Companhia Energética de Minas Gerais

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

INTRODUÇÃO

1.1. A informação é um patrimônio da Cemig e ativo essencial para possibilitar à Empresa cumprir seus objetivos de negócio e atender à sociedade.

1.2. A Cemig reconhece o espaço cibernético como um recurso indispensável para a execução de suas estratégias de negócio.

1.3. A estratégia de segurança cibernética da Cemig baseia-se na aplicação das melhores práticas para proteger o ecossistema de negócios, por meio de um programa de gestão do risco de segurança cibernética.

1.4. Esta Política estabelece diretrizes gerais, princípios e responsabilidades para garantir que as informações da Cemig e de seus clientes sejam protegidas contra divulgação, modificação ou acesso não autorizados.

OBJETIVOS

2.1. Assegurar que a segurança da informação e a segurança cibernética estejam integradas a todas as atividades e processos da Cemig.

2.2. Administrar e reduzir os riscos de segurança da informação e segurança cibernética, fortalecer a imagem da Empresa, atender aos requisitos de negócios e exigências regulatórias e legais.

2.3. Estabelecer processos e implementar tecnologias que permitam à Cemig identificar, prevenir, detectar e reduzir o risco cibernético

PRINCÍPIOS

Cemig fundamenta seus processos e atividades nos seguintes princípios:

3.1.1 Segurança Operacional: as proteções implementadas devem possuir como principal premissa a salvaguarda e respeito à vida humana, garantindo que um incidente de segurança cibernética ou segurança da informação não se torne um acidente que possa causar danos à integridade física de pessoas.

3.1.2 Disponibilidade: as proteções implementadas devem considerar todos os requisitos que mantenham a disponibilidade de sistemas de informação imposta pela necessidade de negócio.

Nenhuma medida de proteção implementada poderá comprometer a disponibilidade ou afetar o desempenho requerido pelo negócio.

3.1.3 Integridade: as proteções implementadas devem garantir a manutenção das condições iniciais das informações, de acordo com a forma com que foram produzidas e armazenadas.

3.1.4 Confidencialidade: as proteções implementadas devem ter como premissa a garantia de que a informação estará acessível apenas a pessoas autorizadas.

3.1.5 Aplicabilidade: os controles de segurança implementados supõem um procedimento exequível e uma estrutura compatível com a organização da Cemig.

3.1.6 Monitoramento: os controles de segurança selecionados devem ser capazes de notificar qualquer evento suscetível a impactar o bom funcionamento ou a proteção dos sistemas de informação.

3.1.7 Rastreabilidade: os sistemas de informação devem possuir registros de ações realizadas,

permitindo que seja possível identificar os responsáveis por elas, bem como o exato momento em que ocorreram.

APLICAÇÃO

4.1. Esta Política aplica-se a todas as atividades da Cemig que envolvam empregados, terceiros, fornecedores, consultores, parceiros e clientes, bem como aos ativos de informação relacionados ao fornecimento dos serviços no espaço cibernético.

COMPROMETIMENTO DA ALTA DIREÇÃO

5.1. O Conselho de Administração, a Presidência e a Diretoria Executiva compreendem a importância da segurança da informação e segurança cibernética para a Cemig.

5.2. Existe o comprometimento com uma gestão efetiva das ações para identificar, mitigar e monitorar os riscos associados às ameaças cibernéticas e para que esta Política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

DIRETRIZES

6.1. Todas as informações adquiridas, processadas, armazenadas e transmitidas são consideradas patrimônio da Cemig e devem ser adequadamente protegidas.

6.2. Toda informação de propriedade da Cemig deve ser utilizada somente para a finalidade autorizada e protegida de riscos e ameaças que possam comprometer sua confidencialidade, integridade ou disponibilidade.

6.3. Os recursos, sistemas, equipamentos e serviços fornecidos para desenvolvimento das atividades profissionais são de propriedade da Cemig e devem ser utilizadas apenas para esta finalidade.

6.4. Os acessos a sistemas informatizados devem utilizar sistemas e tecnologias autorizadas pela Cemig, por meio de credenciais pessoais e intransferíveis e devem seguir os critérios de segurança definidos pela Empresa.

6.5. A Cemig utiliza normas e procedimentos alinhados com esta Política para a definição das medidas de proteção e alcance dos objetivos definidos e uma vez aprovados passam a ser parte integrante desta Política.

6.6. A Cemig poderá monitorar e registrar todas as atividades realizadas, por meio dos recursos disponíveis, com a finalidade de proteção dos ativos e da sua imagem, que poderão ser usados para fins administrativos e legais, além de subsidiar autoridades em caso de investigações.

6.7. As ações de segurança da informação da Cemig devem ser avaliadas periodicamente, com base nas melhores práticas preconizadas pelas normas e frameworks, com o propósito de elevar o nível de maturidade do processo de segurança da informação.

PROCESSOS

7.1. A Cemig utiliza os processos abaixo descritos para assegurar que os controles de segurança sejam implementados e que as informações e os ativos cibernéticos possuam os níveis de proteção adequados:

a. Gestão de ativos: classificação dos ativos de Tecnologia da Informação (TI) e Tecnologia da Operação (TO), incluindo hardware e software, de acordo com a criticidade e objetivos da organização.

b. Gestão de vulnerabilidades: utilização de planos, procedimentos e tecnologias apropriadas para detectar, identificar, analisar, gerenciar e responder a vulnerabilidades e ameaças cibernéticas.

c. Gestão do risco cibernético: execução de processos para identificar, analisar e responder ao risco cibernético nos ambientes de Tecnologia da Informação (TI) e Tecnologia da Operação (TO).

d. Gestão de identidade e acesso: criação e gerenciamento de identidades para as entidades que acessem o ambiente Cemig, com o controle de acesso baseado no menor privilégio, necessidade do negócio e segregação de papéis.

e. Tratamento de incidentes de segurança: utilização de planos, procedimentos e tecnologias para detectar, analisar, mitigar, responder e recuperar de incidentes de segurança cibernética e garantir a continuidade da operação dos serviços e sistemas da Cemig.

f. Monitoramento: atividades e tecnologias para coletar, monitorar e analisar as comunicações de Tecnologia da Informação (TI) e de Tecnologia da Operação (TO) para estabelecer a capacidade de compreensão do ambiente em operação e a habilidade de resposta rápida.

g. Gestão de risco em fornecedores: estabelecimento de controles de segurança para gerenciar o risco cibernético de fornecedores e prestadores de serviços.

h. Conscientização: planos, tecnologias e controles utilizados para criar uma cultura de segurança da informação e assegurar que a força de trabalho possa reconhecer situações de risco e agir corretamente.

i. Arquitetura de segurança: gerenciamento dos processos, controles e tecnologias para a identificação de requisitos de segurança para os ativos cibernéticos e o desenho de controles apropriados para protegê-los.

j. Gestão do programa de segurança da informação: estabelecimento de programa que apoie na governança, no planejamento e na promoção das atividades de segurança cibernética, alinhando os objetivos de segurança aos objetivos da organização.

RESPONSABILIDADES

8.1. A segurança da informação é responsabilidade de cada empregado, terceiro, fornecedor, consultor e parceiro, devendo cada um conhecer e compreender as diretrizes e princípios estabelecidos para o cumprimento desta Política e estarem comprometidos com a proteção adequada de informações e sistemas contra ameaças e riscos.

8.2. Todas as pessoas com acessos ao ambiente Cemig devem participar de atividades de conscientização sobre esta Política, com a finalidade de mitigar possíveis riscos de segurança, compreender as suas responsabilidades e seguir os procedimentos recomendados.

8.3. Todos os colaboradores devem comunicar à área de Segurança da Informação quaisquer descumprimentos da Política de Segurança da Informação e Segurança Cibernética.

8.4. Cabe à Liderança orientar todos sob sua coordenação sobre o conteúdo desta Política, instruções e demais diretrizes de segurança e assegurar o seu cumprimento.

8.5. Cabe ao Comitê de Privacidade, Proteção de Dados e Segurança Cibernética avaliar e monitorar periodicamente as ações de segurança cibernética e segurança da informação, garantir recursos para a execução das atividades e apoiar as ações de promoção dessa Política.

DISPOSIÇÕES FINAIS

9.1. Esta Política será atualizada quando algum fato relevante ou evento ocorrer que motive a sua revisão ou conforme análise e decisão do Comitê de Privacidade, Proteção de Dados e Segurança Cibernética.

9.2. As infrações a esta Política e aos seus documentos relacionados serão consideradas atos de desobediência, sujeitos à aplicação de sanções administrativas diretas e ainda aquelas previstas em legislação vigente.

Política aprovada pelo Conselho de Administração em 18/04/2022