POLÍTICA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA MGS

POL/GRC/010

Data de Publicação
1º/08/2022

ELABORADO POR:	VERIFICADO POR:
Grupo Funcional	Diretoria Executiva, reunião realizada em 20/07/2022: Marcelo Magalhães Rosa Isoni - Diretor-Presidente Helter Verçosa Morato - Diretor Jurídico Lucianna Feres Bichara Peixoto Gomes - Diretora de Recursos Humanos Michel Lopes França Chaves - Diretor de Operações e Serviços Paulo Henrique Fonseca de Melo - Diretor Administrativo e Financeiro

APROVADO POR:

Conselho de Administração, reunião realizada em 27/07/2022:

Valéria Pires Amoroso Lima - Presidente

João Aparecido de Lima - Vice-presidente

Felipe Magno Parreiras de Sousa - Conselheiro

Giovani Domingos Beraldo- Conselheiro

Hindemburgo Chateaubriand Pereira Diniz - Conselheiro

Marcelo Magalhães Rosa Isoni - Conselheiro

HISTÓRICO DE REVISÕES

REV.	DESCRIÇÃO	POR	VER.	APR.	DATA
0	Versão inicial desta Política.	Grupo Funcional	Diretoria Executiva	Conselho de Administração	01/09/21
1	Revisão geral desta Política, tendo sido incluído os itens 3.6, 3.8 e 7.4; alterado os itens 4.1, 4.4, 4.11, 4.19, 5.2, 5.4, 5.6.1, 6.9.3, 7.3, 10.1, parágrafo terceiro do item 6 e inciso III do item 6.10.1.	Grupo Funcional	Diretoria Executiva	Conselho de Administração	01/08/22

SUMÁRIO

1. OBJETIVO

1.1. A presente Política tem por finalidade estabelecer princípios, diretrizes, atribuições e responsabilidades atinentes a segurança da informação no âmbito da MGS - Minas Gerais Administração e Serviços S.A. ("MGS", "Empresa") com o objetivo de garantir um ambiente tecnológico controlado e seguro, bem como proteger os dados pessoais, a privacidade e o acesso à informação, de forma a oferecer as informações necessárias aos processos da Empresa, com confidencialidade, disponibilidade, integridade e autenticidade.

2. APLICAÇÃO

2.1. Esta Política se aplica a Administração Central, Setores, Agentes da MGS, bem como a qualquer pessoa física ou jurídica, de direito público ou privado, com quem a Empresa se relaciona como, por exemplo, cidadãos, fornecedores, clientes e parceiros, que utilizem recursos de tecnologia da informação e comunicação da MGS.

3. DOCUMENTOS DE REFERÊNCIA OU COMPLEMENTARES

3.1. Lei Federal nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD);

3.2. ISO/IEC 27000:2018, que define uma visão geral sobre sistemas de gestão de segurança da informação e de termos e conceitos utilizados;

3.3. Norma ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização, dentre outros;

3.4. Norma ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;

3.5. Política de Privacidade e de Proteção de Dados Pessoais da MGS (POL/GRC/009);

3.6. Resolução da Diretoria Executiva que institui o Comitê de Segurança da Informação (RDE/DJG/005/2021);

3.7. Código de Conduta e Integridade da MGS (COD/GRC/001);

3.8. Regulamentação de Gestão de Incidente de Dados Pessoais (REG/PLN/003);

3.9. Legislação e demais normas aplicáveis.

4. DEFINIÇÕES E SIGLAS

4.1. **Administração Central**: refere-se às seguintes Unidades Administrativas da MGS: Sede, Almoxarifado e Gestão de Documentos; Unidade Regional Caparaó, Mata e Vertentes; Unidade Regional Norte de Minas, Unidade Regional Sudoeste de Minas e outras que possam ser inauguradas;

4.2. **Agente da MGS**: toda pessoa física vinculada diretamente à MGS, incluindo, mas não se limitando a, membros de todos os Conselhos e Comitês Estatutários, seus Diretores, empregados, estagiários;

4.3. **Ativos de informação**: compreendem os meios de armazenamento, transmissão (envio e recebimento) e processamento da informação; os equipamentos, sistemas e estruturas de dados utilizados para tal, bem como os locais onde se encontram esses meios, que são utilizados pela MGS na realização de suas operações;

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

4.5. **Confidencialidade**: propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados;

4.6. **Controle de acesso**: métodos utilizados para garantir que o acesso aos ativos seja autorizado e restrito às necessidades de trabalho e em segurança;

4.7. **Cookies**: é um arquivo que contém um identificador (uma sequência de letras e números), armazenado pelo navegador. O identificador é enviado de volta ao servidor toda vez que o navegador solicita uma página do servidor;

4.8. **Correio eletrônico**: serviço de envio e recebimento de mensagens eletrônicas (e-mails), por meio de *software* de comunicação;

4.9. **Credenciais de acesso**: conjunto composto pelo nome de conta e respectiva senha, utilizada para ingresso ou acesso (login) em equipamentos, rede ou sistema;

4.10. **Dado Pessoal**: informação relacionada a pessoa natural identificada ou identificável, inclusive dado pessoal sensível (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural);

4.11. **Disponibilidade**: propriedade de ser acessível e utilizável sob demanda por pessoa física, sistema e/ou entidade autorizada;

4.12. **Evento de segurança da informação**: ocorrência identificada em decorrência do uso de recursos de TIC e/ou de seu monitoramento, que indica uma possível violação desta Política ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação, inclusive de dados pessoais;

4.13. **Gestor:** Agente da MGS responsável pela gestão de pessoas, atividades, projetos, bens e/ou processos de negócios de um setor da Empresa;

4.14. **GETIN:** Gerência de Tecnologia da Informação;

4.15. **Incidente de segurança da informação**: é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio, ameaçar a segurança da informação ou violar dados pessoais;

4.16. **Informação**: compreende todos os dados produzidos, acessados, transmitidos (enviados e recebidos), manuseados e/ou armazenados em meio impresso e/ou digital;

4.17. **Integridade**: propriedade de precisão e completude;

4.18. **Internet:** denominação dada à rede de informações que permite a interligação de computadores pertencentes às mais diversas organizações ao redor do mundo, oferecendo serviços como sites, e-mails, etc;

4.19. **Recursos de tecnologia da informação e comunicação (ou recursos de TIC)**: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, instalações físicas e/ou lógicas que os abriguem, bem como os ativos de informação da MGS;

4.20. **Segurança da Informação**: conjunto de ações, controles e medidas para assegurar a preservação da confidencialidade, disponibilidade, integridade e autenticidade da informação;

4.21. **Setor**: subdivisão interna na estrutura organizacional da Empresa;

4.22. ***Software***: É um aplicativo ou programa de computador que foi projetado para dar suporte a uma tarefa específica, um processo de negócio ou até mesmo a outro software;

4.23. **Terceiros**: demais pessoas físicas ou jurídicas, tais como clientes, fornecedores, prestadores de serviço, parceiros, dentre outros;

4.24. **TIC**: tecnologia da informação e comunicação;

4.25. **Tratamento de incidentes de segurança da informação**: conjunto de processos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação, a fim de eliminar sua causa identificando e mitigando possíveis vulnerabilidades que possam estar associadas ao incidente e seus impactos;

4.26. **Unidades Administrativas**: unidades físicas da MGS;

4.27. **Usuários**: Agentes da MGS e terceiros que utilizem recursos de TIC da Empresa, desde que previamente autorizados.

5. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

5.1. A MGS adotará medidas de segurança, técnicas e administrativas aptas a proteger os ativos de informação, inclusive os dados pessoais, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

5.1.1. Os terceiros com os quais a MGS se relaciona devem adotar, no que couber, as medidas de segurança mencionadas no item acima, bem como as demais diretrizes desta Política, no tocante às informações que lhes forem disponibilizadas para executar as atividades necessárias e/ou que estejam sob sua guarda.
5.2. O Comitê de Segurança da Informação instituído pela MGS tem caráter consultivo e natureza permanente, para prestar apoio à GETIN e à Diretoria Executiva da MGS, nos termos de normativo interno.

5.3. O uso adequado dos recursos de TIC visa garantir a continuidade das atividades desenvolvidas pela MGS, incluindo, mas não se limitando a, funções exercidas no âmbito da Administração Central da Empresa e os serviços prestados aos clientes.

5.4. Os recursos de TIC pertencentes à MGS, disponíveis para o usuário, serão utilizados em atividades demandadas pela Empresa e/ou relacionadas às suas funções institucionais.

5.4.1. A utilização dos recursos de TIC será monitorada, com a finalidade de detectar divergências entre o disposto na presente Política e normativos internos correlatos ao tema, e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

5.5. A GETIN realizará verificações e/ou aferições para garantir que o uso dos recursos de TIC estejam adequados e promover o planejamento de ações necessárias em tempo hábil, mantendo os seus registros, quando for o caso.

5.5.1. Serão realizadas verificações e/ou aferições ordinárias periódicas, bem como extraordinárias com o intuito de apurar eventos que deponham contra a segurança e as boas práticas no uso dos recursos de TIC, cujos relatórios serão encaminhados ao Comitê de Segurança da Informação.

5.6. As informações geradas e/ou tratadas pela MGS serão classificadas nos termos da legislação e normativo interno aplicáveis.

5.6.1. A MGS providenciará dispositivos de proteção proporcionais ao grau de sigilo e de criticidade da informação, independentemente do suporte em que resida ou da forma pela qual seja veiculada, capazes de assegurar a sua disponibilidade, integridade e autenticidade.

5.7. As informações, sistemas e métodos gerados ou criados pelos Agentes da MGS, no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são de propriedade da Empresa e serão utilizados exclusivamente para fins relacionados às atividades a ela afetas.

5.7.1. Quando as informações, sistemas e métodos forem gerados ou criados por terceiros para uso exclusivo da MGS, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem, salvo autorização prévia e por escrito da MGS.

5.8. Os instrumentos jurídicos firmados pela MGS que envolvam utilização de recursos de TIC devem observar as disposições desta Política.

6. DIRETRIZES ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO

As diretrizes de segurança da informação abrangem os recursos de TIC utilizados em atividades relacionadas às funções institucionais e administrativas da MGS e compreendem, em especial, os seguintes serviços e procedimentos:

6.1. Acesso à Internet

6.1.1. O acesso à Internet dar-se-á, exclusivamente, pelos meios autorizados pela MGS e configurados pela GETIN, sendo expressamente proibido o uso de recursos externos não homologados pela GETIN.

6.1.2. Todo tráfego de Internet será controlado, de forma automática, e poderá ser inspecionado, de acordo com normativo interno aplicável.

6.1.3. A MGS poderá disponibilizar acesso à rede sem fio para usuários ou terceiros, quando as atividades necessitarem deste recurso para sua execução, nos termos de normativo interno correlato.

6.2. Uso do correio eletrônico

6.2.1. O uso do correio eletrônico institucional restringe-se a mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário ou do setor, sendo vedado o uso para fins particulares.

6.2.2. O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança da infraestrutura tecnológica da MGS ou que contenham conteúdo impróprio.

6.3. Controle de acesso

6.3.1. O controle de acesso ao ambiente tecnológico da MGS utiliza a autenticação como mecanismo para certificar as credenciais de acesso (conta de usuário e senha) dos usuários, as quais permitem que eles sejam logicamente identificados, autenticados e autorizados a acessarem um determinado ambiente.

6.3.2. A MGS disciplinará, em normativo interno, a concessão, revogação e suspensão de acessos físicos, lógicos e remotos aos recursos de TIC e seus respectivos controles, observadas as diretrizes estabelecidas na

presente Política, de modo a assegurar que pessoas não autorizadas tenham seus acessos negados, evitando atividades e/ou acessos indevidos, dentre outros.

6.3.3. Os gestores são responsáveis por assegurar que as credenciais de acesso dos respectivos usuários sejam disponibilizadas e utilizadas em conformidade com as necessidades funcionais do trabalho, nos termos de normativo interno aplicável.

6.3.4. Os direitos de concessão de acessos serão revisados periodicamente ou sempre que necessário.

6.3.5. Toda concessão de acesso aos sistemas de informações da MGS deve ser controlada por um método que envolva identificação, autenticação e autorização.

6.3.6. O acesso lógico e remoto dos usuários ao ambiente tecnológico da MGS deve ser feito mediante a utilização de credencial válida de acesso.

6.3.6.1. O usuário terá uma única credencial de acesso em cada ambiente que seja necessário o credenciamento, válida pelo período de vínculo ativo com a MGS, e não deve ser reaproveitada para outros usuários, mesmo após o término da necessidade de uso inicial.

6.3.7. As atividades realizadas por meio de determinada credencial de acesso são de responsabilidade do respectivo usuário.

6.3.8. É proibido aos usuários compartilharem suas credenciais de acesso, bem como realizarem qualquer ação utilizando a credencial de acesso individual ou de grupo para a qual não tenham sido autorizados.

6.3.9. Os registros de atividades com a respectiva identificação dos responsáveis pela requisição, concessão, suspensão e revogação de acesso devem ser devidamente armazenados para fins de análise de segurança da informação, verificação, aferição e auditoria, nos termos da legislação e normativos internos aplicáveis.

6.4. Gestão do uso de dispositivos móveis

6.4.1. Caberá a GETIN gerenciar o uso de dispositivos móveis utilizados dentro e fora do ambiente corporativo da MGS, bem como a homologação e a aprovação de uso destes dispositivos e seus respectivos softwares e aplicativos associados.

6.4.2. A MGS poderá disponibilizar equipamentos e dispositivos móveis aos seus Agentes, para a execução de suas atividades, devendo ser observadas as suas regras de utilização previstas em normativo interno próprio.

6.5. Utilização de dados de navegação

6.5.1. A MGS utiliza o recurso de cookies em seus sistemas web (sistemas acessados via navegador de Internet) para obter um melhor desempenho e experiência de navegação do usuário.

6.5.1.1. Os cookies normalmente não contêm informações que identifiquem pessoalmente um usuário, mas as informações pessoais armazenadas sobre o usuário podem estar vinculadas àquelas armazenadas e obtidas de cookies.

6.5.1.2. O usuário poderá configurar seu navegador a qualquer tempo, de forma a bloquear a utilização dos cookies durante a sua navegação, aceitá-los ou ativar notificações quando forem enviados ao seu computador, smartphone ou qualquer outro dispositivo com acesso à Internet.

6.6. Acesso físico

6.6.1. Os controles de acesso físico à Administração Central da MGS visam restringir o acesso a equipamentos, documentos e suprimentos do ambiente tecnológico da MGS e a proteção das informações e dos recursos de TIC, permitindo-lhes acesso apenas de pessoas autorizadas.

6.6.2. Os recursos de TIC críticos da MGS devem ser mantidos em ambientes reservados, monitorados e com acesso físico controlado, permitido apenas para pessoas autorizadas.

6.6.3. Periodicamente a GETIN deve revisar os acessos aos ambientes tecnológicos reservados, restringindo o acesso apenas a pessoas autorizadas.

6.7. Armazenamento, backup e recuperação de dados

6.7.1. A MGS disponibiliza aos setores da Empresa área de armazenamento em rede para salvaguardar os arquivos relacionados aos trabalhos desenvolvidos, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

6.7.2. São realizados procedimentos de *backup*, testes e recuperação de dados pela GETIN, visando garantir que a salvaguarda das informações seja realizada de forma otimizada, atendendo as necessidades da Empresa, conforme normativo interno aplicável e melhores práticas.

6.8. Gestão de riscos de TIC

6.8.1. A MGS implementará a gestão de riscos nos processos de segurança da informação, observando o disposto na Política de Gestão de Riscos da Empresa e demais normativos internos aplicáveis, de forma a identificar ameaças, reduzir a vulnerabilidade dos ativos de informação e os impactos de eventuais incidentes, dentre outros.

6.8.2. A gestão de riscos é um processo contínuo e deve ser aplicado na implementação e operação da gestão de segurança da informação da MGS, buscando sua melhoria.

6.9. Gestão de incidentes de segurança da informação

6.9.1. A gestão de incidentes de segurança da informação será realizada pela GETIN e tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas, visando minimizar possíveis impactos.

6.9.2. Estão abrangidos os eventos, suspeitos ou confirmados, relacionados à segurança de recursos de TIC e à proteção de dados pessoais, que comprometam o ambiente tecnológico da MGS, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a presente Política e dos quais decorram interrupção, parcial ou total, de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, violação de dados pessoais, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

6.9.3. A gestão de incidentes com dados pessoais tem tratamento específico nos termos de normativo interno próprio.

6.9.4. Qualquer Agente da MGS ou terceiros, que tenha conhecimento ou notícia de incidente de segurança da informação, deverá dar ciência do fato à GETIN, nos termos do normativo interno específico.

6.9.5. O tratamento da informação relativa ao incidente de segurança da informação deve ser realizado de forma a viabilizar e assegurar a confidencialidade, disponibilidade, integridade, e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

6.9.6. O processo de gestão de incidentes de segurança da informação é composto pelas seguintes etapas:

I - detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação;
II - investigação e contenção: compreende a investigação e tratamento do incidente, coleta de dados, comunicação aos setores afetados, proposição e aplicação de ações de contenção, quando necessárias;
III – solução: compreende o controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa raiz de um ou mais incidentes de segurança da informação;
IV - encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente;
V - avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores, bem como a verificação das oportunidades de melhoria e lições aprendidas.

Parágrafo primeiro - Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção de seu histórico e auxiliar na geração de indicadores.

Parágrafo segundo - Deverá ser observado o sigilo de toda e qualquer informação, inclusive de dados pessoais durante o processo de gestão do incidente, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

Parágrafo terceiro - Quando houver indícios de ilícitos criminais constatado durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação deverá ser comunicado para tratativas necessárias.

6.10. Gestão de continuidade de TIC

6.10.1. A gestão de continuidade de TIC da MGS tem por objetivos:

I - manter o correto direcionamento e dimensionamento de recursos de TIC para prover sua gestão de continuidade;
II - reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas da Empresa;
III - manter os sistemas e serviços críticos de TIC em um nível minimamente operável e aceitável durante a ocorrência de um incidente ou desastre, de forma a não interromper as atividades e a prestação de serviços da MGS;
IV - definir os procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade.

6.10.2. A gestão de continuidade de TIC será realizada pela GETIN e deverá observar o resultado das análises de riscos de TIC e da análise de impacto de negócio realizadas, de forma a nortear as estratégias de continuidade.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1. Compete ao Conselho de Administração

I - aprovar a Política de Segurança da Informação da MGS, bem como suas revisões;

II - outras atribuições que lhe forem conferidas pela legislação e demais normas aplicáveis, pela Assembleia Geral, ou pelo Estatuto Social da MGS.

7.2. Compete à Diretoria Executiva

I - submeter a Política de Segurança da Informação, bem como suas revisões à aprovação do Conselho de Administração da MGS;
II - instituir Comitê de Segurança da Informação e definir suas atribuições;
III - implementar e assegurar o cumprimento da Política de Segurança da Informação aprovada pelo Conselho de Administração da MGS;
IV - monitorar o cumprimento da legislação de segurança da informação aplicável;
V - outras atribuições que lhe forem conferidas pela legislação e demais normas aplicáveis, pelo Conselho de Administração, ou pelo Estatuto Social da MGS.

7.3. Compete ao Comitê de Segurança da Informação

I - acompanhar as melhores práticas de segurança da informação, e propor sua adoção, quando aplicável;
II - analisar e propor melhorias na Política de Segurança da Informação e nos normativos internos da MGS atinentes ao tema;
III - acompanhar as ações relativas à segurança da informação, inclusive os indicadores e planos de ação, visando a implementação e o cumprimento da Política de Segurança da Informação;
IV - auxiliar na disseminação da cultura de segurança da informação junto aos usuários de recursos de tecnologia da informação e comunicação (TIC);
V - avaliar os projetos da MGS quanto ao impacto na sua segurança da informação, após análise da GETIN;
VI - dirimir dúvidas e deliberar sobre questões não contempladas na Política de Segurança da Informação e em normativos internos a ela relacionados;
VII - receber comunicações de descumprimento da Política de Segurança da Informação e/ou de normativos internos a ela relacionados, bem como de incidentes de segurança da informação, e realizar as tratativas necessárias;
VIII - solicitar à GETIN, quando necessário, a realização de verificações e/ou aferições extraordinárias, acerca do uso dos recursos de TIC da MGS;
IX - avaliar relatórios e resultados de verificações e/ou aferições, bem como de auditorias apresentados pela GETIN e pela GEAUDI, respectivamente;
X - apresentar à Diretoria Executiva da MGS o monitoramento do cumprimento da Política de Segurança da Informação realizado pelo Comitê.

7.4. As competências e responsabilidades dos setores e dos Agentes da MGS, necessárias ao cumprimento da legislação aplicável e da presente Política, serão objeto de normativo interno.

8. DISPOSIÇÕES FINAIS

8.1. As diretrizes e regras quanto à privacidade e proteção de dados pessoais estão contidas na Política de Privacidade e de Proteção de Dados Pessoais da MGS e em normativos internos correlatos ao tema, devendo ser observados em conjunto com a presente Política.

8.2. As violações dos termos da presente Política sujeitarão ao responsável às sanções cabíveis, conforme normas internas e legislação aplicáveis, sem prejuízo das sanções administrativas, cíveis e penais cabíveis.

8.3. Os casos não previstos na presente Política serão tratados pela GETIN e pelo Comitê de Segurança da Informação, conforme o caso.

8.4. A presente Política será regulamentada em normativo interno específico e atualizada periodicamente e/ou sempre que necessário.

9. GRUPO FUNCIONAL

Nome	Matrícula	Sigla do Setor
Bruno Araújo Soares	92368-3	GEAUDI
Carlos Alberto Soares e Silva	96040-1	CODES
Francis Cristiano Ferreira da Silva Pereira Sobrinho	11598-2	GETIN
Graziela Fernanda Lima Inocêncio	76429-5	COGEC
José Silveira Junior	10436-1	GEAPE
Letícia de Castro Peixoto	38133-5	GEPLAG
Lucimar Lourenço Vicente de Souza	56938-9	GEGOC
Lumena Santos Chaves Ricci	92776-4	GECONSUL
Marcelo Miranda de Melo Silva	87028-0	COINF
Perla Ferreira Salles Breña	88625-2	GEGOC
Rodrigo Carvalho dos Santos	47605-5	COINF
Rogério Guimarães Villaça	23227-6	GEPLAG
Rogério Lara de Vasconcelos	36514-0	GEPLOG

10. VIGÊNCIA

10.1. Esta Política entra em vigor na presente data e revoga sua versão anterior, publicada em 01/09/2021, e quaisquer disposições em contrário.