

Cartilha da Política de Segurança da Informação



Cartilha da Política de Segurança da Informação - POSIC

Na sociedade digital, a disseminação de informações de forma exponencial e acelerada, além do compartilhamento de dados de forma global e com reprodução em larga escala, demanda das instituições o estabelecimento de procedimentos e práticas que resguardecem as informações de forma segura e com atendimento aos pilares da **integridade, confidencialidade e disponibilidade**.

Diante deste cenário, este material objetiva conscientizar e informar todos os servidores, colaboradores e todas as pessoas envolvidas em atividades no âmbito da PGE/CE sobre a importância do tema Segurança da Informação para a Instituição.

O QUE É SEGURANÇA DA INFORMAÇÃO?



A Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os objetivos propostos e às suas oportunidades.



O QUE SIGNIFICA OS TRÊS PILARES PRINCIPAIS DA SEGURANÇA DA INFORMAÇÃO?

Integridade

É a garantia de que a informação esteja livre de qualquer alteração não autorizada, mantendo-se íntegra, conforme foi criada.

Confidencialidade

Busca garantir que a informação seja acessada apenas por pessoas autorizadas.

Disponibilidade

Garantia de que a informação estará disponível sempre que necessário ser acessada.



Exemplos de descumprimento:

Alguém obtém acesso não autorizado ao seu computador e altera informações que tramitam dentro da PGE.

Alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas.

A rede sofre uma grande sobrecarga de dados, ou um ataque de hacker, e por este motivo você fica impossibilitado de fechar o processo de uma licitação em andamento.

O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO E COMO REPORTÁ-LO?

O Incidente de Segurança é um evento não planejado que pode acarretar prejuízos à empresa ou mesmo violar as regras de segurança.



Para melhor entendimento, citamos alguns exemplos:

1

Indisponibilidade de sistemas: em função de alguma vulnerabilidade existente de um sistema na WEB, o acesso ao sistema fica bloqueado para os usuários, ou então fica com performance tão lenta que sua utilização torna-se inviável;

2

Cópia de dados/informações: por algum motivo, seja por um código malicioso (programa do tipo malware) instalado no computador, dados do usuário, ou de sistemas, são capturados e disponibilizados de forma indevida, sem a devida autorização, e muitas vezes sem o devido conhecimento;

3

Sequestro de dados: através da instalação de um código malicioso (malware) no computador, normalmente em função de acesso a páginas internet inseguras, arquivos (dados) armazenados no computador são retirados, ou codificados, de forma que o seu acesso torna-se inacessível, ficando a disponibilidade do mesmo, em alguns casos, vinculada ao pagamento de "resgate";



Caso perceba:

- Comportamentos estranhos de seu computador ou de qualquer recurso tecnológico;
- Comportamentos suspeitos de terceiros ou funcionários;
- Políticas e normas de segurança não sendo seguidas;



Notifique o fato imediatamente à Coordenadoria de Tecnologia da Informação - CTI, abrindo um chamado de incidente de segurança para que sejam tomadas as providências cabíveis.



O QUE GANHAMOS COM A SEGURANÇA DA INFORMAÇÃO?

A adoção de medidas relativas à Segurança da Informação aprimora as atividades da Procuradoria, reduz custos e gerencia melhor os riscos das atividades em que está envolvida; fortalece a sua imagem e cria valor para si, para os servidores, para os colaboradores, terceirizados e para os cidadãos. De modo diverso, a ausência de processos e procedimentos de controles de segurança acarreta na perda da credibilidade, elevação dos custos, entre outros impactos.

E PORQUE TODOS GANHAM?

Porque passamos a ter maior credibilidade, pois, além de um ambiente seguro para desenvolver as tarefas diárias, ganhamos conhecimento das melhores práticas em gestão de segurança da informação, o que faz com que nossos serviços sejam prestados com excelência, gerando impactos positivos para os cidadãos e para toda a sociedade.



Precisamos conhecer todas as normas que fazem parte da política, acessando a nossa Política de Segurança da Informação, através da: **Intranet > Governança Corporativa > Política.**



PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO A SEREM ADOTADAS

Lembre-se, a segurança da informação é responsabilidade de TODOS. Contamos com você!

6 REGRAS PARA ADOTAR:



Nunca insira um **dispositivo móvel** que armazene dados em seu computador.



Crie **senhas** difíceis de serem descobertas e mude-as periodicamente.



Nunca utilize **credenciais** emprestadas para acessos aos sistemas corporativos.



Não anote ou armazene sua **senha** em locais sem proteção, que são visíveis para terceiros.



Não altere as **configurações** dos recursos fornecidos sem a autorização da equipe de TI.



Ao constatar algum comportamento estranho durante o **acesso à Internet**, entre em contato com a equipe de TI.



6 DICAS PRÁTICAS:



Crie o hábito de bloquear sua estação de trabalho ao se ausentar;



Evite manter papéis com dados e informações visíveis na sua mesa de trabalho ao se ausentar;



Cuidado ao abrir anexos de e-mail que você não tenha solicitado;



Não acesse sites que não tenham relação direta com as suas atividades de trabalho;



Não esqueça papéis com dados pessoais e informações da PGE na impressora;



Antes do envio de uma mensagem, pense sobre o conteúdo e avalie se o destinatário deve mesmo receber esta mensagem;



Lembre-se que, para sua segurança, todos os acessos a Internet e todos os e-mails são monitorados.

A PGE possui uma **Política de Segurança de Informação** com as melhores práticas e procedimentos que devem ser seguidas e disseminadas por todos dentro das suas funções e atividades. Lembre-se que **você é responsável por todas as suas ações.**

Caso existam infrações relacionadas a política e normas de segurança cibernética e da informação serão atribuídas penalizações de acordo com as regras previstas na POSIC da PGE/CE



Em caso de dúvidas, consulte a POSIC em conjunto de suas respectivas **NORMAS na INTRANET (Intranet > Governança Corporativa > Política).**

MAIS INFORMAÇÕES:



Ramal: 6313



intranet.pge.ce.gov.br