Publicada no Suplemento ao Boletim Geral n° 197, de 26 de outubro de 2026

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (NOSIC) NO ÂMBITO DO CBMDF

Portaria n° 24, de 26 de outubro de 2026

Institui a Norma de Segurança da Informação e Comunicação – NoSIC, no âmbito do Corpo de Bombeiros Militar do Distrito Federal.

O COMANDANTE-GERAL, no uso das atribuições que lhe conferem os incisos II, III e V, do art. 7°, do Decreto n° 7.163, de 29 de abril de 2010, que regulamenta a organização básica do CBMDF, e considerando o que consta do Processo n° SEI 0053-01619/2011, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1° Fica instituída a Norma de Segurança da Informação e Comunicação – NoSIC, no âmbito do Corpo de Bombeiros Militar do Distrito Federal, de natureza complementar e em conformidade com os princípios e diretrizes instituídos pela Política de Segurança da Informação e Comunicação do Governo do Distrito Federal – PoSIC, aprovada pela Resolução n° 01, de 29 de abril de 2024, do Comitê Gestor de Tecnologia da Informação e Comunicação do Distrito Federal.

CAPÍTULO II
SEÇÃO I
DO ESCOPO DA NORMA

Art. **2°** A Norma de Segurança da Informação e Comunicação – NoSIC do Corpo de Bombeiros Militar do Distrito Federal tem o propósito de limitar a exposição ao risco a níveis aceitáveis e buscar continuamente a disponibilidade, a integridade, a confidencialidade, a autenticidade e o não repúdio das informações necessárias ao cumprimento da missão institucional.

Parágrafo único. Deverão ser observadas as disposições da Lei Federal n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e da Lei Federal n° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), cabendo a sua aplicação às áreas responsáveis pelo tratamento de dados pessoais no âmbito do Corpo de Bombeiros Militar do Distrito Federal.

Art. 3° Esta Norma aplica-se a todas as unidades da estrutura do Corpo de Bombeiros Militar do Distrito Federal e deverá ser observada por todos os militares, colaboradores, consultores externos, prestadores de serviço e qualquer outra pessoa que tenha acesso a dados e informações institucionais, sob pena de responsabilização administrativa, penal, civil ou militar, na forma da lei.

SEÇÃO II
DOS PRINCÍPIOS

Art. 4° A segurança da informação e comunicação no Corpo de Bombeiros Militar do Distrito Federal deverá ser orientada pelos seguintes princípios:

I – simplicidade: controles de segurança simples e objetivos;

II – confidencialidade: a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados;

III – integridade: informação não modificada ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino;

IV – privilégio mínimo: os usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhes foram designadas;

V – 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;

VI – auditabilidade: todos os eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;

VII – mínima dependência de segredos: a segurança do sistema não deve depender exclusivamente da confidencialidade de informações sensíveis, devendo também estar apoiada em mecanismos adicionais de proteção e autenticação;

VIII – resiliência: os controles de segurança devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

IX – defesa em profundidade: os controles de segurança devem ser concebidos em múltiplas camadas, de modo a prover redundância que permita a aplicação de controles adicionais em caso de falha.

CAPÍTULO III
DAS DIRETRIZES GERAIS
SEÇÃO I
DO CICLO DE VIDA DA INFORMAÇÃO

Art. 5° As medidas de proteção devem ser adotadas durante todo o ciclo de vida da informação, compreendendo as fases de criação, manipulação, armazenamento, transporte e descarte.

SEÇÃO II
DAS DISPOSIÇÕES GERAIS ACERCA DAS NORMAS E DOS PROCEDIMENTOS

Art. 6° As determinações e procedimentos compreendidos por esta Norma deverão abordar, sem se limitar, os seguintes aspectos:

I – segurança física;

II – gestão de mudanças;

III – privacidade;

IV – criptografia;

V – acesso à rede;

VI – gestão de senhas e contas de usuário;

VII – dispositivos móveis;

VIII – gestão de incidentes;

IX – plano de continuidade de negócios;

X – proteção à propriedade intelectual;

XI – treinamento e conscientização em segurança da informação.

Parágrafo único. Os Procedimentos de Segurança da Informação e Comunicação - ProSIC descrevem, detalhadamente, as medidas operacionais necessárias para atingir os resultados estabelecidos na presente Norma de Segurança da Informação e Comunicação – NoSIC e na Política de Segurança da Informação e Comunicação – PoSIC, abordando aspectos técnicos e práticos adaptados à realidade institucional. No âmbito do Corpo de Bombeiros Militar do Distrito Federal, os ProSICs serão desenvolvidos pelo Comitê Gestor de Tecnologia da Informação e Comunicação – CGTIC, mediante minuta elaborada pelo Centro de Inteligência - CEINT ou pela Diretoria de Tecnologia da Informação e Comunicação - DITIC, de acordo com as atribuições previstas na Portaria n° 6, de 29 de janeiro de 2025.

SEÇÃO III
DA DIVULGAÇÃO

Art. 7° Esta Norma, assim como as dela decorrentes, deverá ser disponibilizada e agrupada em sítio institucional, em local de fácil acesso, proporcionando ampla difusão, atualização simplificada e fornecimento de informações sobre datas de publicação ou revisão.

Art. 8° Os procedimentos de segurança da informação considerados imprescindíveis à segurança da sociedade ou do Estado poderão ser classificados ou submetidos à restrição de acesso, na forma da lei e da Portaria n° 11, de 1° de abril de 2025, que trata das Diretrizes e Procedimentos relacionados ao Tratamento de Informação Sigilosa ou sob Restrição de Acesso, sendo divulgados apenas àquelas cujas atribuições exijam seu conhecimento.

SEÇÃO IV
DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 9° As instalações em que informações críticas ou sensíveis sejam processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física.

Art. 10. Os equipamentos deverão ser protegidos contra ameaças físicas e ambientais, incluindo aqueles utilizados fora da instalação.

SEÇÃO V
DA AQUISIÇÃO, DO DESENVOLVIMENTO E DA MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

Art. 11. Deverão ser desenvolvidas ações que garantam que a segurança seja parte integrante dos sistemas de informação e comunicação existentes, bem como daqueles que vierem a ser desenvolvidos ou adquiridos.

Art. 12. Todos os requisitos de segurança deverão ser identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados, como parte da justificativa de negócio do sistema de informação.

SEÇÃO VI
DA EDUCAÇÃO CONTINUADA

Art. 13. Para uma efetiva proteção das informações, a Diretoria de Tecnologia da Informação e Comunicação e o Centro de Inteligência, conjuntamente, deverão elaborar plano contínuo de capacitação de recursos humanos em segurança da informação, de modo a promover a preparação dos usuários e a conscientização quanto à responsabilidade individual.

SEÇÃO VII
DAS PENALIDADES

Art. 14. O descumprimento das diretrizes desta Norma, assim como de suas normas e procedimentos vinculados, acarretará sanções administrativas, sem prejuízo das ações cíveis, penais e militares cabíveis.

CAPÍTULO IV
DAS COMPETÊNCIAS E RESPONSABILIDADES
SEÇÃO I
DO COMANDANTE-GERAL DO CORPO DE BOMBEIROS MILITAR DO DISTRITO FEDERAL

Art. 15. Compete ao Comandante-Geral do Corpo de Bombeiros Militar do Distrito Federal:

I – apoiar e exigir o cumprimento desta Norma, além das normas e procedimentos de segurança da informação e comunicação;

II – zelar para que contratos, convênios e outros instrumentos similares elaborados pelo Corpo de Bombeiros Militar do Distrito Federal estejam alinhados à presente Norma e seus instrumentos legais adjacentes;

III – priorizar a capacitação contínua de seus recursos humanos de modo a promover maior independência do Estado na gestão e execução das atividades de segurança da informação e comunicação;

IV – coordenar a execução desta Norma, mobilizando gestores para o seu efetivo cumprimento;

V – promover a cultura de segurança da informação e comunicação;

VI – exercer outras atividades decisórias afetas à gestão de segurança da informação e comunicação no âmbito do Corpo de Bombeiros Militar do Distrito Federal.

SEÇÃO II
DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 16. Considera-se Gestor de Segurança da Informação e Comunicação o bombeiro militar encarregado das ações de segurança da informação e comunicação no âmbito do CBMDF e considera-se o Responsável pela Segurança da Informação e Comunicação o bombeiro militar encarregado por essas ações no âmbito da sua respectiva unidade administrativa.

Art. 17. Compete ao Gestor de Segurança da Informação e Comunicação:

I – presidir o Comitê Gestor de Tecnologia da Informação e Comunicação do CBMDF;

II – monitorar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III – cobrar dos respectivos proprietários a classificação das informações na área sob sua gerência;

IV – propor recursos necessários às ações de segurança da informação e comunicação;

V – realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicação;

VI – propor normas e procedimentos relativos à segurança da informação e comunicação;

VII – definir, após deliberação do Comitê, métricas que permitam aferir a eficiência e eficácia dos controles de segurança.

Parágrafo único. A gestão de segurança da informação deverá ser realizada somente por militares com vínculo efetivo.

Art. 18. Compete aos Responsáveis pela Segurança da Informação e Comunicação das diferentes unidades administrativas do Corpo de Bombeiros Militar do Distrito Federal:

I – zelar e fazer cumprir a Norma de Segurança da Informação e Comunicação do Corpo de Bombeiros Militar do Distrito Federal;

II – 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;

III – aplicar medidas que visem a garantir que o pessoal sob sua supervisão proteja informações da unidade administrativa às quais tenha acesso;

IV – proteger, em nível físico e lógico, os ativos de informação e de processamento da unidade administrativa relacionados com sua área de atuação;

V – 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;

VI – comunicar formalmente o desligamento (exoneração, demissão, transferência, cessão), suspensão ou afastamento preventivo de usuários aos gestores da área de gestão de pessoas e aos proprietários de informações, os quais deverão notificar a área de tecnologia da informação para medidas cabíveis;

VII – 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.

Art. 19. São obrigações dos usuários:

I – observar rigorosamente esta Norma de Segurança da Informação e Comunicação, bem como outros normativos e procedimentos a ela vinculados;

II – assegurar o uso racional dos recursos de tecnologia da informação e comunicação colocados à sua disposição, priorizando o interesse público e institucional;

III – comunicar a área competente acerca de quaisquer riscos ou incidentes de segurança de que venha a tomar conhecimento;

IV – assegurar-se de que as senhas e credenciais para acesso aos ativos de processamento e de informações estejam de acordo com os procedimentos estabelecidos e sejam mantidas sob sigilo, não devendo ser compartilhadas;

V – manter, obrigatoriamente, os dados críticos da sua unidade administrativa em compartilhamentos de rede disponibilizados pela Diretoria de Tecnologia da Informação e Comunicação;

VI – 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;

VII – 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.

SEÇÃO III
DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 20. Compete à Diretoria de Tecnologia da Informação e Comunicação - DITIC, órgão de direção setorial responsável pela direção e pelo planejamento setoriais, bem como pela elaboração de normas e diretrizes das atividades de tecnologia da informação e dos serviços de comunicação:

I – realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes;

II – assegurar o pleno e efetivo funcionamento dos recursos de tecnologia da informação e comunicação disponibilizados;

III – assegurar a integridade e disponibilidade dos ativos que se encontram no seu ambiente computacional;

IV – conjuntamente com o Centro de Inteligência, dar assistência ao Comitê Gestor de Tecnologia da Informação e Comunicação – CGTIC na elaboração de normas e procedimentos de segurança da informação no tocante às informações, comunicações e processos presentes no ambiente computacional;

V – 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;

VI – requisitar informações às demais unidades do CBMDF, realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento desta Norma, no tocante aos ativos informatizados;

VII – elaborar o Plano de Resposta a Incidentes, com o apoio do Centro de Inteligência;

VIII – manter registro das atividades de usuários (logs), de maneira a abranger o máximo de ações possíveis dentro dos sistemas e pelo maior tempo possível;

IX – adotar como padrão de endereço de e-mail corporativo o formato @cbm.df.gov.br;

X – priorizar o uso institucional do acesso à internet, podendo bloquear ou limitar acesso a determinados sítios de internet e estabelecendo categorias passíveis de acesso em horários restritos;

XI – instalar sistemas operacionais nos computadores do Corpo de Bombeiros Militar do Distrito Federal, devidamente licenciados e atualizados;

XII – instalar softwares e mecanismos de proteção, no mínimo antivírus e firewall, devidamente licenciados e atualizados;

XIII – instalar e permitir a instalação apenas de software devidamente licenciado e homologado, de modo a não comprometer a segurança do ambiente;

XIV – manter atualizados os demais itens de software do parque computacional;

XV – conjuntamente com o Centro de Inteligência, elaborar normas e procedimentos complementares a esta NoSIC.

SEÇÃO IV
DO PROPRIETÁRIO DA INFORMAÇÃO

Art. 21. Considera-se proprietário da informação o militar 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.

Art. 22. São obrigações do proprietário da informação:

I – identificar e definir as informações críticas e os requisitos de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio;

II – classificar e rever periodicamente a classificação dos ativos sob sua propriedade que requerem algum grau de sigilo, observando a legislação em vigor;

III – participar do processo de avaliação e aceitação de risco;

IV – participar das decisões relacionadas a qualquer violação de segurança dos ativos sob sua propriedade;

V – autorizar a liberação de acesso à informação sob sua responsabilidade;

VI – revogar a liberação de acesso à informação sob sua responsabilidade, após recebidos comunicados de desligamento, suspensão ou afastamento preventivo de bombeiros militares;

VII – participar da definição dos critérios para estabelecer perfis de acesso a informações sob sua responsabilidade;

VIII – participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

IX – participar, sempre que convocado, das reuniões do Comitê Gestor de Tecnologia da Informação e Comunicação - CGTIC, prestando os esclarecimentos solicitados.

SEÇÃO V
DO CUSTODIANTE DOS ATIVOS DA INFORMAÇÃO

Art. 23. Considera-se custodiante o militar a quem é conferida a responsabilidade de guardar ativos de informação pertencentes a terceiros.

Parágrafo único. A custódia não concede o direito de acesso ao ativo, nem o poder de conceder direito de acesso a outros.

Art. 24. São obrigações do custodiante dos ativos da informação:

I – prestar assistência ao proprietário da informação na definição dos procedimentos operacionais e de controle, referentes a manuseio, armazenamento e disposição final dos ativos;

II – controlar e proteger os ativos sob sua custódia;

III – realizar, verificar e manter cópias de segurança (backups) dos ativos de informação sob sua custódia, a menos que outra solução seja acordada formalmente entre o proprietário da informação e o custodiante;

IV – comunicar à DITIC e ao proprietário da informação qualquer incidente de segurança que afete os ativos sob sua custódia;

V – implementar os controles de segurança e, se necessário, solicitar a contratação de bens e serviços de segurança da informação e comunicação.

SEÇÃO VI
DO GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Art. 25. Fica instituído, no âmbito do Corpo de Bombeiros Militar do Distrito Federal, o Grupo de Resposta a Incidentes de Segurança – GRIS, composto por bombeiros militares vinculados à Diretoria de Tecnologia da Informação e Comunicação - DITIC.

Art. 26. Compete ao GRIS:

I – receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores, sistemas estruturantes, dados trafegados na Rede Corporativa Metropolitana GDFNet e serviços corporativos de tecnologia da informação e comunicação hospedados e sustentados no ambiente tecnológico do Centro de Tecnologia da Informação e Comunicação do Distrito Federal – CeTIC;

II – 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;

III – 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, inclusive por solicitação do Controlador (Encarregado Setorial do CBMDF) nos casos de necessidade de suporte técnico para incidentes de segurança com dados pessoais, conforme dispositivos de triagem e classificação do Guia Orientativo de Respostas a Incidentes de Segurança com dados pessoais no âmbito do CBMDF;

IV – registrar, classificar e filtrar as notificações de incidentes de segurança;

V – executar o Plano de Resposta a Incidentes;

VI – recolher e preservar as evidências para subsidiar a forense computacional;

VII – investigar, com caráter estritamente técnico, as causas dos incidentes no ambiente computacional.

CAPÍTULO V
DA ATUALIZAÇÃO

Art. 27. Esta Norma de Segurança da Informação e Comunicação, assim como os instrumentos normativos e procedimentos dela decorrentes, deverá ser atualizada a cada dois anos, ou sempre que houver mudanças significativas que afetem a base original de avaliação de riscos ou o contexto organizacional.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 28. Esta Portaria entra em vigor na data de sua publicação.

(NB-CBMDF/GABCG/SEAAD -0053-01619/2011)