

As diretrizes e normas de Segurança da Informação da GOINFRA têm como finalidade estabelecer objetivos, responsabilidades e competências para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações e comunicações. Além disso, buscam assegurar a conformidade, padronização e normatização das atividades de gestão da segurança da informação, promovendo a proteção dos ativos informacionais e prevenindo responsabilidades legais para todos os usuários. Essas diretrizes devem ser seguidas e aplicadas em todas as unidades organizacionais que integram a GOINFRA.

1. OBJETIVO

Os objetivos desta política incluem a instituição de diretrizes e normas gerais para o estabelecimento de controles e procedimentos na GOINFRA, garantindo a preservação da informação em relação à sua integridade, confidencialidade, disponibilidade e autenticidade. Além disso, buscam definir competências, responsabilidades e obrigações para o adequado manuseio, tratamento, armazenamento, distribuição, uso e descarte da informação, bem como estabelecer medidas de controle e proteção contra a indisponibilidade, a perda de integridade e o acesso não autorizado a dados e informações no âmbito da GOINFRA.

2. ABRANGÊNCIA

Essa política é aplicável a todos os colaboradores, usuários, terceiros e quaisquer pessoas que tenham acesso às informações pertencentes ou sob a custódia da Agência Goiana de Infraestrutura e Transportes - GOINFRA.

3. DIRETRIZES

3.1 PRINCÍPIOS

A Política de Segurança da Informação da GOINFRA será orientada por princípios fundamentais que asseguram a proteção dos ativos informacionais e a conformidade com normas e regulamentações aplicáveis. Entre esses princípios, destacam-se:

- **Responsabilidade:** Todos os colaboradores devem proteger os ativos de informação e cumprir as diretrizes de segurança da organização.
- **Conhecimento:** Os usuários devem estar cientes e respeitar as normas e regulamentações sobre segurança da informação da GOINFRA.
- **Clareza:** As regras e normas de segurança da informação devem ser elaboradas de forma clara e objetiva.
- **Celeridade:** As respostas a incidentes e falhas devem ser rápidas e eficientes.
- **Garantia de integridade, autenticidade e disponibilidade:** A informação sob custódia da GOINFRA deve ser protegida, respeitando o princípio da transparência e garantindo confidencialidade apenas nos casos previstos em lei.
- **Respeito às normas e regulamentações:** A política deve estar alinhada às regras constitucionais, legais e técnicas que regem a administração pública estadual.
- **Ética:** Os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometer a segurança e a comunicação das informações.

Integridade: Deve-se garantir que a informação não seja alterada ou destruída de maneira não autorizada ou acidental, seja em sua origem, no trânsito ou no destino.

Privacidade: Deve-se assegurar o direito à intimidade, ao sigilo da correspondência e das comunicações, garantindo a proteção de dados pessoais e coletivos.

3.2 TERMOS E DEFINIÇÕES

Para os fins desta política, são estabelecidas as seguintes definições:

Armazenamento: processo de guardar dados digitais em um meio físico ou virtual, permitindo sua recuperação e uso posterior.

Ativo: qualquer componente humano, tecnológico ou físico que sustenta processos de trabalho da GOINFRA, podendo ser classificados como ativos de Informação, Softwares, Físicos, Serviços, Pessoas e Organização.

Autenticidade: garantia de que uma informação, produto ou documento pertence ao autor a quem se atribui.

Ciclo de vida do ativo: abrange desde a criação ou obtenção até o uso, manipulação, compartilhamento, armazenamento, transporte e descarte.

Colaborador: indivíduo que desempenha funções na autarquia, incluindo servidores efetivos, comissionados, temporários, estagiários, terceirizados, prestadores de serviço e consultores.

Confidencialidade: preservação do sigilo das informações, garantindo acesso apenas a pessoas autorizadas.

Conformidade: cumprimento de requisitos legais e organizacionais, incluindo normas e diretrizes internas.

Criptografia: conjunto de técnicas que transformam informações em formato ilegível, acessíveis apenas por destinatários autorizados.

Dados: valores que, quando organizados e interpretados, constituem informações.

Diretrizes e normas: conjunto de políticas de segurança da informação estabelecidas pela GOINFRA.

Disponibilidade: garantia de que a informação estará acessível quando necessária.

Estação de trabalho: computador utilizado para atividades profissionais.

Gestor de informação: indivíduo ou grupo responsável pela administração das informações, garantindo segurança e boas práticas.

Grau de confidencialidade do ativo: classificação dos ativos como público, interno, reservado, secreto e ultrassecreto, conforme legislação vigente.

Incidente de segurança da informação: qualquer evento que comprometa a integridade, disponibilidade ou confidencialidade das informações, incluindo fraude, sabotagem, desvio ou falhas inesperadas.

Informação: conjunto de dados tratados e organizados com valor para a GOINFRA e suas partes interessadas.

Integridade: proteção das informações contra alterações não autorizadas ou acidentais.

Irretratabilidade: garantia de que uma parte envolvida em uma transação ou comunicação não possa negar sua autoria.

- **Privilegio mínimo:** conceito que restringe o acesso de usuários apenas aos recursos necessários para suas atividades.
- **Programa:** conjunto de instruções para a execução de tarefas em um computador.
- **Proprietário:** pessoa ou entidade com responsabilidade autorizada para gerir ativos.
- **Recursos de TI:** equipamentos e dispositivos tecnológicos utilizados na GOINFRA, como sistemas, redes, softwares, impressoras, VPNs, pendrives, tokens e smartphones.
- **Tecnologias da Informação:** conjunto integrado de recursos tecnológicos com um objetivo comum.
- **Usuário interno:** pessoa física ou unidade interna vinculada administrativamente à GOINFRA que utiliza informações da organização.
- **Usuário externo:** pessoa física ou jurídica que faz uso das informações da GOINFRA sem vínculo administrativo com a organização.

3.3 RESPONSABILIDADES

A responsabilidade pela segurança da informação na GOINFRA é compartilhada entre todos os usuários e a Gerência de Tecnologia da Informação. Dessa forma, cabe a todos os usuários que acessam recursos tecnológicos da instituição:

- Promover a segurança de seus próprios acessos, protegendo dados e credenciais de login.
- Seguir as orientações fornecidas pelos setores competentes sobre o uso adequado dos recursos tecnológicos e informacionais.
- Utilizar os recursos tecnológicos de maneira ética, legal e consciente.
- Garantir a integridade e confidencialidade das informações às quais tenham acesso devido ao cargo ou função exercida.

A GOINFRA poderá revogar credenciais de acesso de usuários internos e externos a qualquer momento, caso seja constatado o descumprimento das diretrizes, normas, políticas e demais processos operacionais específicos de segurança e comunicação da informação.

Cada usuário é responsável por eventuais prejuízos ou danos causados à GOINFRA decorrentes do não cumprimento das diretrizes e normas estabelecidas.

Além disso, é expressamente proibida a criação, modificação, execução ou retransmissão de instruções ou programas de computador com o objetivo de obter acesso não autorizado a recursos, configurando tentativa de violação da segurança dos sistemas, o que pode resultar em responsabilização do usuário infrator.

Os gestores de informação têm responsabilidades específicas, incluindo:

- Informar à Gerência de Tecnologia da GOINFRA sobre as necessidades de acesso aos recursos por parte dos colaboradores.
- Promover a classificação dos ativos sob sua responsabilidade, bem como validar, liberar e cancelar acessos conforme necessário.

- Supervisionar os ativos de informação sob sua gestão, garantindo sua integridade física e funcionamento adequado.

A Gerência de Tecnologia tem papel fundamental na segurança da informação da GOINFRA, sendo responsável por:

- Disponibilizar infraestrutura técnica e aplicar as normas de segurança estabelecidas.
- Prestar contas à Diretoria de Gestão Integrada (DGI) sobre a execução da Política de Segurança da Informação.
- Promover capacitação contínua para colaboradores sobre segurança da informação.
- Divulgar e dar publicidade às normas e ações relacionadas à segurança da informação.
- Implementar processos de gerenciamento de riscos e elaborar planos de continuidade de negócios.

Os líderes das unidades gerenciais da GOINFRA devem:

- Conscientizar os usuários internos e colaboradores sobre os conceitos e boas práticas de segurança da informação.
- Incorporar medidas de segurança da informação nos processos de trabalho de suas áreas.
- Comunicar imediatamente ao superior hierárquico e à unidade competente qualquer comprometimento da segurança, falhas, desvios ou violações das regras estabelecidas, para que sejam adotadas as medidas cabíveis.

Os parceiros e terceiros que tenham acesso às informações da GOINFRA devem adotar altos padrões de integridade na condução de seus negócios. Suas atividades devem garantir o sigilo, a confidencialidade e a proteção das informações às quais tenham acesso, assegurando o cumprimento dos direitos de propriedade intelectual durante e após o período de vigência do contrato, convênio ou instrumento congêneres. Para isso, os acordos de confidencialidade e de acesso a dados e informações devem estar expressamente previstos nos contratos firmados.

Todos os colaboradores que tenham acesso a informações da GOINFRA devem assinar um termo de confidencialidade, especificando suas responsabilidades e obrigações em relação ao sigilo dessas informações, tanto durante quanto após o período de vínculo com a instituição.

O uso dos recursos de tecnologia da informação da GOINFRA será regulamentado por norma específica, que respeitará os dispositivos legais e as orientações da Secretaria-Geral de Governo de Goiás (SGG).

3.4 COMPETÊNCIAS NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A Presidência da GOINFRA é responsável pela aprovação das diretrizes e normas específicas de segurança da informação, garantindo sua aplicação em toda a instituição. Além disso, outras áreas possuem competências específicas relacionadas à segurança da informação, sendo elas:

- **Segurança das informações no trabalho remoto e no uso de dispositivos móveis:** Cabe à Diretoria de Gestão Integrada, com suporte da Gerência de TI, propor diretrizes e normas, além

de determinar e implementar procedimentos que garantam a segurança da informação em ambientes de trabalho remoto e no uso de dispositivos móveis.

Gestão do termo de confidencialidade: A Gerência de Gestão e Desenvolvimento de Pessoas deve assegurar que todos os colaboradores assinem o termo de confidencialidade antes do início de suas atividades, mantendo o controle e o arquivamento dos documentos assinados.

Gestão de ativos: A Gerência de Tecnologia é responsável por propor diretrizes e normas, além de determinar e implementar procedimentos para identificação, controle e monitoramento dos ativos da GOINFRA.

Gestão de acesso:

Acesso físico: Compete à Diretoria de Gestão Integrada, com suporte da Gerência de Apoio Administrativo e Logístico, a criação de diretrizes e normas, além da implementação de procedimentos que estabeleçam padrões de segurança física e remota.

Acesso virtual: Cabe à Gerência de Tecnologia propor diretrizes e normas, bem como determinar e implementar procedimentos para controle de acesso virtual, garantindo a gestão de acessos às redes e serviços de TI da GOINFRA.

Gestão de mudanças: A Gerência de Tecnologia deve estabelecer diretrizes e normas que garantam que qualquer mudança no ambiente operacional de segurança da informação seja devidamente homologada e testada, com geração de documentação e registro.

Gestão de backup e restore: A Gerência de Tecnologia deve definir diretrizes e normas para padronizar a gestão das rotinas de backup e restauração, garantindo a realização de testes e simulações necessárias para assegurar a recuperação dos dados, em conformidade com os dispositivos legais e as orientações da Secretaria-Geral de Governo de Goiás (SGG).

Gestão de mecanismos de comunicação: A Comunicação Setorial deve estabelecer diretrizes e normas para garantir a segurança da informação em redes sociais. A normatização interna deve definir critérios, limitações e responsabilidades no uso seguro das redes sociais por usuários que administrem perfis institucionais ou tenham credencial de acesso às redes sociais a partir da infraestrutura da GOINFRA.

Gestão de incidentes de segurança da informação e continuidade do negócio: A Gerência de Tecnologia deve propor diretrizes e normas, além de implementar procedimentos padronizados para resposta e tratamento de incidentes de segurança da informação. O objetivo é minimizar impactos e reduzir interrupções operacionais causadas por desastres ou falhas nos recursos tecnológicos da GOINFRA.

Uso de controles criptográficos: A Gerência de Tecnologia deve estabelecer diretrizes e normas para a aplicação de controles criptográficos, incluindo o uso, proteção e tempo de vida das chaves criptográficas para garantir a proteção das informações.

Conceito de “mesa limpa e tela limpa”: Cabe à Diretoria de Gestão Integrada propor diretrizes e normas, além de implementar procedimentos que garantam a proteção de dados e informações, tanto em formato digital quanto impresso. Essas medidas devem prevenir acessos não autorizados, divulgação indevida, perdas, fraudes e outros riscos, garantindo a adoção do conceito de “mesa limpa e tela limpa” em todas as áreas da GOINFRA.

3.5 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Os dados pessoais coletados pela Agência devem ser tratados exclusivamente para fins autorizados, de forma ética e legal, garantindo o respeito aos direitos dos titulares e em conformidade com a Lei Geral de Proteção de Dados (LGPD). Todo tratamento de dados pessoais deve ter uma finalidade específica e estar fundamentado em uma das bases legais previstas na LGPD, seguindo um ciclo de vida que compreende a coleta, o uso e a exclusão dos dados.

No âmbito da GOINFRA, em conformidade com o artigo 41 da Lei nº 13.709/2018 (LGPD), cabe à Presidência a designação do Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO). As responsabilidades do DPO devem seguir as definições estabelecidas pela LGPD e incluem:

- **Atendimento aos titulares de dados:** Receber e responder reclamações e comunicações dos titulares, prestando os esclarecimentos necessários e adotando providências cabíveis.
- **Interação com a Autoridade Nacional:** Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e tomar as medidas necessárias para garantir a conformidade com a legislação.
- **Orientação interna:** Fornece diretrizes e capacitação para funcionários e contratados da GOINFRA sobre boas práticas de proteção de dados pessoais.
- **Cumprimento normativo:** Executar outras atribuições definidas pelo controlador ou estabelecidas em normas complementares para garantir a conformidade com a LGPD.

3.6 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

O Comitê de Segurança da Informação da GOINFRA deve ser instituído a cada dois anos pela Presidência, sendo sua coordenação de responsabilidade da Gerência de Tecnologia da Informação (TI). Dada a transversalidade do tema, o Comitê deve ser composto, no mínimo, por representantes das seguintes unidades organizacionais:

- Gerência de Tecnologia
- Diretoria de Gestão Integrada
- Diretoria de Controle
- Assessoria de Integridade
- Ouvidoria Setorial
- Procuradoria Setorial
- Comunicação Setorial

As responsabilidades do Comitê de Segurança da Informação incluem:

- Coordenar o SGSI (Sistema de Gestão de Segurança da Informação), garantindo sua implementação e operação eficaz.

Analisar e monitorar os requisitos legais aplicáveis à segurança da informação, assegurando a conformidade legal, especialmente em relação à norma NBR ISO/IEC 27001:2013 e suas extensões.

Relatar o desempenho do SGSI à Diretoria de Gestão Integrada e à Gerência de Tecnologia, promovendo a melhoria contínua da segurança da informação na GOINFRA.

3.7 PENALIDADES

O descumprimento das regras estabelecidas na Política de Segurança da Informação (PSI) da GOINFRA, bem como de suas normas internas de segurança, por usuários internos ou externos, resultará em notificação e poderá acarretar sanções conforme o regime jurídico dos servidores públicos civis da administração direta, autárquica e fundacional do Estado de Goiás (Lei n.º 20.756, de 28 de janeiro de 2020), além de outras legislações vigentes.

3.8 DISPOSIÇÕES FINAIS

A Política de Segurança da Informação (PSI) da GOINFRA, suas normas internas de segurança e eventuais atualizações deverão ser amplamente divulgadas a todos os usuários de informações da Agência Goiana de Infraestrutura e Transportes, garantindo que tenham conhecimento das diretrizes estabelecidas.

Para assegurar sua efetividade e alinhamento com as melhores práticas, a PSI e todas as normas dela decorrentes deverão ser revisadas e atualizadas sempre que necessário, considerando mudanças tecnológicas, normativas e operacionais, não podendo exceder o prazo máximo de um ano para sua revisão.

Fica revogada a Portaria nº 328, de 24 de agosto de 2020.

4. CONTROLE DE REVISÕES

N. da versão	Data	Histórico das alterações
001	15/07/2025	Emissão inicial

5. APROVAÇÃO

Elaborado/ revisado por: Gerência de Tecnologia	Aprovado por: Diretoria de Gestão Integrada	Data de aprovação: 15/07/2025
---	---	---