

## Segurança da Informação

Política de Segurança	1
Classificação das Informações	2
Acesso e cuidados com as Informações da Instituição	2
Tratamento das Informações	2
Incidentes de Segurança	4
Responsabilidades do Usuário	4
Identidades de Usuários e Senhas	5
Uso de Dispositivos Removíveis	5
<b>Outros Assuntos</b>	
Privacidade	2
Registro de Acesso e Monitoramento	3
Acesso à Internet	3
Uso do Correio Eletrônico	4

## Segurança da Informação

Vive-se na era do conhecimento, basta que se observe ao redor e acesse à internet, assista televisão, ouça rádios etc.

As informações estão disponíveis em diversas formas e meios, podendo ser digital, impressa ou escrita, transmitida através dos correios ou por meios eletrônicos, apresentada em filmes, conversas ou chats.

Devido ao aumento da dependência da tecnologia nos negócios modernos, os dados organizacionais estão cada vez mais expostos a várias ameaças virtuais. Diante disso, a segurança da informação veio como uma ferramenta

necessária para proteger as empresas e garantir a continuidade do negócio e a proteção das informações.

Este informativo contém os principais objetivos do trabalho realizado na ALCE. Esta política visa garantir o acesso às informações necessárias para a realização do trabalho de cada colaborador ao mesmo tempo em que protege os dados, os ativos e a imagem da instituição.



## Política de Segurança

A política de segurança consiste em um conjunto de normas e procedimentos que visam proteger os dados e ativos da Assembleia, sendo composta por:

- **Diretrizes de Segurança:** apresenta um direcionamento estratégico e explicita os princípios e objetivos que regem as ações e normativos da Assembleia no quesito segurança;
- **Regulamento interno:** determina as regras para a utilização dos ativos tecnológicos e da manipulação das informações da Entidade;
- **Procedimentos Operacionais:** Consolida a padronização dos

processos da Entidade.

O sucesso da implantação da política de segurança da informação depende do envolvimento de todos os colaboradores da Assembleia. Para tanto, além desta cartilha resumida, o normativo será disponibilizado no Portal do Servidor através do link: [www.portaldoservidor.al.ce.gov.br](http://www.portaldoservidor.al.ce.gov.br) menu Notícias – Tecnologia da Informação.





*“O descarte de informações consideradas confidenciais ou secretas, em forma de listagens, CDs, pendrives ou mesmo impressas deve ser feito mediante destruição do material, de modo a impossibilitar a recuperação das informações.”*

## Acesso e cuidados com as Informações da Instituição

Cada tipo de informação necessita de um tratamento específico, que envolve desde o uso da tecnologia visando impedir acessos a dados digitais até a discricção em conversas particulares sobre temas corporativos.

Você já pensou que tipo de danos a Entidade sofreria se fosse impressa alguma informação confidencial que por descuido seja repassada a terceiros como borrão? Ou descartada no lixo sem a destruição de seu conteúdo? Ou comentada no almoço, em

um restaurante de acesso público?

A ALCE tem em sua custódia dados sigilosos de seus parlamentares e colaboradores, além daqueles necessários a execução de seus objetivos. Por isso, serão concedidos acessos conforme a necessidade de utilização para o cumprimento das obrigações de cada funcionário.

## Privacidade

Existem definições para classificar e tratar de forma adequada os dados da Assembleia, mas e as minhas informações pessoais, como são tratadas?

Elas poderão ser monitoradas ou até mesmo registradas. Mas como isso é possível? E a minha privacidade?

Os recursos tecnológicos da Assembleia devem ser utilizados somente para fins institucionais. Toda a utilização destes recursos poderá ser monitorada e registrada, com vista a identificar eventuais abusos.

## Registro de Acesso e Monitoramento

Com o intuito de identificar atividades prejudiciais ou improdutivas, a Assembleia registra todas as conexões dos usuários (ex: internet, sistemas, correio, estação de trabalho, telefone corporativo, etc), inclusive datas, endereços eletrônicos e serviços acessados, independente se o acesso foi permitido ou negado pelos mecanismos de controle implantados.

### Quer dizer que tudo que eu faço a partir de um computador na Assembleia é monitorado?

Não. Contudo, se houver indícios de transgressão à Política de Segurança da Informação, a Assembleia poderá auditar as ações realizadas a fim de coletar evidências do mau uso dos recursos e passar a monitorar os acessos.



## Acesso à Internet

"Navegar é preciso". Na Assembleia, somente com segurança.

Para isso, o órgão aplica algumas restrições de acesso à internet, definidas em norma, como seguem:

- Todo acesso a sites não liberados devem ser solicitados, caso necessário para o exercício de sua função, ficando sua liberação condicionada à requisição formal com justificativa da necessidade de acesso, a fim de reduzir a probabilidade de contaminação devido ao acesso a sites de origem desconhecida, de conteúdo duvidoso ou que podem conter vírus.
- É estritamente vedado o acesso a sites

relacionados a sexo, violência, racismo, pedofilia, drogas, download de softwares não autorizados, dentre outros similares.

- É vedada a utilização de recursos computacionais da Assembleia para acessar, baixar, enviar ou trafegar informações relativas a recursos desnecessários ou inadequados à execução das atividades funcionais, a saber:

- a) Software de compartilhamento de arquivos;
- b) Jogos;
- c) Imagens, fotos, arquivos multimídia, incluindo filmes,

músicas ou animações.

- d) Softwares ou mecanismos que visam burlar os controles e restrições aplicadas em conformidade com a Política de Segurança da Assembleia.
- e) Qualquer tipo de software não homologado pela equipe de TI da Assembleia.

Assim, fica bloqueado o acesso ao Facebook e ao Youtube, ficando permitido o uso, desde que para manter redes sociais de cunho institucional, para os colaboradores que serão autorizados por seu coordenador, diretor ou parlamentar após a implantação desta Política de Segurança.





## Uso do Correio Eletrônico

O correio eletrônico da Assembleia deve ser utilizado para envio ou recebimento de dados relacionados às atividades corporativas. Logo, não é permitido o uso do e-mail institucional para diversão ou distribuição de mensagens ofensivas, que contenham comentários sobre violência, pornografia, drogas etc.

Dicas importantes:

- Nunca acesse links ou abra anexos enviados por pessoas

desconhecidas ou que tenham origem duvidosa;

- Evite enviar informações confidenciais por e-mail. Contudo, se for necessário, consulte a equipe de tecnologia. Eles certamente irão lhe indicar a melhor maneira.

Leia a Norma de Uso de Correio Eletrônico para maiores detalhes.



## Responsabilidades do Usuário

Todo usuário de computador:

- É responsável pelas ações efetuadas com seu login no ambiente informatizado;
- Deve conhecer e cumprir as determinações da Política de Segurança da Informação da Assembleia;
- Deve gravar os arquivos estratégicos no servidor para que sejam inclusos nos

backups diários;

- Deve manter sigilo sobre as informações confidenciais e secretas da Assembleia, além de manter discrição sobre as demais;
- Deve comunicar à área de TI qualquer ocorrência que, direta ou indiretamente, afete a segurança da informação da Entidade.

## Incidentes de Segurança

Incidente de segurança é todo evento adverso, confirmado ou sob suspeita que atente contra:

- A confiabilidade dos sistemas de informação ou da rede de computadores e
- As normas e diretrizes estabelecidas na Política de Segurança da Assembleia.

Como devo proceder ao identificar um incidente de segurança?

Deve-se entrar em contato com a equipe de tecnologia através do e-mail [atendimentoinformatica@al.ce.gov.br](mailto:atendimentoinformatica@al.ce.gov.br)

## Identidade de Usuários e Senhas

Todo colaborador da Assembleia que utiliza os recursos tecnológicos possui um usuário associado a uma senha pessoal e intransferível.

Com o intuito de prevenir acessos não autorizados em cada login, a equipe de tecnologia irá configurar os servidores para trocar as senhas dos usuários a cada 90 dias e que tenham no mínimo 08 caracteres incluindo letras, números e símbolos.

Recomenda-se que as senhas:

- a) sejam memorizadas, pois é mais seguro do que escrevê-las;

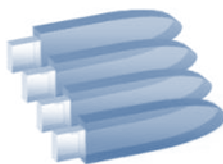
Lembre-se, você sempre será responsável pelas ações executadas com seu usuário!

Você gostaria que alguém soubesse a sua senha do Banco? Obtenha mais informações sobre como criá-la através da Norma de Identidade dos Usuários e Senhas.

***“A credencial do usuário e sua senha são pessoais e intransferíveis.”***

## Uso de Dispositivos Removíveis

É vedado o uso de dispositivos removíveis pessoais para qualquer tipo de transferência e armazenamento de quaisquer tipos de informações.



Caso seja necessária a utilização de tais dispositivos para execução de seu trabalho, o colaborador poderá solicitar, mediante justificativa formal, a autorização de uso ao seu gestor imediato.

O gestor deverá entrar em contato com a Coordenadoria de Planejamento e Informática através do e-mail [atendimentoinformatica@al.ce.gov.br](mailto:atendimentoinformatica@al.ce.gov.br)

**Contatos da Coordenadoria de Planejamento e Informática**

**Telefones**

**(85) 3277-2847**  
**(85) 3277-2848**

**E-mail**

**atendimentoinformatica@al.ce.gov.br**

## Comitê Gestor de Segurança da Informação

A Presidência da Assembleia criou o Comitê Gestor de Segurança da Informação que possui caráter técnico, consultivo e permanente.

Eis algumas das responsabilidades do comitê:

✓ revisar e atualizar a Política de Segurança da Informação, além de

monitorar seu cumprimento;

✓ disseminar a cultura e a Política de Segurança da Informação;

✓ analisar e monitorar os incidentes de segurança da informação, etc.

## Equipe de Tecnologia

A Assembleia conta com uma equipe de tecnologia bastante capacitada. Esta área estará disponível para sanar eventuais dúvidas dos colaboradores sobre a Gestão da Segurança da Informação.

Os contatos e meios de comunicação estão disponíveis ao lado.