# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 1. APRESENTAÇÃO

A **CAGECE** adota esta Política de Segurança da Informação como instrumento fundamental, estabelecendo princípios e normas para assegurar a confidencialidade, integridade e disponibilidade dos seus ativos de TI, informações, e proteção de dados pessoais.

## 2. FUNDAMENTAÇÃO LEGAL

2.1. A presente Política de Segurança da Informação da Cagece está fundamentada em dispositivos legais, regulatórios e normativos que regem o tratamento de dados, a proteção de informações e a responsabilidade das organizações quanto à segurança da informação. Sua elaboração considera os seguintes referenciais legais e técnicos:

2.1.1. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD): Estabelece princípios, direitos e obrigações quanto ao tratamento de dados pessoais, exigindo medidas técnicas e administrativas adequadas para a proteção de dados.

2.1.2. Lei nº 12.965/2014 – Marco Civil da Internet: Define princípios e garantias para o uso da internet no Brasil, incluindo a obrigação de guarda e proteção de dados, privacidade e segurança dos registros.

2.1.3. Código Civil Brasileiro (Lei nº 10.406/2002): Responsabiliza juridicamente o tratamento inadequado de informações que resultem em danos a terceiros.

2.1.4. Decreto nº 8.771/2016: Regulamenta aspectos do Marco Civil da Internet, incluindo os requisitos de segurança, controle de acesso e guarda de registros.

Emenda Constitucional no. 115 – Constituição Federação

2.1.5. ISO 27000: 2022 – Família de Normas

2.1.6. ISO/IEC 27001:2022 – Sistema de Gestão de Segurança da Informação

2.1.7. ISO 31000 – Gestão de Riscos Diretrizes

2.1.8. ISO/IEC 27002:2022 - Código de Práticas para Controles de Segurança da Informação.

2.1.9. ISO/IEC 27701:2019 – Gestão de Privacidade da Informação.

2.30. ISO 27005 – Segurança da informação, segurança cibernética e proteção à privacidade – Orientações para gestão de riscos em segurança da informação

## 3. DEFINIÇÕES E CONCEITOS

3.1. Segurança da Informação: Conjunto de práticas para proteger as informações contra acessos não autorizados, alterações indevidas ou indisponibilidade.

3.2. Confidencialidade: Propriedade que garante que apenas pessoas autorizadas tenham acesso às informações.

3.3. Integridade: Propriedade que assegura que as informações não foram modificadas sem autorização.

3.4. Disponibilidade: Garantia de que a informação estará acessível sempre que necessário.

3.5. Ativo de Informação: Qualquer recurso que contenha ou suporte informações valiosas, como sistemas, bancos de dados, documentos ou pessoas.

3.6. Acesso: Permissão concedida a um usuário, programa ou processo para utilizar dados, sistemas ou recursos.

3.7. Autenticação: Processo de verificar a identidade de um usuário ou sistema, normalmente por senha, biometria ou token.

3.8. Autorização: Permissão para que um usuário, após autenticado, acesse determinados recursos ou informações.

3.9. Controle de Acesso: Mecanismos utilizados para garantir que somente pessoas autorizadas possam acessar determinados recursos.

3.10. Política de Segurança da Informação (PSI): Documento que estabelece as diretrizes e responsabilidades para a proteção das informações da organização.

3.11. Sistema de Gestão de Segurança da Informação (SGSI): Estrutura que reúne políticas, processos e controles para gerenciar os riscos e proteger as informações da organização (ISO 27001).

3.12. Risco de Segurança da Informação: Probabilidade de uma ameaça explorar uma vulnerabilidade e causar impacto aos ativos de informação.

3.13. Vulnerabilidade: Falha ou fraqueza em um ativo ou processo que pode ser explorada por uma ameaça.

3.14. Ameaça: Evento ou agente com potencial de causar danos às informações, como vírus, hackers ou falhas humanas.

3.15. Incidente de Segurança: Ocorrência que compromete, ou pode comprometer, a confidencialidade, integridade ou disponibilidade das informações.

3.16. Plano de Continuidade de Negócios (PCN): Conjunto de procedimentos que garante a retomada rápida das operações após um incidente.

3.17. Backup: Cópia de segurança de dados e sistemas feita para possibilitar sua recuperação em caso de perda ou falha.

3.18. Criptografia: Técnica de codificação de dados para garantir que somente pessoas autorizadas possam acessá-los.

3.19. Logs: Registros automáticos de atividades realizadas em sistemas, usados para auditoria e rastreabilidade.

3.20. Usuário Autorizado: Pessoa ou sistema com permissão formal para acessar ou manipular determinadas informações.

3.21. Dado Pessoal: Qualquer informação que identifique ou possa identificar uma pessoa natural (ex: nome, CPF, e-mail) – conforme LGPD.

3.22. Dado Sensível: Informações pessoais que exigem proteção especial, como dados de saúde, religião, orientação sexual e biometria.

3.23. Titular de Dados: Pessoa física a quem se referem os dados pessoais tratados pela organização.

3.24. Privacidade de Dados: Direito do titular de controlar como seus dados pessoais são coletados, usados, armazenados e excluídos.

3.25. Encarregado (DPO): Pessoa indicada pela organização para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

3.26. Controlador de Dados: Pessoa física ou jurídica que toma decisões sobre o tratamento de dados pessoais.

3.27. Operador de Dados: Pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

3.28. Consentimento: Autorização clara e informada dada pelo titular para o tratamento de seus dados pessoais.

3.29. Governança da Informação: Estrutura de políticas, processos e controles que garantem o uso adequado e seguro das informações.

3.30. Auditoria de Segurança da Informação: Avaliação formal e sistemática dos controles de segurança para verificar sua conformidade com normas, políticas e regulamentos.

3.31. Ataques cibernéticos: Ação maliciosa realizada contra sistemas, redes ou dispositivos com o objetivo de comprometer a confidencialidade, integridade e disponibilidade das informações.

3.32. Antivírus: Software de segurança projetado para detectar, bloquear e remover programas maliciosos como vírus, trojans, Worms e spyware.

3.33. Firewall: Mecanismo de segurança que controla o tráfego de dados entre redes e sistemas, com base em regras definidas.

3.34. IA (Inteligência Artificial): Conjunto de tecnologias que permite que sistemas e máquinas simulem capacidades humanas como aprendizado, raciocínio, reconhecimento de padrões e tomada de decisão.

3.35. Comunicação Criptografada: Transmissão de dados protegida por algoritmos de criptografia, que codificam a informação de forma que apenas o destinatário autorizado consiga acessá-la.

3.36. Malware: Termo genérico para qualquer tipo de software malicioso, criado para causar danos, roubar dados ou acessar sistemas de forma não autorizada.

3.37. TI: Conjunto de recursos, infraestrutura e práticas voltadas para o tratamento da informação por meio de sistemas computacionais, redes, softwares e serviços tecnológicos.

3.38. Software: Conjunto de instruções, programas ou aplicativos executados por um computador ou sistema.

3.39: Comitê de Segurança da Informação: Grupo formado por representantes de áreas estratégicas da organização, responsável por definir, revisar e monitorar as diretrizes, políticas e ações relacionadas a segurança da informação.

3.40. Gestão de Vulnerabilidades: Processo de identificação, avaliação, tratamento e monitoramento de vulnerabilidades em sistemas e aplicações.

3.41. Teste de Penetração (Pentest): Simulação de ataques cibernéticos para identificar falhas de segurança.

3.42. Engenharia Social: Manipulação psicológica de pessoas para que executem ações ou divulguem informações confidenciais.

3.43. Zero Trust: Modelo de segurança que assume que nenhuma entidade (usuário, dispositivo, rede) pode ser confiável por padrão, exigindo verificação rigorosa para cada acesso.

## 4. OBJETIVOS

4.1. A Política de Segurança da Informação da Cagece visa estabelecer diretrizes e controles que garantam a proteção eficaz dos ativos de informação. Os principais objetivos incluem:

-Assegurar mecanismos de segurança robustos que protejam os sistemas de TI contra acessos não autorizados, falhas e ataques

-Proteger a confidencialidade das informações corporativas, evitando divulgação não autorizada.

-Preservar a integridade dos dados, assegurando que as informações sejam precisas e confiáveis.

-Garantir que as informações e sistemas estejam disponíveis para os usuários autorizados quando necessário.

-Estabelecer claramente as responsabilidades de todos os colaboradores, gestores e terceiros em relação à segurança da informação.

-Implementar controles de segurança que sejam monitorados e atualizados continuamente para enfrentar novas ameaças e vulnerabilidades.

-Assegurar que todas as práticas e sistemas estejam em conformidade com as leis e regulamentos aplicáveis.

-Fomentar uma cultura organizacional que reconheça a importância da segurança da informação e incentive boas práticas.

## 5. DIRETRIZES E PRINCÍPIOS

Diretrizes e Princípios da Política de Segurança da Informação:

5.1. Confidencialidade, integridade e disponibilidade: Garantir que as informações estejam acessíveis apenas a pessoas autorizadas, permaneçam íntegras e estejam disponíveis sempre que necessário.

5.2. Proteção dos ativos informacionais: Proteger todos os ativos de informação contra acessos não autorizados, alterações indevidas e indisponibilidades.

5.3. Conduta segura: Exigir que colaboradores, prestadores de serviço e partes interessadas adotem práticas seguras no uso, armazenamento, compartilhamento e descarte de informações.

5.4. Conformidade legal e regulatória: Assegurar o cumprimento das leis, normas e regulamentações aplicáveis à segurança da informação.

5.5. Ética e responsabilidade: Promover uma cultura organizacional baseada em valores éticos e na responsabilidade pelo uso adequado da informação.

5.6. Gestão baseada em riscos: Adotar uma abordagem preventiva, com ações orientadas pela análise e tratamento de riscos relacionados à segurança da informação.

5.7. Conscientização e capacitação: Incentivar a educação contínua e a conscientização dos usuários quanto à importância da segurança da informação.

5.8. Melhoria contínua: Manter processos de revisão e aprimoramento constantes da política e das práticas de segurança da informação.

## 6. CARACTERÍSTICAS

### 6.1. Governança de Segurança da Informação

#### 6.1.1 Alinhamento da segurança da informação aos objetivos de negócios e processos organizacionais.

O alinhamento estratégico entre a segurança da informação e os objetivos de negócios é fundamental para gerar valor e garantir continuidade e conformidade.

Alinhamento Estratégico: A segurança da informação deve ser estrategicamente integrada aos objetivos de negócios, garantindo que as práticas e controles adotados suportem diretamente os processos organizacionais.

Geração de Valor: Implementar controles e práticas de segurança que não apenas protejam os ativos, mas também contribuam para a geração de valor e inovação dentro da organização.

Suporte aos Processos Organizacionais: Assegurar que a segurança da informação favoreça a eficiência dos processos organizacionais, facilitando operações seguras e contínuas.

#### 6.1.2 Estrutura organizacional de Gestão de Segurança da Informação.

Uma estrutura sólida e bem definida é essencial para a governança eficaz da Segurança da Informação na organização.

A organização deve possuir uma estrutura formal de governança dedicada à Gestão de Segurança da Informação, com definição clara de instâncias decisórias, comitês, funções executivas e mecanismos de prestação de contas

que garantam a efetividade do sistema de segurança.

Os papéis e responsabilidades relacionados à segurança da informação devem ser claramente definidos, formalizados e amplamente comunicados em todos os níveis da organização, promovendo a corresponsabilidade e o engajamento contínuo de gestores, equipes operacionais e parceiros.

**6.2. Gestão de Riscos de Segurança da Informação**Uma gestão eficaz de riscos de segurança da informação e privacidade de dados é essencial para a proteção dos ativos da organização e a conformidade com regulamentos legais.

Implementar um processo contínuo de gestão de riscos que inclua identificação, análise, avaliação, tratamento, monitoramento e revisão dos riscos. Alinhar este processo ao contexto organizacional e diretrizes de governança corporativa.

Garantir que a tomada de decisões seja baseada em dados e análises, proporcionando a aplicação proporcional e eficaz de controles.

Adotar sistemas para monitorar eventos, registros e indicadores de segurança da informação, permitindo a detecção precoce de anomalias e respostas eficientes a incidentes.

Estabelecer processos para a melhoria contínua dos controles implementados, garantindo a adaptação a novas ameaças e tecnologias.

Conduzir a gestão de riscos de forma integrada, considerando riscos técnicos, humanos, físicos e ambientais. Essa abordagem equilibrada assegura que todos os aspectos de risco sejam abordados adequadamente.

Incorporar segurança e privacidade desde as fases iniciais do desenvolvimento de sistemas e serviços, em conformidade com legislações como a LGPD e normas internacionais

Garantir que a segurança da informação e a proteção de dados pessoais sejam componentes essenciais desde o início do ciclo de vida de sistemas, serviços, projetos e processos.

**6.3. Controle de Acesso**

O controle de acesso rigoroso é essencial para proteger os ativos de TI e garantir a segurança da informação dentro da organização.

Princípio do Privilégio Mínimo: Garantir que o acesso seja concedido apenas conforme necessário para o desempenho das funções específicas de cada usuário, minimizando a exposição a riscos.

Acesso Restrito: Conceder acesso a serviços, sistemas e ativos de TI apenas a pessoas autorizadas, com a assinatura de um termo de confidencialidade, formalizando o compromisso com a proteção das informações.

Conformidade Legal: Assegurar que o tratamento de dados pessoais por colaboradores, terceiros ou fornecedores ocorra somente com um instrumento formal que garanta a conformidade com a LGPD e outras regulamentações relevantes.

Autenticação Robusta: Implementar autenticação multifator para acessos críticos, assegurando a verificação segura da identidade dos usuários e a integridade do ambiente.

Monitoramento e Revisão: Realizar auditorias regulares de acessos para assegurar que os privilégios estejam atualizados e alinhados com as funções de cada usuário.

Revisão Periódica: Estabelecer revisões periódicas dos direitos de acesso para identificar e corrigir excessos ou incoerências.

Gerenciamento de Identidades: Implementar sistemas de gerenciamento de identidades para assegurar que os acessos sejam eficazmente controlados e monitorados.

**6.4. Segurança Física e do Ambiente**

A segurança física e do ambiente é crucial para garantir a proteção abrangente de pessoas, instalações, equipamentos e dados dentro de uma organização. Assegurar essa proteção requer uma abordagem integrada envolvendo diferentes áreas, como segurança patrimonial e segurança do trabalho.

Integração de Áreas: Ações de segurança da informação devem ser coordenadas com as áreas de segurança patrimonial e do trabalho para maximizar a eficácia das medidas protetivas e melhorar a resiliência organizacional.

Controles de Segurança Física: Implementação de controles robustos para proteger áreas e ativos de TI. Isso inclui barreiras físicas, como portas de segurança e catracas, além de mecanismos avançados de autenticação.

Vigilância Eletrônica: Uso de sistemas de vigilância por vídeo para monitoramento contínuo, garantindo que qualquer atividade suspeita seja detectada e abordada rapidamente.

Gerenciamento de Acesso: Controle estrito sobre quem pode acessar áreas sensíveis, envolvendo registros detalhados de entrada e saída, além de auditorias regulares.

Planos de Resposta a Incidentes: Desenvolvimento de procedimentos claros para resposta a incidentes físicos e ambientais, assegurando que a equipe esteja treinada para reagir eficazmente a quaisquer ameaças.

Treinamento e Conscientização: Formação contínua para funcionários sobre práticas de segurança física, garantindo que todos conheçam as políticas e procedimentos relevantes.

Avaliação de Riscos Ambientais: Identificação e mitigação de riscos ambientais, como incêndios e inundações, através de sistemas de alarme, detectores de fumaça e planos de evacuação adequados.

**6.5. Gestão de Continuidade de Negócios e Gestão de Crises**

A Gestão de Continuidade de Negócios em TI é vital para garantir a resiliência operacional e a recuperação rápida em caso de eventos disruptivos. Este processo envolve várias etapas críticas:

Identificação de Processos Críticos: Determinar quais processos de negócios são essenciais para a operação contínua e o impacto potencial de sua interrupção.

Avaliação de Impactos: Realizar uma análise detalhada dos impactos potenciais de interrupções nos processos críticos e suas implicações financeiras e reputacionais.

Mitigação de Riscos: Implementar medidas proativas para reduzir a probabilidade e o impacto de riscos identificados, alinhando essas ações aos objetivos corporativos.

Estratégias de Contingência: Desenvolver planos de contingência robustos que detalham ações imediatas em caso de falhas, assegurando a continuidade dos serviços essenciais.

Planos de Recuperação: Estabelecer planos detalhados para recuperação de dados e sistemas, garantindo que sejam restaurados ao seu estado operacional com eficiência.

Procedimentos de Retorno à Normalidade: Definir passos claros para retornar a operação normal após a implementação dos planos de recuperação, minimizando o tempo de inatividade.

Testes e Revisões Regulares: Realizar testes regulares dos planos para assegurar sua eficácia e alinhamento contínuo com as mudanças nos objetivos e no ambiente corporativo.

Treinamento e Conscientização: Capacitar regularmente as equipes envolvidas nos procedimentos de continuidade, garantindo que todos estejam cientes de suas responsabilidades.

Comunicação Eficaz: Estabelecer canais de comunicação claros para facilitar a coordenação durante eventos disruptivos, garantindo que todas as partes interessadas sejam informadas oportunamente.

Alinhamento com a Política de Segurança da Informação: Garantir que todas as medidas de continuidade sejam integradas à política geral de segurança da informação, fortalecendo a defesa contra ameaças.

Estrutura de Gestão de Crises: Implementar uma estrutura formal de gestão de crises com fluxos, papéis e responsabilidades bem definidos, garantindo clareza nas ações e decisões durante um incidente.

### 6.6. Gestão de Incidentes de Segurança da Informação

Uma gestão eficaz de incidentes de segurança é essencial para proteger a integridade, confidencialidade e disponibilidade das informações.

Procedimentos Formais de Gestão de Incidentes: Desenvolver e manter procedimentos formais e detalhados para a gestão de incidentes, cobrindo todas as etapas: identificação, registro, classificação, contenção, erradicação, recuperação e análise pós-incidente.

Integração com Continuidade de Negócios: Assegurar que esses procedimentos estejam integrados à estratégia de continuidade de negócios, facilitando respostas ágeis e minimizando impactos.

Conformidade Legal: Alinhar as respostas a incidentes com as obrigações legais e regulatórias para evitar penalidades e proteger a reputação da organização.

Canais de Comunicação e Notificação: Disponibilizar canais de comunicação acessíveis e seguros para que colaboradores e terceiros possam reportar suspeitas ou incidentes de forma rápida e confidencial.

Resposta e Recuperação: Implementar processos para garantir uma resposta imediata e eficaz a incidentes, minimizando os impactos operacionais e garantindo a continuidade dos serviços.

### 6.7 Gestão de Mudanças

Um processo robusto de gestão de mudanças é essencial para garantir a segurança e a continuidade dos serviços de TI.

Processo: Implementar um processo padronizado para formalização, documentação e aprovação de todas as alterações no ambiente de TI, assegurando que todas as mudanças sejam geridas de forma controlada.

Análise de Impacto: Realizar análises detalhadas de impacto para identificar riscos potenciais associados às mudanças e preparar planos de resposta adequados.

Documentação: Manter registros completos que permitam a rastreabilidade das decisões, incluindo responsáveis envolvidos e testes realizados, garantindo transparência e responsabilidade.

Registros de Homologação: Acompanhar mudanças com registros de homologação e validação para assegurar que não comprometam a disponibilidade e integridade dos serviços

Comunicação e Transparência: Assegurar que todas as partes interessadas sejam informadas sobre as mudanças planejadas e concluídas, facilitando a colaboração e o alinhamento organizacional.

### 6.8. Conscientização e Treinamento

A conscientização e o treinamento contínuo são pilares essenciais para fortalecer a segurança da informação na organização.

Promover Cultura de Segurança: Fomentar uma cultura organizacional de segurança, onde todos se sintam responsáveis e engajados na proteção das informações.

Campanhas de Conscientização: Realizar campanhas de conscientização periódicas para manter a segurança da informação como uma prioridade constante.

Programa de Capacitação Contínua Implementar um programa abrangente de capacitação em segurança da informação destinado a todos os colaboradores, terceiros e prestadores de serviços com acesso a dados ou sistemas.

### 6.9. Conformidade com Requisitos Legais e Contratuais

Garantir a conformidade com todas as leis, regulamentos e obrigações contratuais é fundamental para a integridade e segurança organizacional.

Conformidade Legal e Regulatória: Devem ser asseguradas que suas práticas, políticas e controles de segurança da informação estão plenamente conformes com leis e regulamentos aplicáveis, como a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet, legislação anticorrupção e normas técnicas reconhecidas.

Auditorias e Diligências: Conduzir auditorias internas e externas, bem como diligências específicas, para avaliar a eficácia dos controles de segurança e o cumprimento das políticas institucionais.

Identificação de Oportunidades de Melhoria: Utilizar esses processos para identificar oportunidades de melhoria em conformidade e gerar planos de ação corretiva e preventiva, promovendo a melhoria contínua do sistema de gestão de segurança da informação.

## 7. RESPONSABILIDADES

**7.1 Compete ao Gestor de Segurança da Informação**

7.1.1 Desenvolver, definir e revisar regularmente a política de segurança da informação, garantindo que esteja alinhada com os objetivos estratégicos da organização.

7.1.2 Aprovar diretrizes claras e específicas que orientem as práticas de segurança em toda a organização.

7.1.3 Promover uma cultura de segurança robusta em todos os níveis, incentivando a consciência e o compromisso com a segurança da informação.

7.1.4 Implementar eficazmente controles de segurança nos processos sob sua gestão, assegurando que todos os procedimentos estejam em conformidade com as políticas internas e regulamentações, como a LGPD.

7.1.5 Apoiar iniciativas de melhoria contínua, identificando e mitigando riscos emergentes.

7.1.6 Manter, monitorar e atualizar regularmente os controles técnicos e operacionais para garantir sua eficácia.

7.1.7 Preparar e implementar estratégias de respostas rápidas e eficazes a incidentes de segurança, assegurando a continuidade dos sistemas e a proteção de dados.

7.1.8 Gerir os recursos da organização de forma segura, aderindo a políticas relativas a acessos, senhas e uso responsável da informação.

7.1.9 Cumprir cláusulas contratuais de segurança, proteger dados compartilhados, e respeitar todos os requisitos estabelecidos, incluindo confidencialidade.

7.1.10 Conduzir avaliações de risco regulares para identificar vulnerabilidades e implementar estratégias para mitigar riscos potenciais.

7.1.11 Organizar e participar de programas de capacitação para manter habilidades atualizadas e assegurar que a equipe esteja informada sobre as melhores práticas de segurança.

**7.2 Compete ao Conselho de Administração, à Diretoria, à Presidência:**

7.2.1 Apoiar o Gestor de Segurança da informação no exercício de suas atribuições;

7.2.2 Assegurar a alocação de recursos adequados aos programas relacionados à privacidade e proteção de dados.

7.2.3 Incluir a verificação da efetividade das ações previstas nesta política como pauta permanente ou frequente das reuniões mantidas com as demais áreas de gestão.

7.2.4 Implementar no âmbito de seus processos as medidas de governança de dados previstas nesta política.

**7.3 Compete aos Gestores:**

7.3.1 Garantir que os dados sob responsabilidade de sua gerência sejam tratados conforme legislação aplicável e políticas internas da Cagece, assegurando que a privacidade e a segurança sejam prioridades.

7.3.2 Assegurar que colaboradores e prestadores de serviço sob sua supervisão participem regularmente de treinamentos sobre segurança da informação, promovendo uma cultura de segurança robusta.

7.3.3 Trabalhar em conjunto com outras áreas para identificar e mitigar vulnerabilidades e ameaças à segurança da informação.

7.3.4 Colaborar na identificação de riscos durante todas as fases de desenvolvimento ou execução de projetos, comunicando potenciais ameaças à Coordenação de Segurança da Informação.

7.3.5 Comunicar prontamente à Coordenação de Segurança da Informação qualquer incidente relacionado à segurança da informação, facilitando uma resposta ágil e eficaz.

7.3.6 Envolver-se ativamente em projetos que possam impactar a segurança da informação, garantindo que todas as medidas necessárias sejam consideradas.

**7.3 Compete a todos os colaboradores:**

7.3.1 Seguir todas as políticas e diretrizes de segurança da informação estabelecidas pela organização.

7.3.2 Manter-se informado sobre mudanças nas políticas e práticas de segurança.

7.3.3 Proteger informações sensíveis e confidenciais, garantindo que não sejam divulgadas indevidamente.

7.3.4 Utilizar recursos e sistemas de TI de maneira segura e responsável, evitando práticas de risco.

7.3.5 Reportar prontamente quaisquer incidentes ou suspeitas de violação de segurança à equipe responsável.

7.3.6 Estar atento a atividades suspeitas e comunicar possíveis ameaças à segurança sem demora.

7.3.7 Envolver-se ativamente em treinamentos e programas de conscientização oferecidos pela organização.

7.3.8 Promover uma cultura de segurança da informação no ambiente de trabalho, incentivando colegas a seguir boas práticas.

7.3.9 Criar e manter senhas fortes e não compartilhá-las com terceiros.

7.3.10 Assegurar que o acesso a sistemas e informações seja utilizado apenas para finalidades autorizadas.

## 8. VIGÊNCIA

A presente Política entra em vigor a partir do dia 13 de Agosto de 2025, aprovada com a ATA de nº 682ª Reunião do Conselho de Administração da Cagece.

## 9. ANEXOS

Não possui anexos.

## 10. HISTÓRICO DE ALTERAÇÕES

| Documento | Elaborador/Unidade | Revisor/Unidade | Aprovador/Unidade | Alteração | Data de homologação |
|---|---|---|---|---|---|
| PLT-0021 | Claudemir/GETIC | Felipe/GETIC | CAD | - | 13/08/2025 |