

1. Propósito

Determinar os procedimentos necessários para apuração de responsabilidade por atos de infração à Política de Segurança da Informação da ALCE.

2. Escopo

Esta norma aborda as infrações previstas na Política de Segurança da Informação da ALCE.

3. Política

3.1. Classificação das infrações

São três os níveis de infrações que serão apuradas pelo Comitê Gestor de Segurança da Informação:

- a) Alta relevância
- b) Média relevância
- c) Baixa relevância

3.2. Definição

- a) Infrações de alta relevância – Vazamento, intencional ou não, de informações de uso restrito, confidencial ou secreto, através de qualquer meio de transmissão; acesso contumaz a sites de cunho discriminatórios ou que contenham teor relacionado à pedofilia, tráfico de drogas e demais atividades ilícitas; envio de e-mails com assuntos ofensivos, ilícitos, pornográficos, discriminatórios; instalação e/ou utilização de softwares não autorizados previamente pela equipe de tecnologia; compartilhamento e/ou uso de credenciais de acesso à rede e/ou sistemas; adulteração de documentos institucionais ou modificação indevida da classificação atribuída a um documento.
- b) Infrações de média relevância – Vazamento, intencional ou não, de informações de uso interno; acesso, ou tentativa de acesso, a sites pornográficos, de jogos eletrônicos ou de azar, que incitem a violência ou que, de alguma forma, comprometam a segurança dos dados trafegados na Entidade; envio de e-mails com assuntos ilícitos, mas sem fins institucionais, para entes externos; deixar de classificar um documento institucional.
- c) Infrações de baixa relevância – Acesso contumaz a sites não relacionados com o negócio da ALCE; envio contumaz de e-mails com assuntos lícitos, mas sem fins institucionais, para colaboradores da ALCE; utilização de mídias removíveis não autorizadas pela equipe de tecnologia; trafegar informações consideradas de “uso proibido” utilizando recursos tecnológicos da ALCE.

4. Apuração pelo Comitê Gestor de Segurança da Informação

Na existência de indícios do cometimento de atos indevidos por algum colaborador, o Comitê de Segurança da Informação poderá apurar o ocorrido, inclusive solicitando os registros físicos e digitais do colaborador investigado mantidos na Entidade.

Confirmada a existência do ato irregular por parte do colaborador, o Comitê de Segurança da Informação encaminhará o resultado da Apuração para a Diretoria Geral, que solicitará análise jurídica da Procuradoria e encaminhará sugestão a Mesa Diretora.

As sanções administrativas, estão regidas no Estatuto dos Funcionários Públicos Civis do Estado do Ceará (Lei 9.826/74, Capítulo IV – Das Sanções Disciplinares e Seus Efeitos, Art. 196 a 208). A partir de então, Diretoria Geral, Procuradoria Geral e/ou Mesa Diretora irá realizar sua análise com base nos normativos vigentes.

O decisão sobre a necessidade de aplicação de sanção administrativa ao(s) colaborador(es) infrator(es) será da Mesa Diretora, embasado pela apuração do Comitê Gestor de Segurança da Informação, pela Diretoria Geral e pela Procuradoria da ALCE.

5. SANÇÕES ADMINISTRATIVAS

As sanções possíveis para o descumprimento das normas e procedimentos da Política de Segurança da Informação são aquelas descritas no Estatuto da Entidade. No caso dos membros dos órgãos estatutários serão aplicadas as penalidades previstas à legislação.

6. Aprovação

Este documento foi aprovado em 16/08/2013 pela Presidência e é válido a partir da data de sua publicação para todos os colaboradores que utilizam recursos computacionais.

7. Histórico de Revisão

01/06/2012 – Criação da Norma