POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

(REVISÃO 01)

Fortaleza, 2022

SUMÁRIO

1. OBJETIVOS

1.1. A Política de Segurança da Informação da CEGÁS – **PSI-CEGÁS** tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso da Companhia de Gás do Ceará – **CEGÁS,** contra ameaças e vulnerabilidades. Desse modo, a política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

1.2. O propósito da política é orientar a todos os empregados da Companhia de Gás do Ceará – **CEGÁS**, diretores, bem como empregados cedidos pelos sócios, estagiários e prestadores de serviços que façam uso dos meios de comunicação, recursos e/ou serviços eletrônicos sejam estes acessados nas/ou a partir das instalações da empresa através de computadores locais, com acesso remoto ou através de aparelhos para transmissão de voz e/ou dados da empresa no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação, em conformidade com as disposições constitucionais, legais e regimentais vigentes.

1.3. A presente Política de Segurança da Informação está baseada nas recomendações propostas por normas reconhecidas mundialmente como um código de prática para a gestão da segurança da informação, bem como está nas leis vigentes em nosso país.

2. ABRANGÊNCIA

Esta política abrange a todos os empregados da CEGÁS, diretores, bem como empregados cedidos pelos sócios, estagiários e prestadores de serviços que façam uso dos meios de comunicação, recursos e/ou serviços eletrônicos sejam estes acessados nas/ou a partir das

instalações da empresa através de computadores locais, com acesso remoto ou através de aparelhos para transmissão de voz e/ou dados da empresa.

3. DOCUMENTOS DE REFERÊNCIA

3.1 Decreto n° 9.637/2018;

3.2 IN GSI/PR n° 01/2008;

3.3 ABNT NBR ISO/IEC 27001, 27701 e 27002;

3.4 DI.DIREX.001 – Código de Conduta e Integridade da CEGÁS;

3.5 *CIS Controls – Center for Internet Security*;

3.6 Lei Federal nº 13.709/2018 (LGPD).

4. DEFINIÇÕES

Para os efeitos da PSI-CEGÁS, são estabelecidos os seguintes conceitos e definições:

4.1 **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como de usar os ativos de informação de um órgão ou entidade;

4.2 **Ameaça**: qualquer evento que explore vulnerabilidades ou seja causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

4.3 **Análise de riscos**: uso sistemático de informações para identificar fontes e avaliar riscos;

4.4 **Análise/avaliação de riscos**: processo completo de análise e avaliação de riscos;

4.5 **Atividade**: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

4.6 **Ativo**: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha valor para a organização;

4.7 **Ativos de Informação**: os meios de armazenamento, transmissão e processamento; os sistemas de informação; além das informações em si, bem como os locais em que se encontram esses meios e as pessoas que têm acesso a eles;

4.8 **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa, ou por um determinado sistema, órgão ou entidade;

4.9 **Avaliação de riscos**: processo de comparar o risco estimado com critérios predefinidos para determinar a importância do risco;

4.10 **CEGÁS**: Companhia de Gás do Ceará;

4.11 **Celeridade**: as ações de segurança da informação devem oferecer respostas rápidas a incidentes e falhas;

4.12 **Classificação da informação**: identificação dos níveis de proteção que as informações demandam; atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas;

4.13 **Comunicação do risco**: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

4.14 **Confidencialidade**: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

4.15 **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

4.16 **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

4.17 **Desastre**: evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos em sua capacidade de prestar serviços essenciais ou críticos, por um período superior ao prazo de recuperação;

4.18 **Descarte**: eliminação correta de informações, documentos, mídias e acervos digitais;

4.19 **Disponibilidade**: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;

4.20 **DPO:** Data Protection Officer ou Encarregado de Proteção de Dados Pessoais;

4.21 **Estimativa de riscos**: processo utilizado para atribuir valores à probabilidade e consequências de determinado risco;

4.22 **Eficácia**: realização de um trabalho que atinja os resultados esperados;

4.23 **Eficiência**: realização de um trabalho, com presteza, agilidade e eficácia;

4.24 **Ética**: preservação dos direitos dos agentes públicos, sem comprometimento da Segurança da Informação e das Comunicações;

4.25 **Evento de segurança da informação**: ocorrência identificada de procedimento, sistema, serviço ou rede que indica possível perda de controle ou violação da política de segurança da informação, ou situação desconhecida que possa ser relevante para a segurança da informação;

4.26 **Gerenciamento de operações e comunicações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suportem;

4.27 **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada de seu controle;

4.28 **Gestão de continuidade dos negócios**: processo de gestão que identifica ameaças potenciais para uma organização, bem como os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo prevê a definição de estrutura para o aprimoramento da resiliência organizacional, de modo a se responder efetivamente às ameaças e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, assim como suas atividades de valor agregado;

4.29 **Integridade**: propriedade de salvaguarda da exatidão e completeza de ativos;

4.30 **LGPD**: Lei Geral de Proteção de Dados Pessoais, Lei 13.709, de 14 de agosto de 2018.

5. RESPONSABILIDADES

5.1 Comitê de Segurança da Informação

Compete ao Comitê de Segurança da Informação assessorar e atuar na implementação das ações de Segurança da Informação previstas nesta Política, construindo grupos de trabalho, se necessário, para tratar de temas e propor soluções específicas sobre Segurança da Informação. Cabe também ao comitê propor e implementar todos os normativos internos relativos à Segurança da Informação. Este Comitê é formado pelos assessores da Diretoria Executiva e pelo Gerente de Tecnologia da Informação – GERTI, e se reunirá sempre que necessário ou por solicitação da Diretoria.

5.2 Gestor de Segurança da Informação

O Gestor de Segurança da Informação será o Gerente de Tecnologia da Informação, sendo suas competências a promoção da cultura de Segurança da Informação para a **CEGÁS** de

forma contínua, monitorando a implementação da legislação aplicável e pertinente ao domínio da Segurança da Informação e acompanhando todas as investigações e as avaliações dos danos decorrentes de eventual quebra de segurança da informação, assim como realizando o reporte periódico de ação para correção de eventuais problemas estruturais ou pontuais identificados. Também são atribuições do Gestor propor normativos internos relativos à Segurança da Informação, solicitar e propor recursos necessários às ações de Segurança da Informação da CEGÁS, estando constantemente realizando estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação.

5.3 **Equipe de tratamento de incidentes de segurança**

A equipe de **Tratamento de Incidentes de Segurança** será composta por membros da GERTI e especificada em instrução própria**,** estará subordinada ao Gestor de Segurança da Informação. Cabe à equipe de Tratamento de Incidentes de Segurança facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, auxiliando na recuperação de sistemas e realizando as análises de ataques, intrusões e incidentes que podem ocorrer no ambiente da tecnologia da informação da CEGÁS.

5.4 **Colaboradores**

Todos os colaboradores da CEGÁS devem conhecer e cumprir todos os princípios e diretrizes estabelecidos nesta política, adotando os requisitos de controle de segurança especificados em normativos, comunicando tempestivamente ao Gestor de Segurança da Informação incidentes que afetam a Segurança da bem como a manutenção dos processos sob sua responsabilidade aderentes às políticas e normativos internos derivados e específicos de Segurança da Informação.

5.5 **Comitê de proteção de dados**

O Comitê de Proteção de Dados foi criado pela CEGÁS, segundo pauta CEGÁS/GERTI/DAFNº065/2021 de 27 de julho de 2021, em que foram todos os seus membros nomeados e suas funções definidas.

O Encarregado de Proteção de Dados (DPO), tem o papel de orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. Além disso, conforme artigo 41 da LGPD, também são atribuições do DPO aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

O Encarregado de Proteção de Dados representará a Companhia e deverá comunicar, tanto aos titulares dos dados quanto à ANPD (Autoridade Nacional de Proteção de Dados), sobre violações de dados. Com a ajuda do Comitê de Privacidade e amparado por ele, o DPO executará suas funções de acordo com a normativa citada.

O Gerente de Tecnologia da Informação – GERTI, será o responsável por auxiliar o Comitê e o DPO nas implementações que necessitem de intervenções tecnológicas ou de alterações de sistemas.

6. DESCRIÇÃO

6.1 **Princípios**

Esta política reger-se-á por princípios que deverão ser observados por todos e seguidos em toda e qualquer decisão e ou ação a ser executada no cumprimento das obrigações junto a esta Companhia, que são:

6.1.1 Preservação da integridade, autenticidade e irretratabilidade das informações produzidas e recebidas pela CEGÁS;

6.1.2 Transparência das informações públicas de acordo com a legislação vigente;

6.1.3 Garantia da disponibilidade e da confidencialidade das informações que necessitam de restrição de acesso;

6.1.4 Respeito à autoria e à propriedade intelectual das informações;

6.1.5 Promoção da cultura de segurança da informação e comunicações;

6.1.6 Defesa de auditabilidade dos processos; e,

6.1.7 Acesso mínimo aos ativos de informação.

6.2 **Diretrizes gerais**

As diretrizes estipuladas nesta política de segurança devem ser seguidas por todos da CEGÁS a fim de cumprir com o objetivo desta Companhia quando utilizar os meios de informações disponíveis, que são:

6.2.1 Observar sempre o alinhamento com os referenciais estratégicos organizacionais da CEGÁS e a conformidade com a legislação e a regulamentação em vigor;

6.2.2 Otimizar os investimentos proporcionando a eficácia, eficiência e efetividade dos processos organizacionais;

6.2.3 O planejamento das ações de Segurança da Informação deve ser realizado por meio de metodologia baseada em processo de melhoria contínua, considerando o gerenciamento de riscos corporativos;

6.2.4 É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas através de dispositivos móveis;

6.2.5 É inaceitável a violações dos direitos de qualquer pessoa ou empresa protegida pelo direito de cópia, segredo comercial, patente ou outro tipo de propriedade intelectual,

assim como outras leis e regulamentos, incluindo a instalação ou distribuição de softwares "piratas" que não estejam adequadamente licenciados para uso pela CEGÁS;

6.2.6 A cópia não autorizada de materiais com direito de cópia incluindo digitalização, distribuição de fotografias de revistas, livros, músicas, vídeos ou outras origens protegidas por direito de cópia não é aceita pela CEGÁS;

6.2.7 Não é permitido o uso dos recursos computacionais da CEGÁS para obter ou transmitir materiais pornográficos, sobre pedofilia, ofensivos, segregatícios, discriminatórios e que violem leis de trabalho e raciais, entre outros;

6.2.8 A oferta de produtos e/ou serviços (negócios pessoais) é proibida utilizando-se os recursos da CEGÁS;

6.2.9 A criação ou autorização de pontos de acesso, gerar interrupções na segurança da rede de comunicação e utilizar técnicas de obtenção de informação não autorizada sobre a topologia da rede, incluindo acesso a dados dos quais os usuários não estejam expressamente autorizados a acessar, varredura na rede (*port-scan* ou *sniffing*), parada de serviços (DoS), roteamento falsificado e outros como inundação de pacotes (*pinged floods*), ou falsificação/injeção de pacotes (*packet spoofing*) para propósitos maliciosos, a menos que estas obrigações estejam dentro do escopo de obrigações regulares; estão proibidos;

6.2.10 A varredura (busca) de portas (estrutura lógica que permite a comunicação entre computadores clientes e serviços oferecidos por computadores servidores) é expressamente proibida;

6.2.11 O uso de senhas é pessoal e intransferível, e deve respeitar os requisitos mínimos de segurança propostos pelo Comitê de segurança da informação;

6.2.12 Os ativos de informação devem ser inventariados constantemente e protegidos, assim como devem ter identificados os seus gestores e responsáveis e mapeados os riscos a eles associados;

6.2.13 A infraestrutura e recursos tecnológicos destinados à produção, distribuição, arquivamento e preservação de dados e informações devem ser adequadamente protegidos contra indisponibilidade, comprometimento de integridade e confidencialidade, alterações não autorizadas ou acesso indevido, falhas ou interrupções não programadas;

6.2.14 Os dados confidenciais, de acordo com a LGPD, são secretos e valiosos, devendo todos os funcionários os protegerem e o Gestor de Segurança da Informação garantir sua inviolabilidade;

6.2.15 O Gestor de Segurança da Informação deverá, em instrução própria, dispor sobre o bloqueio e controle dos dispositivos móveis, sendo proibida a inserção de dispositivos na rede sem a sua consonância;

6.2.16 O uso de IDs de contas de mídias sociais em nome da CEGÁS deve ser limitado ao Gerente da Gerência de Comunicação e Marketing da CEGÁS e, sendo identificada contas não oficiais, é dever de todos relatar via Ouvidoria, para que sejam tomadas as medidas necessárias;

6.2.17 Todas as informações produzidas por colaboradores da CEGÁS, no exercício de suas atribuições, são patrimônio intelectual da CEGÁS e não cabe a seus criadores qualquer forma de direito autoral, salvo aqueles assegurados por legislação específica;

6.2.18 Todos os arquivos importantes devem ser salvos em local apropriado definido pelo Comitê de Segurança da Informação, sendo que arquivos salvos em discos locais fora do local definido não terão garantia alguma de backup e integridade;

6.2.19 Não é permitido transferir dados confidenciais para outros dispositivos ou contas, a menos que seja absolutamente necessário, sempre compartilhando-os pela rede/sistema da empresa e certificando que os destinatários dos dados sejam pessoas ou organizações devidamente autorizadas e que tenham políticas de segurança adequadas;

6.2.20 O Gestor de Segurança da Informação deverá manter e analisar os registros de incidentes relativos à Segurança da Informação e, em caso de incidente envolvendo os dados sensíveis, deverá comunicar imediatamente o Encarregado pelo Tratamento de Dados Pessoais (*Data Protection Officer*) para que tome as medidas necessárias de acordo com a Lei;

6.2.21 A empresa deverá manter informações classificadas de acordo com o Regulamento de Sigilo da Informação e as informações classificadas como confidenciais e secretas devem ser protegidas por meio de criptografia, bem como *backups* e imagens de segurança;

6.2.22 Devem ser assegurados os recursos necessários à operacionalização desta Política com o total apoio da alta administração.

6.3 **Conscientização**

A CEGÁS deve adotar ações permanentes de caráter preventivo e educativo para comunicação e treinamento de seus colaboradores com o objetivo de desenvolver a cultura de Segurança da Informação.

6.4 **Considerações de Qualidade, Segurança, Meio Ambiente e Saúde (QSMS)**

A impressão do presente documento deve ser feita de forma comprometida com o Meio Ambiente.

6.5 **Atualização e validade**

A segurança da informação, é um assunto de constante acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

Os instrumentos normativos gerados a partir desta PSI deverão ser revisados sempre que se fizer necessário.

Esta PSI tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

6.6 **Aderência e adequações à LGPD**

Esta política se refere ao macro gerenciamento de segurança da informação, sendo que em política específica a proteção de dados pessoais será tratada. Nesta política, em sua revisão anual, foram acrescentados itens para amparar a segurança dos dados pessoais e propiciar mecanismos para que o Gestor de Segurança da Informação possa prover a inviolabilidade de dados que trafegam pela rede da Companhia.

6.7 **Conformidade**

Funcionários, fornecedores ou quaisquer outros envolvidos com a Companhia que observarem quaisquer desvios às diretrizes desta Política, poderão relatar o fato ao Canal de Ouvidoria, podendo ou não se identificar.

Internamente, o descumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem, conforme a respectiva gravidade do descumprimento.

6.8 **Sanções**

O não cumprimento das diretrizes declaradas nesta Política está sujeito a sanções disciplinares, conforme Regimento Interno da Companhia, sendo que os processos administrativos devem ser tratados sob sigilo zelando pela privacidade dos envolvidos.

7. REGISTROS

Identificação	**Armazenamento**	**Grau de sigilo**	**Proteção**	**Recuperação**	**Retenção**	**Disposição**
Instrução de bloqueio e controle	Meio Eletrônico/ físico	Corporativo	Backup/ pasta	Nome	Indeterminado	Não aplicável

HISTÓRICO DE ELABORAÇÃO/ REVISÃO

Versão	Data	Histórico	Aprovação
00	29/09/2020	Emissão	215ª Reunião CONAD - 30/10/2020
01	08/06/2022	Revisão 01	255ª Reunião CONAD – 09/08/2022

8. ANEXOS

Não aplicável.