OT 007 - Backup e Armazenamento de Dados

Faz considerações a definições gerais sobre cópia de segurança de dados e pretende estimular a implantação de políticas de Backup nos Órgãos Setoriais. Para tanto, o texto traz recomendações e sugestões a respeito de locais de armazenamento, formas e tipos de Backup, testes, retenção e restauração da cópia de segurança e define diretrizes de Backup para Data Centers próprios. Vale ressaltar que não é objetivo deste documento o uso de armazenamento de dados em mídias físicas que não se relacionem diretamente com a Tecnologia da Informação e Comunicação como papel, microfilme e tab-jacks por exemplo.

- Introdução
- Definições Importantes
- Considerações gerais sobre Backup
    - Sobre Considerações gerais sobre Backup
    - Recomendações
    - Sugestões
- Locais de Armazenamento e Backup
    - Sobre Locais de Armazenamento e Backup
    - Recomendações
    - Sugestões
- Formas e Tipos de Backup
    - Sobre Formas e Tipos de Backup
    - Recomendações
    - Sugestões
- Testes, Retenção e Restauração de Backup

    - Sobre Testes, Retenção e Restauração de Backup
    - Recomendações

- Diretrizes de Backup para Data Centers Próprios
    - Sobre Diretrizes de Backup para Data Centers Próprios
    - Recomendações
    - Sugestões

- Armazenamento de Dados
    - Sobre Armazenamento de Dados
    - Recomendações
    - Sugestões

- Referências

Introdução

O presente documento estabelece diversas diretrizes técnicas, gerais e específicas, para os Órgãos Setoriais da Prefeitura do Município de São Paulo. É parte integrante das Orientações Técnicas (OT) que foram estabelecidas como instrumento de Governança de Tecnologia da Informação e Comunicação – TIC no Decreto Municipal 57.653, de 07 de abril de 2017, que define a Política Municipal de Tecnologia da Informação e Comunicação.

O objetivo desta OT é padronizar procedimentos e processos de tomada de decisão, bem como disseminar conhecimentos e estimular boas práticas para que os Órgãos Setoriais possam conduzir suas iniciativas de forma embasada e de acordo com o seu grau de maturidade.

Fazem parte do escopo desse documento as diretrizes no que tange à padronização, boas práticas de uso, operação e segurança para a conexão física e lógica, com o objetivo de possibilitar o tráfego controlado de dados entre as redes envolvidas em um nível adequado de riscos.

Sendo a Tecnologia da Informação e Comunicação temática dinâmica e de soluções em constante evolução e transformação, essa Orientação Técnica poderá ser objeto de revisões posteriores, visando estar atualizada de acordo com os conhecimentos mais atuais e alinhada ao contexto da Prefeitura Municipal de São Paulo.

Definições Importantes

Uma **recomendação** é uma diretriz definida pelo Conselho Municipal de Tecnologia da Informação e Comunicação – CMTIC, e estabelece regras, procedimentos ou critérios a serem seguidos por padrão. Desta forma, a sua não adoção deverá ser justificada tecnicamente.

Uma **sugestão** é uma boa prática validada pelo CMTIC e possui um caráter não vinculante, mostrando alternativas ou conhecimentos que poderão ser úteis na busca de soluções.

Os procedimentos descritos nas Orientações Técnicas deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos e acordos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

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.).

Locais de Armazenamento e Backup

Sobre Locais de Armazenamento e Backup

Os backups podem ser armazenados tanto offline quanto online.

Backups offline incluem mídias como pendrive, CD, DVD, Blu-Ray, disco (interno ou externo), cartão de memória (SD, miniSD, microSD, SDHC etc.), fita, etc. Além disso, podem ser feitos no próprio local (on site) ou remotamente (off site).

Backups online incluem ambientes como discos de rede (tanto NAS quanto SAN), datacenter e nuvem (privada ou pública).

Em particular, é necessário atentar para a diferença entre o armazenamento na nuvem e o backup na nuvem. O armazenamento na nuvem pode ser usado para fins de backup, mas não necessariamente realiza backup dos arquivos armazenados .

Para mídias offline, é essencial considerar o tempo de vida útil. Mídias que excederem esse tempo podem continuar funcionais, mas a chance de sofrerem com a degradação passa a ser relevante.

No âmbito desta Orientação Técnica, o tempo estimado de vida útil das mídias offline pode ser consultado na tabela a seguir, considerando-se seu armazenamento e manuseio em condições adequadas. Mídias não contempladas na tabela podem ser consideradas como tendo vida útil indeterminada.

Além disso, os Órgãos Setoriais estão desobrigados de realizar a recuperação de dados armazenados em mídias obsoletas, exceto para dados críticos ao negócio, assim identificados pelo responsável pela área de TIC do Órgão Setorial.

Tabela: Tempo estimado de vida útil das mídias offline[2].

TIPO DE MÍDIA	TEMPO ESTIMADO DE VIDA ÚTIL OFFLINE
Cartões perfurados	Obsoleto, não se recomendando seu uso
Disquetes (5¼, 3½, Zip disk etc.)	Obsoleto, não se recomendando seu uso
LDs e MDs	Obsoleto, não se recomendando seu uso
CDs e DVDs	2 (dois) anos

TIPO DE MÍDIA	TEMPO ESTIMADO DE VIDA ÚTIL OFFLINE
Disco rígido (HD) magnético[1]	4 (quatro) anos
Blu-Ray	5 (cinco) anos
Memória flash (pendrives, cartões de memória etc.)	5 (cinco) anos
Disco rígido (HD) de estado sólido (SSD)	5 (cinco) anos
NAS (Network Attached Storage)	5 (cinco) anos ou a garantia do fabricante, o que for maior
SAN (Storage Area Network) baseado em HD	5 (cinco) anos ou a garantia do fabricante, o que for maior
Fitas/Cartuchos magnéticos	10 (dez) anos
M-Disc	20 (vinte) anos

> 1: Entende-se neste caso como o HD doméstico, seja externo ou interno.
> 2: Adaptado de The 6 Best Impact Drivers in 2025 - Impact Driver Reviews e http://www.popularmechanics.com/technology/gadgets/how-to/g1007/how-longwill-your-discsand-drives-last/.

Para backup offline, a armazenagem das midias físicas também é um aspecto importante a ser considerado, de forma a mitigar eventuais danos por condições ambientais e/ou manuseio humano inadequado.

Ainda, é relevante considerar a questão de escolher entre adotar um backup on site ou off site, incluindo o caso de backup na nuvem. A tabela a seguir mostra o cenário de uso mais apropriado para cada abordagem.

Tabela: Cenários mais apropriados de uso para diferentes locais de backup.

LOCAL DO BACKUP	CENÁRIO APROPRIADO
On site	Recuperação rápida de dados, especialmente se for para pedidos de baixo volume de dados ou para locais de baixa velocidade de conexão (largura de banda de rede).
Off site	Maior necessidade de reduzir o risco de perda de dados em caso de problemas nas instalações físicas do site (local) principal.

LOCAL DO BACKUP	CENÁRIO APROPRIADO
Off site: Nuvem	Mesmo cenário para o caso off site, mas para casos em que há conexão adequada com a internet e não há disponibilidade / viabilidade de ter um site físico para backup.

Para o caso de backup na nuvem, devem-se considerar, no mínimo, os seguintes fatores para a sua contratação:

1. Sistemas suportados pelo fornecedor;
2. Processos disponíveis de backup e restauração e suas interfaces de usuário;
3. Possibilidade de automatização de processos de backup e restauração;
4. Espaço de armazenagem;
5. Restrições de arquivos em termos de tamanho e tipo;
6. Período de retenção de dados;
7. Políticas de privacidade e segurança dos dados;
8. Níveis de suporte oferecidos;
9. Condições relativas à transferência de dados quando do encerramento do contrato

Recomendações

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Escolher os locais de armazenamento de backup, bem como os tipos de mídia, considerando-se o cenário, a criticidade dos dados e as instalações físicas disponíveis.
- Não utilizar mídias obsoletas, por causa da dificuldade de se adquirir leitores e/ou recuperar as informações gravadas nelas.
- Utilizar mídias que estiverem dentro da sua vida útil.
- Quando a mídia original estiver se aproximando do fim da sua vida útil, realizar a cópia integral do backup para uma nova mídia, após sua validação com relação à integridade dos dados.
- Identificar as mídias de armazenamento offline de forma que facilitem a recuperação do dado desejado.
- Armazenar as mídias em local com acesso controlado e acondicioná-las de modo a mitigar a ação de agentes nocivos naturais, notadamente poeira, luz, calor e umidade.
- Para armazenamento off site, avaliar a adequação do link de rede às necessidades de backup e recuperação de dados.
- Para armazenamento off site na nuvem, considerar os diferentes fatores para sua contratação (conforme acima) e implantar uma política de segurança para gestão de usuários e senhas com acesso ao backup na nuvem.
- Avaliar a necessidade de anonimização ou pseudonimização dos dados sensíveis contidos nos armazenamentos sempre que a finalidade da cópia não exigir a identificação do titular, visando a conformidade com a LGPD.
- Para armazenamento e backup off site na nuvem, garantir com o provedor de serviço de armazenamento que o servidor destino do backup esteja localizado em país que possua uma Lei de proteção de dados pessoais no mínimo equivalente à 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- O armazenamento e os backups de dados sensíveis devem ter a criptografia tornada obrigatória (utilizando algoritmos matematicamente seguros).
- Adotar políticas de descarte de mídias para mitigar o risco de exposição indesejada de dados.
- Para provedores externos, deve-se exigir evidências de que o contratado realiza testes de recuperação periodicamente e fornece a documentação completa de backup e recuperação para fins de auditoria.

Sugestões

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Etiquetar e nomear as mídias offline com informações que facilitem a sua localização, constando, por exemplo, um identificador único, o tipo do dado armazenado e a data de gravação.
- Utilizar uma base de dados ou um sistema para realizar a gestão das mídias offline.
- Para o descarte de mídias, avaliar medidas como destruição lógica dos dados (ex: formatação em baixo nível) ou até mesmo a destruição física da mídia (ex: fragmentação física do BluRay).
- Para backup na nuvem, avaliar a adoção de autenticação de dois fatores.

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.

Testes, Retenção e Restauração de Backup

Sobre Testes, Retenção e Restauração de Backup

Para que o backup atenda às suas finalidades, é necessário considerar um procedimento de teste e verificação da sua integridade e legibilidade. Caso contrário, corre-se o risco de encontrar problemas como dados corrompidos e mídias ou formatos obsoletos. Esses procedimentos devem ser feitos periodicamente para detectar preventivamente potenciais fontes de risco e não apenas para fins de auditoria.

Um outro fator a ser considerado no backup é a retenção de dados, ou seja, por quanto tempo eles devem ser armazenados. Deve-se considerar as tabelas de temporalidade de dados em vigor, bem como outras obrigações legais (compliance), a disponibilidade de espaço de armazenamento, seja físico ou lógico, e a disponibilidade orçamentária-financeira.

A restauração do backup é um procedimento para recuperar os dados após uma falha e deve estar contida dentro do plano de backup. Ela pode ser tanto total (restauração integral dos dados) ou parcial (restauração apenas de uma porção limitada de dados).

Recomendações

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Incluir um ou mais procedimentos de verificação de backups na política de backup, contendo no mínimo uma verificação pontual, quando da geração do backup, e uma rotina de verificação periódica.
- Recomenda-se a adoção de metodologias de teste de recuperação, como o Checklist/Walkthrough, para validar o procedimento de restauração e cronometrar o RTO, garantindo que o tempo de recuperação seja operacionalmente executável.
- Em caso de contratação de serviços de backup, incluir um plano de saída no contrato, para manter a continuidade de serviço quando do encerramento do contrato.
- Testar os backups antes da sua restauração.
- Os incluir em Termos de Referência (TR) e contratos de soluções tecnológicas (incluindo serviços de cloud ou datacenter terceirizado) cláusulas específicas sobre RPO, RTO, testes de recuperação e retenção de dados.

Diretrizes de Backup para Data Centers Próprios

Sobre Diretrizes de Backup para Data Centers Próprios

Para Data Centers próprios, ou seja, de propriedade do Órgão Setorial, esta Orientação Técnica define mais algumas diretrizes, além das já apresentadas nas outras seções.

A primeira diretriz versa sobre backup de sistemas de bancos de dados. Divididos tipicamente em camada de apresentação, negócios e dados, tais sistemas apresentam maior complexidade de backup para a camada de dados, que normalmente está armazenado em um Sistema Gerenciador de Banco de Dados. Para eles, os Gerenciadores possuem, via de regra, dois modelos de backup: lógico e físico.

O backup lógico é através do export ou dump das informações em arquivos texto. O backup físico é feito através utilitários específicos, que fazem o backup de arquivos binários em um formato proprietário que deve ser restaurado pelo próprio utilitário.

A tabela a seguir descreve de forma sucinta as duas possibilidades:

Tabela: Comparativo dos dois tipos de backup de Banco de Dados.

BACKUP DE BD	CARACTERÍSTICAS	CENÁRIO IDEAL
Lógico	Permite escolha granular dos dados a serem recuperados; A recuperação pode ser em ambientes diferentes do original.	Armazenamento por longos períodos e/ou recuperação de dados em um ambiente diferente do original.
Físico	Monolítico; Exige o mesmo ambiente de quando o backup foi feito.	Recuperação rápida e/ou integral de dados para um ambiente que não sofreu modificações.

A outra diretriz é para serviços de missão crítica, que exige uma continuidade de negócios bastante rigorosa, com RPO e/ou RTO próximos a zero. Para este caso, a diretriz básica é adotar o uso de um ou mais servidores espelho com sincronização constante.

Recomendações

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Realizar o backup dos sistemas de bases de dados, sendo que a camada de dados deve ter backup lógico e/ou físico.

Sugestões

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Realizar o backup lógico e físico da camada de dados e escolher o que melhor se adequa à situação para a restauração do backup.
- Em relação ao processo de backup, não realizar a sincronização constante de forma automática de remoções, pois podem levar a remoções indesejadas de dados.

Armazenamento de Dados

Sobre Armazenamento de Dados

Os Órgãos Setoriais possuem autonomia para buscar a forma que melhor atende às suas necessidades e disponibilidades, de forma que a sua política interna de armazenamento de dados seja exequível e efetiva.

Em particular, o uso de serviços na nuvem para armazenamento apresenta considerações próprias, incluindo questões de segurança da informação. Para informações específicas sobre serviços de nuvem, devem-se consultar as Orientações Técnicas para computação em nuvem.

Além disso, cuidados básicos de redundância de dados devem estar presentes para Órgãos Setoriais que mantenham Data Centers próprios.

Por fim, para armazenamento de código-fonte e/ou de documentos, o uso de ferramentas de versionamento passa a ser bastante interessante, para que se tenha maior rastreabilidade e consistência nos dados.

Recomendações

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Adotar redundância de dados em multiplos discos físicos utilizando tecnologia RAID ou similar.
- Adotar como diretriz básica o armazenamento dos dados corpoativos em diretórios compartilhados na rede, quando estes existirem, para facilitar o acesso aos dados.
- Criar diretórios (pastas) específicas com restrições de acesso para armazenamento de dados sensíveis.

Sugestões

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Avaliar o uso de ferramentas de sincronização e compartilhamento de dados.
- Avaliar o uso de ferramentas de gestão e auditoria de dados, visando ter melhor visibilidade e rastreabilidade.
- Considerar o uso de ferramentas de versionamento para documentos e códigos-fonte.

Referências

Link: https://en.wikipedia.org/wiki/Backup_site - “Backup Site”, in Wikipedia.
Acessado em: 03.03.2023.

Link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de--dados/guias/guia_lgpd.pdf.BRASIL. GOVERNO DIGITAL. Guia de boas práticas Lei Geral de Proteção de Dados (LGPD). Abr. 2020.
Acessado em: 03.03.2023.

Link: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm BRASIL. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Lei nº 13.709, de 14 de agosto de 2018.
Acessado em: 03.03.2023.

Link: https://www.cert.br/docs/palestras/certbr-rnp2017.pdf - Cert.br. “Backup - o básico cada vez mais essencial”. ZUBEN, Miriam von. Publicado em jun/2017
Acessado em: 03.03.2023.

Link: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Cert.br. “Cartilha de segurança para a Internet - Mecanismos de Segurança”.
Acessado em: 03.03.2023

Link https://pt.wikipedia.org/wiki/Dispositivo_de_armazenamento - “Dispositivo de armazenamento”
Acessado em: 03.03.2023.

Guia: Gartner, Inc. “Discover the Truth About the Use of Disk, Tape and Cloud Backup”. RHAME, Robert; RUSSEL, Dave.
Publicado em 27/03/2017.

Guia: Gartner, Inc. “Designing a Storage Strategy Document”. ANTELMI, Joseph.
Publicado em 22/01/2016.

Guia: Gartner, Inc. “How to Address Three Key Challenges When Considering Endpoint Backup”. RINNEN, Pushan.
Publicado em 19/01/2016.

Link: https://en.wikipedia.org/wiki/Recovery_point_objective - “Recovery Point Objective”, in Wikipedia.
Acessado em: 03.03.2023.

Link: https://en.wikipedia.org/wiki/Recovery_time_objective “Recovery Time Objective”, in Wikipedia. .-
Acessado em: 03.03.2023