POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

GOVERNO DO DISTRITO FEDERAL

(PoSIC/GDF)

GOVERNADOR DO DISTRITO FEDERAL
Agnelo Queiroz

MEMBROS DA JGTIC

Secretaria de Estado de Planejamento e Orçamento – SEPLAN
Titular: Paulo Antenor de Oliveira - Secretário de Estado de Planejamento e Orçamento
Suplente: Renata Márcia Canuto Dumont Galdino

Secretaria de Estado da Casa Civil
Titular: Swedenberger Barbosa - Secretário de Estado da Casa Civil

Secretaria de Estado de Fazenda
Titular: Adonias dos Reis Santiago - Secretario de Estado de Fazenda
Suplente: Luís Ricardo Guimarães Figueirôa

Secretaria de Estado de Transparência e Controle
Titular: Mauro Almeida Noleto - Secretário de Estado de Transparência e Controle
Suplente: Alfredo Murillo Gameiro de Souza

Secretaria de Estado de Ciência, Tecnologia e Inovação.
Titular: Glauco Rojas Ivo - Secretário de Estado de Ciência, Tecnologia e Inovação.
Suplente: Alexandre de Oliveira Lobo – Subsecretário de Inclusão digital e Conteúdos Tecnológicos

EQUIPE DE ELABORAÇÃO DA POSIC-GDF
Secretaria de Estado de Planejamento e Orçamento – SEPLAN
1- Felipe Azevedo Gois
2- Flávio Fernandes dos Santos
3- Rodrigo Moreira Freitas

Secretaria de Estado de Fazenda:
1- Kelly Cristina Fernandes de Macedo
2- Daniela Mirian de Sousa Santos

Secretaria de Estado de Transparência e Controle:
1- Vladimir Wuerges de Souza

Secretaria de Estado de Ciência, Tecnologia e Inovação:
1- Luciano Helou Ramos
2- Rômulo Pinheiro

COLABORAÇÃO
Ricardo de Souza Maia

Sumário

INTRODUÇÃO

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.

Este documento estabelece diretrizes, princípios, responsabilidades e objetivos para a Política de Segurança da Informação e Comunicação (PoSIC) do Distrito Federal, a qual deverá ser adotada e cumprida por todos os servidores, estagiários, prestadores de serviços e demais usuários que utilizem suas informações.

Além disso, esta PoSIC tem como escopo fundamentar todas as ações de proteção às informações das Unidades Administrativas do Governo do Distrito Federal, em atendimento às recomendações do Tribunal de Contas do Distrito Federal (Processo nº 17333/2012) e de outros órgãos de controle.

A Segurança da Informação é matéria atinente a todas as atividades das Unidades Administrativas, sejam atividades meio ou fim, devendo essa responsabilidade ser compartilhada por todas suas áreas.

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

Diversas ações e outros normativos de Segurança da Informação serão implementados com o fim de padronizar e regrar os processos institucionais do Governo do Distrito Federal.

1. OBJETIVO

Art. 1º O objetivo desta política é instituir diretrizes e princípios de Segurança da Informação e Comunicação no âmbito das Unidades Administrativas do Governo do Distrito Federal (GDF), com 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 das Unidades Administrativas.

2. DO ESCOPO DA POLÍTICA

Art. 2º A PoSIC/GDF aplica-se a todas as unidades da estrutura administrativa 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 responsabilidade, na forma da lei.

3. DOS PRINCÍPIOS

Art. 3º O conjunto de documentos que compõe esta PoSIC deverá se guiar pelos seguintes

princípios:

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 devem ser projetados para que possam resistir ou 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.

4. DIRETRIZES GERAIS

4.1. DA ESTRUTURA NORMATIVA

Art. 4º A Estrutura Normativa da Segurança da Informação do GDF é composta por três níveis hierárquicos distintos, relacionados a seguir:

I. **Política** de Segurança da Informação e Comunicação do GDF (PoSIC - GDF): constituída neste documento, define a estrutura, diretrizes gerais, princípios e as obrigações referentes à segurança da informação e comunicação do GDF, servindo de base para elaboração dos demais documentos da estrutura normativa e possui caráter **estratégico**;

II. **Normas** de Segurança da Informação e Comunicação (NoSIC): de caráter **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 Política elaborada pelo GDF;

III. **Procedimentos** de Segurança da Informação e Comunicação (ProSIC): descrevem, 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: A PoSIC do GDF tem caráter corporativo e sua elaboração é de competência exclusiva da JGTIC. As NoSIC(s) são de competência da JGTIC, quando corporativas e das Unidades Administrativas quando contemplarem necessidades específicas das mesmas.

4.2. 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.

4.3. NORMAS E PROCEDIMENTOS COMPLEMENTARES

Art. 6º As normas e procedimentos que complementam esta Política deverão abordar, mas não limitados a estes, os seguintes aspectos: segurança física; gestão de mudanças; privacidade; criptografia; acesso à rede; gestão de senhas e contas de usuário; dispositivos móveis; gestão de incidentes; plano de continuidade de negócios; proteção à propriedade intelectual; treinamento e sensibilização para segurança;

4.4. DA DIVULGAÇÃO

Art. 7º Esta política, bem com suas normas, deverão ser disponibilizadas e agrupadas em sítio institucional em local de fácil acesso, proporcionando ampla difusão e atualização simplificada. Em todos os documentos deverá constar a data de sua 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 requerem

conhecimento das mesmas.

4.5. 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.

4.6. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO E COMUNICAÇÃO

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 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.

4.7. EDUCAÇÃO CONTINUADA

Art. 13 Para uma efetiva proteção das informações, as Unidades Administrativas deverão elaborar um plano contínuo de capacitação de recursos humanos em segurança da informação, de modo a promover maior consciência da responsabilidade individual dos usuários e maior independência do Estado na contratação de serviços de segurança.

4.8. PENALIDADES

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

5. COMPETÊNCIAS E RESPONSABILIDADES

5.1. DA ALTA ADMINISTRAÇÃO

Art. 15 Compete à alta administração das Unidades Administrativas do GDF:

I. Apoiar e exigir o cumprimento da Política, Normas e Procedimentos de Segurança da Informação e Comunicação;

II. Zelar para que contratos, convênios e outros instrumentos similares elaborados pela respectiva Unidade Administrativa estejam alinhados à presente política e suas normas 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 da PoSIC, mobilizando gestores para o cumprimento da Política;

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 sua Unidade Administrativa;

VII. Instituir o Comitê de Segurança da Informação (CSIC) no âmbito da sua Unidade Administrativa.

Parágrafo único. O CSIC será composto minimamente pela seguinte formação:

a) Gestor de Segurança da Informação, que coordenará as atividades do comitê;
b) Um membro da Área de Segurança Física;
c) Um membro da Área de Segurança Digital;
d) Um membro da Área de Processos Administrativos;

e) Um membro da Área de Normas e Legislação.

5.2. DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 16 Compete ao Comitê de Segurança da Informação e Comunicação :

I. Elaborar e atualizar as Normas de Segurança da Informação e Comunicação (NoSIC) e Procedimentos de Segurança da Informação e Comunicação (ProSIC) da sua respectiva Unidade Administrativa , em conformidade com a PoSIC, NoSIC(s) do GDF, EGTI, leis e regulamentos pertinentes;

§ 1º As Unidades Administrativas poderão criar Norma de Segurança da Informação e Comunicação (NoSIC) para complementar a Política de Segurança da Informação do GDF, de acordo com suas necessidades.

§ 2º As Unidades Administrativas que já possuem sua Política de Segurança da Informação publicada deverão revisá-la em conformidade com a PoSIC do GDF e republicá-la em forma de Norma de Segurança da Informação e Comunicação (NoSIC) complementar.

II. Estabelecer um Programa de Gestão de Riscos, atualizando-o quando necessário;

III. Desenvolver um Plano de Continuidade de Negócios, que deverá ser testado periodicamente;

IV. Instituir grupos de trabalho específicos relacionados à segurança da informação;

V. Estabelecer mecanismo de registro e controle de não conformidade a esta Política, Normas e Procedimentos de Segurança da Informação e Comunicação;

5.3. DO GESTOR DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

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

I. Coordenar o Comitê de Segurança da Informação e Comunicações (CSIC);

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 comunicações;

VI. Propor Normas e procedimentos relativos à segurança da informação e comunicações;

VII. Definir métricas que permitam aferir a eficiência e eficácia dos controles de segurança.

Parágrafo Único: A gestão de segurança da informação deverá somente ser realizada por servidores e empregados públicos.

5.4. DO GESTOR DE ÁREA

Art. 18 Compete ao Gestor de Área:

I. Zelar e fazer cumprir a PoSIC;

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 de área ou função 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) de usuários aos Gestores da Área de Pessoas, 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.

5.5. DO USUÁRIO

Art. 19 São obrigações do usuário:

I. Observar rigorosamente esta Política de Segurança de Informação e Comunicação, bem como as Normas 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 quaisquer riscos ou incidentes de segurança que venha a tomar conhecimento;

IV. 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;

V. Manter, obrigatoriamente, os dados críticos da sua Unidade Administrativa em compartilhamentos de rede disponibilizados pela área de TIC;

VI. 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;

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;

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.

5.6. DAS ÁREAS DE TECNOLOGIA DA INFORMAÇÃO DAS UNIDADES ADMINISTRATIVAS

Art. 20 São obrigações da Área de Tecnologia da Informação das Unidades Administrativas ou do custodiante responsável por prover os serviços de tecnologia para a Unidade Administrativa:

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 CSIC 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 da Política e das Normas de Segurança da Informação e Comunicação 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. 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. Caso a Unidade Administrativa possua estrutura própria de provimento de correio eletrônico deverá seguir as determinações desta PoSIC e estabelecer para sua Unidade Administrativa o tamanho limite das mensagens de correio eletrônico para envio e recebimento, incluindo anexos

X. Adotar como padrão de endereço de e-mail corporativo o formato <identificação>@<unidade administrativa>.df.gov.br;

XI. 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.

5.7. DO PROPRIETÁRIO DA INFORMAÇÃO

Art. 21 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. Participar da definição dos critérios para estabelecer perfis de acesso a informações sob sua responsabilidade;

VII. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

VIII. Participar, sempre que convocado, das reuniões do Comitê de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

5.8. DO CUSTODIANTE DOS ATIVOS DA INFORMAÇÃO

Art. 22 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 a 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 contratar, se necessário, bens e serviços de Segurança da Informação e Comunicação.

5.9. DO GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA EM COMPUTADORES (CSIRT)

Art. 23 O CSIRT será responsável por:

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;

VI. Investigar as causas dos incidentes no ambiente computacional.

Parágrafo Único: As Unidades Administrativas que ainda não possuírem estrutura para a criação do CSIRT deverão repassar as responsabilidades para sua área de Tecnologia da Informação e Comunicação ou para a unidade responsável por custodiar os ativos de informação da Unidade Administrativa.

6. ATUALIZAÇÃO

Art. 24 Esta Política, Normas e 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.

§ 1º Caberá à Junta Gestora de Tecnologia da Informação (JGTIC) a responsabilidade pela atualização permanente da estrutura normativa;

§ 2º Caberá às Unidades Administrativas a elaboração de normas e procedimentos de Segurança da Informação e Comunicação nos casos que não forem contemplados pela JGTIC.

7. CONCLUSÃO

Este documento, responsável pela instituição da PoSIC do GDF, norteará 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.

Os dispositivos aqui estabelecidos apresentam as principais atividades a serem desenvolvidas. A sua priorização será definida pelos Gestores e Comitês aqui nominados. Com esta PoSIC, o GDF 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 Política ora apresentada.

ANEXOS

ANEXO I - HISTÓRICO

A Junta Gestora de Tecnologia da Informação e Comunicação do Distrito Federal (JGTIC-DF) reconhece a importância do gerenciamento da Segurança da Informação, entretanto as ações de segurança têm sido implementadas de forma reativa e por iniciativas individuais.

A necessidade da elaboração da Política de Segurança da Informação (PoSIC) decorre do imperativo de atender às recomendações dos Tribunais de Contas e da Secretaria de Estado de Transparência e Controle do Distrito Federal, dentre outros órgãos, bem como estruturar as boas práticas já existentes.

Com a implantação da PoSIC e das demais ações e políticas que dela decorrerão, busca-se garantir a proteção das informações e de outros ativos críticos das Unidades Administrativas do DF, com o intuito de assegurar ao GDF a continuidade de suas atividades.

Para elaboração da PoSIC ora apresentada, foram analisadas as Políticas de Segurança da Informação (PSI´s) das Secretarias de Planejamento, Fazenda e Transparência, o panorama cultural dos usuários das informações e as boas práticas já empregadas.

Para elaboração do documento inicial – PoSIC, foi designado tarefa à Secretaria Executiva da JGTIC que apresentou proposta aos representantes que compõem a Junta Gestora de TIC do DF, que a aprovou.

A partir da instituição da PoSIC do GDF, outras ações e políticas deverão ser elaboradas e implantadas de maneira contínua, como Política de Controle de Acesso Lógico e Físico; Política de Backup; Planos de Continuidade do Negócio, contemplando as três principais áreas meio que

estruturam uma Unidade Administrativa: infraestrutura, pessoas e tecnologia da informação; Política de Descarte de Documentos, entre outras. Esses documentos deverão ser elaborados pelas Unidades Administrativas.

ANEXO II - DOS CONCEITOS E DEFINIÇÕES

Para efeitos desta Política, 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. **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;

III. **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;

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

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

VI. **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;

VII. **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;

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

IX. **Controle de Acesso**: são restrições de acesso a um ativo da organização;

X. **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;

XI. **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;

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

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

XIV. **Diretriz:** o que deve ser feito e como, para atender aos objetivos declarados na política;

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

XVI. **Forense Computacional**: Conjunto de técnicas para coleta e exame de evidências digitais, reconstrução e dados e ataques, identificação e rastreamento de invasores;

XVII. **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;

XVIII. **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.

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

XX. **Gestor de Segurança da Informação e Comunicação**: é responsável pelas ações de segurança da informação e comunicações no âmbito da Unidade Administrativa;

XXI. **Impacto**: Tamanho do prejuízo, medido através de propriedades mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará;

XXII. **Incidente de Segurança**: Qualquer evento que resulte no descumprimento da Política 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;

XXIII. **Integridade**: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

XXIV. ***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;

XXV. **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;

XXVI. **Não repúdio**: garantia de segurança de informação que impede uma entidade de negar ter participado de uma dada operação.

XXVII. **Plano de Continuidade de Negócio (PCN):** documento que estabelece mecanismos para restabelecer a atividade de uma organização, em caso de interrupção.

XXVIII. **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

XXIX. **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;

XXX. **Proteção**: vide Controle de Segurança;

XXXI. **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;

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

XXXIII. **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;

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

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

XXXVI. **Usuário**: Qualquer pessoa, física ou jurídica ou processo em um sistema computacional que faça uso dos recursos de tecnologia da informação e Comunicação relativos ao GDF;

XXXVII. **Vulnerabilidade**: são fragilidades associadas aos ativos que os tornam susceptíveis às ameaças.

ANEXO III - DAS REFERÊNCIAS LEGAIS E NORMATIVAS

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

I. **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;

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

III. **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;

IV. **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;

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

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. **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;

XI. **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;

XII. **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;

XIII. **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;

XIV. **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";

XV. **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;

XVI. **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);

XVII. **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;

XVIII. **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;

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

XX. **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;

XXI. **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;