# PORTARIA Nº 230, DE 12 DE JULHO DE 2022

Institui a Norma de Segurança da Informação e Comunicação – NoSIC, no âmbito da Secretaria de Estado de Economia do Distrito Federal

## CAPÍTULO I
## DAS DISPOSIÇÕES PRELIMINARES

O SECRETÁRIO DE ESTADO DE ECONOMIA DO DISTRITO FEDERAL, no uso da atribuição que lhe confere o art. 105, parágrafo único, incisos I e III da Lei Orgânica do Distrito Federal, bem como o art. 23, XII, do Decreto Distrital nº 39.610, de 01 de janeiro de 2019, resolve:

Art. 1º Instituir Norma de Segurança da Informação e Comunicação – NoSIC, no âmbito da Secretaria de Estado de Economia do Distrito Federal, de natureza complementar e em conformidade com princípios e diretrizes instituídos pela Política de Segurança da Informação e Comunicação do Governo do Distrito Federal – PoSIC, aprovada pela Resolução nº 03, de 06 de novembro de 2018, do Comitê Gestor de Tecnologia da Informação e Comunicação do Distrito Federal.

## CAPÍTULO II

### SEÇÃO I
### DO ESCOPO DA NORMA

Art. 2º A Norma de Segurança da Informação e Comunicação da Secretaria de Estado de Economia 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 que suportam os objetivos estratégicos desta Secretaria.

Parágrafo único. Deverão ser observadas, no que couber, as disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, cabendo a sua aplicação às áreas responsáveis pelo tratamento de dados pessoais no âmbito da Secretaria de Estado de Economia do Distrito Federal.

Art. 3º Esta Norma aplica-se a todas as unidades da estrutura administrativa da Secretaria de Estado de Economia do Distrito Federal e deverá ser fielmente observada por todos os servidores públicos, colaboradores, estagiários, consultores externos, prestadores de serviço e qualquer outra pessoa que tenha acesso a dados e informações do Estado, sob pena de responsabilização administrativa, penal ou civil, na forma da lei.

### SEÇÃO II
### DOS PRINCÍPIOS

Art. 4º O conjunto de documentos que compõe esta Norma deverá ser orientado pelos seguintes princípios:

I - simplicidade: controles de segurança simples e objetivos;

II - privilégio mínimo: usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas;

III - 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;

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

V - mínima dependência de segredos: os controles deverão ser efetivos, ainda que se conheça sua a existência e o seu funcionamento;

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

VII - defesa em profundidade: os controles de segurança devem ser concebidos em múltiplas camadas, de modo a prover redundância que permita a aplicação de controle diverso no caso de falha.

## CAPÍTULO III
## DIRETRIZES GERAIS

### SEÇÃO I
### DO CICLO DE VIDA DA INFORMAÇÃO

Art. 5º 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
### NORMAS E PROCEDIMENTOS – ASPECTOS GERAIS

Art. 6º As determinações e procedimentos compreendidos por esta Norma deverão abordar, mas não limitados a estes, 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; e

XI - treinamento e sensibilização para segurança;

**SEÇÃO III**
**DA DIVULGAÇÃO**

Art. 7º Esta Norma, assim como as dela decorrentes, deverão ser disponibilizadas e agrupadas em sítio institucional em local de fácil acesso, proporcionando ampla difusão e atualização simplificada, assim como fornecimento de informações sobre datas publicação e/ou revisão.

Art. 8º Os procedimentos de segurança da informação, por conter informações sensíveis, deverão ser classificados na forma da lei e divulgados para aqueles cujas atribuições exigem conhecimento das mesmas.

**SEÇÃO IV**
**DA SEGURANÇA FÍSICA E DO AMBIENTE**

Art. 9º As instalações em que as informações críticas ou sensíveis serão 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**
**AQUISIÇÃO, DESENVOLVIMENTO E 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, e também os que forem desenvolvidos e/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 do caso geral de negócios do sistema de informação.

**SEÇÃO VI**
**EDUCAÇÃO CONTINUADA**

Art. 13. Para uma efetiva proteção das informações, as unidades administrativas da Secretaria de Estado de Economia do Distrito Federal deverão elaborar um plano contínuo de capacitação de recursos humanos em segurança da informação, de modo a promover maior preparação e consciência da responsabilidade individual dos usuários.

**SEÇÃO VII**
**PENALIDADES**

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

**CAPÍTULO IV**
**COMPETÊNCIAS E RESPONSABILIDADES**

**SEÇÃO I**
**DO SECRETÁRIO DE ESTADO DE ECONOMIA**

Art. 15. Compete ao titular do cargo de Secretário de Estado de Economia 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 pela respectiva unidades administrativas 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 Comunicações no âmbito da Secretaria de Estado de Economia do Distrito Federal; e

VII - instituir o Comitê de Segurança da Informação no âmbito da Secretaria de Estado de Economia do Distrito Federal e nomear os servidores que farão parte da sua composição.

## SEÇÃO II
## DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 16. Fica criado o Comitê de Segurança da Informação da Secretaria de Estado de Economia do Distrito Federal - CSIC, órgão colegiado que possui as seguintes competências:

I - elaborar e atualizar a Norma de Segurança da Informação e Comunicação – NoSIC, procedimentos de segurança da informação e comunicação em conformidade com a Política de Segurança da Informação e Comunicação do Distrito Federal, objetivos estratégicos da Secretaria, leis e regulamentos pertinentes;

II - elaborar e aprovar normas e procedimentos de segurança da informação e comunicação;

III - coordenar a execução da Norma de Segurança da Informação e Comunicação da Secretaria de Estado de Economia do Distrito Federal, mobilizando gestores para o seu cumprimento;

IV - estabelecer um Programa de Gestão de Riscos, atualizando-o quando necessário;

V - desenvolver um Plano de Continuidade de Negócios, que deverá ser testado periodicamente;

VI - instituir grupos de trabalho específicos relacionados à segurança da informação e comunicação;

VII - estabelecer mecanismos de registro e controle de não conformidade com esta Norma e com procedimentos de segurança da informação e comunicação; e

VIII - exercer outras atividades decisórias afetas à gestão de segurança da informação e comunicações no âmbito da Secretaria de Estado de Economia do Distrito Federal.

Parágrafo único.O Comitê de Segurança da Informação da Secretaria de Estado de Economia do Distrito Federal possui a seguinte composição:

I -um gestor de segurança da informação, que coordenará as atividades do comitê;

II - um membro da área de segurança física;

III - um membro da área de segurança digital;

IV - um membro da área administrativa;

V - um membro da área de normas e legislação; e

VI - um membro da área de gestão de pessoas.

## SEÇÃO III
## DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 17. Considera-se gestor de segurança da informação o servidor responsável pelas ações de segurança da informação e comunicação no âmbito da respectiva unidade administrativa

Art. 18. Compete ao gestor de segurança da informação e comunicação:

I - monitorar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

II - cobrar dos respectivos proprietários a classificação das informações na área sob sua gerência;

III - propor recursos necessários às ações de segurança da informação e comunicação;

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

V - propor normas e procedimentos relativos à segurança da informação e comunicação; e

VI – 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 servidores com vínculo efetivo ou empregados públicos.

Art. 19. Compete aos gestores das diferentes áreas da Secretaria de Estado de Economia do Distrito Federal:

I - zelar e fazer cumprir a Norma de Segurança da Informação e Comunicação da Secretaria de Estado de Economia 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 a que tem 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; e

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. 20. 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, e consonância com a Portaria nº 143 de 24 de maio de 2021, que disciplina a utilização dos recursos e serviços de tecnologia da informação e comunicação no âmbito da Secretaria de Estado de Economia do Distrito Federal ;

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 que as mesmas sejam protegidas e confidenciais, não devendo ser compartilhadas;

V - manter, obrigatoriamente, os dados críticos da sua unidade administrativa em compartilhamentos de rede disponibilizados pela área de tecnologia da informação e comunicação;

VI - não utilizar serviços de e-mail gratuitos para atividades institucionais, visto que tais serviços não possuem garantia de autenticidade, disponibilidade e confidencialidade das informações;

VII - 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; e

VIII - 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.

Art. 21. A gestão de senhas da Secretaria e de todas as suas unidades administrativas obedecerá o seguinte procedimento:

I - As senhas para acesso à rede da Secretaria conterão, no mínimo, 8 caracteres, compostos de pelo menos 3 das 4 categorias a seguir: letras maiúsculas (A – Z), letras minúsculas (a – z), dígitos de base 10 (0 a 9), caracteres especiais (!, $, #, % e outros), de modo que não sejam criadas senhas fracas ou óbvias;

II - Os usuários serão requeridos a alterar as suas respectivas senhas da rede local a cada 90 (noventa) dias, não sendo permitido o uso das últimas 5 (cinco) senhas; e

III - O usuário de rede será bloqueado após a terceira tentativa de acesso com a senha incorreta, sendo o acesso reestabelecido após 5 (cinco) minutos.

Parágrafo Único. Considera-se senhas fracas ou óbvias aquelas em que se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras com significado, dentre outras.

## SEÇÃO IV
## DA SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 22. À Subsecretaria de Tecnologia da Informação, unidade orgânica subordinada à Secretaria de Estado de Economia do Distrito Federal, responsável pela gestão da tecnologia da informação e comunicação desta pasta, do Centro de Tecnologia da Informação e Comunicação do Distrito Federal – CeTIC-DF e da Rede Corporativa Metropolitana GDFNet, compete:

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 - dar assistência ao Comitê de Segurança de Informação e Comunicação na elaboração normas e procedimentos de segurança da informação no tocante às informações, comunicações e processos relativos 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 áreas de sua unidade administrativa, 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;

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 @.df.gov.br;

X - 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;

XI - instalar sistemas operacionais nos computadores da Secretaria, devidamente licenciados e atualizados;

XII - instalar itens de softwares e mecanismos de proteção (minimamente, anti-vírus e firewall nas estações de trabalho) 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; e

XV - editar normas com procedimentos complementares a esta NoSIC.

**SEÇÃO V**
**DO PROPRIETÁRIO DA INFORMAÇÃO**

Art. 23. Considera-se proprietário da informação o servidor 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. 24. 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 nas 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 servidores;

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; e

IX - participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

**SEÇÃO VI**
**DO CUSTODIANTE DOS ATIVOS DA INFORMAÇÃO**

Art. 25. Considera-se custodiante o servidor a quem é conferida a responsabilidade de guardar ativos de informações 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. 26. 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 respectiva área da TIC 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 VII**
**DO GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA (CSIRT)**

Art. 27. Fica criado, no âmbito da Secretaria de Estado de Economia do Distrito Federal, o Grupo de Resposta a Incidentes em Segurança – CSIRT, grupo de servidores vinculados à Subsecretaria de Tecnologia da Informação e Comunicação, com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores, nos sistemas estruturantes, nos dados trafegados na Rede Corporativa Metropolitana GDFNet e nos 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.

Art. 28. Compete ao CSIRT:

I - 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;

II - 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;

III - registrar, classificar e filtrar as notificações de incidentes de segurança;

IV - executar o Plano de Resposta a Incidentes;

V - recolher e preservar as evidências para subsidiar a forense computacional; e

VI - investigar as causas dos incidentes no ambiente computacional.

## CAPÍTULO V
## DA ATUALIZAÇÃO

Art. 29. Esta Norma de Segurança de Informação e Comunicação, assim como instrumentos legais e procedimentos que dela se originarem, deverão ser atualizadas a cada dois anos, ou quando houver mudanças significativas que afetem a base de avaliação de risco original ou o contexto organizacional.

**JOSÉ ITAMAR FEITOSA**