Boletim Interno
Procuradoria-Geral do Distrito Federal

Edição n° 08/2026 – Brasília-DF, 27 de fevereiro de 2026.

ATOS DO GABINETE

PORTARIA Nº 2, DE 25 DE FEVEREIRO DE 2026

Aprova a Norma de Segurança da Informação e Comunicação (NoSIC) da Procuradoria-Geral do Distrito Federal e dá outras providências.

O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício das atribuições que lhe conferem os art. 6º, inciso XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE

Art. 1° Aprovar, na forma do Anexo Único desta portaria, a Norma de Segurança da Informação e Comunicação (NoSIC) da Procuradoria-Geral do Distrito Federal (PGDF).

Art. 2° O Comitê Gestor de Tecnologia da Informação (CGTI/PGDF) e o Comitê Gestor de Segurança da Informação e Comunicação (CGSIC/PGDF) poderão, a qualquer tempo, propor mudanças e atualizações na Norma anexa, de modo a assegurar sua constante adequação à Política de Segurança da Informação e Comunicação (POSIC) do Governo do Distrito Federal.

Art. 3° Esta Portaria entrará em vigor na data de sua publicação.

ANEXO ÚNICO

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (NoSIC) DA PROCURADORIA-GERAL DO DISTRITO FEDERAL (PGDF)

CAPÍTULO I

DA INTRODUÇÃO

Art. 1º A Segurança da Informação é um conjunto de ações de proteção aos ativos de informação contra todas as formas de agressões em seu ambiente físico, lógico e humano.

Art. 2º Este documento estabelece diretrizes, princípios, responsabilidades e objetivos para a Norma de Segurança da Informação e Comunicação da Procuradoria-Geral do Distrito Federal (NoSIC/PGDF), a qual deverá ser adotada e cumprida por todos os procuradores, servidores, estagiários, prestadores de serviços e demais usuários que utilizem as informações da instituição, produzidas ou manipuladas por meio de recursos de tecnologia da informação e comunicação.

Art. 3º Esta NOSIC/PGDF é fundamentada nas recomendações do Tribunal de Contas do Distrito Federal (TCDF) e de outros órgãos de controle do Governo do Distrito Federal.

Art. 4º A Segurança da Informação é matéria atinente a todas as atividades da Procuradoria-Geral do Distrito Federal (PGDF), sejam atividades meio ou fim, devendo essa responsabilidade ser compartilhada por todas as suas áreas.

Art. 5º A informação não está apenas nos sistemas informatizados, mas também em papéis, documentos e pessoas. Portanto, para o sucesso desta NoSIC, é necessário contar com o comprometimento de todos os procuradores, gestores, servidores, estagiários, prestadores de serviços e usuários das informações.

Art. 6º Diversas ações e outros normativos de Segurança da Informação serão implementados com o objetivo de padronizar e regrar os processos institucionais da Procuradoria-Geral do Distrito Federal.

CAPÍTULO II

DO OBJETIVO

Art. 7º O objetivo desta Norma é: a) Garantir os direitos individuais e coletivos dos servidores e prestadores de serviços, principalmente à inviolabilidade da sua intimidade e ao sigilo, quando for o caso, das correspondências e comunicações no âmbito da Procuradoria-Geral do Distrito Federal, e b) Proteger os dados, informações, conhecimentos e inteligência produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação no âmbito da Procuradoria-Geral do Distrito Federal.

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 8º Para efeitos desta Norma, adotam-se os seguintes conceitos e definições:

1. Aceitação de Risco: decisão de aceitar um risco. A aceitação pode ser necessária em razão do custo benefício para se proteger um ativo ou devido ao risco residual remanescente após o tratamento de riscos;

2. Ameaça: são agentes ou condições causadoras de incidentes contra ativos. Exploram as vulnerabilidades, ocasionando perda de confidencialidade, integridade ou disponibilidade; Alta Administração: dirigentes máximos da unidade, como Secretários de Estado e Subsecretários;

3. Análise / Avaliação de Risco: processo de identificação de ameaças e vulnerabilidades associadas a um ativo de modo a estimar a probabilidade e o impacto na ocorrência de um incidente;

4. Armazenamento em nuvem: método de armazenamento de dados que permite que servidores e aplicações acessem os dados por meio de sistemas de arquivos compartilhados, utilizando internet pública ou uma conexão de rede privada dedicada;

5. Ativo: é tudo aquilo que tenha valor para a organização e consequentemente exige proteção;

6. Autenticidade: garantia de que o dado ou informação são verdadeiros. É uma propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma pessoa física específica ou por determinado sistema, órgão ou entidade;

7. Backup / Cópia de Segurança: é o processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais;
8. Classificação da Informação: é o processo de identificar e definir níveis e critérios de proteção adequados para as informações de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a importância para a organização;
9. Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
10. Conhecimento: Conjunto de informações consolidadas em armazenamento físico ou lógico;
11. Controle de Acesso: são restrições de acesso a um ativo da organização;
12. Controle de Segurança: são práticas de gestão de risco (políticas, normas, procedimentos ou mecanismos) que podem proteger os ativos contra ameaças, reduzir ou eliminar vulnerabilidades, limitar o impacto de um incidente ou ajudar na sua detecção;
13. Custódia: responsabilidade de se guardar um ativo para terceiros. A custódia não permite automaticamente o direito de acesso ao ativo, nem a capacidade de conceder direito de acesso a outros;
14. Custodiante: indivíduo a quem é dada a custódia de um ativo;
15. Dado: qualquer elemento bruto de informação que representa fatos, observações, valores ou medidas, armazenados em formatos digitais que ainda não foram processados para se tornar informação;
16. Direito de Acesso: privilégio associado a um usuário para ter acesso a um ativo;
17. Diretriz: o que deve ser feito e como, para atender aos objetivos declarados na política ou norma;
18. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
19. Engenharia Social: tentativa de extrair informações de uma vítima, usando informações corretas ou nome de pessoas conhecidas;
20. Forense Computacional: Conjunto de técnicas para coleta e exame de evidências digitais, reconstrução e dados e ataques, identificação e rastreamento de invasores;
21. Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT - Computer Security Incident Response Team): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;
22. Gestão de Continuidade de Negócios: Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos que essas ameaças, se concretizadas, poderiam causar nas operações da instituição, além de fornecer e manter um nível aceitável de serviço frente a rupturas e desafios à operação normal.
23. Gestão de Riscos: Atividade contínua de identificação, análise, tratamento, aceitação e comunicação de riscos;
24. Gestão de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
25. Gestor de área: responsável por qualquer unidade de uma organização, tais como: chefes de núcleo, coordenadores, gerentes, diretores e todos os demais dirigentes que mantêm subordinados sob sua responsabilidade.
26. Gestor de Segurança da Informação e Comunicação: é responsável pelas ações de segurança da informação e comunicações;
27. Impacto: Tamanho do prejuízo, medido através de propriedades mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará;
28. Incidente de Segurança: Qualquer evento que resulte no descumprimento da Norma de Segurança da Informação e Comunicação que possa representar ameaça aos ativos, tais como: quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à internet ou programas instalados sem conhecimento da área de Tecnologia da Informação;
29. Informação: dados, processados ou não, que podem ser utilizados para produção e difusão de conhecimento, contidos em qualquer meio, suporte ou formato;
30. Informações Críticas: elementos informacionais essenciais para a continuidade operacional e a preservação da existência da organização (consistem nos elementos informacionais essenciais para a continuidade operacional e a preservação da existência da organização);
31. Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
32. Inteligência: capacidade de usar o conhecimento para realizar previsões, resolver problemas, tomar decisões e formular estratégias eficazes;
33. Log: é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Os registros devem conter hora e data das atividades, identificação do usuário, comandos e argumentos executados, identificação da estação local ou da estação remota que iniciou a conexão, entre outros;
34. *Login* de rede: método ou protocolo utilizado para autenticar e conceder acesso a um recurso ou serviço de rede;
35. Logon: processo de autenticação e acesso a um recurso protegido, geralmente feito com credenciais de acesso, de cunho pessoal e intransferível.
36. Monitoramento: atividade de verificação manual ou automática de eventuais ameaças, incidentes de segurança ou quaisquer descumprimentos às diretrizes presentes na Política, Normas ou Procedimentos de Segurança da Informação e Comunicação;
37. Não repúdio: garantia de segurança de informação que impede uma entidade de negar ter participado de uma dada operação.
38. Plano de Continuidade de Negócio (PCN): documentação dos procedimentos e informações necessárias para, em casos de incidentes, garantir a manutenção dos ativos de informação, bem como a continuidade das atividades críticas em local alternativo em nível previamente definido;
39. Plano de Resposta a Incidentes: documento que estabelece metodologias que visam minimizar o impacto de um incidente e permitir o restabelecimento dos serviços o mais rápido possível;
40. Plataformas de Colaboração: ferramentas utilizadas para gerenciar e otimizar a comunicação interna e externa, integrando funcionalidades como troca de mensagens, chamadas de voz e vídeo, compartilhamento de arquivos e gerenciamento de projetos;
41. Proprietário: Indivíduo que, em virtude de suas funções ou atribuições legais, tenha poder de decisão para identificar e classificar as informações geradas por sua área de gerência;
42. Proteção: vide Controle de Segurança;
43. Recursos de Tecnologia da Informação e Comunicação: conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio de hardware e software, a criação, acesso, armazenamento, transmissão e processamento de dados e informações;
44. Risco: é a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará;
45. Segurança da Informação: é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Toda e qualquer informação gerada, adquirida, utilizada

ou armazenada pela Procuradoria-Geral do Distrito Federal é considerada parte do seu patrimônio e deve ser protegida em relação aos aspectos de Confidencialidade, Integridade, Disponibilidade e Autenticidade;
46. Sistemas de Informação: conjunto integrado de componentes e processos usados para coletar, processar, armazenar e distribuir informações, visando o suporte a tomada de decisões, coordenação de atividades e controle organizacional com a finalidade de garantir a eficiência operacional e a conformidade com as normas de Segurança da Informação;
47. Serviço de Mensageria Instantânea: ferramentas de comunicação em tempo real que permitem o envio e recebimento imediato de mensagens entre usuários, oferecendo recursos como compartilhamento de arquivos, chamadas de voz e vídeo, e integração com outras ferramentas;
48. Servidor Público: pessoa física que exerce cargo, emprego ou função pública;
49. Termo de Responsabilidade: termo assinado pelo usuário no qual concorda em acatar todo o conteúdo desta Norma, e, contribuir com a disponibilidade, integridade, confidencialidade e autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes desse acesso;
50. Tratamento do risco: processo de seleção e implementação de controles de segurança;
51. Usuário: Qualquer pessoa, física ou jurídica ou processo em um sistema computacional que faça uso dos recursos de tecnologia da informação e Comunicação relativos à Procuradoria-Geral do Distrito Federal;
52. Vulnerabilidade: falha ou ponto fraco em um sistema, processo, protocolo ou controle de segurança que pode ser explorada por uma ameaça, resultando em um risco para a confidencialidade, integridade ou disponibilidade das informações ou ativos. As vulnerabilidades podem estar presentes em softwares, hardwares, redes, procedimentos ou comportamentos humanos, e sua identificação e mitigação são essenciais para aprimorar a eficácia da segurança da informação.

CAPÍTULO IV
DO ESCOPO DA NORMA
Art. 9º Estão submetidos à Norma de Segurança da Informação da Procuradoria-Geral do Distrito Federal (NoSIC/PGDF) todos os procuradores, servidores, estagiários, prestadores de serviços e demais agentes públicos ou privados que, por força de quaisquer instrumentos, exerçam atividades no âmbito da Procuradoria Geral do Distrito Federal, bem como qualquer pessoa que venha a ter acesso aos ativos de tecnologia da informação do órgão.
Art. 10. A NoSIC/PGDF tem a finalidade de estabelecer diretrizes, normas, controles e procedimentos para a segurança, tratamento e controle dos dados e informações produzidos, garantindo a confidencialidade, integridade e disponibilidade dos dados armazenados ou transmitidos por qualquer meio no âmbito da Procuradoria-Geral do Distrito Federal. Também busca assegurar a transparência, a proteção de dados e o acesso às informações, conforme estabelecido em legislação específica. Além disso, constitui instrumento fundamental para garantir a segurança da informação, apresentando os princípios e os principais requisitos mencionados, bem como outros, como a autenticidade, confiabilidade, anonimato e irretratabilidade.

CAPÍTULO V
DOS PRINCÍPIOS
Art. 11. São princípios que regem a NoSIC/PGDF:
1. Simplicidade: A complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser simples e objetivos;
2. Confidencialidade: A garantia do direito à intimidade e ao sigilo das informações, e que estas não sejam disponibilizadas ou divulgadas para pessoas, entidades ou processos não autorizados;
3. Continuidade do negócio: Planejamento de ações para retenção ou mitigação dos riscos aos dados e informações, assegurando a continuidade das atividades da Procuradoria-Geral do Distrito Federal, por meio da implementação, quando aplicável, de subplanos de continuidade operacional, recuperação de desastres, administração de crises e contingência;
4. Integridade: Garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino;
5. Privilégio mínimo: Usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhes foram designadas;
6. Segregação de função: Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos, bem como permitir maior eficácia dos controles de segurança;
7. Auditabilidade: Todos os eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;
8. Mínima dependência de segredos: Os controles deverão ser efetivos ainda que se conheça a existência deles e como eles funcionam;
9. Defesa em profundidade: Os controles de segurança devem ser concebidos em múltiplas camadas de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado;
10. Resiliência cibernética: Os controles de segurança cibernética, em relação aos dados e informações tutelados, devem ser aplicados por meio de mecanismos de confidencialidade, integridade e disponibilidade;
11. Publicidade e transparência: A divulgação de informações de interesse público de forma clara, exceto aquelas classificadas como sigilosas, segundo lei vigente;
12. Eficiência: Aplicação dos princípios de eficiência, eficácia e efetividade nas ações da NoSIC/PGDF, considerando o custo-benefício e o impacto na resiliência da segurança da informação.

CAPÍTULO VI
DA ESTRUTURA NORMATIVA
Art. 12. A Estrutura Normativa da Segurança da Informação da Procuradoria-Geral do Distrito Federal é composta por dois níveis hierárquicos distintos, conforme a seguir:
1. Normas Técnicas e Legislativas de Segurança da Informação e Comunicação: de caráter estratégico e tático, as normas estabelecem regras para a utilização de ativos e recursos de tecnologia da informação e comunicação com o intuito de atingir os objetivos da NoSIC/PGDF;

2. Controles e procedimentos de Segurança da Informação e Comunicação: descrevem de forma detalhada as medidas operacionais necessárias para atingir os resultados estabelecidos nas Normas e na NOSIC/PGDF, abordando aspectos técnicos e práticos, adaptados à realidade do ambiente.
Art. 13. A NoSIC/PGDF tem caráter corporativo e sua elaboração compete exclusivamente ao Comitê Gestor de Segurança da Informação e Comunicação da Procuradoria-Geral do Distrito Federal (CGSIC/PGDF), com aprovação pelo Comitê Gestor de Tecnologia da Informação (CGTI/PGDF).

CAPÍTULO VII
DO CICLO DE VIDA DA INFORMAÇÃO
Art. 14. As medidas de proteção devem ser adotadas ao longo de todo o ciclo de vida da informação, abrangendo as fases de criação, manipulação, armazenamento, transporte e descarte.

CAPÍTULO VIII
DAS DIRETRIZES GERAIS
Art. 15. São diretrizes gerais da NoSIC/PGDF:
1. A preservação da disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações e conhecimentos que compõem os ativos de informação da Procuradoria-Geral do Distrito Federal.
2. A continuidade das atividades no âmbito da Procuradoria-Geral do Distrito Federal.
3. A economicidade e eficiência na proteção dos ativos de informação.
4. A necessidade e utilidade do acesso aos ativos de informação, com base no princípio da pessoalidade.
5. O cumprimento das normas legislativas e regulamentares, bem como das normas técnicas e dos procedimentos de segurança da informação estabelecidos nesta NoSIC/PGDF.
6. A responsabilização do usuário por atos que comprometam a segurança dos sistemas de informação da instituição.

CAPÍTULO IX
DOS CONTROLES DE SEGURANÇA DA INFORMAÇÃO
Art. 16. Os procedimentos que complementam esta NoSIC abordarão, incluindo, mas não se limitando a, os seguintes controles: controle de acesso à rede; gestão de senhas e contas do usuário; segurança física das instalações e recursos; gestão do tratamento e resposta a incidentes e vulnerabilidades; gestão de riscos relacionados à segurança da informação; gestão de continuidade de negócio; classificação e manuseio adequado das informações; uso seguro da internet e dos recursos de TI; uso do correio eletrônico, do serviço de mensageria instantânea e das plataformas de colaboração; controle de privilégios de usuários e terceiros; gestão e segurança de dispositivos móveis; gestão de mudanças; gestão dos ativos de rede; proteção à propriedade intelectual; e uso responsável das soluções de Inteligência Artificial Generativa conforme Guia de Uso da Inteligência Artificial Generativa (IAG) da Procuradoria-Geral do Distrito Federal.
Art. 17. Devido à criticidade relacionada à segurança da informação e cibernética, esta Norma destaca procedimentos especiais com os seguintes controles: gestão de sistemas de TI (aquisição, desenvolvimento e manutenção de sistemas de TI), e educação continuada em relação à segurança da informação e cibernética.

CAPÍTULO X
DA DIVULGAÇÃO
Art. 18. Esta Norma, bem como as normas dela decorrentes, deverão ser disponibilizadas e agrupadas em sítio institucional em local de fácil acesso, por meio de link ou atalho na área de trabalho dos usuários, proporcionando ampla difusão e atualização simplificada. Em todos os documentos, deverá constar a data de sua publicação e/ou revisão.
Art. 19. Os controles e procedimentos de Segurança da Informação, por conter informações sensíveis, deverão ser classificados na forma da lei e divulgados para aqueles cujas atribuições exigem esse conhecimento.
Art. 20. Na utilização de ferramentas de IA generativa para criação de conteúdo ou informação divulgada pela Procuradoria-Geral do Distrito Federal, deverão ser observadas, obrigatoriamente, as regras dispostas no Guia de Uso da Inteligência Artificial Generativa (IAG) da Procuradoria-Geral do Distrito Federal.

CAPÍTULO XI
DOS PROCEDIMENTOS
Art. 21. Todas as áreas da Procuradoria-Geral do Distrito Federal alcançadas por esta Norma deverão implementar, gradativamente e na medida em que couber a cada área, todos os procedimentos dos controles de segurança da informação, considerados essenciais pelas boas práticas de cibersegurança, formando um conjunto de ações de defesa prioritárias contra ataques cibernéticos mais pervasivos:
1. Controle de acesso à rede:

- O login e a senha de rede, bem como os de sistemas de informação, constituem a identidade do usuário na Procuradoria-Geral do Distrito Federal.
- A identidade do usuário é pessoal e intransferível, sendo este o único responsável pela proteção e confidencialidade de seus dados de acesso.
- Sempre que se afastar da estação de trabalho, o usuário deverá bloquear o acesso, seja encerrando a sessão virtual ou desligando a máquina.
- Os dados dos usuários devem estar atualizados no Sistema de Pessoal da Procuradoria-Geral do Distrito Federal.
- O usuário terá acesso exclusivamente aos sistemas e informações necessários para o desempenho de suas atividades laborais.
- Em caso de afastamento, realocação setorial, mudança de responsabilidades ou atribuições dentro da Procuradoria-Geral do Distrito Federal, deverão ser imediatamente revisados os direitos de acesso e uso dos sistemas e informação.

- No caso de exoneração de cargo em comissão, cargo de natureza especial, cargo efetivo ou mesmo redistribuição ou remoção do servidor, cabe à unidade setorial de pessoal comunicar imediatamente à unidade de tecnologia da informação, para que sejam tomadas as providências necessárias à revogação do acesso do referido usuário.

2. Gestão de senhas e contas do usuário:

- Enquanto a Procuradoria-Geral do Distrito Federal não implementar a Política de Autenticação Multifatorial (MFA), a gestão de senhas e contas do usuário será o controle vigente.
- Caso a Política de MFA seja implantada, esta passará a vigorar imediatamente, sem a necessidade de alteração imediata desta NoSIC/PGDF. Porém, as possíveis adaptações deverão ser alteradas em revisão futura.
- A senha inicial será fornecida exclusivamente ao usuário, de forma direta e pessoal. Não poderá ser fornecida por telefone, mensagens instantâneas ou qualquer outro meio que não assegure a identidade do usuário.
- As senhas de acesso à rede de computadores e aos sistemas utilizados na Procuradoria-Geral do Distrito Federal deverão ter, no mínimo, 8 caracteres, incluindo obrigatoriamente letras maiúsculas, letras minúsculas, números e caracteres especiais.
- O usuário que utilizar ferramenta de IA generativa para criar uma senha, ainda que seja aleatória e atenda aos requisitos descritos acima, deverá seguir as regras dispostas no Guia de Uso da Inteligência Artificial Generativa (IAG) da Procuradoria-Geral do Distrito Federal.
- Não será permitida a reutilização das últimas 5 senhas utilizadas.
- A senha terá validade mínima de 10 dias e máxima de 90 dias, sendo obrigatória a troca imediata após esse período.
- Após 5 tentativas consecutivas de login com a senha incorreta, a conta do usuário será bloqueada por 15 minutos.
- Após o período indicado no item anterior, o acesso será liberado automaticamente ou poderá ser desbloqueado antecipadamente mediante solicitação à Gerência de Suporte, Monitoramento e Atendimento ao Usuário da Procuradoria-Geral do Distrito Federal.
- A concessão de autorização de acesso ao usuário interessado será de responsabilidade do chefe do setor responsável pelo sistema ou pela informação.
- A senha é de responsabilidade exclusiva do usuário, sendo expressamente proibida sua divulgação ou empréstimo. Caso haja suspeita de vazamento de autenticação, a senha deverá ser imediatamente alterada, a pedido do próprio usuário.
- O uso indevido da senha de outro usuário, sem a devida permissão, constitui crime conforme a Lei nº 12.737/2012, inserida no Código Penal Brasileiro, no artigo 154-A – "invasão de dispositivo informático".

3. Segurança física das instalações e recursos:

- As instalações que armazenam informações da Procuradoria-Geral do Distrito Federal devem receber o nível de proteção adequado à sua criticidade, classificação e importância para as operações, missão e visão da Procuradoria-Geral do Distrito Federal.
- As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados.
- Considera-se como nível de proteção a aplicação de soluções de segurança física, tais como: segurança patrimonial, monitoramento por câmeras de vídeo, controle de acesso às instalações críticas por meio de credenciais, senhas, biometria ou tecnologias similares, entre outras.
- O acesso ao Datacenter ou Centro de Processamento de Dados (CPD) deve ser restrito às pessoas devidamente autorizadas, mesmo que sejam usuários internos da Procuradoria-Geral do Distrito Federal.
- O acesso presencial de terceiros deverá ser registrado na recepção das instalações da Procuradoria-Geral do Distrito Federal e deverá ser acompanhado por um servidor da unidade responsável durante todo o período de permanência.
- A segurança física deverá ser gerida de forma compartilhada, com apoio não apenas do setor de Tecnologia da Informação, mas também, prioritariamente, do setor de manutenção predial ou de áreas correlatas.
- Todos os equipamentos deverão ser protegidos contra ameaças físicas e ambientais, incluindo os utilizados fora das instalações da Procuradoria-Geral do Distrito Federal.
- O usuário é responsável pela integridade dos equipamentos computacionais sob sua utilização.

4. Gestão do tratamento e resposta a incidentes e vulnerabilidades:

- Deve ser adotado um processo para o tratamento de incidentes de rede, com o objetivo de solucionar as falhas operacionais identificadas, minimizando os impactos negativos e garantindo o restabelecimento rápido da operação normal da rede de tecnologia da informação da Procuradoria-Geral do Distrito Federal.
- Qualquer incidente de segurança da informação ou cibernético observado pelos usuários em sistemas da Procuradoria-Geral do Distrito Federal deve ser imediatamente comunicado à Equipe de Tratamento e Resposta a Incidentes de Segurança da Procuradoria-Geral do Distrito Federal (CSIRT/PGDF), se instituída, sem prejuízo do registro do chamado na área de atendimento ao usuário. Caso o CSIRT/PGDF ainda não esteja instituída, a comunicação deverá ser encaminhada para a Área de Segurança da Informação da PGDF.
- Caso o sistema não esteja acessível e não haja outro computador disponível nas proximidades (ou seja, em caso de falha generalizada), o chamado poderá ser feito por telefone, ficando a área de atendimento ao usuário responsável pelo registro no sistema de chamados.
- Se o incidente for confirmado, a CSIRT/PGDF deverá adotar medidas corretivas emergenciais, como, por exemplo, isolar a rede de tecnologia da informação de forma tempestiva e realizar a recuperação de dados redundantes, entre outras ações pertinentes à situação.
- Em caso de malware, o sistema infectado deverá ser desligado e desconectado para evitar a propagação do vírus.
- A equipe de segurança da informação deverá documentar o ocorrido, incluindo suas causas, as ações tomadas e as lições aprendidas, com o objetivo de prevenir incidentes semelhantes no futuro.
- São consideradas medidas mínimas do controle:
    - Estabelecer e manter um processo de gestão de vulnerabilidade;
    - Estabelecer e manter um processo de resposta;
    - Executar a gestão automatizada de patches do sistema operacional;

- Executar a gestão automatizada de patches de aplicações;
- Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos;
- Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente;
- Corrigir vulnerabilidades detectadas.

5. Gestão de riscos relacionados à segurança da informação:

- Os investimentos e a criação de controles de segurança necessários devem ser dimensionados de acordo com o valor do ativo protegido e o risco potencial de prejuízos para os negócios, para a atividade fim e para os objetivos institucionais.
- A área de Tecnologia da Informação deverá realizar o processo de avaliação de riscos e seu respectivo monitoramento em relação aos serviços de Tecnologia da Informação disponibilizados para a Procuradoria-Geral do Distrito Federal.
- O processo consistirá na identificação, análise e avaliação final dos riscos de segurança da informação.
- A etapa de análise consiste em quantificar determinado risco, com indicadores usualmente utilizados, de maneira simples e compreensível, e estabelecer uma meta.
- A etapa de avaliação consiste em comparar o resultado do evento de risco com a meta previamente estabelecida.
- Para sistemas de informação considerados críticos, além do processo de avaliação de riscos, deverão ser implementadas medidas que facilitem o monitoramento e a comunicação, com o objetivo de atualizar continuamente as melhores práticas, por meio de aprendizado cíclico.

6. Gestão de continuidade de negócio:

- Deve-se assegurar a prontidão para manter as operações normais da Procuradoria-Geral do Distrito Federal em caso de eventos e incidentes de segurança da informação, minimizando seus impactos na continuidade das funções críticas do negócio.
- No contexto da Procuradoria-Geral do Distrito Federal, entende-se como negócio, a prestação de sua atividade fim.
- As áreas devem elaborar e manter atualizado um plano de continuidade de suas atividades, devendo, no que se refere aos itens relacionados à Tecnologia da Informação, comunicar o setor de Tecnologia da Informação.
- O plano de continuidade deverá consistir, no mínimo, nos seguintes aspectos:
  - Continuidade operacional, visando o planejamento para continuidade dos serviços;
  - Recuperação de desastres, detalhando os procedimentos para armazenamento e recuperação de informações;
  - Administração de crises, que remete à determinação das funções e responsabilidade de cada usuário da unidade;
  - Plano de contingência, de caráter prudencial, que descreve as etapas a serem seguidas caso os aspectos anteriores se mostrem inviáveis, sendo utilizado em última instância.
- O plano de continuidade deverá seguir um ciclo de melhoria contínua, visando à atualização constante dos aspectos mencionados no artigo anterior.

7. Classificação e manuseio adequado das informações:

- As informações sensíveis para a execução dos objetivos, missão e visão da Procuradoria-Geral do Distrito Federal devem ser classificadas pelo responsável pela geração da informação, em conformidade com a Lei Distrital nº 4.990, de 12 de dezembro de 2012 e alterações.
- Se na ocasião do tratamento de informações forem utilizadas ferramentas de IA generativa, a elaboração do "prompt" deve manter os cuidados de classificação e manuseio, de acordo com o Guia de Uso da IA da Procuradoria-Geral do Distrito Federal.

8. Uso seguro da internet e dos recursos de TI:

- O acesso à Internet no âmbito da Procuradoria-Geral do Distrito Federal deve ser realizado exclusivamente para a execução de atividades de interesse público e para aquelas desempenhadas pelo órgão, observando sempre os princípios estabelecidos nesta NoSIC/PGDF, especialmente no que se refere à moralidade administrativa.
- A área de Tecnologia da Informação monitorará os acessos à Internet, recursos e sistemas de informação dentro das dependências da Procuradoria-Geral do Distrito Federal, bloqueando sites com conteúdo suspeito ou perigoso para a execução dos objetivos, missão e visão da Instituição.
- Caso o usuário identifique que algum site suspeito ou perigoso esteja acessível, deverá informar imediatamente à área de Tecnologia da Informação.
- São vedadas as seguintes ações:
  - A instalação de softwares não homologados ou licenciados pelo setor de tecnologia da informação, ou, mesmo sendo licenciados, sem a anuência prévia desse setor;
  - O acesso ou tentativa de acesso a recursos tecnológicos para os quais o usuário não tenha autorização, especialmente aqueles que contenham conteúdo ofensivo, ilegal ou impróprio, ou que sejam de missão crítica para a Procuradoria-Geral do Distrito Federal;
  - A utilização dos recursos tecnológicos da Procuradoria-Geral do Distrito Federal para fins não relacionados às suas atividades institucionais;
  - A prática de qualquer ato que vise tornar indisponível qualquer recurso tecnológico sem a devida autorização;
  - O uso de provedores de acesso externos ou qualquer outra forma de conexão não autorizada no ambiente de rede da Procuradoria-Geral do Distrito Federal.
  - A inobservância dos preceitos éticos relacionados ao uso de IA generativa, ou qualquer ferramenta de "machine learning", desviando do regramento disposto no Guia de Uso da Inteligência Artificial Generativa (IAG) da Procuradoria-Geral do Distrito Federal.
- Durante o uso da Internet, o usuário deve atentar à idoneidade dos endereços eletrônicos acessados, verificando se a página não contém links ou características suspeitas (“pharming”).
- Caso o usuário tenha dúvidas sobre como identificar a integridade de uma página na Internet, deverá contatar a área de Tecnologia da Informação para orientação imediata.

9. Uso do correio eletrônico, do serviço de mensageria instantânea e das plataformas de colaboração:

- O uso do correio eletrônico corporativo é obrigatório para o envio e recebimento de informações e documentos relacionados às atividades institucionais da Procuradoria-Geral do Distrito Federal, sendo vedada a sua utilização para fins pessoais.
- A distribuição de mensagens e informações corporativas e institucionais será comprovada por qualquer meio que demonstre o envio para o endereço eletrônico do destinatário.
- Ao enviar ou responder mensagens eletrônicas, o usuário deve adotar uma comunicação profissional, respeitosa e conforme as normas da ortografia oficial, evitando o uso excessivo de linguagem inadequada ou informal.
- Recomenda-se que, para assuntos urgentes, mensagens rápidas, videoconferências, gestão de trabalho através de grupos, ou atividade similar, o usuário utilize o serviço de mensageria em nuvem contratado pela área de Tecnologia da Informação.
- Recomenda-se que, para envio de documentos institucionais ou qualquer ato administrativo do órgão, sejam utilizadas ferramentas contratadas pela Procuradoria-Geral do Distrito Federal.
- O acesso diário à caixa de mensagens eletrônicas corporativas é responsabilidade exclusiva do usuário.
- Durante o uso do correio eletrônico, o usuário deve atentar à idoneidade das mensagens recebidas, verificando se o conteúdo não contém links ou arquivos anexos suspeitos (como “phishing”).
- Caso o usuário tenha dúvidas sobre como identificar a integridade de uma mensagem eletrônica, deverá contatar o setor de segurança da informação para orientação imediata.
- A área de Tecnologia da Informação, após consulta ao CGSIC/PGDF, adotará medidas para bloquear o acesso, pela rede da Procuradoria-Geral do Distrito Federal, aos servidores de correio eletrônico comerciais, caso seja identificado mau uso.
- Os requisitos de segurança da informação devem ser explicitamente mencionados em todos os termos de compromisso firmados com terceiros.
- A não observância dos procedimentos deste controle é de inteira responsabilidade do usuário.

10. Controle de privilégios de usuários e terceiros:
    - A Procuradoria-Geral do Distrito Federal adotará a política de mínimo privilégio, segundo a qual, mesmo os agentes públicos pertencentes ao quadro do órgão, bem como terceiros, não terão acesso irrestrito a todos os sistemas de informação oferecidos pela instituição.
    - O acesso será concedido exclusivamente ao necessário para que cada usuário execute suas tarefas, limitando a possibilidade de acesso a informações sensíveis e críticas da Procuradoria-Geral do Distrito Federal.
    - Deverão ser realizadas concessões, revisões, ajustes e revogações regulares das permissões dos usuários, a fim de garantir que o acesso esteja sempre adequado às suas atribuições atuais.
    - Será adotada a regra de segregação de funções, que consiste em dividir as responsabilidades por tarefas sensíveis, a fim de reduzir o risco de fraudes e erros.
    - Deverá ser garantido que os usuários não acumulem privilégios que lhes permitam realizar ações críticas sem supervisão. Por exemplo, um servidor que inicia uma transação não deve ser o mesmo que a aprova.
    - Os usuários que não pertencem ao quadro efetivo da Procuradoria-Geral do Distrito Federal, tais como fornecedores, usuários externos, empregados contratados por meio de licitação, entre outros, deverão assinar Termo de Responsabilidade, aderindo a esta NoSIC e ao Guia de Uso de IAG da Procuradoria-Geral do Distrito Federal sujeitando-se integralmente aos seus critérios.
11. Gestão e segurança de dispositivos móveis:
    - Todos os dispositivos móveis cedidos aos usuários pela Procuradoria-Geral do Distrito Federal deverão ser registrados e monitorados pela equipe de TI, com a manutenção de um inventário atualizado.
    - O monitoramento mencionado refere-se à gestão das configurações de segurança, políticas de acesso e medidas de contenção, como bloqueio e apagamento remoto.
    - Os dispositivos móveis cedidos aos usuários deverão ser utilizados, prioritariamente, para atividades corporativas relacionadas à Procuradoria-Geral do Distrito Federal.
    - Os usuários responsáveis pelos dispositivos móveis deverão assinar Termo de Responsabilidade, por meio de sistema de processos internos, comprometendo-se a zelar pela integridade física e lógica dos equipamentos.
    - Em caso de extravio, perda ou roubo do dispositivo por motivos alheios ao usuário, este deverá informar imediatamente à área de Tecnologia da Informação.
    - Caso o usuário utilize um dispositivo móvel pessoal (BYOD) para acessar sistemas da Procuradoria-Geral do Distrito Federal, deverá tomar as precauções necessárias para reduzir a exposição de dados e sistemas institucionais, adotando as devidas medidas de segurança da informação.
12. Gestão de mudanças:
    - Toda mudança relacionada à forma de gestão de informações tratadas pela Procuradoria-Geral do Distrito Federal deve ser registrada e aprovada pelo CGSIC/PGDF.
    - Cada mudança deve passar por uma análise de riscos à segurança da informação, avaliando: possíveis falhas de segurança; impacto na continuidade de serviços públicos; ameaças à integridade de dados sensíveis.
    - Mudanças críticas deverão exigir aprovação obrigatória da alta gestão, com auxílio fundamentado pela CGSIC/PGDF.
    - Em relação aos sistemas ou infraestrutura de TIC da Procuradoria-Geral do Distrito Federal, as alterações devem ser testadas em ambientes controlados (homologação) antes de serem implementadas em produção.
    - Para toda mudança nos sistemas ou infraestrutura de TIC da Procuradoria-Geral do Distrito Federal, deve haver um plano de retorno ao estado anterior caso ocorra falha ("rollback").
    - As medidas relacionadas à gestão de mudanças devem estar alinhadas com a gestão de continuidade de negócio descrita nesta Norma.
13. Gestão dos ativos de rede:
    - Deve ser realizada a gestão contínua (registrar, acompanhar e corrigir) de todos os ativos corporativos de TIC – equipamentos de usuários finais, incluindo computadores portáteis e dispositivos móveis; dispositivos de rede; dispositivos IoT; e servidores –

conectados fisicamente, virtualmente ou remotamente à infraestrutura corporativa de TI, incluindo aqueles em ambientes de nuvem (cloud computing), com o objetivo de conhecer com precisão todos os ativos de hardware da organização que precisam ser monitorados e protegidos.

- São consideradas medidas mínimas dos ativos corporativos:
    - Estabelecer e manter um inventário detalhado de ativos corporativos;
    - Endereçar ativos não autorizados;
    - Usar uma ferramenta de descoberta ativa;
    - Usar o Dynamic Host Configuration Protocol (DHCP) ou ferramentas de gestão de endereço Internet Protocol (IP) para atualizar o inventário de ativos corporativos.
- Deve ser realizada a gestão contínua (registrar, acompanhar e corrigir) de todo software – sistemas operacionais e aplicativos – utilizado, de modo que softwares autorizados possam ser instalados e executados nas máquinas e softwares não autorizados/gerenciados possam ser detectados e tenham a instalação/execução impedida.
- São consideradas medidas mínimas dos softwares:
    - Estabelecer e manter um inventário de software;
    - Assegurar que o software autorizado seja atualmente suportado;
    - Endereçar o software não autorizado;
    - Utilizar ferramentas automatizadas de inventário de software;
    - Lista de permissões de software autorizado;
    - Lista de permissões de bibliotecas autorizadas.
- Deverão ser mantidos, atualizados e licenciados os sistemas e demais itens de software do parque computacional da Procuradoria-Geral do Distrito Federal, permitindo a atualização dos ativos de infraestrutura tecnológica do centro de dados sem obstáculos ou dificuldades, de acordo com o cronograma estabelecido pelos fabricantes contratados.

14. Proteção à propriedade intelectual:

- Deverão ser identificados e registrados todos os bens intelectuais produzidos ou utilizados pela Procuradoria-Geral do Distrito Federal, inclusive os que foram contratados, tais como:
    - Softwares desenvolvidos internamente e externamente;
    - Documentações técnicas e normativas;
    - Metodologias e processos exclusivos;
    - Estudos, relatórios e dados estratégicos;
    - Bases de dados geográficos, estatísticos ou científicos.
- Tais ativos intelectuais devem ser classificados conforme seu nível de sensibilidade (confidencial, restrito, público).
- O acesso aos bens intelectuais deverá estar sujeito a controle rigoroso de acesso, no que concerne aos documentos, códigos-fonte, bancos de dados e demais ativos intelectuais. Tal controle deve estar alinhado ao controle de privilégios, presente nesta Norma.
- Será estabelecido, formalmente, que toda Propriedade Intelectual desenvolvida no exercício da função pública é de titularidade da Procuradoria-Geral do Distrito Federal, e não, do servidor individual ou da empresa contratada.
- Em alguns casos, de decisão da CGSIC/PGDF, deverão ser exigido termos de confidencialidade ("Non Disclosure Agreement - NDA") às empresas contratadas para gestão do bem intelectual.

15. Uso responsável das soluções de Inteligência Artificial Generativa conforme Guia de Uso da Inteligência Artificial Generativa (IAG) da Procuradoria-Geral do Distrito Federal:

- O uso de IA generativa em processos da Procuradoria-Geral do Distrito Federal deverá estar restrito às atividades que respeitem os princípios da legalidade, moralidade e segurança da informação, com atenção especial para a proteção de dados sensíveis e confidenciais, em conformidade com o Guia de Uso da IA da Procuradoria-Geral do Distrito Federal (Portaria nº 160 de 08 de abril de 2025 e alterações).
- Todos os modelos de IA generativa utilizados deverão ser auditados e monitorados regularmente pela Subsecretaria-Geral de Tecnologia da Informação, para garantir que não haja violações de segurança, uso indevido ou comprometimento de dados.
- A Procuradoria-Geral do Distrito Federal adotará medidas de mitigação de riscos associados à IA generativa, incluindo, mas não se limitando a:
    - Implementação de protocolos de segurança para proteger contra o uso malicioso da IA;
    - Avaliação de impacto antes de implementar soluções de IA generativa que envolvam dados pessoais ou sensíveis;
    - Garantia de que os sistemas de IA generativa estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e outras regulamentações pertinentes.
- A Procuradoria-Geral do Distrito Federal garantirá que qualquer uso de IA generativa seja transparente e auditável, permitindo rastreabilidade das decisões tomadas pelas máquinas e proporcionando aos usuários acesso a explicações sobre como os resultados são gerados, especialmente quando esses resultados impactam diretamente os cidadãos ou a administração pública.
- É vedado o uso de IA generativa para a criação de conteúdo ou documentos que possam violar os direitos autorais, promover desinformação ou manipulação, ou infringir normas éticas da Procuradoria-Geral do Distrito Federal.
- Todos os colaboradores da Procuradoria-Geral do Distrito Federal que utilizarem ou implementarem tecnologias de IA generativa deverão ser treinados e capacitados sobre as implicações éticas, legais e de segurança dessa tecnologia, com ênfase na proteção da informação e na privacidade dos dados.
- O Comitê Gestor de Tecnologia da Informação (CGTI/PGDF) será responsável por revisar periodicamente as políticas de uso de IA generativa, avaliando novos riscos e propondo medidas para a mitigação de potenciais ameaças à segurança e à conformidade legal

CAPÍTULO XII
GESTÃO DE SISTEMAS DE INFORMAÇÃO - AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO

Art. 22. Deverão ser desenvolvidas ações que garantam que a segurança seja parte integrante dos sistemas de informação e comunicação existentes, e também os que forem desenvolvidos e adquiridos.

Art. 23. Todos os requisitos de segurança deverão ser identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados, como parte do caso geral de negócios do sistema de informação.

Art. 24. Cabe ao CGTI/PGDF a elaboração de cartilha que estabeleça diretrizes gerais para o desenvolvimento seguro de softwares, que deverá ser amplamente divulgada e disponibilizada às Áreas da Procuradoria-Geral do Distrito Federal para utilização nas rotinas internas e nos seus Termos de Referência.

Art. 25. O desenvolvimento de sistemas de informação, seja interno ou contratado, deverá seguir a metodologia de desenvolvimento de sistemas da Procuradoria-Geral do Distrito Federal, a qual deve incluir mecanismos para garantir que o desenvolvimento e a produção dos sistemas de informação atendam aos níveis de serviço adequados.

Art. 26. Deverão ser implementadas ações que garantam que a segurança seja uma parte integrante dos sistemas de informação e comunicação existentes, bem como dos sistemas que forem desenvolvidos ou adquiridos futuramente.

Art. 27. Todos os requisitos de segurança da informação devem ser identificados na fase de definição de requisitos de um projeto e devidamente justificados, acordados e documentados, como parte da documentação do sistema de informação em questão.

CAPÍTULO XIII
EDUCAÇÃO CONTINUADA

Art. 28. Para uma efetiva proteção das informações, a Área relacionada à Gestão de Pessoas em conjunto com a Área de Segurança da informação da Procuradoria-Geral do Distrito Federal deverão elaborar um plano contínuo de capacitação de recursos humanos em segurança da informação e cibernética, de modo a promover maior consciência da responsabilidade individual dos usuários, maior independência do órgão na contratação de serviços de segurança visando a consecução de sua finalidade institucional.

Art. 29. Deverá ser elaborado um plano de capacitação, abordando, de forma exemplificativa, os seguintes tópicos:

- Contexto atual da segurança da informação e cibernética;
- Reconhecimento dos principais ataques e ameaças ao setor público e suas formas de prevenção, cm atenção especial aos relacionados à engenharia social;
- Melhores Práticas de Tratamento de Dados;
- Causas da exposição não intencional de dados;
- Reconhecimento e Comunicação de Incidentes de Segurança;
- Atualizações de segurança dos ativos corporativos;
- Riscos de conexão e transmissão de dados em redes inseguras;
- Melhores práticas de autenticação;
- Conteúdo e importância da NoSIC/PGDF;
- Correto uso de IA generativa e o Guia de Uso da IA da Procuradoria-Geral do Distrito Federal;
- Competências e conscientização de segurança da informação para funções específicas, e;
- Responsabilidades dos usuários.

Art. 30. A Procuradoria-Geral do Distrito Federal poderá, adicionalmente, adotar capacitações mais específicas para setores estratégicos do órgão.

Art. 31. Todos os membros, servidores, parceiros, licenciados, fornecedores, terceiros e colaboradores eventuais, que utilizem os ativos de rede da Procuradoria-Geral do Distrito Federal, devem assinar Termo de Responsabilidade quanto à confidencialidade dos dados, informações e conhecimentos da Instituição, sob pena de responsabilização administrativa, cível ou criminal, dependendo do gravame.

Art. 32. O modelo do Termo de Responsabilidade encontra-se no APÊNCDICE AO ANEXO desta Portaria.

CAPÍTULO XIV
PENALIDADES

Art. 33. O descumprimento às diretrizes desta Norma assim como às suas normas, controles e procedimentos vinculados acarretará sanções administrativas, sem prejuízo às ações cíveis e criminais cabíveis.

CAPÍTULO XV
COMPETÊNCIAS E RESPONSABILIDADES

Art. 34. Esta NoSIC/PGDF deve ser cumprida por todos os usuários, sejam agentes públicos ou particulares que, por força de contratos administrativos, convênios, protocolos, acordos de cooperação e instrumentos congêneres executem atividades vinculadas ao órgão.

DA ALTA ADMINISTRAÇÃO DA PROCURADORIA-GERAL DO DISTRITO FEDERAL

Art. 35. Compete à Alta Administração, com prévia manifestação do Comitê Gestor de Segurança da Informação e Comunicação:

1. Apoiar e exigir o cumprimento da Política, Normas e Procedimentos de Segurança da Informação e Comunicação;
2. Zelar para que contratos, convênios e outros instrumentos similares elaborados pela Procuradoria-Geral do Distrito Federal estejam alinhados à presente Norma e suas normas adjacentes;
3. Aprovar e determinar a publicação da NoSIC/PGDF e suas modificações;
4. Apoiar a implantação dos controles de segurança da informação observando a coordenação e relevância para toda o órgão;
5. Incentivar a capacitação e conscientização dos agentes públicos e particulares, na condição do artigo 66, sobre a segurança da informação e cibernética;
6. Garantir os recursos necessários para a implantação e gestão da NoSIC/PGDF;
7. Aprovar modificações à NoSIC/PGDF propostas pelo Comitê Gestor de Tecnologia da Informação da Procuradoria-Geral do Distrito Federal;
8. Praticar outros atos inerentes à aplicação e à observância da NoSIC/PGDF;

9. Instituir o Comitê Gestor de Segurança da Informação e Comunicação (CGSIC) no âmbito da Procuradoria-Geral do Distrito Federal e nomear os servidores que farão parte da sua composição.

DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DA PROCURADORIA-GERAL DO DISTRITO FEDERAL - CGSIC/PGDF
Art. 36. Enquanto o CGSIC/PGDF não for instituído, o Comitê Gestor de Tecnologia da Informação (CGTI/PGDF) assumirá todas as atribuições daquele.
Art. 37. Compete ao Comitê Gestor de Segurança da Informação e Comunicação da Procuradoria-Geral do Distrito Federal:
1. Elaborar e atualizar as Normas, Controles e Procedimentos de Segurança da Informação, Cibernética e de Comunicação da Procuradoria-Geral do Distrito Federal, em conformidade com a NoSIC/PGDF, e, congruente com as Normas de Segurança da Informação e Comunicação (NoSIC) do GDF, leis e regulamentos pertinentes;
2. Investigar e avaliar os impactos decorrentes de incidentes de segurança da informação;
3. Estabelecer um Programa de Gestão de Riscos de segurança da informação, atualizando-o quando necessário;
4. Desenvolver um Plano de Continuidade de Negócios no contexto de segurança de redes, que deverá ser testado periodicamente;
5. Coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança da Procuradoria-Geral do Distrito Federal (CSIRT/PGDF);
6. Instituir grupos de trabalho específicos relacionados à segurança da informação e cibernética.
7. Estabelecer mecanismo de registro e controle de não conformidade a esta Norma, Normas e Procedimentos de Segurança da Informação e Comunicação;
8. Realizar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e cibernética;
9. Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança.
Art. 37. Com a instituição da CGSIC, fica instituída também, o grupo de trabalho nominado Equipe de Tratamento e Resposta a Incidentes de Segurança da Procuradoria-Geral do Distrito Federal (CSIRT/PGDF), cuja composição será de caráter prioritariamente técnico (servidores com ampla experiência em termos de resiliência cibernética), e, de livre escolha do coordenador do CGSIC, não se limitando aos membros do Comitê.
Art. 38. As revisões da NoSIC/PGDF, realizadas pelo CGSIC/PGDF, deverão estar alinhadas, com a última revisão da POSIC do Governo do Dsitrito Federal.
Art. 39. O CGSIC/PGDF deverá ser composto, minimamente, pela seguinte formação:

- Gestor de Segurança da Informação, servidor indicado pelo representante máximo do órgão ou entidade, que coordenará as atividades do comitê;
- Dois membros da Área de Segurança de redes;
- Um membro da Área de Manutenção predial ou Segurança física;
- Um membro da Área de Processos Administrativos;
- Um membro da Área de Normas e Legislação;
- Um membro da Área de Gestão de Pessoas.

DO GESTOR DA SEGURANÇA DA INFORMAÇÃO
Art. 40. Compete ao Gestor da Segurança da Informação:
1. Coordenar o CGSIC/PGDF;
2. Monitorar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
3. Cobrar dos respectivos proprietários a classificação das informações na Área sob sua gerência;
4. Propor recursos necessários às ações de segurança da informação e comunicação;
5. Acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
6. Propor Normas e procedimentos relativos à segurança da informação e comunicações;
7. Definir métricas que permitam aferir a eficiência e eficácia dos controles de segurança.
A gestão de segurança da informação deverá somente ser realizada por servidores públicos.

DO GESTOR DE ÁREA
Art. 41. Entende-se como Gestor de Área, qualquer agente público inserido em cargo em comissão ou função de confiança resposável por uma das secretarias, subsecretarias, diretorias, gerências ou núcleos no âmbito da Procuradoria-Geral do Distrito Federal.
Art. 42. Compete ao Gestor de Área:
1. Zelar e fazer cumprir a NoSIC/PGDF;
2. Identificar desvios de conduta na utilização das informações obtidas durante o exercício das funções de seus subordinados e adotar as medidas preventivas e corretivas apropriadas;
3. Aplicar medidas que visem a garantir que o pessoal sob sua supervisão proteja informações da Área a que tem acesso;
4. Proteger, em nível físico e lógico, os ativos de informação e de processamento relacionados com sua área de atuação;
5. Impedir o acesso de pessoal desligado, suspenso ou afastado preventivamente aos ativos de informação sob sua responsabilidade, utilizando-se dos mecanismos previstos no plano de desligamento a ser implementado;
6. Comunicar formalmente o desligamento (exoneração, demissão, transferência, cessão), suspensão ou afastamento preventivo de usuários aos Gestores da Área de Pessoas e aos Proprietários de Informações, os quais deverão notificar a área de Tecnologia da Informação para medidas cabíveis;
7. Colaborar para o levantamento de dados para o Gerenciamento de Riscos da área sob sua gestão e informar novos riscos ainda não mapeados na Área em que atua.

DO USUÁRIO
Art. 43. Entende-se como Usuário, todos os agentes públicos ou particulares que, por força de contratos administrativos, convênios, protocolos, acordos de cooperação e instrumentos congêneres executem atividades vinculadas à Procuradoria-Geral do Distrito Federal.
Art. 44. São obrigações do usuário:
1. Observar rigorosamente esta Norma de Segurança de Informação e Comunicação, bem como as Normas e Procedimentos a ela vinculados;

2. Assegurar o uso racional dos recursos de Tecnologia da Informação e Comunicação colocados à sua disposição, priorizando o interesse público e institucional;
3. Comunicar a Área competente quaisquer riscos ou incidentes de segurança de que venha a tomar conhecimento;
4. Assegurar-se que as senhas e credenciais para acesso aos ativos de processamento e de informações estejam de acordo com os procedimentos estabelecidos e que as mesmas sejam protegidas e confidenciais, não devendo ser compartilhadas, ou seja, toda senha é de uso PESSOAL e INTRANSFERÍVEL;
5. Manter, obrigatoriamente, os dados críticos da sua Àrea em compartilhamentos de rede ou em armazenamento em nuvem disponibilizados pela área de TIC da Procuradoria-Geral do Distrito Federal;
6. Não utilizar serviços de e-mail gratuitos, como GMAIL, HOTMAIL, UOL e outros, para atividades institucionais, visto que tais serviços não possuem garantia de autenticidade, disponibilidade e confidencialidade das informações;
7. Ativar e utilizar adequadamente sua conta de e-mail corporativo apenas para fins institucionais e de forma a não cometer qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou do próprio Estado, em consonância com as determinações legais;
8. Acessar a Internet apenas para navegação em sítios cujo conteúdo esteja adequado aos dispositivos legais, às determinações da Unidade Administrativa e às suas atribuições institucionais.

DA SUBSECRETARIA-GERAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DA PROCURADORIA-GERAL DO DISTRITO FEDERAL - SUTIC/PGDF
Art. 45. Compete à Subsecretaria-Geral de Tecnologia da Informação:
1. Promover a cultura de segurança da informação e cibernética em toda a Procuradoria-Geral do Distrito Federal;
2. Dar apoio técnico ao CGSIC na elaboração normas e procedimentos de segurança da informação no tocante às informações, comunicações e processos relativos presentes no ambiente computacional;
3. Acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança, realizadas pela CGSIC;
4. Propor, quando necessário à CGSIC, recursos necessários às ações de segurança da informação e comunicações;
5. Encaminha modificações à NoSIC/PGDF, propostas pelo CGSIC;
6. Definir estratégias para a implantação da NoSIC/PGDF, com anuência do CGSIC.

DAS DEMAIS ÁREAS DE TECNOLOGIA DA INFORMAÇÃO DA PROCURADORIA-GERAL DO DISTRITO FEDERAL
Art. 46. São obrigações das Áreas de Tecnologia da Informação da Procuradoria-Geral do Distrito Federal, de subordinação da SUTIC/PGDF, ou do custodiante responsável por prover os serviços de tecnologia para o órgão:
1. Promover, em conjunto com a Subsecretaria-Geral de Tecnologia da informação, a cultura de segurança da informação e cibernética em toda a Procuradoria-Geral do Distrito Federal;
2. Realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes;
3. Assegurar o pleno e efetivo funcionamento dos recursos de Tecnologia da Informação e Comunicação disponibilizados;
4. Assegurar a integridade e disponibilidade dos ativos que se encontram no seu ambiente computacional;
5. Dar assistência ao CSIC na elaboração Normas e Procedimentos de Segurança da Informação no tocante às informações, comunicações e processos relativos presentes no ambiente computacional;
6. Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente computacional;
7. Requisitar informações às demais áreas de sua Unidade Administrativa, realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Norma e das Normas de Segurança da Informação e Comunicação no tocante aos ativos informatizados;
8. Elaborar o Plano de Resposta a Incidentes;
9. Manter registro das atividades de usuários (logs), de maneira a abranger o máximo de ações possíveis dentro dos sistemas e pelo maior tempo possível;
10. Solicitar criação e manutenção de ambiente de correio eletrônico institucional ao Custodiante responsável por prover o serviço de correio eletrônico corporativo e deverá seguir as determinações do Custodiante;
11. Adotar como padrão de endereço de e-mail corporativo o formato @pg.df.gov.br;
12. Priorizar o uso institucional do acesso à internet, podendo bloquear e/ou limitar acesso a determinados sítios de Internet e estabelecendo categorias passíveis de acesso em horários restritos;
13. Instalar sistemas operacionais nos computadores de sua Unidade devidamente licenciados e mantê-los atualizados;
14. Instalar itens de softwares (local ou em nuvem) e mecanismos de proteção nas estações de trabalho devidamente licenciados e mantê-los atualizados;
15. Instalar e permitir a instalação apenas de software devidamente licenciado e homologado, de modo a não comprometer a segurança do ambiente;
16. Manter atualizados e licenciados os sistemas e demais itens de software do parque computacional.

DO PROPRIETÁRIO DA INFORMAÇÃO
Art. 47. São obrigações do Proprietário da Informação:
1. Identificar e definir as informações críticas e os requisitos de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio;
2. Classificar e rever periodicamente a classificação dos ativos sob sua propriedade que requerem algum grau de sigilo, observando a legislação em vigor;
3. Participar do processo de avaliação e aceitação de risco;
4. Participar nas decisões relacionadas a qualquer violação de segurança dos ativos sob sua propriedade;
5. Autorizar a liberação de acesso à informação sob sua responsabilidade;
6. Revogar a liberação de acesso à informação sob sua responsabilidade, após recebidos comunicados de desligamento, suspensão ou afastamento preventivo de servidores;
7. Participar da definição dos critérios para estabelecer perfis de acesso a informações sob sua responsabilidade;
8. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

9. Participar, sempre que convocado, das reuniões do CGSIC/PGDF, prestando os esclarecimentos solicitados.

DO CUSTODIANTE DOS ATIVOS DA INFORMAÇÃO
Art. 48. São obrigações do Custodiante dos Ativos da Informação:
1. Prestar assistência ao Proprietário da Informação na definição dos procedimentos operacionais e de controle, referentes a manuseio, armazenamento e disposição final dos ativos;
2. Controlar e proteger os ativos sob sua custódia;
3. Realizar, verificar e manter cópias de segurança (backups) dos ativos de informação sob sua custódia, em conformidade com a Norma de Backup da Procuradoria-Geral do Distrito Federal, a menos que outra solução seja acordada formalmente entre o proprietário da informação e o custodiante;
4. Comunicar a respectiva área da TIC e ao proprietário da informação qualquer incidente de segurança que afete os ativos sob sua custódia;
5. Implementar os controles de segurança e contratar, se necessário, bens e serviços de Segurança da Informação e Comunicação.

DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA DA PROCURADORIA-GERAL DO DISTRITO FEDERAL (CSIRT/PGDF)
Art. 49. Deverá ser instituído uma Equipe de Tratamento e Resposta a Incidentes de Segurança (CSIRT - Computer Security Incident Response Team) da Procuradoria-Geral do Distrito Federal (CSIRT/PGDF), que será responsável por:
1. Suspender, a qualquer tempo, o acesso de usuário ou processo a informações ou recursos de tecnologia da informação e comunicação, quando evidenciados riscos à segurança da informação, notificando, de imediato, o Gestor de Segurança da Informação e Comunicação;
2. Dar tratamento e encaminhamento aos incidentes de redes, tomando as medidas necessárias para conter as ameaças, minimizar os impactos e evitar futuras ocorrências, restabelecendo juntamente com o setor responsável, a integridade, confidencialidade e disponibilidade dos ativos;
3. Registrar, classificar e filtrar as notificações de Incidentes de Segurança;
4. Executar o Plano de Resposta a Incidentes;
5. Recolher e preservar as evidências para subsidiar a forense computacional;
6. Investigar as causas dos incidentes no ambiente computacional.
Art. 50. Enquanto não for instituído o CSIRT/PGDF, todas as atribuições e responsabilidades deste permanecerão com as áreas de Tecnologia da Informação e Comunicação da Procuradoria-Geral do Distrito Federal ou para a unidade responsável por custodiar os ativos de informação do órgão.

CAPÍTULO XVI
DA ATUALIZAÇÃO E DIVULGAÇÃO
Art. 50. Esta Norma, Normas, Controles e Procedimentos que dela se originarem deverão ser atualizadas a cada 2 anos, ou quando houver mudanças significativas que afetem a base de avaliação de risco original ou o contexto organizacional.
Art. 51. É considerada responsabilidade institucional e geral, a divulgação desta NoSIC/PGDF, por todos os usuários da Procuradoria-Geral do Distrito Federal, em seu âmbito interno.
Art. 52. Caberá ao Comitê Gestor de Tecnologia da Informação da Procuradoria-Geral do Distrito Federal (CGTI/PGDF) a responsabilidade pela atualização permanente da estrutura normativa;
Art. 53. Caberá à Procuradoria-Geral do Distrito Federal a elaboração de normas e procedimentos de Segurança da Informação e Comunicação nos casos que não forem contemplados pelo CGTI/PGDF.

CAPÍTULO XVII
CONCLUSÃO
Art. 54. Este documento tem o condão de revisar a última Política de Segurança da Informação da Procuradoria-Geral do Distrito Federal, passando à condição de Norma, e, deverá nortear a elaboração de outros documentos relacionados à Segurança da Informação, os quais deverão observar as diretrizes e terminologias aqui apresentadas no intuito de assegurar um padrão documental.
Art. 55. Os dispositivos aqui estabelecidos apresentam as principais atividades a serem desenvolvidas. A sua priorização será definida pelos Gestores e Comitês aqui nominados. Com esta NoSIC, a Procuradoria-Geral do Distrito Federal reafirma seu compromisso com a segurança de seus ativos e a prestação de serviços de excelência à sociedade e reitera aos usuários de suas informações a responsabilidade no cumprimento da Norma ora apresentada.

CAPÍTULO XVIII
DISPOSIÇÕES FINAIS
Art. 56. O Comitê Gestor de Tecnologia da Informação e Comunicação da Procuradoria-Geral do Distrito Federal (CGTI/PGDF) reconhece a importância do gerenciamento da Segurança da Informação, embora muitas ações de segurança têm sido implementadas de forma reativa e por iniciativas individuais.
Art. 57. A necessidade da elaboração da Norma de Segurança da Informação (NoSIC) decorre do imperativo de atender às recomendações dos órgãos controladores do Distrito Federal, dentre outros, bem como estruturar as boas práticas já existentes.
Art. 58. Com a implantação da NoSIC e das demais ações e políticas que dela decorrerão, busca-se garantir a proteção das informações, da comunicação e de outros ativos críticos da Procuradoria-Geral do Distrito Federal, com o intuito de assegurar a continuidade de suas atividades.
Art. 59. A instituição da NoSIC/PGDF não elimina a necessidade de outras ações e políticas voltadas para a proteção das informações produzidas ou manipuladas com o uso de recursos de tecnologia da informação. Tais ações e políticas deverão ser elaboradas e implantadas de maneira contínua, contemplando as três principais áreas meio que estruturam uma Unidade Administrativa: infraestrutura, pessoas e tecnologia da informação.

CAPÍTULO XIX
DAS REFERÊNCIAS LEGAIS E NORMATIVAS
Art. 60. Na aplicação e na interpretação das diretrizes estabelecidas nesta NoSIC/PGDF, devem ser observados os seguintes atos legislativos e normativos, além das normas técnicas vigentes, sem prejuízo da aplicação dos que vierem a ser editados ou publicados posteriormente:

1. Lei Federal nº 12.965, de 23 de abril de 2014 - Estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil;
2. Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
3. Lei Federal nº 12.737, de 30 de novembro de 2012 - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências;
4. Lei Federal nº 12.735, de 30 de novembro de 2012 - Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências;
5. Lei Federal nº 12.527, de 18 de novembro de 2011 - Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências;
6. Lei Federal nº 9.609, de 19 de fevereiro de 1998 - Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;
7. Decreto Federal nº 7.724 de 16 de maio de 2012 - Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º no inciso II do § 3º do art. 37 e no § 2ºdo art. 216 da Constituição;
8. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;
9. Norma Complementar nº 03/IN01/DSIC/GSIPR - Estabelece diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.
10. Lei Complementar nº 840, de 23 de dezembro de 2011 - Dispõe sobre o regime jurídicos dos servidores públicos civis do Distrito Federal, das autarquias e das fundações públicas distritais;
11. Lei Distrital nº 4.990, de 12 de dezembro de 2012 - Regula o acesso a informações no Distrito Federal previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no art. 216, § 2º, da Constituição Federal e nos termos do art. 45, da Lei federal nº 12.527, de 18 de novembro de 2011, e dá outras providências;
12. Lei Distrital nº 2.572, de 20 de julho de 2000 - Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática;
13. Decreto Distrital nº 45.011, de 27 de setembro de 2023 – Acrescenta o art.269-A ao Decreto Distrital nº 44.330, de 16 de março de 2023, e adota, na Administração Pública Direta e Indireta do Distrito Federal, excetuadas as empresas estatais independentes, a regulamentação editada pela União sobre as contratações de bens e serviços de tecnologia da informação;
14. Decreto Distrital nº 35.382, de 29 de abril de 2014 - Regulamenta o art. 42, da Lei nº 4.990, de 12 de dezembro de 2012, dispõe sobre os procedimentos para credenciamento de segurança, sobre o Núcleo de Segurança e Credenciamento, institui o Comitê Gestor de Credenciamento de Segurança, e dá outras providências;
15. Decreto Distrital nº 25.750, de 12 de abril de 2005 - Regulamenta a Lei nº 2.572, de 20 de julho de 2000, que "Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática";
16. Resolução Distrital nº 1, de 29 de abril de 2024 - Aprova a Política de Segurança da Informação e Comunicação (POSIC) do Governo do Distrito Federal;
17. Resolução Distrital nº 2, de 29 de abril de 2024 - Aprova a Política de Backup e Recuperação de Dados do Governo do Distrito Federal;
18. Portaria da Procuradoria-Geral do Distrito Federal nº 25, de 27 de fevereiro de 2015: Altera a composição do Comitê Gestor de Tecnologia da Informação da Procuradoria-Geral do Distrito Federal, redefine as respectivas atribuições e dá outras providências;
19. Portaria da Procuradoria-Geral do Distrito Federal nº 160, de 08 de abril de 2025: Guia de Uso de Inteligência Artificial Generativa (IAG) na Procuradoria-Geral do Distrito Federal;
20. ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos;
21. ABNT NBR ISO/IEC 27002:2022 - Controles de Segurança da Informação;
22. ABNT NBR ISO/IEC 27005:2023 - Gerenciamento de riscos de segurança da informação;
23. ABNT NBR ISO/IEC 27031:2015 - Tecnologia da informação - Técnicas de segurança - Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação;
24. ABNT NBR ISO/IEC 22301:2024 - Segurança e resiliência - sistema de gestão de continuidade de negócios - Requisitos;
25. ABNT NBR ISO 27701:2019 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes;
26. NIST CSF: Framework de Segurança Cibernética da National Institute of Standards and Technology (NIST);
27. COBIT 2019: Governança e Gestão de Tecnologia da informação;
28. ITIL 4: Gestão de serviços de Tecnologia da informação;

MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

APÊNDICE

TERMO DE RESPONSABILIDADE PARA USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E ADESÃO À NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DA PROCURADORIA-GERAL DO DISTRITO FEDERAL (NoSIC/PGDF)

Nome:

Matrícula:

Cargo:

Documento assinado digitalmente por Cláudio Wladimir de Oliveira
Chefe da Assessoria Especial do Gabinete da Procuradoria-Geral do Distrito Federal

Declaro ter pleno conhecimento:
a) da Norma de Segurança da Informação e Comunicação – NoSIC da Procuradoria-Geral do Distrito Federal (PGDF), publicado pela Portaria nº xxxx de xx/xx/2025, no DODF nº xxx, de xx/xx/2025, que estabelece as diretrizes, normas e procedimentos para a segurança, manuseio, tratamento e controle dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio no âmbito da PGDF;
b) do Guia de Uso da Inteligência Artificial Generativa – IAG da Procuradoria-Geral do Distrito Federal (PGDF), publicado pela Portaria nº 160, de 08/04/2025, no Boletim de Serviços Edição Extra nº 5/2025, de 08/04/2025, que estabelece os princípios, diretrizes e normas para o uso ético, seguro e eficiente de sistemas e ferramentas de IAG no âmbito da PGDF; e
c) Que o descumprimento ou a inobservância das diretrizes, normas, controles e procedimentos estabelecidos nessa Norma e no Guia de Uso da Inteligência Artificial Generativa acarretará na responsabilização administrativa do agente, sem prejuízo de outras medidas que se façam necessárias.

Declaro ainda, que recebi as devidas orientações sobre o conteúdo da Norma de Segurança da Informação e que compreendo integralmente as obrigações aqui assumidas.

Local e data
Assinatura do(a) servidor(a)
Assinatura da Área de TI ou segurança da informação:

PORTARIA Nº 95, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o artigo 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR VINICIUS SILVA PACHECO, matrícula nº 140.990-5, Subprocurador-Geral do Distrito Federal, na Procuradoria do Contencioso em Matéria de Licitações e Contratos, Responsabilidade Civil e Matéria Residual - PROCAD, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo nº 00020-00034920/2018-94.
MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

PORTARIA Nº 96, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR ALAN DO NASCIMENTO GOMES, Procurador do Distrito Federal - Categoria II, matrícula nº 238.749-2, na Procuradoria das Ações Tributárias, da Procuradoria-Geral da Fazenda Distrital, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00008136/2018-21.
MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

PORTARIA Nº 97, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR THIAGO DA SILVA MACEDO, matrícula nº 255.236-1, Procurador do Distrito Federal - Categoria II, na Procuradoria do Contencioso em Matéria de Saúde Pública - PROSAÚDE, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00058969/2024-81.
MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

PORTARIA Nº 98, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR RICARDO HIDEAKI ONO, matrícula nº 255.230-2, Procurador do Distrito Federal - Categoria II, na Procuradoria do Contencioso em Matéria de Saúde Pública - PROSAÚDE, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00058721/2024-10.
MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

PORTARIA Nº 99, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR MATEUS ROCHA DE LISBOA, matrícula nº 1.721.031-3, Procurador do Distrito Federal - Categoria I, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário - PROPES, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00063747/2024-80.
MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

PORTARIA Nº 100, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o artigo 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR IGOR FIORAVANTI MORAIS DE OLIVEIRA, matrícula nº 255.245-0, Procurador do Distrito Federal - Categoria I, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário - PROPES, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo nº 00020-00058670/2024-26.
MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

PORTARIA Nº 101, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o artigo 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR DANIEL DE MORAIS MENDES, matrícula nº 255.256-6, Procurador do Distrito Federal - Categoria I, no Núcleo Trabalhista da Procuradoria do Contencioso em Matéria de Licitações e Contratos, Responsabilidade Civil e Matéria Residual - PROCAD, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo SEI nº 00020-00058929/2024-39.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 102, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR RODRIGO FARIA VIEIRA DOS ANJOS, matrícula nº 255.266-3, Procurador do Distrito Federal - Categoria I, na Procuradoria das Ações Tributárias - PRODAT, da Procuradoria-Geral da Fazenda Distrital, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00058945/2024-21.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 103, DE 25 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR LUCAS DUMONT ÁVILA GARAVINI, matrícula nº 1.723.439-5, Procurador do Distrito Federal - Categoria I, na Procuradoria das Ações de Execução Fiscal, da Procuradoria-Geral da Fazenda Distrital, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00015315/2022-09.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 104, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR ALEXANDRE ALVES COVOLO, matrícula nº 1.723.442-5, Procurador do Distrito Federal - Categoria I , na Procuradoria do Contencioso em Matéria de Pessoal Estatutário, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00005016/2025-09.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 105, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR ANDRÉ CANUTO BEZERRA, matrícula nº 1.721.033-X, Procurador do Distrito Federal - Categoria I, na Procuradoria Especializada em Transação, da Procuradoria-Geral da Fazenda Distrital, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00063744/2024-46.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 106, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR DANIELE PAULINA MARTINS NUNES, Procuradora do Distrito Federal - Categoria I, matrícula nº 256.981-7, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00058934/2024-41.

PORTARIA Nº 107, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR FELIPE DOURADO HUNGRIA, matrícula nº 1.726.297-6, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00041603/2025-53.
MÁRCIO WANDERLEY DE AZEVEDO

Procuradora-Geral do Distrito Federal

PORTARIA Nº 108, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o artigo 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR JOÃO PAULINO DE OLIVEIRA NETO, matrícula nº 255.215-9, Procurador do Distrito Federal - Categoria I, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 0020-00058677/2024-48.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 109, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR KAIO DAVIS CHAVES SILVA, matrícula nº 1.723.441-7, Procurador do Distrito Federal - Categoria I, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00005021/2025-11.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 110, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício da atribuição que lhe confere o art. 6º, incisos XVIII e XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR SENTCLAIR MARINHO DE ASSIS JÚNIOR, matrícula nº 1.723.440-9, Procurador do Distrito Federal - Categoria I, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Distrito Federal. Processo Administrativo nº 00020-00005018/2025-90.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

PORTARIA Nº 111, DE 26 DE FEVEREIRO DE 2026
O PROCURADOR-GERAL DO DISTRITO FEDERAL, no exercício das atribuições que lhe conferem o artigo 6º, inciso XXXV, da Lei Complementar nº 395, de 31 de julho de 2001, RESOLVE:
LOTAR ROBERTA RODRIGUES VIANA, matrícula nº 1.727.010-3, Procuradora do Distrito Federal Categoria I, na Procuradoria do Contencioso em Matéria de Pessoal Estatutário, da Procuradoria-Geral do Contencioso, da Procuradoria-Geral do Consultivo. Processo SEI nº 00020-00055822/2025-10.
MÁRCIO WANDERLEY DE AZEVEDO
Procuradora-Geral do Distrito Federal

ATOS DA SECRETARIA-GERAL DE ADMINISTRAÇÃO

ORDEM DE SERVIÇO N° 32, DE 25 DE FEVEREIRO DE 2026
Designa servidores para compor a equipe de planejamento da contratação de empresa especializada para aquisição/atualização de licença(s) para programa de computador para realização de cópias suplementares (*backup(s)*)
A SUBSECRETÁRIA-GERAL DE ADMINISTRAÇÃO, DA SECRETARIA-GERAL, DA PROCURADORIA-GERAL DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o inciso XI do art. 2º da Portaria nº 238, de 9 de julho de 2021, e considerando o disposto no inciso IV do art. 2º e no inciso IV do art. 10 da Instrução Normativa nº 94, de 23 de dezembro de 2022, da Secretaria de Governo Digital, recepcionada pelo art. 269-A do Decreto nº 44.330, de 16 de março de 2023, bem como as informações constantes no Processo SEI nº 00020-00003912/2026-14, resolve:
Art. 1º Instituir a Equipe de Planejamento da Contratação para a contratação de empresa especializada para aquisição/atualização de licença(s) para programa de computador para realização de cópias suplementares (*backup(s)*)
Art. 2º Designar os servidores abaixo indicados para compor a Equipe de Planejamento da Contratação:
I. PAULO ALVES PEREIRA, matrícula: 34.036-7, da Diretoria de Infraestrutura e Segurança da Informação, como Integrante Requisitante;
II. DOUGLAS RAFAEL MORAIS KOLLAR, matrícula: 226.096-4, da Gerência de Segurança de Rede e Produção, como Integrante Técnico;
III. ANA CLARA MOURA SANDERS, matrícula: 1.712.130-2, da Diretoria de Logística e Documentação, como Integrante Administrativo.
Art. 3º A equipe designada deverá realizar todas as atividades previstas na fase de Planejamento da Contratação, conforme estabelecido na Instrução Normativa SEGES/MGI nº 94/2022, inclusive a elaboração do Estudo Técnico Preliminar, Termo de Referência ou Projeto Básico, análise de riscos e estimativa de preços.
Art. 4º A equipe também deverá apoiar, quando solicitado pelas áreas responsáveis, a fase de Seleção do Fornecedor, e poderá ser requisitada para prestar esclarecimentos e realizar diligências relativas ao Estudo e Planejamento da Contratação até a conclusão do processo, compreendida como a homologação da licitação ou a ratificação da contratação direta.
Parágrafo único. A Equipe de Planejamento da Contratação será automaticamente destituída com a assinatura do contrato, nos termos do art. 29, § 9º da Instrução Normativa nº 94/2022.
Art. 4º Esta Ordem de Serviço entra em vigor na data de sua publicação.
JORDANA CAVALCANTE BARROS
Subsecretária-Geral de Administração

ORDEM DE SERVIÇO Nº 33, DE 25 DE FEVEREIRO DE 2026

Designa servidores para compor a Equipe de Planejamento da contratação de subscrição de licenças de plataforma de desenvolvimento, gerência e monitoramento de software low-code.

A SUBSECRETÁRIA-GERAL DE ADMINISTRAÇÃO, DA SECRETARIA-GERAL, DA PROCURADORIA-GERAL DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o inciso XI do art. 2º da Portaria nº 238, de 9 de julho de 2021, e considerando o disposto no inciso IV do art. 2º e no inciso IV do art. 10 da Instrução Normativa nº 94, de 23 de dezembro de 2022, da Secretaria de Governo Digital, recepcionada pelo art. 269-A do Decreto nº 44.330, de 16 de março de 2023, bem como as informações constantes no Processo SEI nº 00020-00006889/2026-10, resolve:

Art. 1º Instituir a Equipe de Planejamento da Contratação para a contratação de subscrição de licenças de plataforma de desenvolvimento, gerência e monitoramento de software low-code.

Art. 2º Designar os servidores abaixo indicados para compor a Equipe de Planejamento da Contratação:

I. DIEGO CESAR BESSA, matrícula nº 224.746-1, da Diretoria de Soluções em Tecnologia da Informação, como Integrante Requisitante;

II. CLAYTON KENNEDY PASSOS DOS REIS, matrícula nº 172.3154-X, da Gerência de Desenvolvimento de Sistemas, Métrica e Processo de Qualidade, como Integrante Técnico;

III. ANDERSON DE ARAÚJO SANTANA, matrícula nº 251462-1, da Diretoria de Soluções em Tecnologia da Informação, como Integrante Técnico;

IV. AMANDA ALMEIDA DE FREITAS, matrícula nº 256.845-4, da Diretoria de Logística e Documentação, como Integrante Administrativo.

Art. 3º A equipe designada deverá realizar todas as atividades previstas na fase de Planejamento da Contratação, conforme estabelecido na Instrução Normativa SEGES/MGI nº 94/2022, inclusive a elaboração do Estudo Técnico Preliminar, Termo de Referência ou Projeto Básico, análise de riscos e estimativa de preços.

Art. 4º A equipe também deverá apoiar, quando solicitado pelas áreas responsáveis, a fase de Seleção do Fornecedor, e poderá ser requisitada para prestar esclarecimentos e realizar diligências relativas ao Estudo e Planejamento da Contratação até a conclusão do processo, compreendida como a homologação da licitação ou a ratificação da contratação direta.

Parágrafo único. A Equipe de Planejamento da Contratação será automaticamente destituída com a assinatura do contrato, nos termos do art. 29, § 9º da Instrução Normativa nº 94/2022.

Art. 5º Esta Ordem de Serviço entra em vigor na data de sua publicação.

JORDANA CAVALCANTE BARROS

Subsecretária-Geral de Administração

ORDEM DE SERVIÇO Nº 34, DE 25 DE FEVEREIRO DE 2026

Designa servidores para atuarem como fiscais das Notas de Empenho decorrentes de Atas de Registro de Preços destinadas à aquisição de materiais permanentes e de consumo para a Procuradoria-Geral do Distrito Federal.

A SUBSECRETÁRIA-GERAL DE ADMINISTRAÇÃO DA SECRETARIA-GERAL DA PROCURADORIA GERAL DO DISTRITO FEDERAL, no uso da delegação de competência conferida pelo art. 2º, inciso XII, da Portaria nº 238, de 9 de julho de 2021, RESOLVE:

Art.1º. Designar ITALLO GABRIEL ALBUQUERQUE DE ANDRADE, Gerente de Administração Predial e Controle da Frota, matrícula nº 244.357-0, para atuar como fiscal titular, e WALACE ALBUQUERQUE DA CUNHA, Assessor Técnico, matrícula nº 252.066-4, para atuar como fiscal substituto, das Notas de Empenhos emitidas com fundamento nas Atas de Registro de Preços n.º 004/2026, 005/2026, 006/2026, 007/2026, 008/2026, 009/2026, 010/2026, 011/2026, 012/2026, 013/2026, 014/2026, 015/2026, 016/2026, 017/2026 e 018/2026, constantes do Processo SEI nº 00020-00035314/2025-15, cujo objeto consiste na aquisição de refrigeradores, micro-ondas, cafeteiras, bebedouros, lixeiras, utensílios de copa e cozinha e demais itens correlatos, conforme especificações constantes do Edital do Pregão Eletrônico nº 90010/2025 e seus anexos (187430909).

§ 1º O fiscal titular será substituído, em seus afastamentos e impedimentos legais, pelo fiscal substituto designado neste ato.

§ 2º Compete aos fiscais acompanhar, fiscalizar e atestar o recebimento dos bens, registrando todas as ocorrências relacionadas à execução das obrigações decorrentes das Notas de Empenho, adotando as providências necessárias à regularização de eventuais falhas ou inconformidades.

Art. 2º A fiscalização deverá observar o disposto no art. 117 da Lei nº 14.133, de 1º de abril de 2021, no Decreto nº 44.330, de 16 de março de 2023, bem como nas Normas de Planejamento, Orçamento, Finanças, Patrimônio e Contabilidade do Distrito Federal.

Art. 3º Esta Ordem de Serviço entra em vigor na data de sua publicação.

JORDANA CAVALCANTE BARROS

Subsecretária-Geral de Administração

O **Boletim Interno da Procuradoria-Geral do Distrito Federal,** instituído pela Portaria nº 307, de 7 de agosto de 2017, tem o objetivo de tornar públicos atos de caráter interno cuja divulgação no Diário Oficial do Distrito Federal não é exigida por lei.

Os atos divulgados neste Boletim podem ser pesquisados no Sistema Integrado de Normas Jurídicas do Distrito Federal - **www.sinj.df.gov.br**.

PGDF PROCURADORIA-GERAL DO DISTRITO FEDERAL

SAM, Bloco I, Edifício Sede - CEP: 70620-090

MÁRCIO WANDERLEY DE AZEVEDO
Procurador-Geral do Distrito Federal

CARLOS AUGUSTO VALENZA DINIZ
Secretário-Geral

CLAUDIO WLADIMIR DE OLIVEIRA:69610010172

Assinado de forma digital por CLAUDIO WLADIMIR DE OLIVEIRA:69610010172
Dados: 2026.02.27 15:38:43 -03'00'