GOVERNO DO ESTADO DE MINAS GERAIS

Secretaria de Estado de Fazenda

Divisão de Segurança da Informação

Normativo Política de Segurança da Informação 2024 - SEF/STI-GOVERNANÇA-DSI

Belo Horizonte, 06 de novembro de 2024.

Revisão	Emissão	Atualização	Elaborado por	Classificador	Classificação
07	26/12/2006	04/11/2024	Superintendência de Tecnologia da Informação	Rogério Zupo Braga	Reservada

Política de Segurança da Informação

1. OBJETIVO

A Política de Segurança da Informação (PSI) da Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG) é constituída por um conjunto de diretrizes e regras que estabelecem os princípios de tratamento, controle de acesso, proteção e monitoramento das informações processadas, armazenadas e/ou custodiadas pelas unidades administrativas da Secretaria e visa atender aos seguintes princípios:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas devidamente autorizadas. A principal forma de mantê-la é por meio da autenticação e do controle de acesso, que permite restringir o acesso às informações.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- Autenticidade: garantia da identidade de quem está tratando a informação. Possui como consequência o não-repúdio que ocorre quando há garantia de que o usuário não poderá se esquivar da autoria da ação (irretratabilidade). Esse princípio é garantido, por exemplo, com o uso do certificado digital para assinatura de um documento ou de uma mensagem de e-mail.
- Legalidade: Garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica.
- Boa fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, previstos no art. 6º da Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018).

2. ABRANGÊNCIA

O cumprimento desta política é obrigatório e ela se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em suas unidades administrativas, ou fora delas, em razão do acesso às informações da SEF/MG.

Esta política também se aplica, no que couber, a pessoas físicas e jurídicas que possuam vínculo contratual com a SEF/MG ou que tenham acesso aos sistemas, serviços e informações custodiadas, ou sob a guarda

desta secretaria.

3. CONCEITOS E DEFINIÇÕES

- Acesso Local – Conexão entre um dispositivo isolado (terminal ou microcomputador) e uma rede, viabilizada por meio de uma rede de área local, isto é, uma rede cuja abrangência restringe-se a uma área limitada, tal como uma casa, uma escola, um laboratório de computadores, ou um prédio de escritórios.
- Acesso Remoto – Conexão à distância entre um dispositivo isolado (terminal ou microcomputador) e uma rede.
- *Active Directory (AD)* – Implementação de serviço de diretório que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações aos usuários e administradores desta rede.
- Antivírus - Ferramenta de segurança instalada nas estações de trabalho da SEF/MG com a finalidade de prevenir, fazer a varredura, detectar e excluir vírus de um computador. Com o objetivo de aumentar a segurança, o software permanece em execução em segundo plano para fornecer proteção em tempo real contra-ataques de vírus.
- CA Service Desk – Serviço de TI utilizado pela SEF/MG cujos principais recursos incluem gerenciamento de mudanças e de incidentes, suporte de automação, autoatendimento, serviços predefinidos e fluxos de trabalho.
- Certificado Digital – Arquivo eletrônico, assinado digitalmente por uma Autoridade Certificadora, que contém dados de uma pessoa física ou jurídica, utilizados para comprovar sua identidade. O certificado digital é armazenado em uma mídia física, denominada *token*, ou em um dispositivo de *hardware*. Possuindo também, o armazenamento em nuvem possibilitando o acesso à assinatura digital por meio de computador ou dispositivo móvel (*tablet* e/ou smartphone) com acesso à internet.
- Dado pessoal – informação relacionada à pessoa natural identificada ou identificável.
- 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.
- Desktop Virtual – Infraestrutura em nuvem composta por sistemas operacionais e aplicativos em que o ambiente de desktop é separado do dispositivo físico usado para acessá-lo. Os usuários podem acessar os desktops virtuais remotamente, a partir de qualquer dispositivo com acesso à internet.
- DevSecOps: integração das práticas de segurança (Security) dentro do processo de desenvolvimento de software (Development) e operações (Operations), resultando em um ciclo de vida de desenvolvimento de software que incorpora a segurança em todas as etapas. A principal meta do DevSecOps é garantir que a segurança seja uma responsabilidade compartilhada entre todos os envolvidos no ciclo de vida do software, desde desenvolvedores até profissionais de operações e segurança.
- Duplo Fator de Autenticação (DFA) – Componente de gestão de acesso que requer que os usuários provem a sua identidade utilizando pelo menos dois fatores de verificação diferentes antes de terem acesso a um website, aplicação móvel ou outro recurso online. Com o DFA, se um fator for comprometido, o atacante ainda terá ao menos uma barreira adicional para romper antes de obter acesso à conta alvo.
- Equipamento Móvel – Equipamento com capacidade de processamento e armazenamento de dados, passível de utilização por usuários em trânsito. Nesta categoria estão incluídos *notebooks*, *tablets* e celulares do tipo *smartphone*, bem como equipamentos similares.
- Ferramenta de Colaboração – Solução digital pautada em tecnologias móveis, como a computação em nuvem, a telefonia e as APIs (Application Programing Interfaces). O objetivo

principal é promover comunicação efetiva e integrada, seja entre membros de um time corporativo, entre colaboradores e clientes ou mesmo entre usuários de serviços.

- Gestão de Continuidade do Negócio – Conjunto de planos, procedimentos e preparação de uma organização para manter as funções críticas de negócios ou retomar as atividades normais, após ocorrência de um incidente, buscando minimizar os impactos à organização e clientes do negócio.
- Gestão de Mudanças – Processo que torna mais fácil para a organização distribuir solicitações de mudança em sua infraestrutura de TI. Ela ajuda a organização a solicitar, priorizar, autorizar, aprovar, programar e implementar quaisquer mudanças, sejam elas simples ou complexas. Um bom processo de Gerenciamento de Mudanças de TI ajuda a controlar os riscos e reduzir ao mínimo as interrupções nos serviços.
- Gestão de Riscos – Processo de organizar e planejar recursos humanos e materiais de uma empresa de forma a reduzir a níveis aceitáveis os impactos dos riscos na organização, utilizando um conjunto de técnicas que visa minimizar os efeitos dos danos acidentais ou intencionais e priorizando o tratamento dos riscos que possam causar danos legais, operacionais, financeiros e à imagem da empresa, entre outros. O principal objetivo da Gestão de Riscos é avaliar as incertezas de forma a tomar a melhor decisão possível.
- Incidente de Segurança da Informação – Indicação de eventos indesejados ou inesperados que possam colocar em risco as informações armazenadas em meio físico ou eletrônico sob a guarda desta Secretaria ou que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- Informação – É a resultante do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano, animal ou máquina) que a recebe.
- Lei Geral de Proteção de Dados – Lei nº 13.709/2018 que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- Mecanismos de proteção – Barreiras que impedem ou limitam o acesso à informação, propiciando um ambiente controlado, seguro e disponível, geralmente eletrônico, evitando que a informação esteja exposta à exclusão, divulgação, alteração ou acesso não autorizado por indivíduo mal-intencionado.
- Microsoft 365 (M365) - Conjunto de aplicativos que visa manter a conectividade e aumentar a produtividade dos servidores e colaboradores da SEF/MG. Dentre os principais destacam-se: Word, Excel, Power Point, Microsoft Teams, One Drive e Outlook. Para os usuários avançados ou para finalidades específicas, possui ainda o Power BI, Forms, Power Automate, entre outros.
- One Drive for Business - Serviço de nuvem da Microsoft que conecta o usuário a todos os arquivos utilizados por ele. Permite armazenar e proteger os arquivos, compartilhá-los com outras pessoas (dentro e fora da organização) e possuir acesso a eles de qualquer lugar, a partir de quaisquer dispositivos conectados à internet.
- Privilégios de administrador – Permissão que possibilita modificar as configurações do computador inclusive as de segurança. Permite instalar e remover *softwares* e acessar qualquer arquivo existente na máquina.
- Segurança da Informação: Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.
- Serviço de comunicação instantânea – Aplicação que permite o envio e o recebimento de mensagens em tempo real.
- Serviço de correio eletrônico – Sistema de mensageria utilizado na Internet, que tem a função de possibilitar o envio e o recebimento de mensagens entre usuários, grupos ou sistemas

computacionais.

- Teletrabalho – prestação de serviços preponderantemente fora das dependências da SEF/MG, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo.
- VPN (*Virtual Private Network*) – Forma de comunicação que permite que uma ou mais máquinas acessem uma rede privada, utilizando como infraestrutura as redes públicas, tais como a Internet. Os dados trafegam na rede de forma segura, utilizando encapsulamento, criptografia e autenticação.

4. DIRETRIZES

4.1. Tratamento da Informação

4.1.1. A Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG) trata os dados sob custódia do órgão de forma proporcional e não excessiva, na quantidade mínima necessária ao cumprimento de suas obrigações legais, execução de políticas públicas e regular exercício das competências previstas na Lei nº 23.304/2019 e no Decreto nº 47.794/2019, bem como para constituir o crédito tributário pelo lançamento, assim entendido como o procedimento administrativo tendente a verificar a ocorrência do fato gerador da obrigação correspondente, determinar a matéria tributável, calcular o montante do tributo devido e identificar o sujeito passivo, nos termos da Lei nº 5.172/1966.

4.2. Proteção da Informação

4.2.1. As informações geradas, adquiridas, armazenadas, processadas, transmitidas e descartadas pelas unidades administrativas da SEF/MG devem ter mecanismos de proteção adequados, baseados em controles, procedimentos e tecnologias implementadas, estabelecidos pela Superintendência de Tecnologia da Informação (STI), de forma a resguardar sua confidencialidade, integridade, disponibilidade, autenticidade e o seu uso em conformidade com os princípios que regem a Administração Pública.

4.2.2. As técnicas de proteção da informação devem estar em conformidade com a legislação vigente, o Código de Conduta Ética do Servidor Público e da Alta Administração Estadual, das normas de Segurança da Informação da Organização Internacional de Normalização (ISO), com a Lei Geral de Segurança da Informação (LGPD) e pelo sigilo fiscal conforme determinado pelo Código Tributário Nacional (CTN).

4.3. Classificação da Informação

4.3.1. As informações devem ser classificadas de forma a serem protegidas adequadamente, conforme legislação prevista para cada tipo de informação no âmbito da Secretaria de Estado de Fazenda.

4.3.2. Os procedimentos para classificação das informações da SEF/MG serão definidos por comissão específica, criada para esta finalidade.

4.3.3. O processo de classificação das informações levará em conta os dados pessoais e sensíveis nos termos da LGPD.

4.4. Ciclo de Vida dos Dados

4.4.1. Contempla as estratégias que visam a resolver a questão da existência da grande massa de dados tratados no âmbito da SEF/MG, que devem ser avaliados/analisados sob o ponto de vista do negócio, utilizando a combinação de processos, políticas, software e hardware, tendo em vista utilização de tecnologia apropriada para contemplar cada estágio do ciclo de vida dos dados. Engloba as etapas de Planejamento, Coleta/Criação, Armazenamento/Persistência, Uso, Arquivamento e Exclusão dos dados.

4.4.2. Esse processo deverá levar em conta as necessidades das áreas de negócio, observando

as leis, normas e regulamentos vigentes.

4.5. Controle de Acesso às Informações

4.5.1. Toda informação utilizada pelas unidades da SEF/MG deve ter seu acesso controlado e o uso permitido apenas aos usuários devidamente autorizados.

4.5.2. As informações referentes aos cidadãos, que estejam sob a custódia da SEF/MG, devem ter seu acesso e uso controlado e restringido, visando à garantia: do direito individual e coletivo das pessoas; da inviolabilidade de sua intimidade; do sigilo de suas informações; dos direitos fundamentais de liberdade e de privacidade e do livre desenvolvimento da personalidade da pessoa natural, nos termos previstos em Lei e na Constituição Federal de 1988.

4.6. Educação em Segurança da Informação

4.6.1. Os usuários devem ser instruídos pela Superintendência de Tecnologia da Informação (STI), para a correta e segura utilização das informações, dos recursos computacionais e dos sistemas e serviços disponibilizados pela SEF/MG.

4.6.2. A STI possui a responsabilidade de promover a conscientização em segurança da informação dos usuários da SEF/MG por meio da oferta de treinamento e capacitação; da elaboração e envio de informativos e comunicados sobre o tema e do esclarecimento de dúvidas de forma a resguardar a confidencialidade, integridade, disponibilidade, autenticidade das informações e o seu uso em conformidade com os princípios que regem a Administração Pública.

4.7. Segurança da Informação

4.7.1. A segurança da informação é dever e responsabilidade de todos. Os usuários devem zelar pela segurança das informações a que tenham acesso com base nas diretrizes e regras estabelecidas pela STI e no disposto na Política de Segurança da Informação vigente. segurança da informação é dever e responsabilidade de todos. Os usuários devem zelar pela segurança das informações a que tenham acesso com base nas diretrizes e regras estabelecidas pela STI e no disposto na Política de Segurança da Informação vigente.

4.8. Gestão de Continuidade de Negócios

4.8.1. A SEF/MG deve elaborar e manter atualizado o plano de continuidade de negócios, em conformidade com os objetivos estratégicos da Secretaria, de forma a reduzir os impactos decorrentes da interrupção de sistemas/aplicações/serviços críticos causada por desastres ou falhas da segurança.

4.9. Gestão de Riscos

4.9.1. A STI deve implementar e manter processo de gestão de riscos com vistas a minimizar possíveis impactos à confidencialidade, à integridade e à disponibilidade das informações da SEF/MG.

4.9.2. O processo deverá ser implementado com base nas diretrizes e regras estabelecidas na legislação que aborda o tema no âmbito da SEF/MG e no Plano de Tratamento de Riscos.

4.9.3. O processo de gestão de riscos no âmbito da STI deve possibilitar a seleção e priorização dos ativos e processos de negócio a serem protegidos, bem como a definição e implantação de controles para a identificação e tratamento das vulnerabilidades de segurança. As medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os possíveis danos que venham a ser provocados por falhas de segurança.

4.10. Gestão de Mudanças

4.10.1. A Gestão de Mudanças permite minimizar o impacto das interrupções dos serviços; acelerar o processo de implementação das mudanças; acompanhar o progresso das mudanças na

infraestrutura de TI; tornar o processo mais transparente, melhorando a comunicação com as partes interessadas; identificar, de forma rápida, a implementação de quaisquer alterações se algo der errado e melhorar a estimativa de custo para quaisquer alterações propostas.

4.10.2. O planejamento de mudanças deve contemplar atividades relativas à análise de riscos, execução e validação da mudança, recuperação em casos de falhas e monitoramento da recuperação.

4.11. Gestão de Incidentes

4.11.1. Incidentes de Segurança da Informação são todos e quaisquer eventos adversos, sob suspeita ou confirmados, que possam comprometer as informações, ativo de informação ou serviços, que tem sua integridade, confidencialidade ou disponibilidade comprometida. Como incidentes de segurança, podemos citar:

- controles de segurança da informação ineficazes;
- violação das expectativas de confidencialidade, integridade ou disponibilidade das informações;
- erros humanos;
- não compliance com a Política de Segurança da Informação da SEF/MG, políticas específicas ou normas aplicáveis.

4.11.2. A STI deve estabelecer, implementar e manter um sistema de gestão de incidentes em segurança da informação que contemple os processos para registro, análise e tratamento dos incidentes.

4.11.3. Os usuários devem ser conscientizados pela STI sobre a importância de efetuarem o registro dos incidentes de segurança da informação de que tiverem ciência, bem como a forma adequada de fazê-lo.

4.12. Gestão de Vulnerabilidades

4.12.1. Desenvolver um plano que permita avaliação e rastreamento contínuo de vulnerabilidades em todos os ativos presentes na infraestrutura da organização, objetivando remediar tais vulnerabilidades e minimizar a janela de oportunidade para sua exploração por potenciais atacantes. O plano deve, necessariamente, incluir o monitoramento de fontes públicas e privadas para manter-se atualizado sobre novas informações relacionadas a ameaças e a vulnerabilidades.

4.13. Desenvolvimento de sistemas, serviços e aplicações corporativas

4.13.1. O desenvolvimento de sistemas, serviços e aplicações corporativas ou departamentais para os ambientes analíticos e/ou transacionais pelas unidades administrativas da SEF/MG deverá observar as diretrizes estabelecidas pela STI.

4.14. Monitoramento e visibilidade

4.14.1. A Superintendência de Tecnologia da Informação (STI) monitora os sistemas/serviços críticos de TI com o objetivo de garantir a continuidade dos negócios, a segurança dos dados e a eficiência operacional.

4.14.2. A importância desse monitoramento reside na capacidade de detectar e responder rapidamente a falhas, ameaças de segurança e outros incidentes que possam comprometer a integridade e a disponibilidade dos sistemas/serviços.

4.14.3. As principais ações incluem a implementação de sistemas de monitoramento em tempo real, a análise contínua de logs e métricas de desempenho, a configuração de alertas para atividades anômalas, a realização de auditorias regulares de segurança e o estabelecimento de protocolos de resposta a incidentes.

4.14.4. A STI deve estabelecer programas de treinamento e capacitação de forma a manter a

equipe de TI habilitada e informada sobre as melhores práticas de segurança e monitoramento, garantindo que possam agir de forma proativa para mitigar riscos e resolver problemas antes que causem impactos significativos.

4.15. Registro de Logs e Auditoria

4.15.1. As trilhas de auditoria são essenciais para a obtenção das evidências cronológicas importantes para a SEF/MG, por meio do conjunto de registros e/ou destino, além de fonte de registros que fornecem evidências documentais da sequência de atividades que afetaram, em qualquer tempo, uma operação, procedimento específico, ou evento.

4.15.2. Compete aos gestores dos processos críticos da SEF/MG, juntamente com a STI, definir parâmetros de geração e retenção das trilhas de auditoria para fins de monitoramento dos sistemas, serviços e aplicações.

4.16. Proteção à Propriedade Intelectual

4.16.1. Todos os procedimentos apropriados devem ser implementados no âmbito da SEF/MG para garantir a conformidade com os requisitos legais, regulamentares e contratuais relacionados aos direitos de propriedade intelectual, e sobre o uso de produtos de softwares, incluindo os direitos de propriedade intelectual, os autorais de software ou documento, direitos de projetos, marcas, patentes e licenças de código fonte.

4.16.2. A STI deve assegurar que:

4.16.3. A aquisição de software seja realizada por meio de fontes conhecidas e de reputação, para garantir que o direito autoral não está sendo violado;

4.16.4. Os registros sejam estruturados e mantidos de forma adequada, permitindo identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

4.16.5. Sejam implementados controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não está excedido;

4.16.6. Verificações sejam realizadas para que somente produtos de software autorizados e licenciados sejam instalados.

4.17. Liderança e Comprometimento

4.17.1. A SEF/MG estruturou o Comitê Estratégico de Governança (CEG) e o Comitê de Tecnologia e Segurança da Informação (CTSI) e a Divisão de Segurança da Informação demonstrando sua liderança e comprometimento em relação ao Sistema de Gestão da Segurança da Informação (SGSI) em conformidade com os requisitos da norma de segurança ISO vigente. Dessa forma, a Alta Direção busca:

4.17.2. Assegurar que a Política de Segurança da Informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da SEF/MG conforme definido no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC).

4.17.3. Garantir a integração dos requisitos do SGSI dentro dos processos da SEF/MG, mantendo todos os regulamentos e procedimentos atualizados em conformidade com os processos implementados.

4.17.4. Assegurar a disponibilidade dos recursos necessários para o SGSI, através da manutenção dos contratos vigentes, investimentos na área de segurança da informação, alocação de pessoas e definição de responsabilidades sobre segurança da informação dentro das áreas competentes.

4.17.5. Comunicar a importância da gestão eficaz da segurança da informação por meio de Workshops, Treinamentos, Educação a Distância (EaD), publicação de informativos.

4.17.6. Assegurar que o SGSI alcance os resultados pretendidos acompanhando e realizando

análise crítica sobre os indicadores de desempenho dos processos.

4.17.7. Orientar e apoiar as pessoas para que contribuam para a eficácia do SGSI.

4.17.8. Promover a melhoria contínua, realizando periodicamente Reuniões de análise crítica, processos de auditoria e acompanhamento de indicadores.

4.17.9. Apoiar outros papéis relevantes da gestão para demonstrar como a liderança se aplica às áreas sob sua responsabilidade definindo hierarquia entre as áreas e responsabilidades.

4.18. Objetivos de Segurança da Informação

4.18.1. O Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) publicado anualmente, detalha os objetivos estratégicos de segurança da informação da SEF/MG e o plano de ação para alcançá-los. Os objetivos foram definidos de acordo com a norma ISO 27001, alinhados com esta política de segurança da informação e em conformidade com as diretrizes da alta gestão da SEF/MG, e refletem as necessidades específicas de proteção dos ativos de informação.

5. REGRAS GERAIS

5.1. Acesso Físico

5.1.1. Toda e qualquer pessoa que necessitar ingressar na SEF/MG, exceto na área destinada para o atendimento ao público, deverá ser devidamente identificada, nas áreas de recepção e deverá receber crachá para ser usado em local visível.

5.1.2. As pessoas mencionadas no item anterior que acessarem os locais de acesso restrito da SEF/MG deverão ser acompanhadas durante o período de permanência, por um custodiante autorizado.

5.1.3. É vedada a entrada de qualquer pessoa não autorizada nas dependências internas da SEF/MG.

5.1.4. As instalações de armazenagem de dados de tecnologia da informação devem ser protegidas de forma a evitar acesso não autorizado.

5.1.5. É obrigatório que todos os colaboradores, fornecedores e visitantes, tenham alguma forma visível de identificação.

5.2. Acesso Lógico

5.2.1. O acesso lógico, seja ele local ou remoto, aos sistemas, aplicações e serviços disponibilizados pela SEF/MG é feito por meio de autenticação empregando login/senha ou certificado digital, sendo responsabilidade do usuário manter o sigilo de todas as senhas, que são de uso pessoal e intransferível, bem como cuidar do certificado digital fornecido pela SEF/MG.

5.2.2. Sempre que aplicável, será habilitado o Duplo Fator de Autenticação (DFA) para acesso aos sistemas, aplicações e serviços disponíveis no ambiente da SEF/MG visando aumentar a segurança.

5.2.3. Os acessos dos usuários aos sistemas, aplicações e serviços disponibilizados pela SEF/MG poderão ser bloqueados pela STI ou unidade responsável, em caráter temporário, caso haja ameaça à segurança das informações, nos termos previstos nesta Política.

5.2.4. Os acessos são restritos às atividades profissionais do usuário e suficientes ao desempenho de suas tarefas.

5.2.5. A concessão, alteração e bloqueio de acesso lógico ao serviço de diretório, Active Directory, para autenticação dos usuários nos sistemas, aplicações e serviços disponibilizados pela SEF/MG, que utilizam esse serviço deve observar o disposto no Procedimento Operacional Padrão (POP) Concessão de Acesso Lógico – Login de Rede.

5.2.6. As permissões de acesso aos sistemas fazendários, aplicações do M365 e seus benefícios dos colaboradores desligados; bem como dos servidores aposentados; falecidos; cedidos a

outro órgão; exonerado de ofício/a pedido; em licença para tratar de interesse particular, para acompanhamento de cônjuge, para assumir cargo de direção ou representação sindical e para assumir mandato serão revogadas quando o fato for informado à STI pelas Superintendências responsáveis pela gestão dos sistemas, pela Superintendência de Planejamento, Gestão e Finanças (SPGF) e/ou pelo responsável de unidade.

5.2.6.1. O bloqueio resultará na perda de todos os acessos e permissões, incluindo as licenças associadas ao Microsoft Office 365.

5.3. Política de Senhas

5.3.1. Sempre que possível, os sistemas, aplicações e serviços devem ser configurados para:

5.3.2. Bloquear o acesso do usuário quando houver 05 (cinco) tentativas de logon incorretas.

5.3.3. Fornecer senha temporária, obrigatoriamente alterada no primeiro acesso.

5.3.4. Proibir a reutilização, pelo usuário, das últimas 05 (cinco) senhas.

5.3.5. O Procedimento Operacional Padrão (POP) Concessão de Acesso Lógico – Login de Rede contém o detalhamento das regras relacionadas a concessão de acesso lógico e política de senhas.

5.4. Teletrabalho

5.4.1. Tem o objetivo de flexibilizar o trabalho, de modo a permitir ao servidor/colaborador desempenhar suas funções e responsabilidades relativas ao cargo e outras atividades autorizadas, em um local de trabalho diferente das unidades fazendárias, onde o funcionário normalmente trabalha.

5.4.2. As diretrizes e regras que regulamentam o teletrabalho no âmbito da SEF/MG estão descritas em legislação específica.

5.4.3. O acesso remoto à rede fazendária é permitido por meio de Virtual Private Network (VPN).

5.4.4. As instruções e regras de instalação, configuração e uso da VPN encontram-se disponíveis no Portal da Segurança da Informação.

5.4.5. Outras formas de acesso remoto à rede Fazendária da SEF/MG, são proibidas até que sejam testadas, aprovadas e homologadas pela STI.

5.4.6. Os servidores/colaboradores devem manter cuidados especiais com vistas a reduzir a exposição a ameaças cibernéticas no ambiente de teletrabalho, tais como:

5.4.6.1. Usar uma conexão segura para se conectar à rede da Secretaria;

5.4.6.2. Evitar se conectar à rede fazendária por meio de Wi-Fi público desprotegido.

5.4.6.3. Evitar armazenar dados e informações fora do ambiente controlado e monitorado pela SEF/MG (sistemas, serviços e aplicações corporativos, estações de trabalho patrimoniadas, servidores de arquivos e serviços de nuvem homologados pela STI).

5.4.6.4. Certificar-se de que computador/notebook pessoal está com o sistema operacional, antivírus, aplicativos e demais ferramentas atualizadas.

5.4.6.5. Fazer uso de senhas fortes e/ou biometria no computador/notebook, dispositivo móvel pessoal e, utilizar, sempre que possível, o DFA nos sistemas, serviços e aplicações disponibilizados pela STI.

5.4.6.6. Usar apenas os aplicativos homologados pela STI para compartilhar e armazenar dados.

5.4.6.7. Evitar imprimir e armazenar documentos em papel com informações confidenciais em ambiente fora das unidades fazendárias.

5.4.7. É de responsabilidade do proprietário usar somente softwares legalizados em seu equipamento particular.

5.4.8. A SEF/MG não se responsabiliza pela segurança da infraestrutura física, lógica e problemas de segurança e/ou mal funcionamento quando a origem for de contratação particular do usuário.

5.4.9. Serão criados e armazenados os logs dos acessos remotos contendo informações do usuário, data, hora e outros dados específicos por período legal ou superior, para tratamento de incidentes, auditorias e/ou processos judiciais.

5.4.10. A concessão do acesso remoto será revogada caso ocorra uma das seguintes hipóteses:

5.4.10.1. exoneração ou aposentadoria de servidor;

5.4.10.2. cessão de servidor;

5.4.10.3. qualquer afastamento de servidor com duração superior a noventa dias;

5.4.10.4. cessação do vínculo;

5.4.10.5. fim do vínculo com a contratada;

5.4.10.6. transcurso de mais de sessenta dias sem qualquer acesso;

5.4.10.7. no caso de solicitações novas, não havendo o primeiro acesso no período de quinze dias da efetivação do acesso; ou

5.4.10.8. caso haja atividades suspeitas, tráfego malicioso ou grande volume de tráfego partindo da conexão.

5.5. Certificado Digital

5.5.1. O fornecimento de certificado digital se dará por solicitação formal do responsável da unidade acompanhada da justificativa do uso para as atividades laborais.

5.5.2. O uso do certificado digital é individual, pessoal e intransferível. A guarda do dispositivo token e das senhas é de responsabilidade dos usuários.

5.5.3. Os certificados digitais deverão ser revogados quando for constatada a perda, o extravio ou o roubo dos dispositivos utilizados para seu armazenamento ou bloqueio ocasionado pelo esquecimento da senha de acesso.

5.5.4. Quando o titular do certificado digital se aposentar ou se desligar da SEF/MG poderá optar por permanecer com o dispositivo, mediante o ressarcimento dos valores pagos pelo Estado na aquisição.

5.5.5. O dispositivo token deve ser devolvido à STI em caso de revogação, vencimento ou não necessidade de utilização.

5.5.6. As informações relativas ao Certificado Digital se encontram disponíveis no Portal da Segurança da Informação.

5.6. Correio Eletrônico

5.6.1. O serviço de correio eletrônico disponibilizado aos usuários é de propriedade da SEF/MG e seu uso deve ser obrigatório e restrito às atividades profissionais.

5.6.2. A SEF/MG, por intermédio da STI, reserva para si o direito de monitorar o uso dos serviços de correio eletrônico, de armazenamento em nuvem e de comunicação instantânea institucionais, bem como o conteúdo das mensagens, arquivos e informações.

5.6.3. Quando houver ameaça à segurança das informações ou quando constatado o uso indevido do serviço, a STI poderá reter e/ou eliminar mensagens e arquivos, bem como poderá bloquear usuários, de forma temporária.

5.6.4. A SEF/MG possui ferramentas de análise de conteúdo de e-mails implementada no ambiente com o objetivo de prevenir o recebimento de mensagens maliciosas/indesejadas, que possam colocar em risco a infraestrutura de TI.

5.6.5. O serviço de correio eletrônico é uma ferramenta usada para compartilhamento de informações e arquivos. Apesar de muito útil e de ser utilizada de forma massiva, é importante que os usuários tenham ciência de que não existe garantia de entrega/recebimento da mensagem. Diversos fatores como falha na conexão, indisponibilidade do serviço, retenção em quarentena podem impedir o envio/recebimento de e-mails. Por isso, sempre que o assunto for extremamente importante, confirme com o destinatário o recebimento e marque, sempre que necessário, as opções de confirmação de recebimento e de leitura.

5.6.6. O serviço de correio eletrônico é permitido somente para as atividades profissionais dos usuários, não sendo permitido enviar ou arquivar mensagens que não estejam relacionadas as atividades desta Secretaria, ou que contenham:

5.6.6.1. Assuntos que provoquem assédio, perturbação a outras pessoas ou que prejudiquem a imagem da Secretaria;

5.6.6.2. Temas difamatórios, discriminatórios, caluniosos, degradantes, ofensivos, violentos, ameaçadores, material obsceno, material pornográfico, ilegal ou antiético;

5.6.6.3. Fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais da Secretaria;

5.6.6.4. Compartilhar arquivos com códigos executáveis ou qualquer outra extensão que possa apresentar risco à segurança da informação.

5.6.7. O Procedimento Operacional Padrão (POP) Concessão de Acesso Lógico – E-mail contém o detalhamento dos processos e das regras relacionadas aos serviços de correio eletrônico e de comunicação instantânea institucional.

5.7. Estações de Trabalho e Equipamento Móveis

5.7.1. As estações de trabalho e os equipamentos móveis disponibilizados aos usuários são de propriedade da SEF/MG e o uso deve ser restrito às atividades profissionais.

5.7.2. Somente software autorizado pela STI deve ser instalado nas estações de trabalho, sendo proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais.

5.7.3. Somente softwares regularmente licenciados e adquiridos pela SEF/MG (licenças pagas) ou open source para uso em ambiente corporativo poderão ser utilizados nas estações de trabalho.

5.7.3.1. A utilização de software não licenciado ou considerado “pirata” constitui infração prevista na Lei nº 9.609/1998 (http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm);

5.7.4. Os dispositivos e serviços sem utilização nas estações de trabalho devem ser desabilitados.

5.7.5. A concessão de privilégios de administrador nas estações de trabalho é restrita. As exceções deverão ser formalizadas pelo responsável da unidade e o pedido analisado pela STI.

5.7.6. A STI tem a prerrogativa de realizar auditorias de conformidade em todas as estações de trabalho e dispositivos móveis de propriedade da SEF/MG.

5.7.7. Os serviços de expansão, substituição ou manutenção das estações de trabalho serão executados somente pela STI ou sob a supervisão da superintendência.

5.7.7.1. É vedado aos usuários a aquisição e instalação de qualquer hardware/periférico nas estações de trabalho da SEF/MG, salvo se devidamente autorizado pela STI.

5.7.8. É vedada a utilização de equipamentos particulares, isto é, aqueles não fornecidos pela SEF/MG, na rede fazendária.

5.7.8.1. Excepcionalmente, equipamentos particulares poderão ser conectados à rede WIFI segregada com acesso somente à Internet, desde que disponível na unidade, mediante solicitação da chefia da unidade e autorização prévia e expressa da STI.

5.7.9. As atualizações e correções de segurança do sistema operacional ou aplicativos

somente poderão ser feitas após a devida validação em ambiente de homologação e testes.

5.7.9.1. Os usuários são parte fundamental no processo de atualização dos pacotes de funcionalidades e de segurança do sistema operacional e das diversas aplicações presentes na estação de trabalho, devendo seguir as orientações encaminhadas pela STI.

5.7.10. É vedado aos usuários realizar movimentação das estações de trabalho, dentro ou fora da unidade, sem a prévia e expressa autorização da STI.

5.8. Armazenamento de Dados

5.8.1. Os servidores de arquivos disponibilizados na rede fazendária devem ser utilizados exclusivamente para armazenamento de informações relacionadas às atividades profissionais do usuário.

5.8.2. Toda informação da SEF/MG deve ser armazenada nos servidores da rede fazendária.

5.8.2.1. Alternativamente, os usuários poderão utilizar o drive de armazenamento na nuvem disponibilizado pela SEF/STI (One Drive for Business) para o armazenamento dos arquivos de trabalho e backup das informações.

5.8.3. Por questões de segurança e privacidade, é vedado o compartilhamento de arquivos com o público externo.

5.8.3.1. As exceções devem ser direcionadas à STI para análise.

5.8.4. Os dados críticos da Unidade Administrativa devem ser mantidos em compartilhamentos de rede disponibilizados pela STI de forma a garantir o processo de backup e restore dos dados.

5.9. Uso da internet

5.9.1. O serviço de Internet é disponibilizado pela SEF/MG para execução das atividades profissionais dos usuários.

5.9.2. A SEF/MG, por intermédio da STI, reserva para si o direito de monitorar o uso da Internet disponibilizada, bloqueando e/ou restringindo o acesso a arquivos ou sítios que comprometam o funcionamento da rede fazendária, prejudiquem as atividades profissionais ou coloquem em risco a Segurança das Informações custodiadas pela SEF/MG.

5.9.2.1. As solicitações de permissão especial de acesso à Internet devem ser formalizadas pelo responsável da unidade e o pedido analisado pela STI.

5.9.3. O usuário deve zelar pelo bom uso da Internet, respeitando direitos autorais, regras de licenciamento de software, direitos de propriedade, privacidade e proteção de propriedade intelectual.

5.9.4. O acesso à Internet, por meio da rede fazendária, deve ser efetuado somente por equipamentos autorizados pela STI.

5.9.5. O portal Intranet da SEF/MG destina-se ao compartilhamento de informações e à colaboração dos usuários que atuam nesta Secretaria, com conteúdo mantido pelos editores de cada unidade, sob coordenação da Assessoria de Comunicação Social e Comissão de Comunicação Social.

5.10. Youtube

5.10.1. O acesso ao Youtube, plataforma de compartilhamento de vídeos da Google, é autorizado de forma irrestrita dentro da rede fazendária visando possibilitar o acesso a eventos ao vivo, a conteúdos que possam auxiliar no desempenho das atividades laborais, ao treinamento e à capacitação, entre outros.

5.10.2. Por se tratar de serviço de streaming, a utilização deve se dar de forma consciente pelos usuários devido ao impacto que o uso indevido pode causar nos links de comunicação.

5.10.3. É responsabilidade do usuário e da chefia imediata zelar pela utilização adequada dos recursos disponibilizados pela STI para o desempenho das atividades profissionais.

5.10.4. A permissão de acesso ao Youtube poderá ser revogada a qualquer tempo, se constatado o uso abusivo do serviço que venha a causar impacto no link de comunicação da unidade de exercício do usuário.

5.11. Aplicativos de mensagens instantâneas

5.11.1. É vedado o uso de aplicativos de mensagens instantâneas como WhatsApp, Telegram, WeChat e similares, no âmbito da rede fazendária, tendo em vista o risco de indisponibilidade dos serviços, aplicações e sistemas corporativos causado por malware e outras pragas virtuais que possam vir a ser disseminados por meio do uso dessas ferramentas;

5.11.2. A política de uso dos aplicativos de mensagens instantâneas destaca que a utilização dos serviços é por conta e risco do usuário e está sujeita a diversas ressalvas dentre as quais destacam-se:

5.11.2.1. A inexistência de garantias expressas ou tácitas de não violação e proteção contra vírus de computador ou outros códigos nocivos;

5.11.2.2. A não garantia que os serviços estarão em funcionamento, livres de erros, protegidos ou seguros;

5.11.2.3. A não garantia que os serviços funcionarão sem interrupções, atrasos ou imperfeições.

5.11.3. O uso da ferramenta em dispositivos pessoais (smartphones, tablets e notebooks) para tratar assuntos relacionados ao trabalho também não é recomendado pela STI.

5.11.4. Sob a ótica da privacidade dos dados e da conformidade com a LGPD, o uso de aplicativos de mensagens instantâneas também não é recomendado pela STI, devido à falta da transparência no que diz respeito aos dados coletados, bases legais e finalidades do tratamento.

5.12. Microsoft Teams

5.12.1. O Microsoft Teams é a ferramenta de comunicação e colaboração adotada pela SEF/MG e o seu uso é obrigatório para todos os usuários da rede fazendária.

5.12.2. O Microsoft Teams possui recursos de mensagens instantâneas, chamadas e vídeo. Oferece ainda colaboração de documentos e integração de aplicativos, trazendo agilidade, eficiência e melhor produtividade ao ambiente corporativo.

5.13. Reuniões Virtuais

5.13.1. Excepcionalmente, ferramentas como Google Meet, Webex, Zoom, entre outras, poderão ser utilizadas para a realização de reuniões virtuais em substituição ao Microsoft Teams. Elas se encontram liberadas para uso na rede fazendária por meio dos navegadores web, na condição de participante/ouvinte.

5.13.2. A instalação dos aplicativos na versão desktop das soluções supracitadas para participação como palestrante/orador na reunião depende de análise e aprovação da STI, mediante justificativa fundamentada, pois é necessária a realização de configurações específicas no ambiente.

6. RECOMENDAÇÕES

Recomenda-se aos usuários:

6.1. Trocar sua senha sempre que existir qualquer indício de comprometimento do sistema, do serviço ou da própria senha.

6.2. Configurar, sempre que estiver disponível, o fator adicional de autenticação com vistas a aumentar a segurança nos serviços, sistemas e aplicações disponibilizados pela SEF/MG.

6.3. Não utilizar a senha de acesso aos sistemas, serviços e aplicações da SEF/MG em ambientes externos.

6.4. Evitar o acesso remoto à rede fazendária em locais públicos.

6.5. Não utilizar o crachá de identificação fora das instalações da SEF/MG.

6.6. Manter a mesa de trabalho sempre limpa, sem papéis e mídias expostas.

6.6.1. Informações com restrição de acesso não devem ser deixadas à vista sobre mesas de trabalho ou em quaisquer outros suportes que não disponham de mecanismos de controle de acesso, devendo ser destruídas antes de serem descartadas, seja em papel ou em meio eletrônico.

6.6.2. Computadores pessoais e terminais de computador não devem apresentar senhas na tela e não devem permanecer logados, caso o usuário esteja ausente.

6.7. Evitar discutir assuntos relacionados às atividades profissionais em locais públicos.

6.8. Não abrir mensagens de correio eletrônico:

6.8.1. Cujo assunto, remetente ou conteúdo sejam de origem desconhecida e/ou suspeita.

6.8.2. Contendo links e/ou arquivos anexados de origem desconhecida e/ou suspeita.

6.9. Não divulgar o endereço eletrônico, fornecido pela SEF/MG, para recebimento de mensagens particulares, alheias aos interesses ou atividades da Secretaria.

6.10. Não deixar os equipamentos móveis sob sua responsabilidade desprotegidos.

6.11. Não armazenar arquivos que contenham informações da SEF/MG em equipamentos e mídias particulares.

6.12. Evitar utilizar outro serviço de correio eletrônico que não seja o institucional da SEF/MG nos equipamentos conectados à rede fazendária.

6.13. Evitar alimentar-se ou ingerir líquidos próximo às estações de trabalho.

6.14. Ao compartilhar assuntos de trabalho, em qualquer local, dentro ou fora do ambiente de trabalho, a partir de qualquer tipo de canal, mídia, ferramenta ou tecnologia, deve-se respeitar a ética, a legislação vigente e cumprir com seu dever de sigilo profissional, aplicando a melhor técnica disponível para garantir a segurança da informação no nível exigido pela relevância dela.

6.15. Adotar cultura sem papel, em que documentos só devem ser impressos se forem necessários, considerando a existência da tramitação eletrônica, como também em atendimento à legislação e às normas internas de sustentabilidade. Alinhada à PSI com resguardo do acesso ao conteúdo destes documentos que, porventura, sejam esquecidos em locais de impressão.

7. RESPONSABILIDADES

7.1. **É de responsabilidade dos usuários:**

7.1.1. Conhecer e cumprir integralmente todas as diretrizes e regras desta Política de Segurança da Informação, bem como os procedimentos, os regulamentos e as instruções de trabalho.

7.1.2. Responder pelo:

7.1.2.1. Acesso aos sistemas e serviços, por meio de sua identificação.

7.1.2.2. Uso do equipamento móvel sob sua responsabilidade.

7.1.3. Utilizar, obrigatoriamente, apenas os sistemas disponibilizados e autorizados pela SEF/MG para enviar e receber informações profissionais.

7.1.4. Utilizar e manter o crachá funcional em local visível durante sua permanência nas instalações da SEF/MG.

7.1.5. Avisar à chefia imediata ou ao superior:

7.1.5.1. A perda, o furto ou o desaparecimento de qualquer ativo da SEF/MG.

7.1.5.2. A presença de pessoas sem identificação nas dependências da SEF/MG.

7.1.5.3. Os incidentes de segurança da informação e registrá-los em ferramenta disponibilizada pela STI no momento da constatação do fato.

7.1.6. Proteger as informações a que tenha acesso armazenadas em papel ou meio magnético.

7.1.7. Apresentar, em caso de furto, roubo ou extravio do dispositivo móvel, o Boletim de Ocorrência Policial, no prazo máximo de 48 (quarenta e oito) horas do fato ocorrido, à área responsável pelo patrimônio do órgão ou entidade.

7.1.8. Notificar a STI os casos de violação das regras e eventuais falhas de Segurança da Informação mediante registro de incidente de segurança.

7.1.9. Conscientizar o público externo de sua circunscrição acerca da importância da Segurança das Informações na SEF/MG e do cumprimento do disposto nesta política.

7.2. **É de responsabilidade do responsável pela unidade:**

7.2.1. Orientar os usuários sob sua coordenação sobre a necessidade de conhecer e cumprir a política de segurança da informação.

7.2.2. Zelar pela correta utilização, limpeza e organização da Sala de Equipamentos – SEQ existente nas unidades fazendárias, bem como pelo correto acesso aos sistemas e serviços da SEF/MG por parte dos usuários sob sua coordenação;

7.2.3. Realizar, no mínimo semestralmente, uma análise crítica dos direitos de acesso dos usuários sob sua coordenação e solicitar os ajustes necessários.

7.2.4. Informar à Superintendência de Planejamento, Gestão e Finanças (SPGF) as movimentações de servidores e usuários para que sejam providenciados, pela STI e pelas unidades gestoras, os ajustes nas permissões de acesso a serviços e sistemas mantidos ou utilizados pela SEF/MG.

7.3. **É de responsabilidade da Superintendência de Tecnologia da Informação - STI:**

7.3.1. Proteger a informação e garantir a sua confiabilidade.

7.3.2. Gerir a arquitetura informacional.

7.3.3. Gerir a arquitetura e a infraestrutura tecnológica.

7.3.4. Gerir a governança de Tecnologia de Informação e Comunicação – TIC da SEF/MG.

7.3.5. Gerir o processo de inovação e prospecção de TIC provendo alternativas tecnológicas que mais agreguem valor, com foco no atendimento das necessidades de informação da SEF/MG.

7.3.6. Prover o sítio eletrônico, a intranet e os mecanismos de acesso digital para os usuários dos serviços, respeitando os padrões de desenvolvimento e de prestação de serviços eletrônicos definidos pela Política Estadual de TIC.

7.3.7. Propor, incentivar e viabilizar a implantação de soluções de governo digital, alinhadas às ações de governo, com foco na otimização dos processos, e na melhoria contínua da qualidade dos serviços públicos e do atendimento ao cidadão, às empresas, aos servidores e ao próprio governo.

7.3.8. Gerir, em articulação com a Superintendência de Fiscalização (SUFIS), a auditoria digital da SEF/MG, relativamente aos aspectos de tecnologia da informação.

7.3.9. Exercer as atividades relacionadas à forense computacional junto às unidades administrativas da SEF/MG.

7.3.10. Exercer a coordenação do Núcleo de Transformação Digital.

7.3.11. Orientar a elaboração de projetos na rede física e acompanhar os trabalhos de execução.

7.3.12. Propor diretrizes e normas de caráter geral, políticas e estratégias em segurança da informação.

7.3.13. Elaborar o planejamento e a gestão da Segurança da Informação.

7.3.14. Elaborar os documentos necessários à Segurança da Informação.

7.3.15. Elaborar, divulgar às partes interessadas, manter e aperfeiçoar os indicadores de

Segurança da Informação.

7.3.16. Propor, implementar, manter e melhorar o Plano de Continuidade de Negócios, no que se refere aos ativos sob sua responsabilidade.

7.3.17. Analisar os incidentes de Segurança da Informação, recomendar as ações corretivas e implementá-las no âmbito de sua competência.

7.3.18. Assegurar que o Sistema de Gestão da Segurança da Informação (SGSI) esteja em conformidade com os requisitos da norma ISO sobre Segurança da Informação vigente.

7.3.19. Relatar o desempenho do SGSI à Alta Direção.

7.3.20. Fazer constar nos contratos firmados com fornecedores o anexo do Termo de Confidencialidade, como condição para que possa ser concedido o acesso aos ativos de informação disponibilizados pela SEF/MG.

7.3.21. Garantir o sigilo e a confidencialidade das informações enviadas e processadas por aplicações em dispositivos móveis disponibilizadas aos cidadãos.

7.3.22. Gerar, manter e proteger as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a SEF/MG.

7.3.23. Garantir a disponibilidade dos sistemas, serviços e aplicações e a integridade e disponibilidade das informações armazenadas no data center da SEF/MG.

7.3.24. Bloquear e revogar os acessos aos sistemas, aplicações e serviços, de acordo com as informações recebidas da SPGF e da chefia imediata do usuário.

7.3.25. Efetuar backup e restore dos arquivos armazenados nos servidores da rede fazendária.

7.3.26. Manter e proteger as informações custodiadas pela Secretaria de Estado de Fazenda mesmo fora do ambiente da SEF, por exemplo aquelas armazenadas em nuvem (cloud).

7.3.27. Estabelecer e fazer cumprir os procedimentos de controle de acesso físico ao Data Center da SEF/MG.

7.3.28. Adotar práticas de programação segura no desenvolvimento das aplicações da SEF/MG, visando minimizar o número de vulnerabilidades e eliminar aquelas consideradas críticas.

7.4. **É de responsabilidade da Divisão de Segurança da Informação:**

7.4.1. Executar os projetos e atividades de segurança da informação aprovados pelo Comitê Estratégico de Governança (CEG) e pela Alta Direção da STI.

7.4.2. Atuar como referência em Segurança da Informação, provendo suporte às unidades da SEF/MG e trabalhando no desenvolvimento de soluções que atendam aos requisitos de segurança.

7.4.3. Promover a atualização da Política de Segurança da Informação e apresentá-la ao Comitê de Tecnologia e Segurança da Informação para validação e encaminhamento ao CEG.

7.4.4. Elaborar, implementar e acompanhar os indicadores de segurança da informação.

7.4.5. Gerenciar o tratamento dos incidentes de segurança.

7.4.6. Acompanhar a implementação dos controles e soluções de segurança no ambiente de TI da SEF/MG.

7.4.7. Apoiar o processo de gestão dos riscos de segurança da informação da SEF/MG.

7.4.8. Promover campanhas de conscientização em Segurança da Informação, com o apoio da Assessoria de Comunicação Social.

7.4.9. Relatar sobre o desempenho do Sistema de Gestão da Segurança da Informação (SGSI) da SEF/MG para o Gabinete da STI.

7.4.10. Orientar aos usuários a respeito das responsabilidades e dos procedimentos de segurança da informação.

7.5. **É de responsabilidade da Assessoria de Comunicação Social:**

7.5.1. Exercer as competências estabelecidas na legislação vigente, com foco em:

7.5.1.1. Auxiliar a Divisão de Segurança da Informação na elaboração de campanhas relacionadas à conscientização em Segurança da Informação.

7.5.1.2. Elaborar, em parceria com a STI, o plano de comunicação desta Política de Segurança da Informação e demais assuntos pertinentes à Segurança da Informação.

7.6. **É de responsabilidade da Controladoria Setorial:**

7.6.1. Exercer as competências estabelecidas na legislação vigente, com foco em:

7.6.1.1. Executar as atividades de auditoria do Sistema de Gestão de Segurança da Informação (SGSI) da SEF/MG, com vistas a agregar valor ao processo e assegurar a conformidade com as normas de Segurança da Informação da família ISO.

7.6.1.2. Verificar o cumprimento da Política de Segurança da Informação, atuando em conformidade com sua competência estabelecida em lei.

7.6.1.3. Definir parâmetros de geração e retenção das trilhas de auditoria, juntamente com a STI, para fins de auditoria e controle.

7.6.1.4. Propor à Corregedoria a aplicação das punições previstas em Lei e no estatuto do Servidor Público aos usuários que descumprirem o disposto na Política de Segurança da Informação da SEF/MG.

7.7. **É de responsabilidade da Corregedoria:**

7.7.1. Exercer as competências estabelecidas na legislação vigente, com foco em:

7.7.1.1. Apurar o fato e, quando devido, aplicar as sanções previstas em Lei e no Estatuto do Servidor Público aos usuários que descumprirem o disposto na Política de Segurança da Informação da SEF/MG.

7.7.1.2. Definir parâmetros de geração e retenção das trilhas de auditoria, juntamente com a STI, para fins de auditoria e controle.

7.8. **É de responsabilidade da Superintendência de Planejamento, Gestão e Finanças:**

7.8.1. Exercer as competências estabelecidas na legislação vigente, com foco em:

7.8.1.1. Manter atualizadas as movimentações de pessoal da SEF/MG e informar, mensalmente, as alterações, inclusive desligamentos, à STI e às Superintendências responsáveis pela gestão dos sistemas.

7.9. **É de responsabilidade do Comitê Estratégico de Governança:**

7.9.1. Exercer as competências estabelecidas na legislação vigente, com foco em:

7.9.1.1. Deliberar sobre as diretrizes e a Política de Segurança da Informação da SEF/MG;

7.9.1.2. Garantir o apoio institucional para promover a gestão de riscos e controles internos, em especial os seus recursos e o relacionamento entre as partes interessadas;

7.9.1.3. Deliberar sobre a Política de Gestão de Riscos e Plano de Gestão de Riscos da SEF/MG, os níveis de apetite e tolerância a riscos, bem como avaliar o seu desempenho.

7.10. **É de responsabilidade do Comitê de Tecnologia e Segurança da Informação:**

7.10.1. Exercer as competências estabelecidas na legislação vigente, com foco em:

7.10.1.1. Apoiar a implementação e o cumprimento da Política de Segurança da

Informação, visando garantir a confidencialidade, a integridade e a disponibilidade das informações processadas, armazenadas ou custodiadas pelas unidades administrativas da SEF/MG.

8. VEDAÇÕES

Não é permitido:

8.1. Fornecer a senha de acesso aos sistemas e serviços da SEF/MG a outro usuário.

8.2. Acessar qualquer sistema, aplicação ou serviço da SEF/MG por meio da identificação de outro usuário.

8.3. Utilizar senhas compartilhadas para acesso a qualquer sistema, aplicação ou serviço da SEF/MG, exceto nos casos em que seja impossível a implantação de senha individual, desde que devidamente autorizado pela STI.

8.4. Violar os lacres das estações de trabalho.

8.5. Alterar a configuração de hardware e de software da estação de trabalho.

8.6. Movimentar as estações de trabalho, periféricos e ou equipamentos de rede sem autorização da STI.

8.7. Compartilhar diretórios (pastas) das estações de trabalho sem autorização da STI.

8.8. Realizar o upload de qualquer software licenciado à SEF/MG ou de dados de propriedade da SEF/MG sem a autorização da STI.

8.9. Utilizar software de comunicação instantânea, exceto se autorizado pela STI.

8.10. Utilizar serviços de nuvem pública como DropBox, GoogleDrive, iCloud, entre outros, para armazenar informações da SEF/MG, salvo exceções devidamente autorizadas pela STI.

8.11. Armazenar, acessar e ou repassar, utilizando os equipamentos e/ou serviços disponibilizados pela SEF/MG, arquivos:

8.11.1. Que contenham conteúdo ilícito, tais como pedofilia, pornografia, racismo, entre outros.

8.11.2. Cujo conteúdo implique na violação de quaisquer leis ou incentive crimes.

8.12. Tentar, por qualquer meio, causar a indisponibilidade dos serviços, servidores ou recursos de rede.

8.13. Desabilitar o antivírus ou realizar qualquer alteração nas configurações da ferramenta.

8.14. Utilizar outra ferramenta de antivírus que não a homologada para uso pela STI.

8.15. Ao visitante:

8.15.1. Conectar equipamentos particulares à rede fazendária.

8.15.2. Acessar as estações de trabalho da SEF/MG sem autorização do responsável pela unidade.

9. PENALIDADES

9.1. O não cumprimento desta política por parte dos usuários sujeitará o responsável à suspensão temporária do acesso aos recursos informacionais e de comunicação desta Secretaria e às penalidades previstas em Lei.

10. DISPOSIÇÕES FINAIS

10.1. Os detalhamentos das regras gerais estabelecidas nesta política estão descritos nos procedimentos operacionais padrão - POP, regulamentos e instruções de trabalho classificados por tema e disponíveis no Portal da STI na Intranet.

10.2. Dúvidas, críticas e sugestões referentes a esta Política de Segurança da Informação devem ser encaminhadas à Divisão de Segurança da Informação da Diretoria de Governança Tecnológica (DSI/DGT/STI).

10.3. Todo caso de exceção às determinações da Política de Segurança da Informação deve ser analisado de forma individual, aplicável apenas ao caso concreto, dentro dos limites e motivos que o fundamentaram.

10.4. Esta Política de Segurança da Informação entra em vigor na data de sua publicação e deverá ser revista no prazo máximo de 03 (três) anos.

11. APROVAÇÃO E ASSINATURAS

Os membros do Comitê Estratégico de Governança estabelecem e aprovam esta Política de Segurança da Informação.

Secretaria de Estado de Fazenda de Minas Gerais