Assembleia Legislativa do Estado do Ceará

# ASSEMBLEIA LEGISLATIVA DO ESTADO DO CEARÁ - ALCE

*As informações contidas neste documento são restritas à* ALCE*, não podendo ser divulgadas a terceiros sem a devida permissão, por escrito, desta.*

*Este documento deve ser usado única e exclusivamente para o conhecimento das Normas de Segurança da Informação da Instituição, não podendo ser copiado ou alterado, no todo ou em parte, sem a devida permissão, por escrito, da* ALCE.

*O uso indevido deste documento estará sujeito às punições previstas em lei.*

# Sumário

## 1. Objetivo

Estabelecer as responsabilidades, melhores práticas, recomendações e políticas de uso aceitável e permitido aos recursos de TI por meio de diretrizes e normas, resguardando a segurança das informações da instituição.

Preservar a segurança das informações da ASSEMBLEIA LEGISLATIVA DO ESTADO DO CEARÁ - ALCE (ALCE), garantindo a sua confidencialidade, integridade e disponibilidade.

## 2. Público Alvo

Este Regulamento aplica-se a todos os usuários dos recursos computacionais da ALCE, sejam funcionários, terceirizados e prestadores de serviço.

## 3. O que é Segurança da Informação

Devido ao constante aumento da dependência dos negócios por redes e sistemas interconectados, a informação está cada vez mais exposta a um número crescente e uma grande variedade de ameaças.

A informação pode existir em muitas formas: impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, a informação deve ser tratada de forma adequada levando-se em consideração os aspectos da segurança da informação e o valor que possui para a ALCE.

A Segurança da Informação é a proteção da informação contra vários tipos de ameaças para garantir a continuidade das operações, minimizar riscos aos quais a instituição está exposta, evitar danos inesperados e garantir o retorno sobre os investimentos realizados na instituição.

A segurança da informação é caracterizada pela preservação de:

a) **Confidencialidade:** Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

b) **Integridade:** Garantia de que a informação não será modificada ou destruída por pessoas não autorizadas ou de forma inadequada que modifique ou inutilize a informação;

c) **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A segurança da informação é melhorada a partir da implementação de um conjunto de controles adequados; incluindo políticas, processos, procedimentos, estruturas organizacionais e tecnologia. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e constantemente melhorados, para garantir que os objetivos do negócio e de segurança específicos da instituição sejam atendidos.

## 4. Por que precisamos de uma Política de Segurança

A falta de uma definição em como utilizar e manter o nível de segurança dos seus ativos, desde o acesso à Internet por parte dos colaboradores até as informações que podem ou não ser compartilhadas com entidades externas, pode colocar os negócios da ALCE em risco abrindo margem para prejuízos financeiros ou mesmo à sua imagem perante a sociedade, caso ocorra um incidente de segurança (invasão, vazamento de informação, quebra de sigilo, modificação não autorizada de informações etc.)

A gestão da segurança da informação necessita da participação e envolvimento de todos os colaboradores da ALCE. Para que as responsabilidades, requisitos e ações esperadas e recomendadas sejam padronizados e comunicados para toda a organização; faz-se necessário o registro de todos os aspectos relacionados à segurança, para devida divulgação, aceitação por toda a organização e contínuo treinamento.

A política de segurança consiste em um conjunto de definições e procedimentos que explicam como proteger os ativos da ALCE.

## 5. A Política de Segurança da ALCE

A Política de Segurança da ALCE demonstra de forma clara a responsabilidade da Instituição para com seus ativos de informação e expectativas para com seus colaboradores. O cumprimento desta Política depende do comprometimento de todos.

A Diretoria da ALCE considera a Política de Segurança uma questão estratégica aos negócios da Instituição e incentiva a todos a estarem engajados com a filosofia de segurança da informação em suas atividades diárias.

O não cumprimento das normas de segurança pode levar à execução de penalidades definidas na Política de Segurança.

A Política de Segurança da ALCE está estruturada da seguinte forma:

**Política de Segurança (Diretrizes):** Apresenta os direcionamentos da direção da Instituição quanto à segurança da informação. Explicita os objetivos e princípios que devem reger as ações da ALCE em relação à segurança.

**Regulamento Interno de Segurança (Normas):** Conjunto de normas gerais e específicas que apoiam as Diretrizes de Segurança e detalham o que deve ser feito para realizar o cumprimento adequado.

**Procedimentos:** Conjunto de documentos com instruções passo a passo informando como realizar uma determinada tarefa. Tarefas críticas devem ser regidas por procedimentos para evitar erros.


Todos os colaboradores devem estar cientes do conteúdo da Política de Segurança e assinar o Termo de Uso dos Sistemas de Informação (TUSI). Convém que todos os colaboradores assinem este documento como parte dos termos e condições iniciais de contratação.

Aos fornecedores e terceiros que não estejam cobertos por um contrato existente, deverá ter assinado um acordo de confidencialidade, antes de ter acesso ao ambiente de TI da ALCE.

## 6. Responsabilidades

O Comitê Gestor de Segurança da Informação da ALCE é um comitê de caráter técnico, consultivo e permanente para questões relacionadas à Segurança da Informação, estando diretamente subordinado ao Conselho Deliberativo da ALCE.

O Comitê Gestor de Segurança da Informação é formado por representantes das áreas: Controladoria, Departamento de Recursos Humanos, Coordenadoria de Planejamento e Informática e Procuradoria da Entidade.

Compete ao Comitê Gestor de Segurança da Informação:

- Supervisionar a execução, revisar e atualizar a Política de Segurança da Informação;
- Disseminar a cultura e a Política de Segurança da Informação;
- Analisar e monitorar os incidentes de Segurança da Informação;

- Analisar, acompanhar e avaliar as principais iniciativas de Segurança da Informação na ALCE;
- Promover a elaboração, atualização, validação e divulgação da Política de Segurança da Informação;
- Promover a elaboração e implantação de planos de contingência e recuperação de desastres;
- Coordenar as ações para implantação da Política de Segurança da Informação;
- Tomar decisões sobre as questões que lhe tenham sido encaminhadas;
- Interpretar, recomendar sanções e deliberar sobre aspectos desta Política que precisem de esclarecimentos.

# 7. Normas Gerais

## 7.1. Responsabilidades dos Usuários de Computador

7.1.1. Todo usuário de computador é responsável pelos atos e acessos realizados com sua identificação de acesso no ambiente informatizado;

7.1.2. Manter sigilo sobre as informações consideradas confidenciais da ALCE;

7.1.3. Manter arquivos importantes à Instituição armazenados no servidor de arquivos, a fim de que sejam inclusos na rotina de cópia de segurança (backup);

7.1.4. Remover, da rede e das estações de trabalho e notebooks, os arquivos temporários não mais necessários ou arquivos que se refiram a assuntos alheios aos interesses da Instituição;

7.1.5. Conhecer e cumprir as determinações da Política de Segurança da Informação da ALCE;

7.1.6. Comunicar à área de TI qualquer ocorrência que, direta ou indiretamente, afete a Segurança da Informação da ALCE.

## 7.2. Proteção de Propriedade Intelectual

7.2.1. Todo material produzido por colaboradores da ALCE que esteja relacionado ao negócio da Instituição é de propriedade desta;

7.2.2. É vedado o armazenamento ou uso de músicas, vídeos e arquivos pessoais nos ativos da ALCE;

7.2.3. É vedada a instalação ou uso de softwares não homologados para uso nos ativos de TI da ALCE.

## 7.3. Registro de Acesso e Monitoramento

7.3.1. Toda conexão do usuário (ex: rede, internet, sistemas, correio, estação de trabalho, telefone corporativo, etc.) pode ser monitorada e registrada visando garantir o cumprimento desta Política.

# 8. Normas Específicas

## 8.1. Para Colaboradores

Essa seção contém a relação de normas específicas que se aplicam a todos os colaboradores e seus objetivos.

### 8.1.1. NC-001 - Norma de Identidade dos Usuários e Senhas

**Propósito:** Determinar as práticas para uso de credenciais de acesso aos recursos de TI da ALCE, assim como as questões de segurança referente às senhas de acesso à rede e sistemas.

### 8.1.2. NC-002 - Norma de uso do Correio Eletrônico

**Propósito:** Determinar as práticas necessárias ao uso do correio eletrônico, a fim de evitar o mau uso do serviço e reduzir as chances de comprometimento da segurança dos equipamentos.

#### 8.1.3. NC-004 - Norma de Utilização da Internet

**Propósito:** Determinar as práticas referentes ao acesso à Internet utilizando os recursos de TI da Instituição.

#### 8.1.4. NC-005 - Norma de Utilização de Mídias Removíveis

**Propósito:** Determinar as práticas referentes ao uso de mídias removíveis que armazenem ou transportem informações da ALCE ou de sua responsabilidade.

#### 8.1.5. NC-006 - Norma de Utilização de Softwares de Mensagem Instantânea

**Propósito:** Determinar as práticas referentes ao uso de serviços de mensagem instantânea.

#### 8.1.6. NC-008 - Gestão de Incidentes de Segurança da Informação

**Propósito:** Determinar as práticas referentes à identificação, comunicação e tratamento de incidentes de segurança ocorridos na ALCE.

#### 8.1.7. NC-011 - Norma de Utilização de Notebooks

**Propósito:** Determinar as práticas referentes ao uso de notebooks para desempenho das funções dos colaboradores da ALCE, dentro ou fora de suas dependências.

#### 8.1.8. NC-013 – Manual de Sanções Administrativas

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

### 8.2. Para Equipe de TI

Essa seção contém a relação de normas específicas que se aplicam somente à equipe de TI e seus objetivos.

#### 8.2.1. NC-003 - Aquisição e Desenvolvimento Interno de Sistemas

**Propósito:** Determinar as práticas referentes aos processos de aquisição e desenvolvimento interno de sistemas.

#### 8.2.2. NC-007 - Gestão de ativos de T.I. (hardware, software e área de T.I.)

**Propósito:** Definir os critérios para a elaboração e manutenção de inventário tecnológico. Com o devido registro e conhecimento dos recursos utilizados pela ALCE será possível protegê-los de forma adequada e garantir conformidade com regulamentações em vigor.

#### 8.2.3. NC-010 - Segurança Física e Patrimonial

**Propósito:** Determinar as práticas referentes ao acesso às instalações físicas da ALCE e proteção de seu patrimônio.

#### 8.2.4. NC-012 - Norma de Continuidade de Negócios

**Propósito:** Determinar os requisitos e ações necessárias para a manutenção da continuidade da operação da ALCE em caso de desastres.

# 9. Sanções

A não observância dos preceitos do Regulamento Interno de Segurança da Informação da ALCE, suas Normas e Procedimentos, implicará na avaliação pelo Comitê de Segurança da Informação e possível aplicação de sanções administrativas, cíveis e penais previstas no NC-013 - Manual de Sanções Administrativas da ALCE, Código Penal (Decreto-Lei N°2.848/40, com as alterações da Lei N° 9.983/00 e no Decreto N°2.910/98), no Novo Código Civil (Lei 10.406 de 10/01/2002), Estatuto do Servidor Público ou em qualquer outra legislação que regule ou venha regular esta matéria.

# 10. Outros Documentos

## 10.1 Termo de Aceite

## 10.2 Cartilha de Segurança

# 11. Glossário

**Acesso Externo** – Todo acesso de rede cujo ponto de origem está localizado fora das instalações da organização.

**Acesso Interno** – Todo acesso de rede cujo ponto de origem está localizado dentro das instalações da organização.

**Acesso Remoto** – Todo acesso realizado a um dispositivo de rede (servidor, estação de trabalho, firewall, roteador etc.), através de uma conexão, onde não existe interação presencial com o dispositivo acessado.

**Ameaças** – Uma ameaça é qualquer ocorrência potencial, mal intencionada ou não, que possa prejudicar de alguma forma a organização.

**Armazenamento de Arquivos** – É o ato de guardar, armazenar arquivos de forma eletrônica. Quando salva-se um arquivo em um disco rígido, DVD, CD, pendrive ou um servidor de arquivos, este arquivo está sendo armazenado para uma futura consulta ou alteração.

**Ataque** – Um ataque é uma ação que explora uma vulnerabilidade ou concretiza uma ameaça. Exemplos de ataques são o envio de dados mal intencionados a um aplicativo ou sobrecarga de uma rede para tentar a interrupção de um serviço.

**Backup** – Backup, ou cópia de segurança, é o ato de copiar dados (arquivos, imagens, configurações etc.) de um dispositivo para outro, para que possa ser restaurado no caso da perda dos dados originais, o que pode envolver perda acidental de dados ou até mesmo danificação dos dados originais.

**Banco de dados** – Bancos de dados (ou bases de dados) são conjuntos de registros dispostos em estrutura regular que possibilita a reorganização dos mesmos e produção de informação. Um banco de dados normalmente agrupa registros utilizáveis para um mesmo fim.

**Contingência / Plano de contingência** – Tem o objetivo de descrever as 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 a organização. Pode compor um conjunto de documentos conhecido como Plano de Continuidade dos Negócios.

**Continuidade dos negócios / Plano de continuidade dos negócios** – Conjunto de documentos que tem por objetivo estruturar e manter atualizadas as atividades necessárias à contingência das operações da organização, bem como o retorno à sua normalidade quando possível.

**Correio Eletrônico** – Também chamado de e-mail, é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação (rede de computadores, internet).

**Credencial de Acesso** – Vide login.

**Custódia** – Guarda de um bem, documento, arquivo, de uma informação, de maneira física ou eletrônica.

**Direitos Autorais** – São denominações usualmente utilizadas em referência ao rol de direitos outorgados aos autores de obras intelectuais (literárias, artísticas ou científicas), músicas digitais (MP3), dentre outros. Neste rol encontram-se dispostos direitos de diferentes naturezas.

**Endereço IP** – Sigla para *Internet Protocol* (Protocolo de Internet) é um conjunto de números que representa a identificação de um determinado dispositivo de rede (computadores, firewall, roteadores etc.) em uma rede privada ou pública.

**FTP** – Sigla para *File Transfer Protocol* (Protocolo de Transferência de Arquivos) é uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na Internet.

**Homologado** – Software, sistema, aplicação, ou dispositivo, que passou por suas fases de testes com sucesso e está pronto para ser utilizado em ambiente de produção.

**Incidente de Segurança** – Qualquer fato ou evento que possa afetar a segurança da organização.

**Internet** - Conglomerado de redes em escala mundial de milhões de computadores interligados pelo Protocolo de Internet (IP) que permite o acesso a informações e todo tipo de transferência de dados. A Internet é a principal tecnologia de informação e comunicação.

**Intranet** - Rede de computadores privada baseada no conjunto de protocolos da Internet. Todos os conceitos da Internet aplicam-se também a uma Intranet.

**Licença de Uso -** Significa de que forma um programa pode ser usado, informando se o direito de usá-lo deve ser pago (o exemplo mais famoso é o sistema operacional Windows), se pode ser usado gratuitamente (freeware, como muitos programas em sites de downloads) e se o usuário possui total direito sobre ele.

**Login** - Conjunto de caracteres solicitado aos usuários que necessitam acessar um sistema computacional. Alguns sistemas computacionais solicitam um login e uma senha para a liberação do acesso.

**Login de Acesso** - Vide Login.

**Produção, Ambiente de** - Ambiente controlado que disponibiliza sistemas e aplicações utilizadas no dia-a-dia de uma organização. Uma aplicação normalmente é disponibilizada em ambiente de produção após a realização de diversos testes (performance, qualidade, segurança etc.).

**Recuperação de desastres / Plano de recuperação de desastres** – Conjunto de atividades que permite o retorno à normalidade após a interrupção de um processo crítico de negócio e após ter sido acionado o plano de contingência. Pode compor um conjunto de documentos conhecido como Plano de Continuidade dos Negócios.

**Rede / Rede de computadores** – Consiste de dois ou mais computadores e outros dispositivos conectados entre si de modo a poderem compartilhar seus serviços como dados, impressoras, mensagens (e-mails), etc. A Internet é um amplo sistema de comunicação que conecta muitas redes de computadores. Existem várias formas e recursos de

vários equipamentos que podem ser interligados e compartilhados, mediante meios de acesso, protocolos e requisitos de segurança.

**RISI** – Sigla para Regulamento Interno de Segurança da Informação, constitui um documento que tem por objetivo definir práticas, atribuir legalmente responsabilidades, obrigações, penalidades, direitos e expectativas de acesso aos usuários. É elaborado com base na utilização de diretrizes de segurança mundial, como a norma NBR ISO/IEC 27002, normativas nacionais (provimentos, resoluções e decretos), observando também as legislações ordinárias como o Código Civil, Código Penal e Consolidação das Leis do Trabalho.

**Sistemas de Informação** - É a expressão utilizada para descrever um sistema automatizado, ou mesmo manual, que abrange pessoas, máquinas, e métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário.

**Site** - Conjunto de páginas Web, isto é, de hipertextos acessíveis geralmente pelo protocolo HTTP na Internet. O conjunto de todos os sites públicos existentes compõe a World Wide Web (ou simplesmente Web). As páginas num site são organizadas a partir de um endereço básico, onde fica a página principal, que possui ligações com as demais páginas disponíveis.

**TI** - O termo Tecnologia da Informação (TI) serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação. Também é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como o modo como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas.

**TIC** – Sigla para Tecnologia da Informação e Comunicação, corresponde ao conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios.

**TUSI** – Sigla para Termo de Uso dos Sistemas da Informação, é um instrumento aplicado aos usuários e/ou pessoas contratadas pela corporação, objetivando legitimar o controle de atividades, e outras considerações visando reforçar a inexistência de expectativa de privacidade, sempre de acordo com as tendências jurisprudenciais do direito nacional e internacional, especificamente para ações correlatas à segurança da informação.

**Vírus** - Programa malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.

**Vulnerabilidade** - Ponto fraco de uma rede ou sistema que possibilita um ataque. Isso pode ocorrer devido a um mau projeto, erros de configuração ou técnicas inadequadas e inseguras de codificação.

**Web** - A World Wide Web (também conhecida apenas como Web ou WWW) é um sistema de documentos em hipermídia que são interligados e acessados a partir da Internet. Os documentos podem estar na forma de vídeos, sons, hipertextos e figuras. Para visualizar estes documentos deve-se usar um programa conhecido como navegador (browser). O ato de seguir links é comumente chamado de "navegar" ou "surfar" na Web.