Considerações gerais sobre Backup

Sobre Considerações gerais sobre Backup

O backup, ou a cópia de segurança dos dados, deve ser considerado como a última linha de defesa de proteção dos dados. Desta forma, o backup não prescinde das demais medidas relativas à segurança da informação, sejam elas boas práticas de mercado ou dispostas em outras Orientações Técnicas. Tais medidas incluem aspectos como conscientização de usuários, atualização de sistema operacional e uso de antivírus, entre muitas outras possibilidades.

Além do viés de segurança, o backup também pode ser utilizado para recuperação de versões anteriores de arquivos e dados, bem como o arquivamento de dados raramente alterados e pouco acessados.

O Órgão Setorial é responsável pela gestão dos seus backups, bem como da sua política de backups.

O backup deve ser planejado para que seja coerente com as necessidades do Órgão Setorial, visando ter adequada segurança dos dados e alinhamento aos objetivos e realidades do Órgão. Caso contrário, corre-se o risco de ter gastos e esforços operacionais desnecessários.

Existem quatro perguntas fundamentais para o backup:

1. **O que copiar?**
2. **Onde copiar?**
3. **Quando copiar?**
4. **Como copiar?**

As respostas para essas perguntas moldarão a política de backup do Órgão Setorial. As seções subsequentes explorarão alguns aspectos a serem considerados sobre as questões acima.

Recomendações

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Definir, documentar e divulgar a política de backup para o Órgão Setorial, estabelecendo procedimentos alinhados com as suas necessidades e objetivos.
- Explicitar na política de backup as respostas para as quatro questões fundamentais de backup: o que, onde, quando e como.
- A política de backup deve explicitar as datas de frequência para a realização de backups e para a execução de testes de restauração.
- Considerar as disponibilidades técnicas, físicas, orçamentárias e de pessoal para a elaboração e atualização da política de backup.
- Realizar uma ou mais cópias de segurança para os seguintes dados, no mínimo:
  - Imagem do sistema: incluindo o sistema operacional, os programas padrão instalados, configurações e arquivos padrão dos usuários.
  - Dados realmente importantes: A análise da importância dos dados deve ser feita no contexto das atividades de negócio do Órgão Setorial, visto que o mesmo dado pode ter importâncias diferentes para Órgãos diferentes, e suas conclusões devem estar refletidas na política de backup. Esta classificação deve determinar as metas específicas de RPO (Recovery Point Objective) e RTO (Recovery Time Objective).
- Definir RPO e RTO para, no mínimo, dados de maior criticidade.
- Realizar o backup com foco nos dados ou arquivos corporativos e não nos arquivos pessoais dos usuários.
  - Dados ou arquivos corporativos são aqueles utilizados, ou que impactam, nas atividades do Órgão Setorial: Para esta classificação, o Órgão Setorial deverá adotar a supremacia da essência sobre a forma. Desta forma, arquivos alegados como pessoais devem ser considerados como corporativos, se eles impactarem nas atividades do Órgão Setorial.
- Não realizar o backup de arquivos que possam conter códigos maliciosos nem de arquivos que possam ter sido modificados/substituídos por agentes externos não autorizados.
- Garantir que todos os procedimentos técnicos de restauração sejam formalizados e padronizados, possuam documentação atualizada e estejam disponíveis e acessíveis a todos os servidores de TIC envolvidos nas operações de recuperação.
  - Executar a revisão periódica dos procedimentos técnicos de restauração e sua respectiva documentação.
- Os prazos de retenção de backups devem estar alinhados às tabelas de temporalidade de dados em vigor no Município e às obrigações legais, em especial as impostas pela LAI (Lei nº 12.527/2011) e LGPD (Lei nº 13.709/2018).
- O órgão deve estabelecer um processo sistematizado, formalizado e documentado para o ciclo completo de manejo, posse, categorização, retenção e descarte de dados, incluindo os sensíveis.

- No caso de backup em nuvem (cloud), o Órgão Setorial deve consultar a OT 009 - Aquisições de Serviços de Computação em Núvem, além de seguir as diretrizes desta Orientação Técnica.

Sugestões

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Investir na capacitação dos servidores de TIC do Órgão Setorial para aprimorar e atualizar os seus conhecimentos sobre as diversas possibilidades e tecnologias de backup.
- Evitar o backup de arquivos binários (executáveis e bibliotecas), pois podem conter *arquivos maliciosos*[1] ou corrompidos, que acabarão sendo recuperados em caso de restauração de backup.
- Criar uma ou mais listas de arquivos que não serão objeto de backup.
- Fazer o backup apenas dos dados confiáveis.

> 1: Os *arquivos maliciosos* podem ser tanto danosos (vírus, cavalos de Troia, ransomware e demais tipos de malware) quanto programas potencialmente indesejados (adware, etc.).