

DETRAN-DF – Departamento de Trânsito do Distrito Federal



**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E
COMUNICAÇÕES - POSIC**

**BRASÍLIA
2017**

Folha nº: 115

Processo: 055.013503/2007

Rub.: [assinatura] Mat.: 2510677

[assinatura] *[assinatura]* *[assinatura]*



GOVERNO DO DISTRITO FEDERAL
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES



ELABORADO POR:

Joran Ermison Lopes Freire – Chefe do Núcleo de Segurança de Infraestrutura

Weliton Fonseca Amaral – Servidor do Núcleo de Banco de Dados

REVISADO POR:

Felipe Elias da Silva – Gerente de Suporte e Segurança de Infraestrutura

APROVADO POR:

Reynaldo Baggio da Silveira – Diretor de Tecnologia da Informação e Comunicação

Folha nº: 116

Processo: 055.013503/2007

Rub.: 1000 Mat.: 2510677



GOVERNO DO DISTRITO FEDERAL
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
CAMPO DE APLICAÇÃO



Esta norma se aplica no âmbito da Direção Geral, Diretorias e unidades equivalentes a estas, além das Juntas Administrativas e de Controle.

Folha nº: 117

Processo: 055.013503/2007

Rub.: 1000 Mat.: 2510677



1 ESCOPO

- 1.1 A Política de Segurança da Informação e Comunicações (POSIC) tem por finalidade estabelecer as diretrizes estratégicas, competências e responsabilidades para o manuseio, tratamento, controle e proteção das informações custodiadas ou de propriedade do Detran-DF de forma a preservar a disponibilidade, integridade, confidencialidade e autenticidade das informações.
- 1.2 Essa Política aplica-se a todos os membros da Entidade, sejam eles servidores, colaboradores, fornecedores, prestadores de serviços ou estagiários que, oficialmente, executem atividades vinculadas à atuação institucional do Detran-DF, seja no âmbito da Direção Geral, Diretorias e Juntas Administrativas e de Controle.

2 CONCEITOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
Ameaças	conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
Ativo	qualquer bem, tangível ou intangível, que tenha valor para a organização.
Ativos de informação	os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
Autenticidade	propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
Classificação da informação	atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação.
Confidencialidade	propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

Folha nº: 118

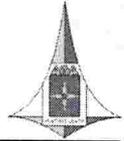
Processo: 055.013503/2007

Rub.: [assinatura] Mat.: 2510677

[assinatura] [assinatura] [assinatura]



GOVERNO DO DISTRITO FEDERAL
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES



	comunicações.
Quebra de segurança	ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.
Recursos computacionais	recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, computadores, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura.
Segurança da informação e comunicações	ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
Vulnerabilidades	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.

3 PRINCÍPIOS

Eficiência	propriedade de que a POSIC e suas Normas busquem um melhor resultado possível, por meio das suas diretrizes e normatizações, visando auxiliar para que a atividade administrativa seja exercida com presteza, perfeição e rendimento funcional.
Ética	propriedade de que a POSIC e suas Normas devem seguir os valores morais de conduta.
Impessoalidade	propriedade de que a POSIC e suas Normas devem servir para todos, sem preferências ou aversões pessoais ou partidárias.
Legalidade	propriedade de que a POSIC e suas Normas devem atuar no âmbito das leis.
Moralidade	propriedade de que as diretrizes estabelecidas nesta POSIC e suas Normas preservarão a moral, os princípios éticos, a boa-fé e a lealdade.
Publicidade	propriedade de que a POSIC e suas Normas terão publicidade e serão levadas ao conhecimento de toda a Entidade, buscando garantir atuação transparente do Poder Público.

4 DIRETRIZES GERAIS

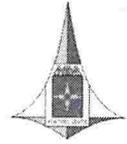
Folha nº: 119

Processo: 055.013503/2007

Rub.: 1000 Mat.: 2510677



GOVERNO DO DISTRITO FEDERAL
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES



4.5.1 Elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de SIC em vigor.

4.6 Controles de Acesso

4.6.1 Devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas de pessoal autorizado. No caso de sistemas críticos, convém que sejam criados ambientes reservados, de uso exclusivo, para abrigá-los.

4.6.2 Os computadores e sistemas do Detran-DF devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação do acesso deve ser claramente definido e registrado.

4.7 Uso de email

4.7.1 O e-mail corporativo deve ser de uso restrito para as atividades vinculadas à atuação institucional, sendo assim o Detran-DF deverá definir regras claras e precisas de uso do e-mail institucional, com o objetivo de evitar o uso para fins particulares, abuso de direito ou violação à imagem do Detran-DF.

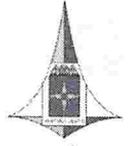
4.8 Acesso a internet

4.8.1 O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela Entidade, observando-se sempre a conduta compatível com os princípios definidos nesta POSIC. Para tanto o Detran-DF deverá controlar o acesso à Internet, com o objetivo de evitar que os recursos computacionais sejam utilizados em desrespeito às leis, aos costumes e à dignidade da pessoa humana.

Folha nº: 120

Processo: 055.013503/2007

Rub.: 120 Mat.: 2510677



4.13.1 A segurança dos recursos humanos deve ser consolidada por meio de ações que promovam a cultura de SIC no âmbito do Detran-DF.

4.14 Gestão de operações e comunicações

4.14.1 A gestão de operações e comunicações deve ter como base uma metodologia de processo de gestão de mudanças e garantir a operação segura e correta dos recursos de processamento da informação de forma que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.

4.15 Criptografia

4.15.1 O uso de recursos criptográficos deve ter, no mínimo, parâmetros e padrões dos algoritmos de Estado definidos na NC09/IN01/DSIC/GSI/PR para todas as informações que tenham sido classificadas em qualquer grau de sigilo; inclusive nos entendimentos, contratos, termos ou acordos de aquisição e manutenção de equipamentos, dispositivos móveis, sistemas, aplicativos ou serviços que dispõem desses recursos.

4.16 Desenvolvimento seguro de software

4.16.1 O processo de desenvolvimento de software deve conter regras que permitam a segurança das aplicações no que diz respeito aos acordos de licenciamento, propriedade dos códigos e direitos de propriedade intelectual; bem como os requisitos de documentação específicos de segurança para as aplicações a serem adquiridas ou desenvolvidas interna ou externamente.

5 PENALIDADES

5.1 O descumprimento das disposições constantes nessa política e nas normas complementares sobre segurança da informação caracteriza

Folha nº: 121

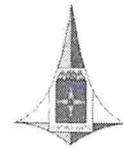
Processo: 055.013503/2007

Rub.: [assinatura] Mat.: 2510677

[assinatura] [assinatura] [assinatura]



GOVERNO DO DISTRITO FEDERAL
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES



trato de assuntos relativos à segurança da informação e comunicações;

- g) Propor Normas e procedimentos relativos à segurança da informação e comunicações.

6.3. Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Detran-DF

- a) Recolher provas o quanto antes após a ocorrência de um incidente de SIC;
- b) Executar uma análise crítica sobre os registros de falha para assegurar que as mesmas foram satisfatoriamente resolvidas;
- c) Investigar as causas dos incidentes de SIC;
- d) Implementar mecanismos para permitir a quantificação e monitoramento dos tipos, volumes e custos de incidentes e falhas de funcionamento; e
- e) Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

7 DISPOSIÇÕES FINAIS

- 7.1 Essa POSIC deve ser revisada e atualizada periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

8 VIGÊNCIA

- 8.1 Esta Norma entra em vigor na sua data de publicação.

Folha nº: 122

Processo: 055.013503/2007

Rub.: Arsh Mat: 2510677

Felipe Welton