SUBSECRETARIA DE MODERNIZAÇÃO TECNOLÓGICA - SSP/DF

Relatório da NoSIC

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

CAPÍTULO I
DO ESCOPO E OBJETIVOS

Art. 1 A Norma de Segurança da Informação e Comunicação – NoSIC da SSP/DF, desdobrada da Política de Segurança da Informação e Comunicação – PoSIC do GDF, descrita na Resolução nº 03 de 06 de novembro de 2018, tem como escopo a fundamentação dos princípios e requisitos de segurança da informação, em atendimento às recomendações dos Órgãos de Controle, para o manuseio, processamento, armazenamento e transmissão da informação por meios digitais no âmbito da Secretaria de Estado de Segurança Pública do Distrito Federal - SSP/DF, não sendo considerados nesta Norma, o manuseio, processamento, armazenamento e transmissão da informação pelos meios físicos.

Art. 2 A implantação da NoSIC na Secretaria de Estado de Segurança Pública do Distrito Federal tem o objetivo de:
I - Melhorar a disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam os objetivos estratégicos da SSP/DF
II - Garantir os direitos individuais e coletivos dos servidores e prestadores de serviço no que diz respeito à inviolabilidade da sua intimidade e o sigilo das informações pessoais;
III - Limitar a exposição ao risco a níveis aceitáveis.

Art. 3 A presente Norma aplica-se a todas as unidades da estrutura administrativa da Secretaria e deverá ser fielmente observada por todos os servidores públicos, colaboradores, estagiários, consultores externos e prestadores de serviços.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 4 A NoSIC e os procedimentos derivados dela, deverão se guiar pelos seguintes princípios, descritos no Capítulo III da PoSIC do GDF:
I. Simplicidade: A complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser 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 a existências deles e como eles funcionam;

VI. Resiliência: Os controles de segurança deverão ser projetados para que possam resistir e se recuperarem dos efeitos de um desastre;

VII. 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.

VIII. Conscientização: Os usuários devem estar conscientizados da necessidade de segurança de sistemas de informação e redes e do que eles podem fazer para aumentar a segurança.

IX. Responsabilidade: Todos os participantes são responsáveis pela segurança de sistemas de informação e redes.

X. Arquitetura e implementação de segurança: Os usuários devem incorporar a segurança como um elemento essencial de sistemas de informação e redes.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Seção I - Estrutura Normativa

Art. 5 A presente norma é parte de um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

I. Política de Segurança da Informação e Comunicação (PoSIC): de caráter estratégico, define a estrutura, diretrizes gerais e as obrigações referentes à segurança da informação e comunicação, servindo de base para elaboração dos demais documentos da estrutura normativa sendo, no GDF, elaborada e mantida pelo Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC) do Governo do Distrito Federal (PoSIC/GDF);

II. Normas de Segurança da Informação e Comunicação (NoSIC): de caráter tático, e constituída neste documento, define as normas e estabelecem regras para a utilização de ativos e recursos de tecnologia da informação com o intuito de atingir os objetivos da Política;

III. Procedimentos de Segurança da Informação e Comunicação (ProSIC): descreve, detalhadamente, as medidas operacionais necessárias para atingir os resultados estabelecidos nas Normas e na Política, abordando aspectos técnicos e práticos, adaptados à realidade do ambiente.

Parágrafo único. Caberá ao Subcomitê de Segurança da Informação e Comunicação (SSIC) da SSP/DF, a responsabilidade pela elaboração da minuta e proposta de atualização permanente da NoSIC, quando no âmbito da Secretaria.

Seção II - Diretrizes gerais da PoSIC do GDF

Art. 6 Devem ser observadas as diretrizes gerais do ciclo de vida da informação, normas e procedimentos complementares, divulgação, segurança física e do ambiente, aquisição, desenvolvimento e manutenção de sistema de informação e educação continuada descritas no Capítulo IV da PoSIC do GDF.

CAPÍTULO IV
DAS DIRETRIZES ESPECÍFICAS

Seção I - Gestão da Segurança da Informação e Comunicações (GESIC)

Art. 7 São diretrizes da Gestão da Segurança da Informação e Comunicação:

I - Todos os mecanismos de proteção utilizados para a SIC, em atendimento aos objetivos definidos nesta NoSIC, devem ser mantidos com o intuito de garantir a continuidade dos negócios da SSP/DF.

II - As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido, e alinhada com a gestão de riscos organizacional.

III - Todos os termos de compromisso celebrados entre a instituição e terceiros devem citar explicitamente os requisitos de segurança da informação e comunicações da SSP/DF, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Norma, devendo também ser exigido termo de confidencialidade.

Seção II Gestão de riscos e segurança da informação e comunicação (GRISC)

Art. 8 A GRSIC é um conjunto de processos que permite identificar, analisar, avaliar e estabelecer os controles para o tratamento de riscos a que estão sujeitos os ativos de informação da SSP/DF, e tem como diretrizes:

I - A GRSIC deve ser implementada no âmbito da SSP/DF, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, desenvolvendo critérios para a aceitação de riscos e identificação dos níveis aceitáveis de risco, devendo ser atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou oportunamente, em função de inventários de ativos, mudanças, ameaças ou vulnerabilidades. Desta forma, as áreas responsáveis por ativos de informação deverão implementar processo contínuo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIC.

II - O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas perante incidentes de SIC.

Seção III - Gestão de continuidade (GECON)

Art. 9 A GECON é um processo de gestão que identifica riscos potenciais aos ativos de informação da SSP/DF, assim como possíveis impactos nas operações de negócio, caso essas ameaças se concretizem, com o objetivo de garantir a continuidade nas operações. Para isso, devem ser observadas as seguintes diretrizes:

I - As áreas da SSP/DF deverão manter processo de GECON, com vistas a responder efetivamente aos incidentes de SIC e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da SSP/DF, além de recuperar perdas de ativos de informação.

II - Todas as áreas da SSP/DF que dependam de recursos de Tecnologia da Informação e da Comunicação deverão elaborar Planos de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrência de eventos ou sinistros, bem como estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços, assegurando a disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

Seção IV - Gestão de incidentes de segurança da informação

Art. 10 São diretrizes da Gestão de incidentes de segurança da informação:

I - A Coordenação de Infraestrutura (CINF) deverá manter Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), com a responsabilidade de receber, analisar

e responder notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

II - Todos os funcionários e partes externas devem estar cientes sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível.

III - Os eventos e incidentes de SIC devem ser comunicados, registrados e tratados de acordo com um Plano de Gerenciamento de Incidentes específico.

Seção V - Monitoramento, auditoria e conformidade

Art. 11 O monitoramento, auditoria e conformidade de ativos de informações observarão o seguinte:

I - O uso dos recursos de Tecnologia da Informação e Comunicações disponibilizados pela SSP/DF é passível de monitoramento e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade, com o objetivo de identificar tentativas de violações e incidentes de segurança da informação, bem como determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes;

II - A entrada e saída de ativos de informação da SSP/DF deverá ser registrada e autorizada por autoridade competente mediante procedimento formal;

III - Realizar análises críticas regulares da eficácia da GESIC, levando em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas;

IV - A Ouvidoria da SSP/DF será responsável por manter canal de comunicação para recebimento de denúncias de infração a qualquer parte desta NoSIC.

Seção VI - Controle de acesso e uso de senhas

Art. 12 O controle de acesso e uso de senhas observarão o seguinte:

I - O login e a senha de rede e de sistemas de informação são a identidade do colaborador dentro do âmbito da SSP/DF e, todas as atividades associadas a este login, serão atribuídas a este colaborador.

II - O colaborador terá acesso apenas a sistemas de informação e pastas compartilhadas que necessite para realizar a atividade laboral.

III - O acesso aos sistemas de informação e pastas compartilhadas pelo colaborador, devem ser solicitadas pelo superior hierárquico, ao administrador de acesso.

IV - Quando da exoneração do cargo, afastamento, alteração de lotação ou mudança de responsabilidade de um colaborador, o seu superior imediato deve comunicar imediatamente aos administradores de acesso para que os direitos sejam revistos.

V - Devem ser criados e mantidos procedimentos de autorização, controle e revogação de acessos à rede e serviços de redes.

VI - As contas e senhas são de uso pessoal e intransferível e não devem ser divulgadas para quaisquer outras partes, incluindo autoridades e lideranças.

VII - O colaborador deve evitar manter anotadas a informação de senhas, a menos que elas possam ser armazenadas de forma segura e o método de armazenamento esteja aprovado.

VIII - O colaborador deve alterar as senhas, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.

IX - A criação e alterações de senhas devem ser realizadas seguindo o requisito de segurança determinado pela SMT.

X - Os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.

Seção VII - Gerenciamento de direitos de acesso privilegiado

Art. 13 O gerenciamento de direito de acesso privilegiado observará os seguintes itens:

I - O direito de acesso privilegiado será concedido a usuários conforme a necessidade de uso e com base em eventos alinhados com a política de controle de acesso, baseado nos requisitos mínimos para sua função;

II - A concessão de direitos de acesso privilegiado deve ser controlada por meio de um processo de autorização formal, onde deve estar definido os requisitos para expirar estes direitos.

III - Os direitos de acesso privilegiados devem ser atribuídos a um login de usuário diferente daqueles usados nas atividades normais do negócio, e atividades normais do negócio não devem ser desempenhadas usando contas privilegiadas.

Seção VIII - Da Segurança física

Art. 14 São diretrizes da segurança física:

I - Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado, de acordo com a sua criticidade.

II - O acesso ao parque tecnológico da SSP/DF deve ser restrito às pessoas devidamente autorizadas.

III - Devem ser tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

Seção IX - Da Classificação da Informação

Art. 15 São diretrizes da Classificação da informação:

I - Toda informação criada, manuseada, armazenada, transportada ou descartada da SSP/DF será classificada de acordo com a Portaria 149 de 26 de outubro de 2021 (Lei nº 12.527, de 18 de novembro 2011).

II - O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pela SSP/DF e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

III - As informações sob gestão da SSP/DF devem dispor de segurança, de maneira a serem adequadamente protegidas quanto ao acesso e uso.

IV - Para aquelas consideradas de alta criticidade, serão necessárias medidas especiais de tratamento, com o objetivo de limitar a exploração de informações exclusivas da instituição.

Seção X - Do uso de e-mail e de acesso à internet

Art. 16 O correio eletrônico é um recurso de comunicação institucional da SSP/DF e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta NOSIC e dos procedimentos específicos, além das demais diretrizes do Governo Distrital e Federal.

Seção XI - Gestão de ativos de informação

Art. 17 São diretrizes da Gestão de ativos de informação:

I - A gestão de ativos de informação da SSP/DF deverá observar procedimentos específicos para garantir a sua operação segura e contínua.

II - Os ativos de informação da SSP/DF deverão ser inventariados, com a classificação em termos de valor, requisitos legais, sensibilidade e criticidade da informação para a SSP/DF, e serão atribuídos aos respectivos responsáveis.

III - O responsável pode ser um indivíduo ou uma entidade que controla todo o ciclo de vida de um ativo.

IV - Seu uso deverá ser exclusivamente institucional, vedada a utilização para fins em desconformidade com os interesses da SSP/DF.

V - O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em normas e legislação específica de classificação de informação.

VI - É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela SSP/DF.

VII - Todos os funcionários, fornecedores e terceiros devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.

Seção XII - Criptografia

Art. 18 São diretrizes da Criptografia:

I - Deverá ser definida política sobre o uso de controles criptográficos para maximizar os benefícios, minimizar os riscos do uso de técnicas criptográficas e para evitar o uso incorreto ou inapropriado

II - Deverá ser definida política sobre o uso, proteção e ciclo de vida das chaves criptográficas, a ser desenvolvida e implementada ao longo de todo o seu ciclo de vida.

III - Deverão ser consideradas na implementação da política criptográfica da organização, as leis ou regulamentações e restrições nacionais aplicáveis ao uso de técnicas criptográficas, nas diferentes partes do mundo, e das questões relativas ao fluxo transfronteiras de informações cifradas.

Seção XIII - Aquisição, desenvolvimento e manutenção de sistemas de informação

Art. 19 A aquisição, desenvolvimento e manutenção de sistemas de informação observarão os seguintes itens:

I - As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança, com vistas a garantir o respeito aos atributos básicos de segurança da informação, e a implementação de mudanças deve ser controlada utilizando procedimentos formais de controle de mudanças.

II - Os requisitos relacionados com segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes

III - Os controles e requisitos de segurança da informação devem refletir o valor da informação envolvida para o negócio e o seu potencial impacto negativo, que possa resultar de uma falha da segurança da informação, bem como considerar o processo de autorização e provisionamento de acesso privilegiado.

IV - Os critérios para aceitação de produtos devem ser definidos, o qual dará garantia de que os requisitos de segurança identificados são atendidos

V - Os desenvolvedores devem utilizar técnicas de programação segura, e os testes e as análises críticas de código verifiquem a necessidade de uso dessas técnicas.

VI - No desenvolvimento terceirizado, deve-se obter a garantia de que a parte externa está em conformidade com essas regras para o desenvolvimento seguro.

VII - O acesso ao código-fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) serão estritamente controlados, com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais, bem como para manter a confidencialidade de propriedade intelectual valiosa

VIII - Será mantido um registro de auditoria de todos os acessos a código-fonte de programas;

IX - A manutenção e a cópia das bibliotecas de programa-fonte estão sujeitas a procedimentos estritos de controles de mudanças

Seção XIV - Conscientização, educação e treinamento em SIC

Art. 20 A aquisição, desenvolvimento e manutenção de sistemas de informação observarão os seguintes itens:

I - A SSP/DF deverá promover continuamente a capacitação, reciclagem e o aperfeiçoamento de todos os usuários da instituição, por meio de programas de conscientização em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança dentro da instituição.

II - O programa de conscientização deve ser atualizado regularmente de forma que esteja alinhado com as políticas, normas e procedimentos relevantes de segurança da informação da Organização

III - O programa de conscientização deve ser planejado levando em consideração os papéis e responsabilidades dos colaboradores do órgão e, onde relevante, as expectativas da organização quanto à conscientização das partes externas.

Seção XV - Plano de investimentos em SIC

Art. 21 Os investimentos em segurança da informação e comunicações serão realizados de forma planejada e consolidados em um Plano de Investimentos em SIC e, no que couber, no Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC), respeitando-se o Plano de Aquisições da SSP/DF. O Plano de Investimentos em SIC deverá ser reavaliado quando houver revisão orçamentária ou revisão de prioridades das ações de SIC.

Seção XVI - Propriedade intelectual

Art. 22 As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual da SSP/DF e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o direito de autoria, quando for o caso. É vedada a utilização de patrimônio intelectual da SSP/DF em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

Seção XVII - Contratos, convênios, acordos e instrumentos congêneres

Art. 23 Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta NoSIC.

I - O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta norma aos empregados, prepostos e todos os envolvidos em atividades vinculadas à SSP/DF.

II - O encerramento de contrato, convênio ou acordo deve incluir requisitos de segurança da informação e responsabilidades legais existentes e, onde apropriado, responsabilidades contidas em quaisquer acordos de confidencialidade e os termos e condições de trabalho que continuem por um período definido após o fim do contrato, convênio ou acordo.

Seção XVIII - Do uso de dispositivos móveis e computação em nuvem

Art. 24 O uso de dispositivos móveis e computação em nuvem observarão os seguintes itens:

I - O uso de recursos de Computação em Nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por procedimentos específicos, e medidas de segurança apropriadas devem ser adotadas para a proteção contra os riscos do uso de recursos de computação e comunicação móveis.

II - Os colaboradores devem assinar acordo de conhecimento das responsabilidades para porte dos dispositivos móveis da SSP/DF, renunciando direitos autorais dos dados de negócio, que permita a exclusão remota dos dados pela Secretaria no caso de roubo, furto ou perda do dispositivo móvel ou ainda, quando não mais houver autorização para o uso dos serviços, levando-se em consideração a legislação sobre privacidade.

III - Os dispositivos móveis contendo informações importantes, sensíveis e/ou críticas para o negócio devem ser protegidos contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização.

IV - Deverá ser estabelecido um procedimento específico que leve em consideração requisitos legais, securitários e outros requisitos de segurança da organização para casos de furto, roubo ou perda de dispositivos móveis.

V - Não será permitido o uso de mecanismos de comunicação não institucionais

CAPÍTULO V
DAS PENALIDADES

Art. 25 O descumprimento às diretrizes desta Norma, assim como os procedimentos vinculados, acarretará sanções administrativas em primeira instância, sem prejuízo às ações cíveis e criminais cabíveis.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 26 Devem ser observadas as competências e responsabilidades da Alta Administração, do Comitê de segurança da informação e comunicação e do Gestor da segurança da informação e comunicação, Gestor da área, Usuário, Área de Tecnologia da informação, Proprietário da informação, Custodiante dos ativos da informação e Grupo de respostas a incidentes de segurança, descritas no Capítulo V da PoSIC do GDF.

Seção I - DA GESTÃO EM SEGURANÇA DA INFORMAÇÃO

Art. 27 A gestão corporativa de segurança da informação deverá ser realizada por servidores públicos efetivos.

Seção II - DO SUBCOMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (SSIC)

Art. 28 Compete ao Subcomitê de Segurança da Informação e Comunicação as atribuições descritas na seção I do Capítulo V da Portaria Nº 167, de 22 de novembro de 2021, que institui a CGTIC e seus Subcomitês no âmbito da SSP/DF.

Seção III - DO COMITÊ INTERNO DE GOVERNANÇA PÚBLICA E GESTÃO ESTRATÉGIA – (Cigesp)

Art. 29 Compete ao Comitê interno de Governança Pública e Gestão Estratégia a atribuição descrita no Capítulo II, artigo 4ª, inciso VI da Portaria 56 de 7 de junho de 2019:

I - Promover, com apoio institucional da Controladoria-Geral do Distrito Federal, a implantação de metodologia de gestão de riscos.

Seção IV - DA SMT

Art. 30 Compete à Subsecretaria de Modernização Tecnológica as atribuições descritas no Capítulo X do Decreto n° 40.079, de 04 de setembro de 2019, que aprova o Regimento Interno da Secretaria de Estado de Segurança Pública do Distrito Federal.

CAPÍTULO VII
DA ATUALIZAÇÃO

Art. 31 Esta norma, bem como os Procedimentos que dela se originaram, deverão ser atualizadas com periodicidade mínima anual ou quando mudanças significativas, que afetem a base de avaliação de risco original, ocorrerem.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Para efeitos desta Norma, adotam-se os seguintes conceitos e definições:

I. 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;

II. Agente responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

III. Alta Administração: para efeitos desta política, considera-se alta administração os ocupantes dos cargos de Secretário de Estado, Secretário Executivo e Subsecretários da SSPDF;

IV. Ameaça: são agentes ou condições causadoras de incidentes contra ativos. Exploram as vulnerabilidades, ocasionando perda de confidencialidade, integridade ou disponibilidade;

V. 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;

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

VII. Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

VIII. Autenticidade: garantia de que o dado ou informação são verdadeiros;

IX. 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;

X. 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;

XI. Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

XII. Contingência: descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

XIII. Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XIV. 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;

XV. Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

XVI. Credencial de segurança / credencial de acesso: certificado, dispositivo ou recurso, tais como senhas, tokens ou documentos, concedido por autoridade competente, que habilita determinado usuário ou processo a ter acesso a dados ou informações em diferentes graus de sigilo;

XVII. 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;

XVIII. Custodiante: indivíduo a quem é dada a custódia de um ativo;

XIX. Dado: representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

XX. Direito de Acesso: privilégio associado a um usuário para ter acesso a um ativo;

XXI. Diretriz: descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;

XXII. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

XXIII. Evento de Segurança da Informação: ocorrência de uma violação à Política de Segurança da Informação e Comunicação ou falha nos Controles de Segurança;

XXIV. Gestão de Continuidade de Negócios: Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

XXV. Gestão de Riscos: Atividade contínua de identificação, análise, tratamento, aceitação e comunicação de riscos;

XXVI. 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, informação do usuário, comandos e argumentos executados, identificação da estação local ou estação remota que iniciou a conexão, entre outros.;

XXVII. Monitoramento: Atividade de verificação manual ou automática de eventuais ameaças, incidentes de segurança ou quaisquer descumprimentos às diretrizes presentes na Política, Norma ou Procedimentos de segurança da informação e comunicação

XXVIII. Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

XXIX. Política de Segurança da Informação e das Comunicações (PoSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

XXX. Processo: instruções executadas por um programa de computador;

XXXI. Programa de Computador: Sequência finita de instruções bem definidas e não ambíguas, disponibilizadas, normalmente, por meio de um arquivo executável, para realizar uma tarefa determinada num ambiente computacional;

XXXII. 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;

XXXIII. Proteção: vide Controle de Segurança;

XXXIV. Protocolo: convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

XXXV. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXVI. Recursos de Tecnologia da Informação: 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;

XXXVII. Risco: é a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará;

XXXVIII. Sala Cofre: é uma sala fortificada que pode ser instalada em uma instituição, provendo um local seguro de invasões e outras ameaças. São ambientes projetados para resistir a vários tipos de catástrofes. Suportam, por exemplo, temperaturas de até 1.200 graus Celsius, inundações, cortes bruscos de energia, gases corrosivos, explosões e até ataques nucleares;

XXXIX. Sala Segura: sala que proporciona um ambiente seguro no Datacenter, oferecendo maior garantia no armazenamento de informações eletrônicas. Uma Sala Segura possui gerador próprio, instalação elétrica independente, paredes especiais, piso elevado, ar-condicionado, detecção e combate a incêndios, iluminação, sinalização de emergência e monitoração do ambiente;

XL. Segurança da Informação e Comunicação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XLI. Servidor de Rede: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

XLII. Servidor Público: pessoa física que exerce cargo, emprego ou função pública;

XLIII. Sistemas de Informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

XLIV. Sistema de Segurança da Informação: proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando estasegurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

XLV. Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XLVI. Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XLVII. Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XLVIII. Tratamento do risco: processo de seleção e implementação de controles de segurança;

XLIX. Trilhas de Auditoria: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

L. Usuário: Qualquer pessoa, física ou jurídica ou processo em um sistema computacional que faça uso dos recursos de tecnologia da informação relativos à SSPDF;

LI. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

ANEXO II
REFERÊNCIAS LEGAIS E NORMATIVAS

Foram utilizadas as seguintes referências legais e normativas para elaboração desta política:

I. Lei Federal nº 12.965, de 23 de abril de 2014 - Estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil;

II. 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;

III. 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 tipificarcondutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências;

IV. Lei nº 13.709, de 14 de agosto de 2018 - Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

V. Resolução nº 03, de 06 de novembro de 2018 – Aprova a revisão da Política de Segurança da Informação e Comunicação (PoSIC) do Governo do Distrito Federal;

VI. Decreto Federal nº 7724 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;

VII. 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;

VIII. Decreto Federal nº 4.553, de 27 de dezembro de 2002 - Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IX. Instrução Normativa nº 04 de 12 de novembro de 2010 – IN 04/SLTI/MPOG - Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal;

X. Instrução Normativa nº 01 de 04 de abril de 2019 – IN01 SGD/ME - 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.

XI. Instrução Normativa nº 31 de 23 de março de 2021 - Altera a Instrução Normativa nº 1, de 4 de abril de 2019, que 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.

XII. 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;

XIII. Decreto Distrital nº 34.637, de 06 de setembro de 2013 - Dispõe sobre a contratação de bens e serviços de Tecnologia da Informação no âmbito da Administração Direta e Indireta do Distrito Federal, e dá outras providências;

XIV. 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;

XV. Decreto Distrital nº 33.528, de 10 de fevereiro de 2012 – Dispõe sobre a aprovação de Estratégia Geral de Tecnologia da Informação - EGTI, elaborada pelo Comitê Gestor de Tecnologia da Informação e Comunicação e dá outras providências;

XVI. 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";

XVII. 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;

XVIII. ABNT NBR 15999-1:2007 - Gestão de continuidade de negócios - Estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN);

XIX. ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos. Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação documentado dentro do contexto dos riscos de negócio globais da organização;

XX. ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação - Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização;

XXI. ABNT ISO GUIA 73:2009 - Gestão de riscos - Vocabulário - Fornece as definições de termos genéricos relativos à gestão de riscos;

XXII. 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;

XXIII. Portaria nº 41, de 20 de fevereiro de 2013 - Institui o Comitê de Segurança da Informação e Comunicações da Secretaria de Planejamento e Orçamento do Distrito Federal (CSIC/SEPLAN);

XXIV. Portaria nº 20, de 31 de janeiro de 2005 - Dispõe sobre Política de Segurança e Uso de Recursos Computacionais no âmbito da Secretaria de Estado de Gestão Administrativa e dá outras providências.

XXV. Decreto n° 40.079, de 04 de setembro de 2019 - Aprova o Regimento Interno da Secretaria de Estado de Segurança Pública do Distrito Federal.

XXVI. Portaria nº 167, de 22 de novembro de 2021 - Institui e define as regras gerais do Comitê de Governança e Gestão de Tecnologia da Informação e de Comunicação (CGTIC) da Secretaria de Segurança Pública do Distrito Federal - SSP/DF.

XXVII. Portaria nº 139, de 24 de setembro de 2021 - Estabelece a Política de Gestão de Riscos da Secretaria de Estado de Segurança Pública e dá outras providências.

XXVIII. Portaria nº 149, de 26 de outubro de 2021 - Regulamenta o acesso e o tratamento a dados, informações, documentos, instalações e materiais sigilosos no âmbito da Secretaria de Estado de Segurança Pública do Distrito Federal.

XXIX. Portaria nº 56, de 07 de junho de 2019 - Institui, nos termos do Decreto n° 39.736, de 28 de março de 2019, o Comitê Interno de Governança Pública e Gestão Estratégica - Cigesp, para garantir o desenvolvimento e a apropriação das melhores práticas de governança de forma contínua e progressiva, nos termos estabelecidos pelo Conselho de Governança Pública - CGov.

SUBSECRETARIA DE MODERNIZAÇÃO TECNOLÓGICA SSP/DF