Deméter – Política de Backup

Versão 1.0

Brasília, dezembro de 2022

**Controle de versões**

|  |  |  |  |
| --- | --- | --- | --- |
| Data | Vers**ão** | Descriç**ão** | Autor |
| 15/12/2022 | 1.0 | Feitio do documento | Carlos Coelho |

1. Introdução

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

2. Escopo

* Esta política se aplica a TODOS os dados contidos banco de dados relacional MySQL de Deméter.
* **NÃO** serão salvaguardados nem recuperados dados armazenados localmente nos computadores.

3. Termos e Definições

Referência *→ PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA.*

Recovery Point Objective (RPO): Ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

Recovery Time Objective (RTO): Tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

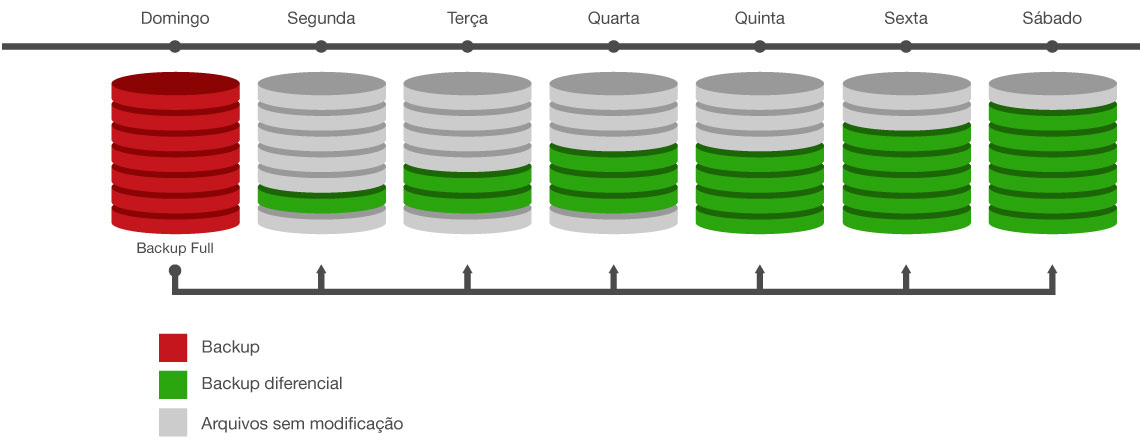
4. Declarações da política

4.1. Dos princípios gerais

1. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
2. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
3. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
4. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
5. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
6. Visando a maior proteção do sistema, convém que cópias de segurança sejam protegidas através de encriptação.

4.2 Do tipo de backup

1. Visando o bom e rápido funcionamento do software, fica definido como método de backup: backup diferencial. Funcionamento → Após a realização do primeiro backup completo, cada backup diferencial compara o conteúdo a ser copiado com o último backup full e copia todas as alterações realizadas.



4.3. Da frequência e retenção de dados

1. Os serviços de TI críticos (tabelas que contenham dados de cliente, produtos e pedidos) do software devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir: diária / 5 dias.
2. A solicitação de salvaguarda dos dados deve ser realizada de maneira automatizada, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I – Escopo (dados digitais a serem salvaguardados);

II – Tipo de *backup* (completo, incremental, diferencial);

III – Frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV – Retenção;

V – RPO;

VI – RTO.

4.4. Do uso da rede

1. Deve se considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados conectada, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços que utilizam a rede.
2. A execução do backup deve ser feito preferencialmente no momento em que há menos trafego na rede de dados, visando a plena execução e o baixo impacto nos horários de utilização do sistema.

4.5. Do armazenamento

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

I – A criticidade do dado salvaguardado;

II – O tempo de retenção do dado;

III – A probabilidade de necessidade de restauração;

IV – O tempo esperado para restauração;

V – O custo de aquisição da unidade de armazenamento de backup;

VI – A vida útil da unidade de armazenamento de backup.

1. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 15 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
2. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.
3. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

4.6. Do procedimento de restauração de backup

1. O cronograma de restauração de dados:

* Backups externos serão disponibilizados em aproximadamente 12 horas de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;
* Backups externos serão disponibilizados em aproximadamente 24 horas de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.