a cada 2 anos.

7.2.1.2. Extraordinariamente sempre que identificada a necessidade.

7.2.1.3. Por encaminhamento do Representante da Diretoria e aprovação do Presidente do CGEE.

7.2.2. Para normas:

7.2.2.1. Extraordinariamente sempre que identificada a necessidade.

7.2.2.2. Por encaminhamento do Comitê de Segurança da Informação e aprovação do Presidente do CGEE.

7.2.3. Para procedimentos:

7.2.3.1. Extraordinariamente sempre que identificada a necessidade.

7.2.3.2. Por encaminhamento do Núcleo de Segurança da Informação e aprovação do Comitê de Segurança da Informação.

ANEXO I - TERMO DE CIÊNCIA E RESPONSABILIDADE

Formato para ciência eletrônica

Deve ser coletada a ciência do colaborador por meio de barreira de navegação no login da rede ou publicado na Intranet com envio para o correio eletrônico corporativo de todos, conforme descrito abaixo:

Termo de Ciência e Responsabilidade

Confirmo que estou ciente do conteúdo da Política de Segurança da Informação do CGEE, e reafirmo meu dever de cumprir, disseminar e manter-me sempre atualizado com as regras lá estabelecidas.

Formato impresso para assinatura

Termo de Ciência e Responsabilidade

Eu, _____, pelo presente, confirmo que estou ciente do conteúdo da Política de Segurança da Informação do CGEE, e reafirmo meu dever de cumprir, disseminar e manter-me sempre atualizado com as regras lá estabelecidas.

_____, __/___/_____

Local, Data

_____

Assinatura do Colaborador