

Política de Segurança Corporativa da Assembleia Legislativa do Estado do Ceará



**Assembleia Legislativa
do Estado do Ceará**



Agenda



Projeto Realizado



Política de Segurança da ALCE



Próximos passos

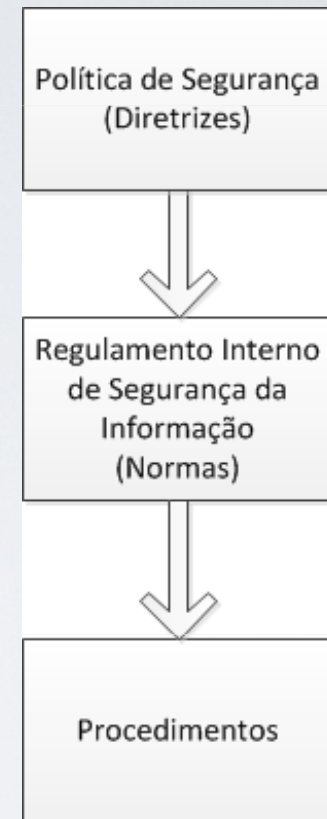


Projeto realizado

- Definição/Revisão da Política de Segurança da ALCE
- Documento foi revisado com Diretores e aprovado pela Presidência
- Determina as expectativas, uso aceitável e deveres de cada colaborador em relação a Segurança da Informação
- Formalmente em vigor à partir desta data (26/08/2013)

Política de Segurança?

- Um conjunto de definições e procedimentos que explicam como proteger os ativos da ALCE.
- A Política 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.



Por que?

- Quem e por que faz uso de uma Política de Segurança
- Criação de um Comitê Gestor de Segurança da Informação com poderes e responsabilidades de deliberar sobre a Segurança da Informação
- Normas de utilização

Que normas?

- Norma de Identidade dos Usuários e Senhas
- Norma de uso do Correio Eletrônico
- Norma de Utilização da Internet
 - Facebook
 - Youtube
- Norma de Utilização de Mídias Removíveis
- Norma de Utilização de Softwares de Mensagem Instantânea
- Gestão de Incidentes de Segurança da Informação
- Norma de Utilização de Notebooks

Norma de Identidade dos Usuários e Senhas

- É vedado fornecer usuário e senha para outras pessoas;
- É vedado usar usuário e senha de outras pessoas, mesmo se autorizado;
- Senha com pelo menos 08 caracteres incluindo letras, números e símbolos;
- Senha deve ser alterada a cada 90 dias, não devendo reutilizar a última senha;
- Senhas não utilizadas em 60 dias serão desabilitadas.

Norma de uso do Correio Eletrônico

- O colaborador é o único responsável pelo envio de mensagens;
- Só deve ser usado para fins institucionais;
- Não abrir links ou anexos de remetentes desconhecidos ou e-mails suspeitos de conter vírus;
- É vedado ao usuário realizar cadastro do e-mail corporativo em listas ou sites que não façam parte do interesse da instituição.

Aquisição e Desenvolvimento Interno de Sistemas

- É vedado a outras áreas da ALCE a contratação direta de sistemas e/ou soluções tecnológicas sem que o processo de avaliação seja aprovado pela área de Coord. De Planejamento e Informática.

Norma de Utilização da Internet

- É estritamente proibido o acesso a sites relacionados a sexo, violência, racismo, pedofilia, drogas, download de softwares etc;
- Sites considerados maliciosos, que podem comprometer a segurança dos recursos computacionais ou que contenham vírus podem ser bloqueados automaticamente;
- É vedada, salvo expressa solicitação e autorização da coordenação ou parlamentar: sites para compartilhamento de arquivos, jogos, imagens, fotos, filmes, músicas, redes sociais etc.

Norma de Utilização de Mídias Removíveis

- O acesso a mídias removíveis é liberado. Ficando vedado o uso de informações sigilosas fora da Assembleia Legislativa. As mídias removíveis somente devem ser usadas para o exercício das funções dos colaboradores da ALCE;
- É aconselhável que os dispositivos de armazenamento removíveis sejam verificados por antivírus antes do uso;
- Caso um usuário não autorizado tenha que utilizar informações de outros setores ou informações tidas como de USO INTERNO ou CONFIDENCIAIS, deverá solicitar à área responsável a autorização para o uso.

Norma de Utilização de Softwares de Mensagem Instantânea

- É permitido o uso de mensagens instantâneas para fins institucionais;
- É expressamente vedado o uso de transferência de arquivos através de softwares de mensagem instantânea, mesmo quando realizado entre pessoas autorizadas a utilizar este serviço.

Gestão de ativos

- Deve ser mantido um inventário atualizado dos equipamentos e softwares, permitindo a identificação de:
- Características físicas do equipamento;
- Softwares instalados;
- Sejam eles notebooks ou computadores de mesa.

Gestão de Incidentes de Segurança da Informação

- Incidentes de segurança devem ser reportados através do e-mail atendimentoinformatica@al.ce.gov.br
- É de responsabilidade do Comitê de Segurança o devido tratamento dos incidentes de segurança e adoção de medidas necessárias a sua contenção e correção;
- São consideradas faltas graves e sujeitas a ações disciplinares: não comunicação de incidentes que tenha conhecimentos ou realizar ações que visam ocultar ações executadas e incidentes ocorridos.

Segurança Física e Patrimonial

- Não é permitido o trânsito de colaboradores, terceiros ou visitantes nas dependências da ALCE sem a devida identificação (crachá ou impressão digital) para colaboradores, terceiros ou visitantes;
- Em especial, devem ter acesso controlado: Data Center, Local com informações de funcionários e Locais com informações CONFIDENCIAIS e/ou SECRETAS;
- A ALCE possui um sistema de CFTV, com câmeras em quantidades e locais adequados, com armazenamento de imagens por um período superior a 30 (trinta) dias.

Norma de Utilização de Notebooks

- Todos os gabinetes e setores deverão comunicar por escrito: nome e matrícula do servidor que usa notebook pessoal para desempenhar suas funções. Ficando vedado o uso de notebooks pessoais ou de terceiros, não autorizados. (Informar até 26 de Agosto de 2013);
- Todos os arquivos utilizados para exercício das funções diárias devem estar armazenados no servidor de arquivos (backup);
- Usuários de notebooks da ALCE que queiram que os dados fiquem criptografados devem solicitar ao setor de Informática.

Norma de Continuidade de Negócio

- Plenário: *“poderá, por deliberação da Mesa Diretora, ad referendum da maioria absoluta dos Deputados, reunir-se, eventualmente, em outro local” e “Em casos especiais, e por deliberação de 2/3 de seus membros, a Assembleia poderá funcionar, excepcionalmente, fora de sua sede”*
- Tecnologia da Informação: deverá manter uma Política de Backup detalhada e solução de contingência para serviços identificados como críticos e outros que sejam necessários estar disponíveis em caso de urgência.

Manual de Sanções Administrativas

- Infrações de alta, média e baixa relevância
- Na existência de indícios do cometimento de atos indevidos por algum colaborador, o Comitê de Segurança da Informação poderá apurar o ocorrido;
- Confirmada a existência do ato irregular, o Comitê encaminhará o resultado da Apuração para a Diretoria Geral, que solicitará análise jurídica da Procuradoria e encaminhará sugestão a Mesa Diretora.

Manual de Sanções Administrativas

- As sanções 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 decisão sobre a aplicação de sanção fica a cargo da Mesa Diretora.

Onde consultar os documentos?

- Cartilha com principais pontos foram entregues no início desta palestra
- Documentos completos estão disponíveis na Intranet [Site da AL > Portal do Servidor > Notícias > Tecnologia da Informação > Política de Segurança](#)
- “Todo colaborador, funcionário, terceirizado e fornecedor que tenha acesso a recursos da ALCE deve conhecer, aceitar e cumprir a Política de Segurança da Informação da instituição.”

Próximos Passos

- Todos deverão conhecer a Política de Segurança
- Acessar Intranet e ler documentos
- Qualquer dúvida entrar em contato com a área de Coordenadoria de Planejamento e Informática
 - atendimentoinformatica@al.ce.gov.br
 - Ramal 2847 ou 2848



Assembleia Legislativa do Estado do Ceará



www.energytelecom.com.br



www.coresec.com.br