

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

NR04 - Backup e Restauração de Dados

Setembro/2022



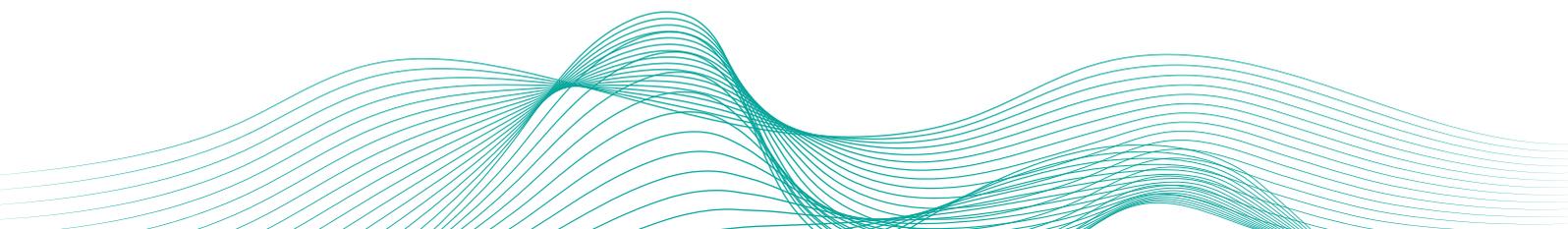
CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO

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. BACKUP E RESTAURAÇÃO DE DADOS	3



1. INTRODUÇÃO

O backup é um processo fundamental para garantir a salvaguarda das informações de uma Instituição, enquanto em ocorrências de problemas, é necessária a realização da restauração de dados, retornando a informação para sua posição normal.

2. OBJETIVO

Este controle tem o intuito de definir as premissas sobre a execução, manutenção e solicitações de backup (cópias de segurança) e restore (restauração da cópia de segurança).

Os tipos mais comuns de backup utilizados são:

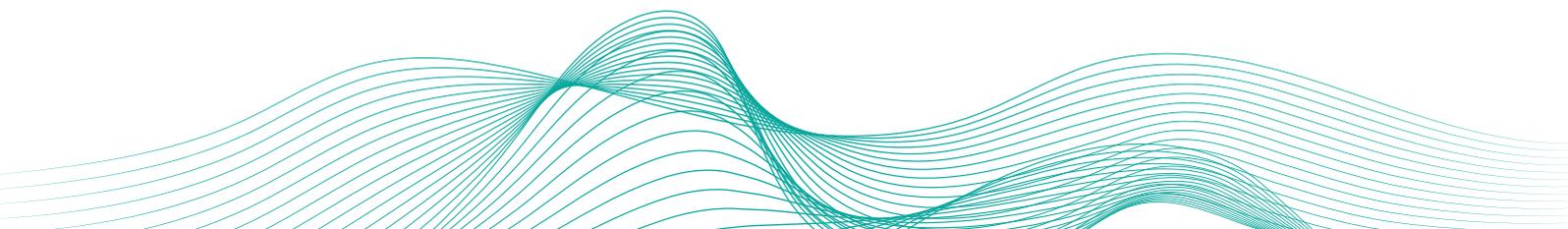
- **Completo:** conjunto de backup que contém toda a informação originalmente destinada à guarda;
- **Incremental:** conjunto de backup que contém apenas os últimos registros alterados após o último backup realizado, seja ele completo ou incremental;
- **Diferencial:** conjunto de backup que contém todos os últimos registros alterados após o backup completo.

3. ABRANGÊNCIA

Estes controles se aplicam a todos os ativos de informação que armazenam dados (file servers, bancos de dados, aplicações, outros) da PGE-CE.

4. BACKUP E RESTAURAÇÃO DE DADOS

- 4.1. Deverá existir uma área na rede para as atividades institucionais dos colaboradores, onde essa área terá cobertura de backup diário (realizado pelo menos uma vez ao dia);
- 4.2. Arquivos gravados localmente (no drive "C:" por exemplo) não terão cobertura de backup, não tendo garantia e podendo ser perdidos caso ocorra alguma falha no computador;
- 4.3. Todos os backups devem ser gerenciados por sistema que permita



- o agendamento automático, e deverão ser executados, preferencialmente, fora do horário comercial;
- 4.4. Deverá existir uma retenção de, pelo menos, 6 (seis) meses para o ambiente de produção;
 - 4.5. O agendamento dos backups deverá ser agrupado em rotinas automatizadas de backups diários, semanais e mensais;
 - 4.6. Para os serviços mais críticos como arquivos (file server) e bancos de dados, deve existir uma área de recuperação rápida onde os dados serão sincronizados, pelo menos, duas vezes ao dia;
 - 4.7. Os backups deverão ser sistematicamente armazenados em ambiente externo ao datacenter (backup offsite), em cofre anti-incêndio e anti-impacto e com umidade controlada, para preservar contra a deterioração das fitas;
 - 4.8. O acesso ao cofre deverá ser controlado e monitorado por câmeras de segurança;
 - 4.9. As unidades de execução de backup (biblioteca de fitas) devem estar instaladas em locais de acesso restrito e monitorado;
 - 4.10. Deverá ser realizado, sistematicamente, e de forma aleatória, um processo de restauração de backup, visando avaliar o processo de restore;
 - 4.11. Os responsáveis pela gestão do sistema de backup deverão realizar avaliações frequentes para identificar falhas, atualizações e/ou novas versões do produto, ciclo de vida, melhorias dentre outros que sejam necessários ao funcionamento do sistema;
 - 4.12. As solicitações de restauração de dados deverão ser realizadas através da Central de Serviços da PGE-CE, e deverão conter informações de forma clara, com o local, nome de arquivo ou pasta e data que deverá ser restaurada a informação;
- 