POLÍTICA DE

BACKUP E RESTAURAÇÃO (T.I.)

POLI-0006-01

MANTENHA APENAS UM: CONFIDENCIAL | **RESTRITO** | USO INTERNO | PÚBLICO

Obs. Este documento contou com a contribuição da Innocenti Advogados (consultora externa)

Controle de Versões

Data	Versão	Comentários	Autor
01.06.2022	1.0	Versão Inicial	Mariana M. Carregaro
13.01.2024	2.0	Revisão	Mariana M. Carregaro
13.01.2025	3.0	Revisão	Mariana M. Carregaro

Identificação e Classificação

Código do Documento	Tipo	Classificação
POLI-0006-01	Política	Restrito

Equipe e Responsáveis Envolvidos

Profissionais Envolvidos
Mariana M. Carregaro – Consultora Externa (Innocenti Advogados)
Lidiane P. dos Reis Barros – Encarregada

Documentos de Apoio ou Relacionados

Documentos de Apoio
Política de Segurança da Informação (T.I.)
Política de Incidente de Segurança (T.I.)
Política de Gestão de Continuidade do Negócio (T.I.)
Política de Gestão de Risco (T.I.)
Política de Notificação de Violação (T.I.)
Evidência e Controle das Vulnerabilidades Cibernéticas

Aprovação da Diretoria Responsável

Diretor Responsável	Ratificação	Data
Alexandre Gonçalves Duarte	APROVADO	13.01.2025

Introdução

A política de backup de dados fornece uma documentação abrangente das regulamentações aplicáveis na **Epeople** e medidas tomadas de backup de dados. Também serve como evidência para terceiros de que o controle de disponibilidade exigido legalmente é executado de forma adequada.

É dever da **Epeople** fornecer segurança de tecnologia e proteção de dados em seu ambiente. Inclusive, a administração corporativa é diretamente responsável por isso, inclusive de maneira pessoal em determinados casos.

Responsabilidades e Atribuições

O departamento de Tecnologia da Informação será o Administrador de Backup, ficando responsável pela política e procedimentos relativos aos serviços de backup e restauração dos dados, bem como de guardar as mídias móveis e assegurar o cumprimento das normas aplicáveis.

São atribuições do Administrador de Backup:

- propor modificações visando o aperfeiçoamento da política de backup;
- criar e manter as tarefas de backup;
- configurar a ferramenta de backup;
- criar e manter mídias;
- testar o backup e a restauração;
- criar notificações e relatórios;
- verificar periodicamente os relatórios gerados pela ferramenta de backup;
- restaurar os backups em caso de necessidade;
- gerenciar mensagens e logs diários dos backups, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequência e os erros na sua execução sejam eliminados;

- fazer manutenções periódicas dos dispositivos de backup;
- fazer o carregamento das mídias necessárias para os backups programados;
- comunicar ao Administrador do Recurso os erros e ocorrências nos backups; e
- fazer o armazenamento das mídias de backup em cofre apropriado.

Escopo do Backup e sua Formalização

Todo e qualquer ativo de TI que armazene dados deverá ser considerado para avaliação de inclusão no processo de backup. O responsável por cada recurso deverá definir quais diretórios e arquivos serão incluídos no backup, tendo como prioridade:

- arquivos de configurações de sistemas operacionais e aplicativos instalados em servidores;
- arquivos de log dos aplicativos, inclusive log da ferramenta de backup e restauração;
- informações e configurações de banco de dados;
- conteúdo de repositórios de dados associados a sistemas;
- arquivos institucionais de usuários (documentos e e-mails);
- arquivos de aplicações desenvolvidas pela **Epeople** ou quaisquer outros não descritos neste documento, mas que a perda de suas informações gere prejuízo a **Epeople**.

O Administrador de Backup ou o Administrador de Recurso que pleiteia a inclusão de uma informação deverá definir quais diretórios e arquivos que não serão incluídos na rotina, tendo como referência:

- arquivos do sistema operacional ou de aplicações que podem ser recolocados através de uma nova instalação; e
- arquivos temporários.

Para os aplicativos e/ou bancos de dados devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante.

Os procedimentos de backup deverão ser atualizados quando houver:

- novas aplicações desenvolvidas;
- novos locais de armazenamento de dados ou arquivos;
- novas instalações de bancos de dados;
- novos aplicativos instalados;
- outras informações que necessitem de proteção através de backups deverão ser informadas ao Administrador de Backup, pelo Administrador de Recurso.

Prazo de Retenção

A retenção dos backups deve observar os seguintes prazos:

- diário: dez últimos dias;
- semanal: seis últimas semanas;
- mensal: sessenta últimos meses;
- semestral: permanente;

Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização e número de leitura/gravação. A mídia não deverá ultrapassar 30 anos de armazenamento, devendo, nesse caso, ser copiada para outra mídia, destruída de forma segura e descartada em lugar destinado para tal, obedecendo as leis ambientais.

Sempre que necessário deverá ser realizada a atualização das mídias de backup com a finalidade de preservar o acesso aos dados nelas contidas

Procedimento de Restauração

Os backups deverão ser testados diariamente quanto à integridade e recuperabilidade dos objetos, de maneira amostral. Caso seja detectada falha no backup ou se este estiver incompleto, novo

backup deverá ser executado com vistas ao seu armazenamento. Para todos os testes realizados deverá ser gerado um relatório.

Descarte das Mídias

O descarte das mídias de backup imprestáveis ou inutilizáveis deverá ser feito pelo Departamento de Segurança da Informação mediante solicitação do Administrador de Backup.

As mídias de backup a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido aos dados por pessoas não autorizadas conforme preconiza a Política de Segurança da Informação.

Condições Legais

A legislação exige certos controles por meio de medidas técnicas e organizacionais, tanto com o tratamento de dados para propósitos próprios quanto com o tratamento de dados autorizados; neste contexto, um controle de disponibilidade se aplica em particular.

A verificação dos controles ou medidas técnicas e organizacionais é, entre outras coisas, para ser fornecida aos titulares dentro do escopo do tratamento de dados autorizados.

Riscos

- Erro humano: operação incorreta, acidente, sabotagem, ataque.
- Interrupções técnicas: avaria técnica, falha de hardware etc.
- Força maior, acidentes, catástrofes, água, foro etc.
- Ameaças significativas feitas à **Epeople**.

Tipos de Backup

- ✓ **Backup Completo**: O backup completo ou full, pode ser considerado a base para todos os outros tipos de backups (backup incremental e diferencial). Ele consiste em uma cópia completa dos dados, arquivos e volumes para o armazenamento de destino. Nesse modelo, todas as vezes em que um backup é necessário, o backup anterior a ele é descartado ou mantido, e o novo é feito, ou seja, todos os arquivos e dados são copiados a cada backup.

- ✓ **Backup Incremental**: O backup incremental surgiu justamente para sanar a necessidade do backup completo de copiar todos os dados e arquivos a cada nova execução. Nesse modelo, só é necessária uma cópia completa de todos os arquivos uma única vez, pois todos os outros backups só carregam os dados alterados desde o último carregamento.

- ✓ **Backup Diferencial**: No backup diferencial, assim como no incremental, é executado primeiro um backup completo com a cópia de todos os dados, e depois outras execuções subsequentes. A diferença aqui é que enquanto no backup incremental cada execução copia apenas os dados que foram alterados desde o último backup, independentemente do tipo, no diferencial é feito uma cópia de todos os arquivos alterados desde o **BACKUP COMPLETO.**

Regulamentos Gerais

- O backup de dados deve ser executado de forma responsável e competente;
- Nenhum desvio acidental de modelo de autorização de backup de dados;
- Confidencialidade e obrigação de proteção de dados;
- O TI é responsável pela administração; e
- Determinar a necessidade de confidencialidade, integridade e disponibilidade por parte da **Epeople**.

Implementações Técnicas

- Criar um plano de backup;
- Determinar o período de retenção e o número de gerações;
- Coordenação com a Política de Gestão de Continuidade do Negócio (TI);
- Documentação de login suficientes: especialmente dados de backup, escopo de backup, parâmetros de backup;
- Organize o procedimento de recuperação;
- Criar diretório de inventário;
- Garantir a avaliação de logs;
- Testes de reconstrução de dados / restauração de dados e exercícios de emergência;
- Configurar os controles necessários, especialmente o controle de acesso.
- Implementar os requisitos de proteção para a confidencialidade, integridade e respeito à lei;
- Especifique e proteja as rotas de transporte;
- Alocar capacidades: taxa de transferência, volume, quantidade de dispositivos de armazenamento de dados;
- Implementar requisitos para backup contínuo (notebooks, PDA/ MDA, banco de dados, arquivos abertos, dados do sistema, dados de log etc.);
- Assegurar, especialmente, o controle de acesso, controle de permissão de acesso, controle de entrada, controle de separação, também no que diz respeito à conjunto de backup de dados.