

ANEXO I

CONCEITOS E DEFINIÇÕES

1. Para os fins da Política de Segurança da Informação do DETRAN/AL, fica estabelecido o significado dos seguintes termos e expressões:

a) alta administração – corpo dos dirigentes máximos do DETRAN/AL, conforme definição normativa ou decisão consensual. Geralmente abrange diretor-presidente, seu substituto imediato, demais diretores e gerentes;

b) ativo de informação: o patrimônio composto por todos os dados e informações geradas, custodiadas, manipuladas, utilizadas ou armazenada no DETRAN/AL, bem assim todos os elementos de pessoal (colaboradores que manuseiam os ativos), infraestrutura, tecnologia, hardware e software necessários à execução dos processos da organização;

c) autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

d) colaborador: todas as pessoas envolvidas com o desenvolvimento de atividades do DETRAN/AL de caráter permanente, continuado ou eventual, incluindo autoridades, servidores, prestadores de serviço, consultores e estagiários;

e) confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

f) diretrizes de segurança da informação: ações que definem a Política de Segurança da Informação do DETRAN/AL, visando a preservar a disponibilidade, integridade, confiabilidade e autenticidade das informações da Instituição;

g) disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

h) Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

i) gestor de segurança da informação: servidor público efetivo responsável pelas ações de segurança da informação do DETRAN/AL;

j) incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada

de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um tempo inferior ao tempo objetivo de recuperação;

k) incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

l) integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada, ou acidental;

m) parceiro conveniado: órgão ou entidade conveniado ao DETRAN/AL, mediante convênios, acordo de cooperação técnica ou instrumentos congêneres;

n) recursos de Tecnologia da Informação: conjunto formado pelos bens e serviços de tecnologia da informação que constituem a infraestrutura utilizada na produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação da informação;

o) responsável pelo ativo de informação: servidor público responsável pela salvaguarda do ativo de informação;

p) risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade;

q) risco de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação, ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

r) segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

s) servidor público: toda pessoa legalmente investida em cargo público;

t) Sistema de Gestão de Segurança da Informação: é um conjunto de pessoas, processos e procedimentos, baseado em normas e na legislação vigente, que uma organização deve implementar para prover segurança no uso de seus ativos de informação de modo a preservá-los quanto aos aspectos de disponibilidade, integridade, confidencialidade e autenticidade, independentemente do meio em que se encontram; e

u) vulnerabilidades: fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, e podem ser corrigidas ou evitadas por uma ação interna de segurança da informação.

ANEXO II

REFERÊNCIAS LEGAIS E NORMATIVAS

1. Esta norma foi elaborada em conformidade às seguintes referências legais e normativas:

- a) [Lei nº 9.503, de 23 de setembro de 1997\(Código de Trânsito Brasileiro\)](#);
- b) [Lei nº 12.527, de 18 de novembro de 2011](#), que regula o acesso a informações;
- c) [Lei nº 13.460, de 26 de junho de 2017](#), que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública;
- d) [Lei nº 13.709, de 14 de agosto de 2018](#), Lei Geral de Proteção de Dados Pessoais (LGPD);
- e) [Lei nº 13.726, de 8 de outubro de 2018](#), que racionaliza atos e procedimentos administrativos dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e institui o Selo de Desburocratização e Simplificação;
- f) [Decreto nº 9.637, de 26 de dezembro de 2018](#), que institui a Política Nacional de Segurança da Informação;
- g) [Decreto nº 10.222, de 5 de fevereiro de 2020](#), que aprova a Estratégia Nacional de Segurança Cibernética;
- h) Lei Estadual nº 8.087, de 11 de janeiro de 2019, que dispõe sobre a transparência e o acesso à informação pública no estado de Alagoas;
- i) Decreto Estadual nº 26.320, de 13 de maio 2013, que dispõe sobre o acesso a informações públicas de que trata a lei federal nº 12.527, de 18 de novembro de 2011;
- j) Decreto Estadual nº 35.143, de 15 de agosto de 2014, que dispõe sobre a regulamentação do Sistema Estadual de Informática e Comunicação do Estado de Alagoas;
- k) ISO 22301/IEC - Sistemas de Gestão de Continuidade de Negócios;
- l) ABNT NBR ISO/IEC 27001 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação;
- m) ABNT NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação; e
- n) ABNT NBR ISO/IEC 27005 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação.

