Formas e Tipos de Backup

Sobre Formas e Tipos de Backup

Uma das grandes definições a serem tomadas com relação ao backup é a quantidade de cópias a serem mantidas.

Os Órgãos Setoriais possuem autonomia para buscar a forma que melhor atende às suas necessidades. Como ponto de partida, pode-se citar a Regra 3-2-1, que preconiza a geração de pelo menos 3 (três) cópias dos dados (uma primária e dois backups), que devem ser armazenadas em pelo menos 2 (duas) mídias diferentes, sendo que 1 (uma) das cópias deve ser off site ou ao menos offline.[1]

Outra definição que deve ser tomada é o tipo de backup e a periodicidade com que ela deve ser feita.

> 1: Outras formas de backup utilizados que podem ser citadas são: Backup to Disk, then data moved to tape (D2D2T), Backup to
> Disk (D2D), Backup to Disk, then data moved to lower tier of disk (D2D2D), Backup to tape (D2T), Backup to disk, then data moved to cloud (D2D2C) e Backup to cloud (D2C).

Existem quatro tipos de backup, elencados na tabela a seguir.

Tabela: Comparativo dos diferentes tipos de backup.[2]

TIPO	DESCRIÇÃO	VANTAGENS	DESVANTAGENS
Completo	Copia todos os dados; Serve como referencial para os demais tipos.	Mais básico e completo; Cópia de todos os dados em um único conjunto de mídia; Recuperação simples.	Mais demorado; Ocupa mais espaço.
Incremental	Copia apenas os dados alterados ou criados após o último completo ou incremental.	Menor volume de dados; Mais rápido; Ocupa menos espaço de armazenamento.	Recuperação mais complexa (primeiro um completo e depois todos os incrementais).
Diferencial	Copia os dados alterados ou criados desde o último backup completo.	Recuperação mais rápida que o incremental (precisa só do último completo enquanto o incremental precisa do completo e dos incrementais).	Ocupa mais espaço que o incremental e menos que o completo; gasta mais tempo que o incremental e menos que o completo.

TIPO	DESCRIÇÃO	VANTAGENS	DESVANTAGENS
Progressivo	Similar ao incremental mas com maior disponibilidade dos dados.	Recuperação automatizada e mais eficiente (não precisa descobrir os conjuntos a serem recuperados).	Recuperação mais lenta que o diferencial e o completo (precisa analisar diferentes conjuntos para terminar o processo).

> 2: Retirado de: Backup - o básico cada vez mais essencial, CERT.br.

Já a periodicidade se refere à frequência de geração ou atualização de backups e deve ser estabelecida com base no apetite ao risco da perda de dados, considerando-se que, quanto maior a frequência das cópias, menor será a perda de dados, mas maiores serão os gastos e mais complexa poderá ser a recuperação.

Além de backups periódicos, o Órgão Setorial poderá realizar backups extemporâneos, sempre que entender que há algum risco iminente, que pode incluir eventos como, por exemplo:

- Mau funcionamento;
- Mensagens de logs e consoles de monitoramento sobre falhas;
- Alteração/atualização de sistemas;
- Envio a serviços de manutenção;
- Incidentes de segurança da informação.

A política pode também estabelecer metas de RPO (Recovery Point Objective) e RTO (Recovery Time Objective), conforme as necessidades de negócio.

Para fins desta Orientação Técnica, define-se o RPO como o intervalo de tempo aceitável entre o momento do último backup do dado e o momento da falha .

Por outro lado, o RTO é o intervalo de tempo necessário para a restauração de um processo sem comprometer a continuidade de negócio . Tanto o RPO quanto o RTO podem ser incorporados dentro de níveis de serviço.

Outra questão relevante é a segurança do backup. Além das questões físicas de integridade das mídias, deve-se considerar a segurança lógica dos dados, especialmente em termos de confidencialidade e integridade.

Em termos de procedimentos operacionais de geração de backup, o Órgão Setorial poderá fazer de forma manual ou automatizada, conforme as necessidades e realidades do Órgão, podendo inclusive utilizar ferramentas, seja de mercado ou desenvolvidas, para essa finalidade.

Recomendações

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Criptografar backups de dados potencialmente sensíveis ou não classificados como público conforme a legislação vigente
  relativa ao acesso à informação.
  - Utilizar algoritmos considerados matematicamente seguros para a criptografia, evitando o uso de algoritmos considerados como fragilizados ou quebrados matematicamente
- Quando tecnicamente viável, realizar backup dos dados corporativos gerados, mantidos ou geridos pelo usuário quando houver razoável certeza de que ele será removido, cedido, exonerado ou demitido, visando mitigar o risco da perda de dados relevantes.
- Definir uma lista de riscos iminentes, que ensejam a realização de um backup extemporâneo dos dados.
- Realizar backup dos dados relevantes quando forem identificados um ou mais riscos iminentes para os dados.
- Realizar periodicamente um backup completo dos dados e backups de outros tipos entre dois backups completos, visando mitigar o risco da perda de dados.
- Para os backups periódicos, utilizar ferramentas que automatizem o processo, parcial ou totalmente, para reduzir a ocorrência de erros manuais e ganhar maior aderência à (?)

Sugestões

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Realizar um backup completo no mínimo uma vez por mês, se possível uma vez por semana, e os outros tipos de backup no mínimo uma vez por semana, se possível uma vez por dia.
- Gerar e armazenar as informações relativas à integridade dos dados de backup (checksum ou hash), realizando-se a sua conferência quando da sua recuperação.
- Definir RPO e RTO para dados de maior criticidade.
- Definir RPO e RTO dentro de acordo de níveis de serviço (SLA – Service Level Agreement) em caso de contratação de um prestador de serviços de backup.