Ministério da Fazenda
Procuradoria-Geral da Fazenda Nacional

Política de Segurança da Informação e Privacidade dos Dados

ORIGEM

Coordenação-Geral de Tecnologia da Informação - CGTI/PGFN

REFERÊNCIA NORMATIVA E BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27001:2006
ABNT NBR ISO/IEC 27002: (17799:2005)
ABNT NBR ISO/IEC 23894:2023
LEI GERAL DE PROTEÇÃO DE DADOS (LGPD 13.709/18)
ABNT NBR ISO/IEC 27017:2016
INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021 GSI/PR

CAMPO DE APLICAÇÃO

Esta política se aplica no âmbito da Procuradoria-Geral da Fazenda Nacional

SUMÁRIO

1 OBJETIVO

1.1 A Política de Segurança da Informação e Privacidade dos Dados objetiva estabelecer princípios, diretrizes, responsabilidades e competências para implementar a Gestão de Segurança da Informação (GSI) e garantir a privacidade dos dados na PGFN.

1.2 A GSI da PGFN tem como intuito a aplicação de controles - processos, políticas, práticas, ações - para assegurar a autenticidade, confidencialidade, integridade, disponibilidade e irretratabilidade da informação, conforme definidos na seção 5 desta Política, seja em ambiente físico ou em ambiente computacional em nuvem..

1.3 A GSI da PGFN se aplica, no que couber, no relacionamento com órgãos públicos ou entidades privadas.

1.4 A Política de Segurança da Informação e Privacidade dos Dados abrange as Procuradorias Regionais da Fazenda Nacional, suas unidades e o Órgão Central da Procuradoria-Geral da Fazenda Nacional.

1.5 Os princípios, diretrizes, responsabilidades e competências de segurança da informação previstos nesta Política aplicam-se a todos os colaboradores que tenham acesso às informações e aos recursos de tecnologia da informação da PGFN.

1.6 Os instrumentos normativos gerados a partir desta Política aplicam-se a todos os colaboradores que tenham acesso às informações e aos recursos de tecnologia da informação da PGFN.

2 CONCEITOS E DEFINIÇÕES

3 Para os efeitos desta política, aplicam-se os seguintes termos e definições:

- **Agente Público**: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
- **Ambiente computacional em nuvem**: ambiente cujos recursos físicos não são gerenciados ativamente pelo órgão. Podem ser de nuvem privada ou nuvem pública.
- **Ameaça**: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;
- **Ativos de Informação**: os meios de armazenamento, de transmissão e de processamento, os sistemas de informação, bem como os locais onde se encontram esses meios, e as pessoas que a eles tem acesso;
- **Capacitação, Conscientização, Sensibilização em SI:** habilitação no conhecimento de segurança da informação e comunicações que permite a um indivíduo aplicá-lo na rotina pessoal e profissional, atuar como multiplicador do tema e utilizar seus conceitos e procedimentos na organização;
- **Colaboradores:** procuradores, servidores, terceirizados, consultores, auditores, estagiários, agentes públicos, que detenham acesso aos ativos de informação da PGFN;
- **Conformidade em SI**: cumprimento da legislação, normas e procedimentos relacionados à SI da PGFN;
- **Controle**: quaisquer processos, políticas, práticas, ações que modificam um risco de SI;

- **Diretriz:** descrição de uma forma específica para atingir algo, mas de forma menos detalhada do que um procedimento.
- **Evento de Segurança da Informação**: ocorrência identificada por um sistema, serviço ou monitoramento indicando uma possível violação da política de segurança da informação ou uma falha de controles, bem como uma situação previamente desconhecida que possa ser relevante para a segurança da informação;
- **Gestão de SI**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;
- **Incidente**: um ou mais Eventos de Segurança da Informação, não desejáveis ou inesperados, que tenham uma significativa probabilidade de comprometer as operações da PGFN e ameaçar a segurança da informação;
- **Política de Segurança da Informação e Privacidade**: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da gestão de segurança da informação, considerando a privacidade dos dados;
- **Risco de SI**: potencial associado à probabilidade de exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto para a organização;
- **Segurança da Informação (SI):** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- **Sistema de Gestão da Segurança da Informação da PGFN (SGSI-PGFN):** é o conjunto de processos e procedimentos, baseado em normas e na legislação vigente, que uma organização deve implementar para prover segurança no uso de seus ativos tecnológicos de modo a preservá-los quanto aos aspectos de disponibilidade, integridade, confidencialidade e autenticidade, independentemente do meio em que se encontram.;
- **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da SI;
- **Termo de Responsabilidade**: termo assinado pelo colaborador no qual concorda em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que acessar, bem como assumir responsabilidades decorrentes de tal acesso;
- **Tratamento da Informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
- **Valor do Ativo de Informação**: valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado; e
- **Vulnerabilidade**: fraqueza em um ativo ou em um controle que pode ser explorada por uma ou mais ameaças.

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais para o uso dos dispositivos móveis pela APF, devem considerar, prioritariamente, os requisitos legais e a estrutura do órgão ou entidade, além de estarem alinhadas à Política de Segurança da Informação e Comunicações do órgão ou entidade, a qual deve contemplar recomendações sobre o uso desses dispositivos.

4.2 As ações de Gestão da Segurança da Informação (GSI) da PGFN são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

4.3 Confidencialidade: a informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de acesso e uso apenas às pessoas físicas, sistemas, órgãos ou entidades para os quais ela é destinada;

4.4 Integridade: a informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais;

4.5 Disponibilidade: a informação gerada ou adquirida deve estar disponível às pessoas físicas, sistemas, órgãos ou entidades no momento em que eles necessitam dela para qualquer finalidade;

4.6 Autenticidade: garantia de que a pessoa física, sistema, órgão ou entidade identificada em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e de a mensagem ou informação não foi alterada após o seu envio ou validação;

4.7 Irretratabilidade: garantia de que a informação possua a identificação do seu emissor, que o autentica como o autor da informação, garantindo-se o não repúdio;

4.8 Informação como ativo – a informação é um ativo que, como qualquer outro ativo necessário às atividades laborais, tem valor para a PGFN e consequentemente necessita ser adequadamente protegido;

4.9 Garantia da privacidade – respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem das pessoas e instituições, nos termos da lei.

4.10 Continuidade dos trabalhos - garantia de continuidade dos processos e serviços essenciais para o funcionamento da PGFN;

4.11 Conformidade: das normas derivadas dessa Política e das ações de segurança da informação com a legislação e regulamentos aplicáveis;

4.12 Educação e comunicação: como alicerces fundamentais para o fomento da cultura em segurança da informação na PGFN.

5 DIRETRIZES GERAIS

5.1 As diretrizes constituem os principais pilares da Gestão de Segurança da Informação (GSI) e garantia da privacidade dos dados, norteando a elaboração de normas complementares no âmbito da PGFN.

5.2 As Políticas ou normas complementares de segurança da informação deverão observar as diretrizes da Política de Segurança da Informação e Privacidade dos Dados, descritas nas seções seguintes, por temas de Segurança da Informação.

5.3 Fica instituído o Sistema de Gestão de Segurança da Informação - SGSI-PGFN com o objetivo de identificar as necessidades da PGFN quanto aos requisitos de segurança da informação e implementar o processo de gestão de riscos de segurança da informação.

5.4 O Sistema de Gestão de Segurança da Informação da PGFN tem a seguinte composição:

5.5 Gestor de Segurança da Informação da PGFN, indicado pelo Comitê Estratégico de TI (CETI-PGFN), aprovado pelo Comitê de Gestão Estratégica (CGE-PGFN);

5.6 Equipe de tratamento e resposta a incidentes em redes computacionais da PGFN; e

5.7 Comitê Estratégico de TI (CETI-PGFN) como Comitê para Gestão em Segurança da Informação.

6 DIRETRIZES PARA CLASSIFICAÇÃO DA INFORMAÇÃO

6.1 A Classificação da Informação objetiva assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a PGFN, e observará as seguintes diretrizes:
6.2 Considerar as necessidades do negócio para compartilhar ou restringir a informação bem como os requisitos legais;
6.3 Classificar outros ativos além dos ativos de informação, de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo;
6.4 Atribuir aos proprietários de ativos de informação a responsabilidade por sua classificação;
6.5 Estabelecer um esquema de classificação que inclua convenções para classificação e critérios para análise crítica da classificação ao longo do tempo;
6.6 Alinhar a Classificação da Informação (esquema de classificação) com a norma complementar de Controle de Acesso;
6.7 Incluir a Classificação da Informação nos processos da organização;
6.8 Indicar, nos resultados da Classificação, o valor dos ativos em função da sua sensibilidade e criticidade para a PGFN, em termos da confidencialidade, integridade e disponibilidade, bem como atualizar a Classificação de acordo com as mudanças do valor do ativo de informação, sensibilidade e criticidade ao longo do seu ciclo de vida.

7 DIRETRIZES PARA TRATAMENTO DE DADOS E INFORMAÇÃO

7.1 Tratamento de Dados e Informação objetiva assegurar a segurança da informação nas atividades de produção, recepção, categorização, utilização, reprodução, transmissão, distribuição, acesso, transporte, arquivamento, armazenamento, avaliação e destinação (eliminação ou guarda permanente), bem como controle da informação restrita ou sigilosa e observará as seguintes diretrizes:

7.2 Estabelecer Política de Governança e Gestão de Dados, Informação e Conhecimento da PGFN, que contemple a segurança no processo de transformação de dados em informações, depois em decisões e ações que resultam em valor agregado para as áreas de negócios da PGFN;

7.3 Considerar como de propriedades da PGFN os dados, as informação e o conhecimento produzidos no exercício das funções da PGFN;

7.4 Incluir no conceito de ativos de informação corporativos da PGFN os meios de armazenamento, transmissão e processamento, os sistemas de informação, os locais onde se encontram esses meios e as pessoas que a eles tem acesso;

7.5 Considerar nas atividades de gestão de dados:

a) Todos os dados e informações produzidos, custodiados, mantidos ou recebidos no âmbito da PGFN;
b) Todos os dados armazenados em infraestrutura própria, terceira ou nuvem;
c) Os processos de captação, geração, armazenamento, integração, utilização, compartilhamento, divulgação, retenção e descarte de dados e informações;
d) Os sistemas de informação, análise dos dados e aplicações desenvolvidos, adquiridos, instalados ou utilizados;

7.6 Não considerar na Classificação, nem no Tratamento das informações, os seguintes dados pessoais, quando vinculados a uma pessoa natural:

a) Dados sobre origem racial ou étnica;
b) Dados sobre convicção religiosa;
c) Dados sobre opinião política;
d) Dados sobre filiação a sindicato ou a organização de caráter religioso, filosófico ou político;
e) Dados referentes à saúde ou à vida sexual;
f) Dados genéticos ou biométricos.

7.7 Atenção aos princípios e obrigações estabelecidos na Lei Geral de Proteção de Dados (LGPD) - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

8 DIRETRIZES PARA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

8.1 A Gestão de Incidentes de SI deverá assegurar um enfoque consistente e efetivo, incluindo a comunicação sobre fragilidades e eventos de segurança da informação, e observará as seguintes diretrizes:

a) Estabelecer as responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação;
b) Estabelecer acordos com a alta administração para garantir que as pessoas responsáveis pela gestão dos incidentes de segurança da informação entendem as prioridades da organização para tratar com os incidentes de segurança da informação;
c) Estabelecer canais apropriados de comunicação da direção para relato dos eventos de segurança da informação;
d) Garantir que os funcionários e partes externas que usam os sistemas e serviços de informação da PGFN sejam instruídos a registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços;
e) Estabelecer um ponto de contato que avalie cada evento de segurança da informação usando uma escala de classificação de incidentes e eventos de segurança da informação, para decidir se é recomendado que o evento seja classificado, bem como priorizado, como um incidente de segurança da informação;
f) Estabelecer base de conhecimento para registro de análise e resolução dos incidentes de segurança da informação, com a finalidade de se reduzir a probabilidade ou o impacto de incidentes futuros;
g) Definir procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências, levando-se em conta a cadeia de custódia, a segurança da evidência, das pessoas, papéis e responsabilidades dos envolvidos, competência do pessoal, documentação, resumo do incidente.

9 DIRETRIZES PARA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

9.1 A Gestão de Riscos de Segurança da Informação da PGFN observará o Plano Estratégico Institucional e as normas internas referentes à Gestão de Riscos Corporativos da PGFN, e observará as seguintes diretrizes:

a) Estabelecer Política de Gestão de Riscos de SI;
b) Considerar a aplicação das diretrizes da norma ABNT NBR ISO/IEC 27005 na elaboração da Política de Gestão de Riscos de SI, bem como nos trabalhos da tecnologia da informação (TI) da PGFN na avaliação de riscos, tratamentos de riscos, aceitação de riscos, comunicação de riscos, monitoramento e análise crítica dos riscos.

10 DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DE CONTINUIDADE

10.1 A Segurança da Informação deverá ser considerada na garantia da recuperação das atividades da PGFN no caso de ataques cibernéticos que possam comprometer os dados e continuidade dos trabalhos da PGFN.

10.2 Deve ser estabelecida a Política de Cópias de Segurança (Backup) da PGFN que define:

a) Os acordos da área de TI com a área de negócio responsável dos dados e/ou sistemas;
b) Documentação de quais dados (bases de dados, sistemas de arquivos, imagens de servidores) serão feitos os backups;
c) Periodicidades (diária, semanal, mensal);
d) Tipos (completo, diferencial ou incremental);
e) Quantidades de cópias;
f) Locais de armazenamento;
g) Tempos de retenção das cópias;
h) Requisitos específicos de segurança em função dos dados copiados (controle de acesso, localização remota, criptografia);
i) Definição dos planos de backup para dados e /ou sistemas
j) Realizar cópias de segurança (backups) integrais dos sistemas críticos da PGFN, de modo a permitir sua rápida recuperação em caso de necessidade;
k) Realizar, periodicamente, testes de restauração (restore) das cópias de segurança (backups) da PGFN, de modo a atestar seu funcionamento em caso de necessidade;
l) Proteger adequadamente as cópias de segurança (backups) da PGFN, por meio de mecanismos de controle de acesso físico e lógico;
m) Armazenar as cópias de segurança (backups) da PGFN em ao menos um destino não acessível remotamente;
n) Estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa;
o) Garantir a verificação da validade e eficácia dos controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares;
p) Assegurar, por meio de redundância suficiente, a disponibilidade dos recursos de processamento da informação;

11 DIRETRIZES PARA REGISTRO E MONITORAMENTO DE EVENTOS

11.1 O Registro e Monitoramento de Eventos garantirá que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares, observando-se as seguintes diretrizes:

a) Garantir que, por meio de medidas apropriadas de proteção de privacidade, os registros (log) de eventos protejam os dados confidenciais e informações de identificação pessoal;
b) Garantir que os administradores de sistemas não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades;
c) Garantir que os registros de eventos (log) e seus recursos sejam protegidas contra acesso não autorizado e adulteração;
d) Considerar a utilização de sistema de detecção de intrusos gerenciado fora do controle dos administradores de rede e de sistemas para monitorar a conformidade das atividades dos administradores dos sistemas e de rede;
e) Garantir que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.

12 DIRETRIZES PARA AUDITORIA DE CONFORMIDADE

12.1 A Auditoria de Conformidade visa evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à SI e de quaisquer requisitos de segurança e observará as seguintes diretrizes:

a) Identificar, documentar e manter, para cada sistema de informação da PGFN, os requisitos legislativos, estatutários, regulamentares e contratuais pertinentes;
b) Estabelecer procedimentos apropriados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários;
c) Garantir a privacidade e proteção das informações de identificação pessoal conforme requerido por legislação e regulamentação pertinente, quando aplicável;
d) Garantir que os controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes;

13 CONTROLE DE ACESSO À INFORMAÇÃO

13.1 O Controle de Acesso à Informação deverá limitar o acesso aos dados, à informação e aos recursos de processamento, observando-se a privacidade e as seguintes diretrizes:

a) Estabelecer Política de Controle de Acesso à Informação, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios da PGFN;
b) Estabelecer normativos de uso dos recursos de processamento da informação, que serão anexos da Política de Controle de Acesso à Informação;
c) Observar as diretrizes para “Segurança física e do ambiente” estabelecidas nesta política;
d) Garantir a segregação de funções de controle de acesso, como pedido de acesso, autorização de acesso, administração de acesso;
e) Manter arquivo dos registros de todos os eventos significativos, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta;
f) Aplicar os princípios de controle de acesso “necessidade de conhecer” e “necessidade de uso”.
g) O princípio “necessidade de conhecer” refere-se a garantir o acesso somente à informação que se necessita para desempenhar as tarefas.

h) O princípio "necessidade de uso" refere-se à permissão para acessar os recursos de processamento da informação (equipamentos de TI, aplicações, procedimentos, salas) necessários para desempenhar a tarefa, função e papel.

14 DIRETRIZES PARA A SEGURANÇA NAS COMUNICAÇÕES

14.1 A Segurança nas Comunicações garantirá a proteção das informações em redes e dos recursos de processamento da informação que os apoiam, observando-se as seguintes diretrizes:

a) Garantir o gerenciamento e controle das redes para proteger as informações nos sistemas e aplicações;
b) Identificar e incluir, em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados, mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede;
c) Garantir que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes;
d) Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas;
e) Estabelecer acordos para transferência segura de informações entre a PGFN e partes externas;
f) Garantir, por meio de norma específica, a proteção das informações que trafegam em mensagens eletrônicas, bem como estabelecer regras de acesso e utilização de correio eletrônico;

15 DIRETRIZES PARA A SEGURANÇA EM RECURSOS HUMANOS

15.1 A Segurança em Recursos Humanos deverá assegurar que colaboradores (procuradores, servidores, terceirizados, colaboradores, consultores, auditores, estagiários) ou partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados, observando-se as seguintes diretrizes:

a) Assegurar que os colaboradores da PGFN e partes externas estejam conscientes e cumpram as suas responsabilidades com relação à SI;
b) Garantir que todos os colaboradores da PGFN e, quando pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções;
c) Estabelecer um processo disciplinar formal, implantado e comunicado, para tomar ações contra agentes públicos que tenham cometido uma violação de SI.
d) Proteger os interesses da PGFN como parte do processo de mudança ou encerramento da contratação de funcionário.
e) Quando um agente público for alocado para desempenhar o papel de SI, a PGFN observará os acórdãos do TCU e certificará se o candidato tem a competência necessária para executar as atividades de SI.

16 DIRETRIZES PARA GESTÃO DE ATIVOS E VULNERABILIDADES

16.1 Os ativos serão gerenciados de acordo com diretrizes, estratégias e procedimentos estabelecidos pela CGTI em alinhamento com a política de gerenciamento de vulnerabilidades.

16.2 Será estabelecida a política e procedimentos de gestão de vulnerabilidades, que visam atender às diretrizes:

a) Garantir que que o inventário de ativos seja completo, atualizado, consistente e alinhado com outros inventários;
b) Classificar cada um dos ativos identificados, de acordo com as normas, processos ou procedimentos derivados das diretrizes de “Classificação e Tratamento da Informação”;
c) Identificar os respectivos proprietários de cada ativo;
d) Garantir que que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo;
e) Regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades.
f) Ações e boas práticas que devem ser observadas para minimizar a ocorrência de vulnerabilidades nos ativos da PGFN.

17 DIRETRIZES PARA GESTÃO DE RISCOS NO USO DE INTELIGÊNCIA ARTIFICIAL

17.1 O uso de ferramentas de inteligência artificial no âmbito da PGFN deve observar as boas práticas de ética e segurança. Devem ser observados os preceitos estabelecidos na Lei Geral de Proteção de Dados (Lei Nº 13.709/2018) e os normativos ABNT NBR ISO/IEC, em especial a norma 23894, que trata de gestão de risco no uso de Inteligência Artificial.

17.2 A CGTI e CETI-PGFN estabelecerão política de gestão de risco e segurança no uso de inteligência artificial, considerando, no mínimo:

a) Avaliação de riscos: Avaliação de riscos associados ao uso de sistemas de inteligência artificial em seus mais variados tipos, como os modelos generativos, modelos de LLM (Large Language Models), modelos baseados em regras, modelos especialistas, modelos de aprendizado de máquina, entre outros.
b) Responsabilização: responsabilidade pelas ações e decisões dos sistemas de inteligência artificial ou as ações e decisões tomadas em decorrência do uso desses.
c) Qualidade e Proteção de dados: critérios de qualidade, atualidade e relevância dos dados para o fim a que se destinam assim como critérios de proteção dos dados utilizados para treinamento dos modelos de IA.
d) Transparência e explicabilidade: trata da transparência dos sistemas de IA consiste em fornecer informações adequadas sobre um sistema, a fim de permitir avaliar o desenvolvimento, o funcionamento, a aplicação e a utilização de sistemas de IA em relação aos seus objetivos.
e) Atualizações e manutenção: trata da atualização e modificação nos sistema de IA a fim de corrigir defeitos ou ajustar-se a novos requisitos. Devem ser considerados os critérios de treinamento e manutenção de sistemas que usam aprendizado de máquina a fim de que os sistemas permaneçam seguros e eficazes ao longo do tempo.
f) Treinamento Ético e Responsável: Garantir que os profissionais envolvidos no desenvolvimento, implementação e uso de sistemas de IA tenham treinamento em ética e responsabilidade em IA.

18 DIRETRIZES PARA OS CONTROLES CRIPTOGRÁFICOS

18.1 Os Controles Criptográficos deverão assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação, observando-se as seguintes diretrizes:

18.2 Estabelecer o uso de controles criptográficos para a proteção da informação;

a) Estabelecer o uso, proteção e ciclo de vida das chaves criptográficas;
b) Garantir que que os equipamentos utilizados para gerar, armazenar e guardar as chaves sejam fisicamente protegidos;
c) Considerar a norma ISO/IEC 11770 para gestão de chaves.

19 DIRETRIZES PARA A SEGURANÇA FÍSICA E DO AMBIENTE

19.1 A Segurança Física e do Ambiente prevenirá o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da PGFN, observando-se as seguintes diretrizes:

a) Definir perímetros de segurança para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis;
b) Considerar as diretrizes relacionadas com "Perímetro de segurança física" da norma NBR ISO/IEC 27002;
c) Proteger as áreas seguras por meio de controles apropriados de entrada, para assegurar que somente pessoas autorizadas tenham acesso permitido;
d) Manter e monitorar uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acessos;
e) Garantir a proteção física contra desastres naturais, ataques maliciosos ou acidentes;
f) Incluir o controle dos funcionários, fornecedores e partes externas que trabalham em áreas seguras.

20 DIRETRIZES PARA A GESTÃO DE MUDANÇAS

20.1 A gestão de mudanças controlará as mudanças na PGFN, nos processos, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, observando-se as seguintes diretrizes:

a) identificar e registrar as mudanças significativas;
b) Planejar e realizar testes das mudanças;
c) Avaliar impactos potenciais, incluindo impactos de segurança da informação;
d) Estabelecer procedimento formal de aprovação das mudanças propostas;
e) Verificar se os requisitos de SI foram atendidos;
f) VI - Comunicar os detalhes das mudanças para todas as pessoas relevantes;
g) Estabelecer procedimentos de recuperação, incluindo procedimentos e responsabilidades para interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados;
h) Garantir um processo emergencial de mudança para permitir uma implementação rápida e controlada de mudanças, necessárias para resolver um incidente.
i) Os procedimentos relacionados com mudanças terão responsabilidades de gestão formais, bem como registro de auditoria, para garantir que haja um controle satisfatório de todas as mudanças.

21 DIRETRIZES PARA A GESTÃO DA CAPACIDADE

21.1 A gestão da Capacidade garantirá que a utilização dos recursos seja monitorada e ajustada, e as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido dos sistemas, levando-se em conta a criticidade do negócio do sistema em questão.

22 DIRETRIZES PARA À AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

22.1 A Aquisição, Desenvolvimento e Manutenção de Sistemas garantirá que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação da PGFN, observando-se as seguintes diretrizes:

a) Garantir que os requisitos relacionados com SI sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes;
b) Garantir que os contratos com os fornecedores atendam aos requisitos de segurança identificados e, caso não se atenda algum requisito especificado, aplicar a gestão de riscos para aplicação de controles associados, antes da contratação;
c) Considerar as normas ABNT NBR ISO IEC 27005 e a ABNT NBR ISO 31000, as quais fornecem diretrizes sobre o uso de processos de gestão de riscos, para identificar controles que atendam aos requisitos de SI;
d) Garantir que a SI está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação;
e) Garantir a supervisão e monitoramento das atividades de desenvolvimento de sistemas terceirizado.

23 DIRETRIZES PARA O RELACIONAMENTO NA CADEIA DE SUPRIMENTOS

23.1 O Relacionamento na Cadeia de Suprimentos garantirá a proteção dos ativos da PGFN que são acessíveis pelos fornecedores, observando-se as seguintes diretrizes:

a) Estabelecer Política para que a PGFN identifique e exija os controles de SI para tratar, especificamente, do acesso do fornecedor às informações da organização;
b) Deverão ser consideradas as diretrizes da norma ABNT NBR ISO/IEC 27002 para o estabelecimento da Política de SI no relacionamento com os fornecedores.

24 DIRETRIZES DE SEGURANÇA PARA O USO DE DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

24.1 A Gestão de dispositivos móveis e trabalho remoto garantirá a publicação de uma Política com medidas que apoiem a segurança da informação no gerenciamento de riscos decorrentes do uso de dispositivos móveis, para prover a segurança das informações no trabalho remoto e no uso de dispositivos móveis, observando-se as seguintes diretrizes:

a) Cuidados especiais devem ser tomados para assegurar que as informações do negócio não sejam comprometidas em uso de dispositivos móveis.
b) A Política de dispositivos móveis levará em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos.
c) A Política para uso de dispositivos móveis considerará a conscientização dos colaboradores para garantir
d) O controle de acesso por meio de conexões criptografadas;
e) A proteção contra códigos maliciosos;
f) A prática de backups;
g) O uso seguro dos serviços web e aplicações web.

24.2 O trabalho remoto e uso de dispositivos móveis deverá estabelecer medidas, controles de proteção, para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos, considerando:

a) A utilização de técnicas de criptografia;
b) O uso de informação de autenticação secreta;
    - Garantir que sejam programados treinamentos para as pessoas que usam dispositivos móveis, como forma de aumentar a conscientização quanto aos riscos adicionais decorrentes desta forma de trabalho.
    - Considerar a provisão de equipamentos apropriados às atividades de trabalho remoto, com a finalidade de evitar o uso de equipamentos de propriedade particular que não estejam sob controle da PGFN;
    - Definir o trabalho permitido, o período de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços que o usuário do trabalho remoto está autorizado a acessar;
    - Conscientização quanto a regras e diretrizes sobre o acesso de familiares e visitantes ao equipamento e à informação;
    - Considerar a provisão de suporte e manutenção de hardware e software proprietários da PGFN;
    - Garantir a auditoria e monitoramento da segurança;
    - Considera-se trabalho remoto todas as formas de trabalho fora das dependências das unidades da PGFN, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: “ambientes de telecommuting”, “local de trabalho flexível”, “ trabalho remoto” e “trabalho virtual”.

25 POLÍTICA DE MESA LIMPA E TELA LIMPA

25.1 A Política de mesa limpa e tela limpa levará em conta a classificação da informação, requisitos contratuais e legais, e o risco correspondente e aspectos culturais da PGFN, observando-se as seguintes diretrizes:

a) As informações sensíveis ou críticas, em papel ou em mídia de armazenamento eletrônicas, serão guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando a unidade escritório está desocupada;
b) Os computadores e terminais devem ser mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegida por tela de bloqueio, senhas ou outros controles, quando não usados;
c) Documentos que contêm informação sensível ou classificada devem ser removidos de impressoras imediatamente;
d) A Política deverá considerar a redução do risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho.

26 PROCEDIMENTOS PARA TRANSFERÊNCIA DE INFORMAÇÕES

26.1 Procedimentos e controles de transferências formais, deverão garantir a proteção da transferência de informações, por meio do uso de todos os tipos de recursos de comunicação, observando-se as seguintes diretrizes:

a) Procedimentos para proteger a informação transferida contra interceptação, cópia, modificação, desvio e destruição;
b) Procedimentos para detecção e proteção contra código malicioso que pode ser transmitido através do uso de recursos eletrônicos de comunicação;
c) Procedimentos para proteção de informações eletrônicas sensíveis que sejam transmitidas na forma de anexos;
d) Norma para o uso aceitável dos recursos eletrônicos de comunicação;
e) Garantir o uso de técnicas de criptografia para proteger a confidencialidade, a integridade e a autenticidade das informações;
f) Estabelecer controles e restrições associados à retransmissão em recursos de comunicação como, por exemplo, a retransmissão automática de mensagens eletrônicas (e-mails) para endereços externos;
g) Orientar as pessoas para adotar precauções apropriadas não revelando informações confidenciais;
h) Conscientizar os colaboradores para não manter conversas confidenciais em locais públicos, escritórios abertos, canais de comunicação inseguros e locais de reunião.
i) Garantir que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas;
j) Garantir a proteção das mensagens contra acesso não autorizado, modificação ou negação de serviço, combinado com o esquema de classificação adotado pela organização;
k) Estabelecer controles para aprovação prévia para o uso de serviços públicos externos tais como sistemas de mensagens instantâneas, redes sociais e compartilhamento de arquivos;
l) Conscientizar os colaboradores envolvidos na transferência de informações para estarem cientes das práticas de segurança e das ameaças potenciais, como phishing e engenharia social.

27 PRIVACIDADE DOS DADOS

27.1 A Gestão da Privacidade dos Dados observará os preceitos estabelecidos na Lei Geral de Proteção de Dados (LGPD) assim como os princípios da finalidade, adequação, necessidade, responsabilização e prestação de contas, bem como as seguintes diretrizes:

a) Assegurar a preservação da intimidade e privacidade das pessoas naturais, nos termos da lei;
b) Assegurar a proteção dos dados pessoais e a preservação do sigilo das pessoas jurídicas, nos termos da lei;
c) Respeitar a privacidade, à inviolabilidade da intimidade, da honra e da imagem das pessoas e instituições, nos termos da lei;
d) Não realizar tratamento de dados para fins discriminatórios, ilícitos ou abusivos;

27.2 Não realizar tratamento de dados, quando os dados vinculados a uma pessoa natural forem:

a) dados sobre origem racial ou étnica;
b) dados sobre convicção religiosa;
c) dados sobre opinião política;
d) dados sobre filiação a sindicato ou a organização de caráter religioso, filosófico ou político;
e) dados referentes à saúde ou à vida sexual;
f) dados genéticos ou biométricos;

27.3 Quanto ao tratamento de dados:

a) A coleta e armazenamento de dados deve estar fundamentada na necessidade de uso e na previsão legal para coleta, armazenamento e uso;
b) Quando se tratarem de dados pessoais, poderão ser coletados, desde que sejam fornecidos com o consentimento do titular, ou, ainda, que a coleta seja permitida com fundamento em outra base legal prevista em lei;
c) A utilização dos dados deve ser feita exclusivamente para o propósito que foram coletados, não sendo permitido o uso ou compartilhamento para fins diversos ao original;
d) Os titulares dos dados podem exercer seus direitos previstos na Lei Geral de Proteção de Dados, para tal, será disponibilizado um canal de contato divulgado no portal da PGFN;
e) Incidentes de segurança que devem ser comunicados à Autoridade Nacional de Proteção de Dados, em conformidade com o disposto na Lei Geral de Proteção de Dados.

28 POLÍTICA DE USO DE ESTRUTURA DE NUVEM PÚBLICA

28.1 O uso de estrutura soluções de computação em nuvem no âmbito da PGFN deve seguir os requisitos mínimos de segurança da informação, alinhados à INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021 do GSI:

a) Requisitos para a transferência de serviços para um provedor de serviço de nuvem;
b) Requisitos de implementar atualizações e gerenciamento de vulnerabilidades;
c) Requisitos de gerenciamento de identidades e de registros (logs);
d) Requisitos de uso de recursos criptográficos;
e) Requisitos de segregação de dados e da separação lógica;
f) Requisitos de gerenciamento da nuvem e segurança;
g) Requisitos de tratamento da informação;

28.2 Será estabelecida, em decorrência desta política, a Política de Segurança em Nuvem no âmbito da PGFN.

29 COMPETÊNCIAS E RESPONSABILIDADES

29.1 Todos os colaboradores das unidades da PGFN são responsáveis:

a) Por conhecer os princípios, diretrizes e responsabilidades desta política;
b) Por implementar ações de Segurança da Informação e garantia da Privacidade dos Dados, observando de forma específica as atribuições pertinentes a cada cargo e/ou função;
c) Pela segurança dos ativos, credenciais ou contas de acesso, e processos que estejam sob sua responsabilidade e por todos os atos executados com sua identificação;
d) Comunicar à Coordenação-Geral de Tecnologia da Informação do Diretoria de Gestão Corporativa da PGFN sobre falhas ou vulnerabilidades porventura identificadas nos ativos de informação da PGFN;
e) É proibida a exploração de falhas ou vulnerabilidades porventura existentes nos ativos de informação da PGFN.

29.2 Compete ao Gestor de Segurança da Informação da PGFN:

a) Representar a PGFN no Comitê Estratégico de Segurança da Informação do Ministério da Fazenda;
b) Apreciar e aprovar propostas do Ministério da Fazenda, quanto à organização do Sistema de Gestão de Segurança da Informação, observando as peculiaridades da PGFN;
c) Apreciar e encaminhar as propostas de Políticas e normativos derivados dessa política;
d) Integrar os trabalhos da equipe de tratamento e resposta a incidentes em redes computacionais da PGFN;
e) Gerenciar a implementação e consolidação das ações de Segurança da Informação e garantia da Privacidade dos Dados

29.3 Compete ao Comitê Estratégico de TI (CETI-PGFN) as seguintes atribuições:

a) Assessorar na implementação e consolidação das ações de Segurança da Informação e garantia da Privacidade dos Dados;
b) Indicar o Gestor de Segurança da Informação da PGFN;
c) Constituir equipes de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação e garantia da Privacidade dos Dados;
d) Propor normas e procedimentos relativos à Segurança da Informação e garantia da Privacidade dos Dados no âmbito da PGFN, inclusive alterações à esta política;
e) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;
f) Promover a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização e capacitação;
g) Caberá a cada membro do Comitê Estratégico de TI incluir em pauta as questões de Segurança da Informação relativas à sua Adjuntoria ou Departamento de origem.

29.4 Compete à Coordenação-Geral de Tecnologia da Informação da Diretoria de Gestão Corporativa da PGFN, conforme processos da cadeia de valor de "Governança e Gestão de TI" da PGFN:

29.5 Quanto à governança de TI, planejar, elaborar, implementar e monitorar:
a) Política de Governança e Gestão de Dados, Informação e Conhecimento da PGFN;
b) Política de Gestão de Riscos de Segurança da Informação da PGFN;
c) Política de Cópias de Segurança (Backup) da PGFN
d) Política de Controle de Acesso da PGFN;
e) Política de Relacionamento na Cadeia de Suprimentos;
f) Política de Dispositivos móveis e trabalho remoto;
g) Política de mesa limpa e tela limpa;
h) Política de gestão de vulnerabilidades.

29.6 Quanto à gestão de soluções de TI:
a) Definir, instituir e sustentar processos de TI e ferramentas para a implementação e monitoramento das Políticas supracitadas;
b) b) Avaliar, tratar, aceitar, comunicar, monitorar e analisar criticamente os riscos de segurança da informação.

29.7 Quanto à gestão de segurança da informação:
a) Implantar o Sistema de Gestão da Segurança da Informação da PGFN (SGSI-PGFN), com integração das atividades de gestão de incidentes e de riscos de segurança cibernética, física e organizacional, a fim de que sejam mitigados ou eliminados;
b) Estabelecer canais apropriados de comunicação entre as unidades da PGFN para relato dos eventos de segurança da informação;
c) Estabelecer as responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação;
d) Estabelecer base de conhecimento para registro de análise e resolução dos incidentes de segurança da informação, com a finalidade de se reduzir a probabilidade ou o impacto de incidentes futuros;

29.8 Compete às unidades de TI da PGFN, inclusive das Procuradorias Regionais da Fazenda Nacional, quanto ao processo da cadeia de valor "gestão de segurança da informação" da PGFN:

a) Liderar projetos de implementação de controles internos nas unidades da PGFN para a gestão de riscos de segurança da informação;
b) Integrar os trabalhos da equipe de tratamento e resposta a incidentes em redes computacionais da PGFN;s ;
c) Realizar o Registro e Monitoramento de Eventos de segurança da informação;
d) Garantir que a utilização dos recursos de TI seja monitorada e ajustada;
e) Garantir que as projeções de recursos de TI sejam feitas para necessidades de capacidade futura, garantindo o desempenho das atividades das unidades da PGFN, levando-se em conta a criticidade do negócio;

30 DAS PENALIDADES

30.1 As ações que violem essa política ou os controles determinados em normas específicas serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor.

31 DAS DISPOSIÇÕES FINAIS

31.1 Os contratos de prestação de serviços e convênios devem contemplar, no que couber, as normas descritas nesta política.

31.2 O Comitê Estratégico de TI (CETI-PGFN) é responsável por indicar o Gestor de Segurança da Informação da PGFN para aprovação do Comitê de Gestão Estratégica (CGE);

31.3 A Coordenação-Geral de Tecnologia da Informação, da Diretoria de Gestão Corporativa da PGFN, é responsável por produzir e implementar as Políticas decorrentes desta Política de Segurança da Informação e Privacidade dos Dados, que deverão ser aprovadas pelo CETI-PGFN.

31.4 A Política de Segurança da Informação e Privacidade dos Dados, bem como todos os instrumentos normativos gerados a partir dela, devem ser revisados, sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal.

32 VIGÊNCIA

32.1 Esta política entra em vigor no primeiro dia útil do mês subsequente à data de publicação da sua aprovação.