



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

NR12 - Aquisição, Desenvolvimento e Manutenção de Sistemas

Setembro/2022



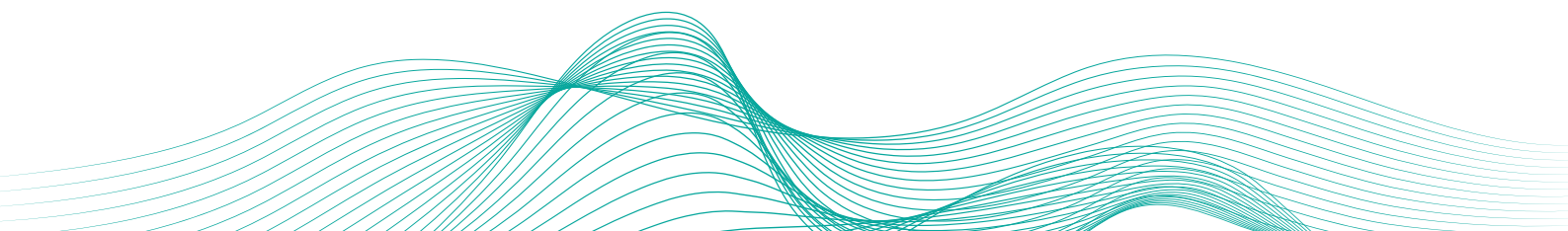
CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO

CONTROLE DE VERSÕES

Versão	Data	Responsável	Alteração principal
00	07/11/2022	Coordenadoria de TI	Elaboração inicial

SUMÁRIO

1. INTRODUÇÃO	3
2. OBJETIVO	3
3. ABRANGÊNCIA	3
4. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS	3



1. INTRODUÇÃO

As aplicações são o meio principal de produtividade, onde os usuários conseguem manipular a informação de forma confiável. Elas podem ser adquiridas ou desenvolvidas e, para garantir a qualidade e a integridade das aplicações, se faz necessária a definição de controles que abordem seus requisitos gerais.

2. OBJETIVO

Definir padrões que norteiam o processo de aquisição, desenvolvimento e manutenção de sistemas de informação, visando assegurar a disponibilidade dos serviços suportados por estes sistemas.

3. ABRANGÊNCIA

Estes controles se aplicam a todos os usuários internos e externos que utilizam o recurso de TIC da PGE-CE.

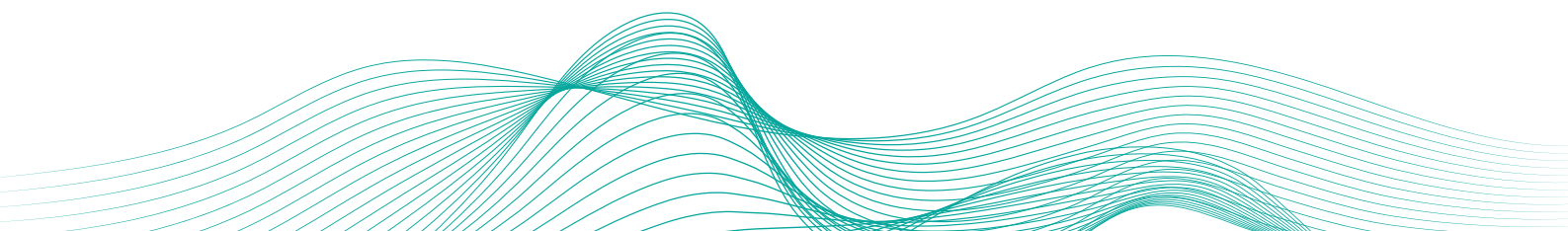
4. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Propriedade intelectual:

- 4.1. Toda e qualquer informação produzida ou recebida pelos colaboradores (internos e externos), em resultado da função exercida e/ou atividade profissional contratada, torna-se, imediatamente, de titularidade da Instituição.

Aquisição de sistemas de informação:

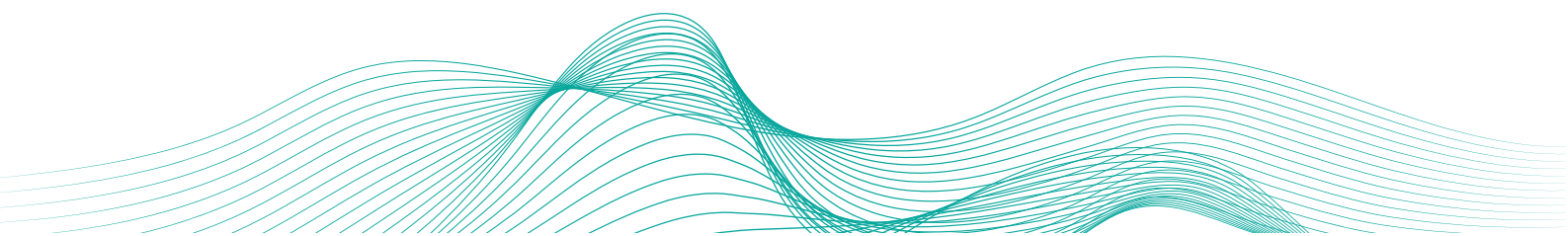
- 4.2. A área de TI será a responsável pelo detalhamento técnico do produto ou serviço a ser adquirido;
- 4.3. Deverá ser elaborado um estudo de viabilidade contendo o detalhamento das soluções analisadas para que seja justificada a escolha do sistema contratado;
- 4.4. As atividades desde encerramento do contrato deverão estabelecer em suas cláusulas, no mínimo:



- I. A entrega das versões finais dos produtos e sua documentação;
- II. A transferência de conhecimento sobre a solução contratada;
- III. A revogação de perfis de acesso;
- IV. A eliminação de caixas postais.

Desenvolvimento e manutenção de sistemas de informação:

- 4.5. Todos os sistemas devem possuir documentação que deve ser armazenada em local seguro e controlado, sendo proibido o armazenamento ou divulgação em ambiente público ou pessoal, tais como discord, github, trello e outros similares;
- 4.6. Para toda mudança realizada nos sistemas implementados, as respectivas documentações deverão ser atualizadas;
- 4.7. Os sistemas devem possuir controles para que os usuários tenham acesso apenas aos recursos necessários ao seu trabalho (perfil de acesso);
- 4.8. Toda informação de autenticação (senhas) deverão ser armazenadas de forma criptografada;
- 4.9. Deverão ser suprimidos os comentários com informações sensíveis (senha, token, etc) no código fonte das aplicações;
- 4.10. Devem existir trilhas de auditoria nas transações efetuadas pelos usuários e nos acessos ao código-fonte;
- 4.11. Os códigos fonte das aplicações deverão ser armazenados em plataforma de versionamento, de forma controlada e com permissões de acesso apenas aos colaboradores envolvidos na aplicação;
- 4.12. A plataforma de versionamento deverá ser hospedada internamente na PGE-CE, sendo acessada no ambiente interno ou através de VPN;
- 4.13. Os códigos fonte das aplicações não deverão ser modificados através de editores de código em ambiente de produção, com exceção dos arquivos de configuração de variáveis e conexão com o banco de dados;
- 4.14. Caso haja a necessidade de alteração direta em alguma parte do código em ambiente de produção, esta alteração deverá ser realizada pela equipe responsável pela hospedagem da aplicação,



- mediante solicitação formal do Gestor de TI, e um backup do código deverá ser realizado antes da alteração;
- 4.15. Deverá ser aplicado a todos os sistemas a segregação dos ambientes de desenvolvimento, homologação e produção;
 - 4.16. Deverá existir a segregação dos acessos de usuário para cada ambiente (produção, homologação e desenvolvimento);
 - 4.17. Os sistemas em ambiente de produção deverão ser atualizados sempre a partir da última versão contida no repositório de versionamento;
 - 4.18. Antes de disponibilizar nova versão de uma aplicação em ambiente de produção, faz-se necessário que o usuário realize os testes necessários e formalize a homologação para posterior liberação e entrada em ambiente de produção;
 - 4.19. As bases de dados dos ambientes de produção, homologação, testes e desenvolvimento devem ser utilizadas especificamente para suas respectivas funcionalidades, não sendo permitido a utilização de uma base de dados para funcionalidades diferentes da especificada;
 - 4.20. Todo e qualquer incidente de segurança detectado no ambiente de Software deverá ser reportado a Coordenação de TI e formalizado através da Central de Serviços, para verificação pela área responsável pelas operações relacionadas a segurança da informação.

