

Política de Segurança da Informação – CGEE

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 a 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.

4.2. 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 intelectual
- 4.4.1. As 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. Penalidades

4.5.1. 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.

5. Papéis e responsabilidades

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

5.2. Conselho de Administração

5.2.1. Responsável pela aprovação e publicação da Política de Segurança da Informação.

5.3. Diretoria Colegiada

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

5.4. Representante da Diretoria

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

5.5. Comitê de segurança da informação

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

5.6. Núcleo de segurança da informação

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

5.7. Responsável por ativo de informação

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

5.8. Usuário de informação

5.8.1. Qualquer pessoa que por força de vínculo com o CGEE tenha necessidade de acesso ou uso de ativo de informação custodiado ou de propriedade do Centro.

5.9. Agente externo

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

6. Aprovação e atualização da PSI

6.1. 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.

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

6.2.1. Para a PSI:

6.2.1.1. Ordinariamente a cada 2 anos.

6.2.1.2. Extraordinariamente sempre que identificada a necessidade.

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

6.2.2. Para normas:

6.2.2.1. Extraordinariamente sempre que identificada a necessidade.

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

6.2.3. Para procedimentos:

6.2.3.1. Extraordinariamente sempre que identificada a necessidade.

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