TecnoTech
Sistemas

# POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Tecnotech Sistemas

Felipe Santos de Andrade / Wanderson Camara dos Santos

# Política de Backup e Restauração de dados digitais

Tecnotech Sistemas

Diretoria de Implementação e Projetos

Política criada sob a supervisão de

Romney Dutra / Lucas Diniz - Prolinx

Março de 2023

# Abreviaturas e siglas

**Administrador de backup:** Responsável pelos procedimentos de configuração, execução e monitoramento de backup e pelo acompanhamento dos testes nos procedimentos de restore.

**Administrador de recurso:** Responsável pela operação de serviços ou equipamentos do CTIC, bem como pela realização dos testes de restore.

**Backup full:** Cópia de segurança de dados computacionais.

**Backup total:** Backup em que todos os dados são copiados integralmente (cópia de segurança completa).

**Backup incremental:** Backup em que somente os arquivos novos ou modificados são copiados.

**Backup diferencial:** Backup em que os arquivos novos ou modificados da base de dados incremental são copiados.

**Clientes de backup:** Todo equipamento servidor no qual é instalado o cliente de backup.

**Disaster Recovery:** Estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica.

**Mídia:** Meio físico no qual se armazenam os dados de um backup.

**Retenção:** Período de tempo em que o conteúdo da mídia de backup deve ser preservado.

**Restore:** Restauração de arquivos computacionais.

# Conteúdo

# Lista de Figuras

# Lista de Tabelas

# Capítulo 1

# INTRODUÇÃO

Este documento estabelece a política de backups e restauração de arquivos digitais que estão armazenados no parque tecnológico da tecnotech sistemas. O objetivo desta política é garantir a integridade, confidencialidade e disponibilidade dos dados e informações críticas da empresa.

Para cumprir com esta política, a tecnotech sistemas tem implantado um sistema de backup automatizado e seguro, que faz cópias regulares dos arquivos digitais importantes. Os backups serão armazenados em locais seguros e devidamente protegidos, para que possam ser recuperados rapidamente em caso de necessidade

# Capítulo 2

# PROPÓSITO

Todas as áreas da empresa serão responsáveis por garantir a conformidade com esta política, incluindo a realização de testes de restauração periódicos e a manutenção de backups atualizados. A segurança e integridade dos dados é uma responsabilidade compartilhada por todos os colaboradores da tecnotech sistemas.

# Capítulo 3

# DECLARAÇÕES DA POLÍTICA

Essa Política de backup da TECNOTECH SISTEMAS é baseada em princípios como confidencialidade, legalidade, autenticidade, conformidade, controle de acesso, integridade e disponibilidade. Os dois últimos são fundamentais para todas as ações e diretrizes da política.
Em Tecnologia da Informação, o backup e a proteção de dados são usados para manter a continuidade dos negócios, replicar dados, recuperar dados após desastres e reduzir os custos de infraestrutura.
As rotinas de backup são projetadas para permitir a recuperação de dados no menor tempo possível, principalmente quando os serviços de TI ficam indisponíveis. Preferencialmente, as soluções de backup são automatizadas.

As rotinas de backup têm requisitos mínimos diferenciados com base no tipo de serviço de TI ou dados salvaguardados. Os serviços de TI críticos da organização têm prioridade.
Quando possível, o armazenamento de backup é realizado em um local diferente da infraestrutura crítica. É preferível ter um local remoto para armazenar cópias extras dos principais backups, como os backups de dados de serviços críticos.
Recursos de infraestrutura são reservados para testar a restauração do backup. Em situações em que a confidencialidade é importante, as cópias de segurança são protegidas por criptografia.

# Capítulo 4

# REGRAS GERAIS

O objetivo do serviço de backup para tecnotech é garantir a segurança das informações e a sua recuperação em um curto espaço de tempo, especialmente em situações de indisponibilidade de serviços dependentes desses dados.

Os procedimentos de backup devem ser atualizados sempre que houver:

- Desenvolvimento de novas aplicações;
- Novos locais de armazenamento de dados ou arquivos;
- Novas instalações de bancos de dados;
- Instalação de novos aplicativos;
- Outras informações que precisem ser protegidas por meio de backups.

# Capítulo 5

# ATRIBUIÇÕES DOS RESPONSÁVEIS

AS RESPONSABILIDADES

O administrador e o operador de backup da TECNOTECH SISTEMAS serão indicados pelo sócio diretor.
A responsabilidade de administrar os serviços de backup e restore será do administrador e o operador de backup ou por terceiros, que atuará como o gestor dessa área. O gestor será responsável pela criação, implementação e cumprimento das políticas e procedimentos relacionados aos serviços de backup e restore, incluindo a guarda das mídias móveis e o cumprimento das normas aplicáveis.

## 5.1 São atribuições do administrador de backup:

- Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela TECNOTECH SISTEMAS;
- Providenciar a criação e manutenção dos backups;
- Configurar as soluções de backup;
- Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
- Definir os procedimentos de restauração e neles auxiliar;

- **Verificar diariamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;**
- **Tomar medidas preventivas para evitar falhas;**
- **Reportar imediatamente ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;**
- **Gerenciar mensagens e registros de auditoria (LOGs) diários dos backups;**
- **Disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;**
- **Propor modificações visando ao aperfeiçoamento da Política de Backup e Recuperação de Dados Digitais, objeto desta Portaria;**
- **Providenciar a execução dos testes de restauração.**

## 5.2 São atribuições do operador de backup:

- **Restaurar ou recuperar os backups em caso de necessidade;**
- **Operar e manusear as unidades de armazenamento de backups;**
- **Informar ao administrador de backup qualquer problema que impossibilite a restauração de um backup;**
- **Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;**
- **Definir os procedimentos de restauração e neles auxiliar;**
- **Verificar diariamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;**

## 5.3 São atribuições das áreas técnicas:

- **Solicitar restaurações de dados, com anuência do gestor da informação;**
- **Sanar dúvidas técnicas do administrador de backup acerca das informações salvaguardadas;**
- **Validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;**
- **Validar, tecnicamente, o resultado dos testes de restauração dos backups;**

## 5.4 São atribuições do gestor da informação:

- **Solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;**
- **Validar, negocialmente, o resultado das restaurações eventualmente solicitadas;**
- **Validar, negocialmente, o resultado dos testes de restauração dos backups;**

**A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações. O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.**

# Capítulo 6

# AMPLITUDE DA POLÍTICA DE BACKUP DA TECNOTECH

**A política de backup engloba os seguintes itens do processo de backup.**

- **Tipos de backup**
- **Rotinas de backup gerais**
- **Backups especiais**
- **Tempo de retenção dos backups**
- **Tempo de Restauração**

# Capítulo 7

# SERVIÇOS DE BACKUP DA TECNOTECH

**O backup é essencial para atender às diversas áreas de negócio da tecnotech. Com o objetivo de melhorar a operacionalização do serviço, as rotinas de backup foram classificadas da seguinte forma:**

- **File Server**
- **Web**
- **Active Directory**
- **Disaster Recovery Linux**
- **Máquinas virtuais Linux**
- **Bancos de dados SQL Postgresql**

## 7.1 TIPOS DE BACKUPS

**Existem basicamente dois tipos de backup: Backup Full (Completo) e incremental. O backup Full tem a função de copiar todos os arquivos indicados, enquanto o backup Incremental cópia somente o que foi alterado desde o último backup Full.**

## 7.2 BACKUP DE SERVIDOR DE WEB

**Para os servidores web com uma retenção de um mês, serão realizados backups Full todo dia primeiro do mês, especificamente em qualquer dia da semana pois o backup ocorre de forma automática. Não haverá backup aos sábados e domingos, exceto em casos em que os responsáveis pelo ambiente solicitarem.**

## 7.3 BACKUP DE SERVIDOR DE DOCUMENTOS E PDFS

**Para o backup do servidor com documentos e PDFs possui a retenção de um mês, são realizados backups Full no primeiro dia do mês, combinados com backups Incrementais de segunda a domingo. Podendo haver backups aos sábados e domingos.**

## 7.4 BACKUP DE MAQUINAS VIRTUAIS

**Para o backup de máquinas virtuais com uma retenção de seis dias, o backup será executado diariamente por snapshot, a menos que haja uma solicitação específica do responsável pelo servidor. Os dados das máquinas virtuais serão arquivados normalmente, de acordo com a sua classificação (Infraestrutura, Banco de Dados, WEB, etc.. . . ).**

# Capítulo 8

# BACKUP DE BANCOS DE DADOS DE PRODUÇÃO

**Para os bancos de produção, os backups ocorrem diariamente de forma incremental iniciando as 22:00, podendo se estender ate a madrugada de forma automática pelo pgbackrest e snapshot na plataforma da Azure. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao sócio diretor através do e-mail: dev@tecnotech.org. A aprovação para execução da alteração depende da anuência do responsável pelos dados.**

# Capítulo 9

# BACKUP DE BANCOS DE DADOS DE DESENVOLVIMENTO

**Para os bancos de desenvolvimento, os backups full ocorrem todos os dias e são armazenados no Github.**

**Abaixo, segue a tabela com a frequência, período e retenção dos backups de desenvolvimento:**

**A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao sócio diretor através do e-mail: dev@tecnotech.org. A aprovação para execução da alteração depende da anuência do responsável pelos dados.**

# Capítulo 10

# REPLICAÇÃO DO BANCO DE DADOS

**Para garantir a segurança dos bancos de dados da TecnoTech, adotamos uma estratégia de replicação de dados que consiste em realizar um backup completo diario dos bancos de dados e replicados para um local externo, fora do local de origem. em caso de falhas ou problemas no local de armazenamento principal, os dados estarão protegidos e poderão ser recuperados com segurança. É importante ressaltar que esse processo de replicação de dados é essencial para minimizar os riscos de perda de informações críticas da empresa.**

# Capítulo 11

# SOLICITAÇÃO DE RESTAURAÇÃO

O atendimento de solicitações de restauração de arquivos, e demais componentes segue o seguinte fluxo:

- O usuário entra em contato com o Service Desk para relatar um incidente ou solicitar suporte.
- O Service Desk registra o incidente ou solicitação e tenta resolvê-lo por meio de soluções conhecidas, seguindo o catálogo de serviços.
- Se o incidente ou solicitação exigir a intervenção do administrador e o operador de backup, o Service Desk encaminha a requisição para a equipe responsável.
- O administrador e o operador de backup avaliam a requisição e, se necessário, executa as ações necessárias para resolver o incidente ou atender à solicitação.
- A O administrador e o operador de backup informa ao Service Desk o resultado da sua intervenção.
- O Service Desk, por sua vez, comunica o resultado final ao usuário e fecha o chamado no sistema de suporte.

**O tempo de recuperação de dados é diretamente proporcional ao volume de dados necessários para a restauração. Como referência, estima-se que para cada 20GB de dados, o tempo de recuperação seja de uma hora, considerando apenas o tempo de atendimento da Equipe de Operações e Produção.**

**É importante ressaltar que essa é apenas uma estimativa e o tempo real pode variar de acordo com a complexidade do ambiente, a velocidade do hardware utilizado, a qualidade dos backups e outros fatores. Além disso, é importante lembrar que o tempo de recuperação não contempla o tempo necessário para a comunicação entre o usuário e o Service Desk para reportar o incidente ou solicitação de restauração.**

# Capítulo 12

# TESTES DE BACKUP

Os backups serão verificados periodicamente:

Os backups devem ser testados periodicamente, mensalmente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.
Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha. Tanto o tipo de testes e ações são registrados no relatório de testes no modelo publicado nesse documento: Procedimentos Teste Continuidade do Backup.

A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da TECNOTECH SISTEMAS.

Os testes devem ser realizados em todos os backups produzidos independente do ambiente podendo ser aleatórios o gerais. Os testes de restauração dos backups devem ser realizados, por amostragem mensalmente, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis na TECNOTECH SISTEMAS.

**Os testes devem ser realizados em todos os backups produzidos independente do ambiente podendo ser aleatórios o gerais. Os testes de restauração dos backups devem ser realizados, por amostragem mensalmente, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis na TECNOTECH SISTEMAS.**

# Capítulo 13

# DISASTER RECOVERY

O nosso plano de disaster recovery para garantir a recuperação dos dados em caso de falhas ou desastres, contamos com uma máquina configurada para o backup dos bancos de dados que utiliza snapshots com retenção de 04 dias para os sistemas que estão em clouds. Além disso fazemos o backup da camada de aplicação na AWS para montar uma VM com o Apache e rotinas de backup para recuperação.

## 13.1 DIRETRIZES PARA RESTAURAÇÃO DE DADOS

As ferramentas e sistemas que são utilizados para fazer backup de dados, incluindo o PgBackRest para banco de dados e o DUPLICATI para arquivos gerados pelo sistema. Ambas as ferramentas utilizam criptografia para proteger os dados armazenados. O PgBackRest criptografa o repositório com base em uma senha fornecida pelo usuário, enquanto o DUPLICATI utiliza criptografia AES-256 forte para proteger a privacidade dos dados. Além disso, o DUPLICATI também pode utilizar o GPG para criptografar o backup. Para armazenar os backups, utilizamos os serviços do Amazon Web Services, Inc - Bucket S3. O repositório do backup pode ser configurado em um bucket S3.

# Capítulo 14

# CONCLUSÃO BEM-SUCEDIDA DO BACKUP

Após a conclusão bem-sucedida do backup, serão realizadas verificações e configurações, conforme descrito abaixo, para garantir a correta execução dos procedimentos.

- Verificar geração de boletos.
- Verificar limite de upload de documentos (PROTOCOLOS, CERTIÕES etc).
- Verificar rotinas no CRON (WEB e BD)(Rotinas, Views etc).
- Verificar regra de upload de arquivo no ambiente do profissional.
- verificar banco read-only.
- Verificar pasta de imagens das malas diretas.
- Verificação do GHOST Qware.
- Verificar os horários das Regiões (TIMEZONE).
- Verificar rotinas no CRON homologação .
- Verificar banco do dos correios.
- Monitoramento com zabbix.
- Monitoramento com wazuh prolinx.

- **Permissão de Gravação nos diretórios LOG e IMAGES.**
- **Permissão de Gravação nos diretórios do Serviços.**
- **Modificar conexão no CONFIG (Adapt e Serviços).**
- **Geração dos Arquivos de integração com o SISCONT.**
- **Configurar backup no duplicati.**
- **Ajustar url interna de impressao.**
- **Envio de ARTs CONFEA.**
- **Configurar o envio de e-mail e firewall.**
- **Desativar QWARE no servidor antigo.**
- **Liberação do IP no CONFEA.**
- **Liberação SERPRO Carteira PRO-ID.**

# Capítulo 15

# TRANSPORTE E ARMAZENAMENTO DOS BACKUPS

As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

- A importância dos dados que estão sendo salvaguardados;
- Por quanto tempo os dados precisam ser mantidos;
- A probabilidade de precisar restaurar os dados;
- Quanto tempo levará para restaurar os dados;
- O custo da unidade de armazenamento de backup;
- Por quanto tempo os dados precisam ser mantidos;
- A vida útil da unidade de armazenamento de backup;

**É responsabilidade do administrador de backup avaliar diferentes tecnologias disponíveis para realizar as cópias de segurança e propor a melhor solução para cada caso específico. Técnicas de compressão de dados podem ser usadas, desde que os gestores de informações considerem aceitável o aumento do tempo de restauração dos dados. As rotinas de backup devem prever a ampliação da capacidade dos dispositivos de armazenamento envolvidos.**

**As unidades de armazenamento utilizadas nos backups devem ser mantidas em locais apropriados, com controle de fatores ambientais como umidade, temperatura, poeira e pressão, além de serem acessíveis apenas por pessoas autorizadas pelo administrador de backup. Além disso, as condições ambientais devem estar de acordo com as especificações do fabricante das unidades de armazenamento.**

**Quando for necessário descartar unidades de armazenamento utilizadas em backups, elas devem ser fisicamente destruídas para evitar o uso indevido de informações e o descarte deve ser feito de forma sustentável e ambientalmente correta.**

**Todos os backups serão armazenados na nuvem da AWS, utilizando Bukect s3 dependerá das especificações escolhidas e das configurações, que podem ser adaptadas conforme a necessidade. Os dados serão armazenados na nuvem da AWS. A mídia utilizada para os backups será identificada de forma clara e armazenada em uma área segura de acesso restrito, somente para pessoas autorizadas ou para o fornecedor de armazenamento externo contratado pela TECNOTECH SISTEMAS.**

**Durante o transporte, a mídia armazenando os backups da AWS não será deixada sem supervisão em nenhuma circunstância. Será garantido que a mídia seja transportada com segurança e cuidado, sob a supervisão direta de uma pessoa autorizada pela TECNOTECH SISTEMAS.**

**Os backups completos diários serão mantidos por um período de 4 dias e armazenados no local em um cofre à prova de água ou fogo fisicamente protegido, localizado em uma sala separada do data center. No entanto, quando o backup é armazenado na nuvem AWS, o período de retenção pode ser configurado conforme a necessidade da organização, utilizando os recursos de armazenamento seguro oferecidos pela plataforma.**

**Serão mantidos backups completos mensal por um período de 1 mês, e enviados a um local de armazenamento de mídia virtual protegido, de acordo com as políticas de segurança da nuvem AWS. Após 1 mês, os dados serão deletados seguindo as melhores práticas de segurança de dados.**

**A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados, A TI garantirá a destruição física da mídia antes do descarte.**

## 15.1 DESCARTE DOS BACKUPS

**A mídia de backup será retirada e descartada conforme descrito neste documento:**

**A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.A TI garantirá a destruição física da mídia antes do descarte. A Equipe de Proteção de Dados é responsável pela destruição de dados, conforme o calendário de retenção.Os dados devem ser excluídos, triturados ou destruídos, dependendo do formato e do nível de confidencialidade, de acordo com os controles apropriados para evitar a perda permanente de informações importantes. Os Dados que contêm informações sensíveis e confidenciais devem ser destruídos como lixo confidencial, sujeitos à eliminação eletrônica segura. O processo de destruição deve ser totalmente documentado e aprovado pela Equipe de Proteção de Dados.**

# Capítulo 16

# MUDANÇAS NA POLÍTICA DE USO DA INTERNET CORPORATIVA

**A presente versão 1.0 desta Política de uso da internet corporativa foi atualizada pela última vez em: 03/05/2023. O editor se reserva o direito de modificar, a qualquer momento as presentes normas, especialmente para adaptá-las às evoluções, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Esta Política de correio eletrônico poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual se convida o usuário a consultar periodicamente esta seção.**

# Capítulo 17

# CONTROLE DE VERSÕES

Tabela 17.1: Tabela de versões

| Versão | Descrição | Responsável | Publicação |
|---|---|---|---|
| 1.0 | Versão para divulgação | Wanderson câmara - Felipe Andrade | 07/03/2023 |
| | | | |
| | | | |
| | | | |

# Capítulo 18

# CONCORDÂNCIA

**Eu li e entendi a Política de Backup e Restauração de dados digitais da TECNOTECH SISTEMAS. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da TECNOTECH SISTEMAS.**

---

**Assinatura do funcionário Data**