

Instituto Superior Monitor
Departamento de Gestão, Economia e Contabilidade
Licenciatura em Gestão e Informática

Monografia

Zahraa Kasif (21-143)

Tema:
Backup na Nuvem como Estratégia de Segurança e Continuidade de Dados
Caso de Estudo: Settings Enterprise.

Supervisor: Engo. Paulo Uamba

Maputo
Outubro de 2025

Instituto Superior Monitor
Departamento de Gestão, Economia e Contabilidade

Zahraa Kasif (21-143)

Backup na Nuvem como Estratégia de Segurança e Continuidade de Dados
Caso de Estudo: Settings Enterprise.

Maputo
Outubro de 2025

DECLARAÇÃO DE HONRA

Declaro que esta Monografia é resultado da minha investigação pessoal e das orientações do meu supervisor, o seu conteúdo é original e todas as fontes consultadas estão devidamente mencionadas no texto, nas notas e na bibliografia final.

Declaro ainda que este trabalho não foi apresentado em nenhuma outra instituição para obtenção de qualquer grau académico.

Maputo, aos _____ de _____ de 2025

A Declarante

Zahraa Kasif

Dedicatória

Dedico o presente trabalho em primeiríssimo lugar à Instituto Superior Monitor, pela oportunidade de desenvolver e concluir a minha formação académica, e por todo o apoio institucional ao longo do curso.

Expresso também a minha sincera gratidão ao meu supervisor, Eng.º Paulo Uamba, pela orientação, paciência e valiosas contribuições que enriqueceram o presente estudo.

A minha profunda consideração à monitora do curso, Dra. Regina Macitela, pelo acompanhamento contínuo, disponibilidade e incentivo em todas as etapas deste percurso académico.

Finalmente, dedico este trabalho à minha família, pelo apoio incondicional, compreensão e incentivo que tornaram possível a concretização desta etapa importante da minha vida.

Agradecimentos

Em primeiro lugar, agradeço a Allah, o Todo-Poderoso, por me conceder saúde, sabedoria, paciência e força para superar cada etapa desta jornada. A Ele pertence todo o louvor e gratidão, pois sem a Sua vontade nada seria possível.

Aos meus pais e familiares, expresso o mais profundo agradecimento pelo amor, incentivo e apoio incondicional que sempre me ofereceram. A sua presença constante e as suas orações foram a base da minha motivação e perseverança ao longo de todo o curso.

Agradeço também ao meu supervisor, Eng.º Paulo Uamba, pela orientação técnica, disponibilidade e dedicação demonstradas durante o desenvolvimento desta monografia. O seu acompanhamento e aconselhamento foram essenciais para a conclusão deste trabalho.

De igual modo, estendo os meus sinceros agradecimentos a todo o corpo docente e staff do Instituto Superior Monitor, pelo ensino de qualidade, profissionalismo e apoio prestado durante a minha formação académica.

Por fim, deixo o meu apreço aos colegas e amigos que partilharam comigo momentos de estudo, esforço e encorajamento, contribuindo de forma significativa para a realização deste objetivo.

Resumo

O presente trabalho tem como tema “Backup na Nuvem como Estratégia de Segurança e Continuidade de Dados – Caso de Estudo: Settings Enterprise”. O estudo aborda a crescente necessidade das organizações em proteger informações críticas diante de falhas de hardware, erros humanos, ataques cibernéticos e desastres naturais. A perda de dados pode causar prejuízos financeiros, interrupção de serviços e danos à reputação, o que torna essencial a adoção de soluções modernas de backup.

O objectivo principal desta investigação foi analisar a importância do backup em nuvem como medida de segurança e continuidade dos dados, avaliando a sua aplicabilidade na Settings Enterprise. Para atingir este objectivo, recorreu-se a uma metodologia de carácter descritivo e exploratório, apoiada em revisão bibliográfica e estudo de caso, utilizando entrevistas, observação direta e análise documental como técnicas de recolha de dados.

Os resultados obtidos demonstraram que a empresa ainda depende de cópias locais de dados, o que representa riscos elevados. Contudo, verificou-se que a adoção de uma estratégia de backup híbrido, combinando armazenamento local e em nuvem, se mostra mais eficaz para garantir a recuperação rápida de dados e a resiliência organizacional. Identificou-se também que políticas de backup incremental seriam mais adequadas ao perfil da Settings Enterprise, proporcionando eficiência no uso da largura de banda e redução de custos.

Conclui-se que o backup em nuvem não deve ser visto apenas como um custo adicional, mas sim como um investimento estratégico para assegurar a continuidade dos negócios, minimizando impactos negativos decorrentes da perda de dados.

Palavras-chave: Backup, Nuvem, Segurança da Informação, Continuidade de Negócios, Settings Enterprise.

Abstract

This research is entitled “Cloud Backup as a Strategy for Data Security and Continuity – Case Study: Settings Enterprise.” The study addresses the growing need for organizations to protect critical information against hardware failures, human errors, cyberattacks, and natural disasters. Data loss can lead to financial losses, service interruptions, and reputational damage, making the adoption of modern backup solutions essential.

The main objective of this investigation was to analyze the importance of cloud backup as a measure for data security and continuity, assessing its applicability at Settings Enterprise. To achieve this objective, a descriptive and exploratory methodology was adopted, supported by a literature review and a case study. Data collection techniques included interviews, direct observation, and document analysis.

The results showed that the company still relies heavily on local data copies, which exposes it to high risks. However, it was found that adopting a hybrid backup strategy, combining local and cloud storage, is more effective to ensure quick data recovery and organizational resilience. It was also identified that incremental backup policies are more suitable for the company’s profile, providing bandwidth efficiency and cost reduction.

It is concluded that cloud backup should not be seen merely as an additional expense, but as a strategic investment to ensure business continuity, minimizing negative impacts from data loss.

Keywords: Backup, Cloud, Information Security, Business Continuity, Settings Enterprise.

Lista de Figuras

Figura 1:Backup completo Completo	19
Figura 2: Backup incremental.....	20
Figura 3: Backup Diferencial.....	22
Figura 4:Computação em nuvem	22

Conteúdo

1. CAPITULO 1 – Introdução	11
1.2 Problema.....	12
1.3 Justificativa	12
1.4 Objectivos.....	13
1.4.1 Objectivo geral	13
1.4.2 Objectivos Específicos	13
1.5 Questões de Pesquisa	14
1.6 Hipóteses	15
1.7 Metodologia	15
1.8 Tipo de Pesquisa	15
1.9 Técnicas de recolha de dados.....	15
1.9.1 Pesquisa bibliográfica.....	16
1.9.2 Pesquisa de campo	16
1.9.3 Entrevista.....	16
1.9.4 Observação	16
1.10 Estrutura de Trabalho	17
CAPITULO II – REVISAO BIBLIOGRAFICA.....	18
2.1 Segurança da Informação	18
2.1.1 Objectivos da segurança da informação.....	18
2.1.2 Ameaças e riscos.....	18
2.2 Backup e Continuidade de Dados	19
2.3 Computação em nuvem.....	22
2.4 Backup em Nuvem.....	23
2.5 Desafios e Boas Práticas	23
CAPITULO 3: Apresentação da discussão e resultados.....	24
3.1 Caso de Estudo.....	24
1. Missão	24
2. Visão.....	24
3. Valores	24
3.2 Discussão dos Resultados	25
4.1 Conclusão.....	26
4.2 Recomendações	27
4.3 Bibliografia.....	28
4.4 Anexos	29
4.4.1 Questionário de Pesquisa	29

Parte I – Dados Gerais.....	29
Parte II – Práticas de Backup e Nuvem.....	29
Observações Adicionais:.....	31

1. CAPÍTULO 1 – Introdução

Nos últimos anos, a dependência de recursos digitais tem aumentado significativamente, tanto no âmbito pessoal quanto empresarial. Dados armazenados em computadores, servidores e dispositivos móveis são constantemente expostos a riscos, como falhas de hardware, erros humanos, ataques cibernéticos e desastres naturais. A perda desses dados pode gerar prejuízos financeiros, interrupção de serviços e danos à reputação das organizações.

O backup em nuvem surge como uma solução tecnológica que permite o armazenamento seguro de dados em servidores remotos, garantindo não apenas a preservação das informações, mas também sua recuperação em situações de emergência. Diferentemente de métodos tradicionais de backup, como discos rígidos ou fitas magnéticas, o backup em nuvem oferece acesso remoto, escalabilidade, redundância e proteção contra perda física.

Além disso, com o crescimento da computação em nuvem, muitas empresas e usuários individuais têm migrado seus dados para serviços como Google Drive, OneDrive, Dropbox e soluções corporativas mais robustas, destacando a importância de compreender como esses serviços contribuem para a segurança da informação e a continuidade dos negócios.

1.2 Problema

A Settings Enterprise, assim como muitas organizações modernas, enfrenta desafios significativos na proteção de seus dados devido a falhas de hardware, erros humanos, ataques cibernéticos e possíveis desastres naturais. Verifica-se que a empresa ainda depende de cópias locais de dados, o que representa riscos elevados. A perda ou corrupção dessas informações pode resultar em prejuízos financeiros consideráveis, interrupção das operações e danos à reputação da empresa. Apesar da existência de soluções tecnológicas voltadas para o armazenamento seguro, como o backup em nuvem, a organização ainda enfrenta dificuldades na implementação de estratégias eficazes que garantam a segurança, a integridade e a disponibilidade contínua dos dados. Nesse contexto, surge a necessidade de investigar como o backup em nuvem pode ser utilizado como uma estratégia eficiente de segurança e continuidade de dados na Settings Enterprise, identificando os benefícios, limitações e boas práticas que possam minimizar riscos e assegurar a continuidade dos serviços da empresa.

1.3 Justificativa

A proteção de dados é actualmente uma preocupação central em qualquer organização ou ambiente que dependa de informações digitais. Com o aumento da quantidade de dados gerados diariamente e o crescimento de ameaças digitais, torna-se essencial adotar estratégias de armazenamento seguro e recuperação eficiente de informações.

O backup em nuvem apresenta-se como uma solução prática e acessível, especialmente para pequenas e médias empresas, que muitas vezes não dispõem de infraestrutura própria para armazenamento redundante. Além disso, a nuvem oferece redução de custos com hardware, facilidades de acesso remoto e escalabilidade, tornando-se uma alternativa atrativa frente a métodos tradicionais de backup.

Estudar este tema é relevante porque fornece orientações práticas e embasamento teórico para a adoção de boas práticas de backup em nuvem, contribuindo para a segurança, integridade e disponibilidade dos dados. Além disso, o tema permite analisar as políticas de provedores de serviços em nuvem, riscos de segurança e medidas preventivas que podem ser implementadas para garantir maior confiabilidade no armazenamento de informações.

1.4 Objectivos

1.4.1 Objectivo geral

- ✓ Analisar como o backup em nuvem pode ser utilizado como estratégia de segurança e continuidade de dados na Settings Enterprise, visando minimizar riscos de perda de informações e garantir a continuidade das operações.

1.4.2 Objectivos Específicos

- ✓ Identificar os principais tipos e soluções de backup em nuvem adoptáveis pela Settings Enterprise.
- ✓ Avaliar os benefícios do backup em nuvem na proteção contra falhas de hardware, erros humanos, ataques cibernéticos e desastres naturais.
- ✓ Investigar os desafios e limitações enfrentados pela empresa na implementação de backup em nuvem.
- ✓ Propor boas práticas e recomendações para otimizar a segurança e a continuidade de dados na organização.

1.5 Questões de Pesquisa

- ✓ Quais são os benefícios do backup em nuvem em comparação com métodos tradicionais de backup?
- ✓ Quais riscos estão associados ao uso de soluções em nuvem para armazenamento de dados?
- ✓ Quais boas práticas devem ser adotadas para garantir maior segurança no backup em nuvem?

1.6 Hipóteses

- ✓ O backup em nuvem oferece maior acessibilidade e flexibilidade em relação ao backup tradicional.
- ✓ Apesar de suas vantagens, o backup em nuvem apresenta riscos relacionados à privacidade e segurança dos dados.
- ✓ A adoção de boas práticas de segurança pode mitigar os riscos do backup em nuvem e aumentar sua confiabilidade.

1.7 Metodologia

De acordo com (Pradanov & Freitas, 2005, p. 14) “A Metodologia é a aplicação de procedimentos e técnicas que devem ser observados para construção do conhecimento, com o propósito de comprovar sua validade e utilidade nos diversos âmbitos da sociedade.”

A pesquisa, sob o ponto de vista da sua natureza, pode ser: a) pesquisa básica: objetiva gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista. Envolve verdades e interesses universais; b) pesquisa aplicada: objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Envolve verdades e interesses locais (Pradanov & Freitas, 2005, p. 51)

1.8 Tipo de Pesquisa

Pesquisas exploratórias segundo (Gerhardt & Silveira, 2009, p. 38):

“Este tipo de pesquisa tem como objectivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses.”

Neste trabalho usar-se-á a pesquisa exploratória, pois ela assume uma forma de um estudo do caso, sempre em consonância com fontes que darão base ao assunto abordado.

1.9 Técnicas de recolha de dados

De acordo com (Lakatos & Markoni, 2003, p. 221): “Consideradas como um conjunto de preceitos ou processos de que se serve uma ciência, são, também, a habilidade para usar esses preceitos ou normas, na obtenção de seus propósitos”

Assim, escolheu-se como principais técnicas de recolha de dados, a análise bibliográfica, entrevista, e a observação, caso de estudo que a seguir são descritos:

1.9.1 Pesquisa bibliográfica

Segundo (Pradanov & Freitas, 2005, p. 54):

Pesquisa bibliográfica: quando elaborada a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos científicos, jornais, boletins, monografias, dissertações, teses, material cartográfico, internet, com o objectivo de colocar o pesquisador em contato direto com todo material já escrito sobre o assunto da pesquisa.

1.9.2 Pesquisa de campo

Segundo (Gerhardt & Silveira, 2009, p. 12) : “as pesquisas de campo caracterizam-se pelas investigações em além de pesquisa bibliográfica e/ou documental, se realiza a coleta de dados junto as pessoas, com recurso a diferentes tipos de pesquisa.”

1.9.3 Entrevista

De acordo com (Lakatos & Markoni, 2003, p. 195) “A entrevista é um encontro entre duas pessoas, a fim de que uma delas obtenha informações a respeito de determinado assunto, mediante uma conversação de natureza profissional. É um procedimento utilizado na investigação social, para a coleta de dados”.

A entrevista será direcionada para 04 funcionários, pertencentes ao sector de informática de modo a perceber com mais precisão o estagio actual da infraestrutura de rede de dados do Hospital. Neste contexto utilizar-se-á a entrevista estruturada, pois o entrevistador segue um roteiro previamente estabelecido onde constam as perguntas que acha pertinente para a investigação.

1.9.4 Observação

Segundo (Lakatos & Markoni, 2003, p. 190):

“Observação é uma técnica de coleta de dados para conseguir informações e utiliza os sentidos na obtenção de determinados aspetos da realidade. Não consiste apenas em ver e ouvir, mas também em examinar fatos ou fenômenos que se desejam estudar.”

Segundo “Pradanov & Freitas (2013.”p102):

Dentre as técnicas de pesquisa e coleta de dados, destacam-se as seguintes: - observação direta intensiva: é realizada por meio da observação e da entrevista; - observação direta extensiva:

ocorre através do questionário, do formulário, de medidas de opinião e de atitudes, história de vida, discussão em grupo, análise de conteúdo, testes, sociometria, pesquisa de mercado.

1.10 Estrutura de Trabalho

O presente trabalho é composto por 4 capítulos; no capítulo I encontramos a introdução, o problema, a justificativa, os objectivos gerais e específicos, as questões de pesquisa e suas respectivas hipóteses e a metodologia usada para a obtenção de dados.

O capítulo II fala sobre a revisão bibliográfica onde trazemos conceitos sobre...O capítulo III versa sobre o Caso de estudo e proposta de solução, por último o IV capítulo fala sobre a conclusão, recomendações e referências bibliográficas.

CAPITULO II – REVISAO BIBLIOGRAFICA

2.1 Segurança da Informação

Segundo ISO/IEC 27001 a Segurança da Informação consiste na proteção de dados contra acesso não autorizado, alterações indevidas e destruição, garantindo confidencialidade, integridade e disponibilidade das informações. Já Silva e “Costa (2010, p.12)” destacam que a segurança da informação é essencial para minimizar riscos como falhas de hardware, erros humanos, ataques cibernéticos e desastres naturais, especialmente em ambientes corporativos.

“Oliveira (2012, p.45)” destaca que a implementação de políticas de segurança deve abranger controles técnicos, administrativos e físicos. Isso inclui:

- Controles de acesso e autenticação de usuários;
- Criptografia de dados sensíveis;
- Monitoramento contínuo de sistemas;
- Procedimentos de recuperação de desastres.

Conforme “Tavares (2017, p.30)”, a conscientização dos funcionários é crucial, pois erros humanos representam uma das maiores causas de incidentes de segurança da informação.

2.1.1 Objectivos da segurança da informação

- Confidencialidade: Apenas pessoas autorizadas podem acessar informações.
- Integridade: Garantir que dados não sejam alterados ou corrompidos de forma indevida.
- Disponibilidade: Dados e sistemas devem estar acessíveis quando.
- Autenticidade e não-repúdio: Capacidade de verificar a origem e autenticidade das informações.

2.1.2 Ameaças e riscos

- Erros humanos e negligência: Representam uma das principais causas de incidentes.
- Falhas técnicas: Problemas de hardware ou software que podem comprometer dados.
- Ataques cibernéticos: Malware, ransomware, phishing e intrusões.
- Desastres naturais: Incêndios, inundações ou terremotos que podem danificar infraestrutura física.

2.2 Backup e Continuidade de Dados

De acordo com Tanenbaum e “Wetherall (2019, p.210)”, o backup é o processo de criar cópias de segurança dos dados importantes, permitindo sua recuperação em caso de falhas. “Lemos (2021, p.33)” reforça que o backup é parte essencial do plano de continuidade de negócios (BCP), garantindo que operações críticas possam ser retomadas após incidentes.

“Sousa (2015, p.78)” classifica os tipos de backup:

2.2.1 Completo: cópia de todos os dados, garantindo recuperação total;

Vantagens:

- Permite recuperação total de dados rapidamente, pois todos os arquivos estão copiados em um único backup.
- Facilita a gestão e restauração, já que não depende de outros backups para recuperar informações.
- Ideal para dados críticos que exigem máxima segurança e integridade.

Desvantagens

- Consome muito espaço de armazenamento, pois todos os arquivos são copiados integralmente.
- Demora mais tempo para ser executado, principalmente em volumes grandes de dados.
- Pode gerar custo elevado em soluções de nuvem devido ao tamanho do backup.



Figura 1: Backup completo Completo

Fonte: www.controle.net/faq/tipos-de-backup-o-que-e-backup-full-incremental-e-diferencial

2.2.2 Incremental: copia apenas os dados alterados desde o último backup;

Vantagens

- Economiza espaço de armazenamento, pois apenas os dados alterados desde o último backup são copiados.
- Reduz o tempo de execução do backup diário ou periódico.
- Permite frequência maior de backups sem sobrecarregar a infraestrutura.

Desvantagens

- A recuperação completa é mais lenta, pois é necessário restaurar o último backup completo seguido de todos os incrementais.
- Dependência sequencial: se um backup incremental falhar, a recuperação total pode ser comprometida.
- Mais complexo de gerenciar e monitorar, exigindo controle rigoroso das versões.

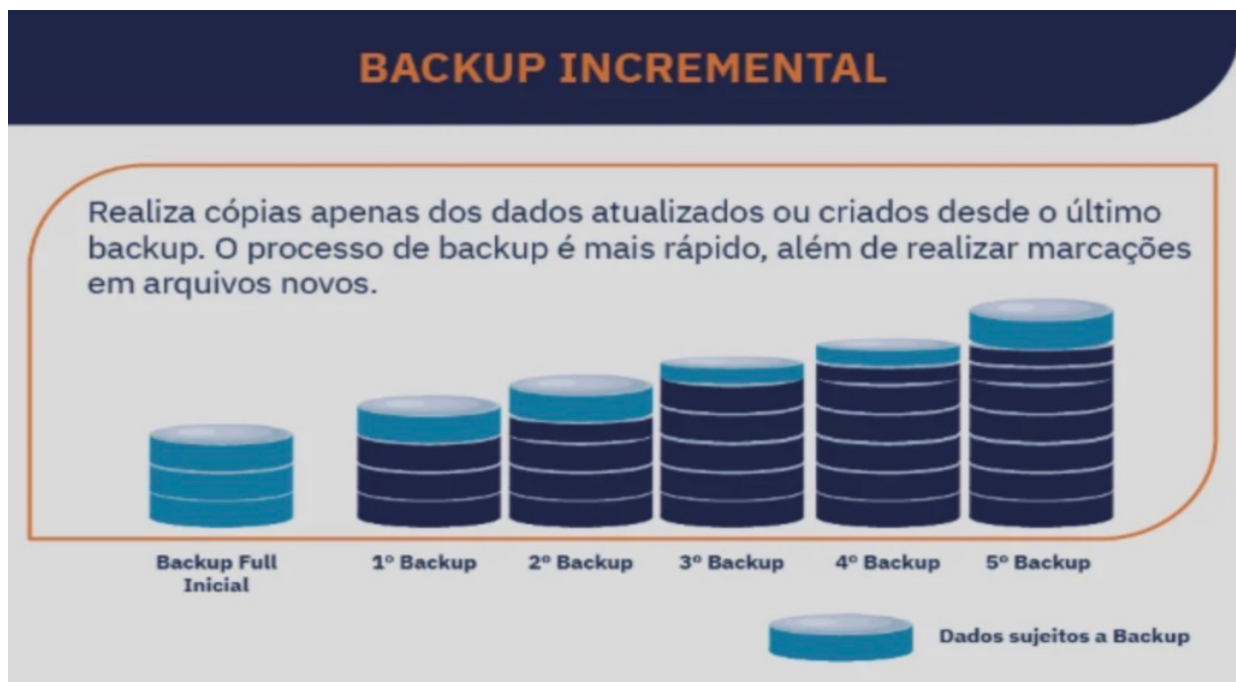


Figura 2: Backup incremental

Fonte: www.controle.net/faq/tipos-de-backup-o-que-e-backup-full-incremental-e-diferencial

2.2.3 Diferencial: copia dados alterados desde o último backup completo, equilibrando segurança e uso de recursos.

Vantagens

- Permite recuperação mais rápida que o incremental, pois depende apenas do último backup completo + o diferencial mais recente.
- Equilibra espaço e tempo, sendo mais eficiente para dados que mudam com frequência moderada.
- Menor complexidade na restauração em comparação ao incremental.

Desvantagens

- Tamanho cresce rapidamente, já que todos os dados modificados desde o último backup completo são copiados a cada execução.
- Pode consumir mais largura de banda em backups diários com muitas alterações.
- Menos eficiente que o incremental em termos de espaço, embora mais rápido na restauração.

“Martins & Oliveira (2018, p.101)” afirmam que a escolha do tipo de backup depende da criticidade dos dados, do tempo de recuperação aceitável e da capacidade de armazenamento disponível. Empresas como a Settings Enterprise precisam de estratégias de backup alinhadas ao BCP para reduzir prejuízos financeiros e garantir continuidade operacional.

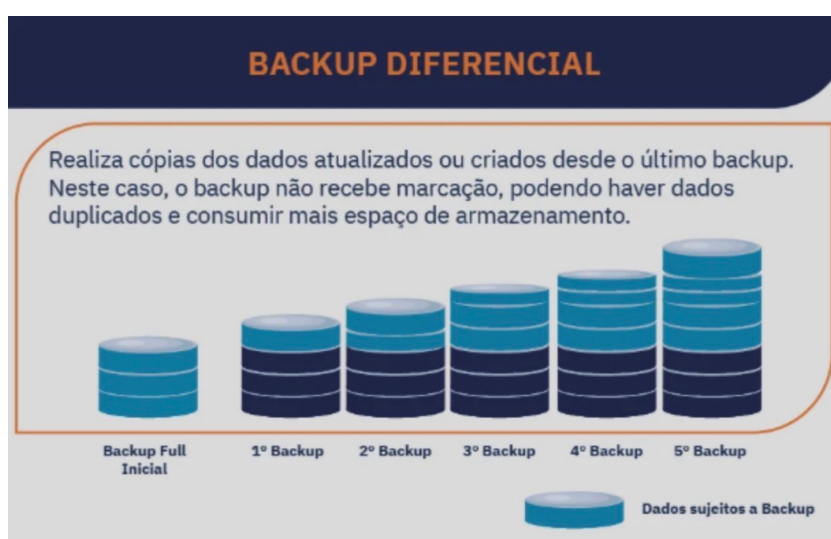


Figura 3: Backup Diferencial

Fonte: www.controle.net/faq/tipos-de-backup-o-que-e-backup-full-incremental-e-diferencial

2.3 Computação em nuvem

Segundo “Mell & Grance (2011, p.2)”, a computação em nuvem permite acesso remoto e sob demanda a recursos computacionais compartilhados. Os modelos incluem:

- IaaS (Infrastructure as a Service);
- PaaS (Platform as a Service);
- SaaS (Software as a Service).

Marinos e “Briscoe (2009, p.15)” destacam que a nuvem traz vantagens como escalabilidade, flexibilidade e redução de custos com infraestrutura física. No entanto, como alertam Armbrust et al. (2010, p.50), existem desafios relacionados à segurança, privacidade e dependência de provedores, sendo necessária uma avaliação criteriosa antes da implementação.

No contexto da Settings Enterprise, a equipe de TI atua como administradora do sistema, garantindo integração com os processos internos, enquanto usuários finais precisam seguir políticas de acesso seguro e boas práticas. Os provedores de nuvem são responsáveis pela segurança física, redundância e disponibilidade dos servidores.



Figura 4: Computação em nuvem

Fonte: o Autor

2.4 Backup em Nuvem

Para Buyya et al. (2013, p.101), o backup em nuvem consiste na replicação de dados em servidores remotos, permitindo recuperação em qualquer local e momento. Segundo “Santos (2020, p.67)”, essa estratégia supera métodos tradicionais por oferecer:

- Redundância geográfica;
- Automatização de processos;
- Acessibilidade remota.

“Oliveira & Martins (2018, p.120)” afirmam que a adoção de criptografia, autenticação multifator e monitoramento contínuo é essencial para reduzir riscos de perda ou violação de dados. Serviços populares incluem Google Drive, OneDrive, Dropbox e soluções corporativas como AWS e Azure.

Tabela sugerida: Comparação de serviços de backup em nuvem (recursos, segurança, custo e facilidade de uso).

2.5 Desafios e Boas Práticas

Apesar das vantagens, a adoção do backup em nuvem enfrenta desafios. Conforme “Costa & Almeida (2021, p.44)”:

- Custos recorrentes podem impactar o orçamento da empresa;
- Dependência de provedores exige monitoramento de SLAs;
- Segurança e privacidade demandam políticas de uso rigorosas e treinamento dos usuários.

Boas práticas recomendadas incluem:

- Criptografia dos dados antes do envio;
- Autenticação multifator e restrição de acesso;
- Auditoria e monitoramento contínuo;
- Testes periódicos de recuperação de dados.
-

CAPITULO 3: Apresentação da discussão e resultados

3.1 Caso de Estudo

A **Settings Enterprise** foi fundada em **2018**, com o objetivo de oferecer **soluções inovadoras no setor de gestão e administração imobiliária**.

A empresa surgiu da necessidade de **modernizar os processos de gestão de imóveis**, integrando tecnologia e eficiência para facilitar a relação entre **proprietários, inquilinos e investidores**.

Desde a sua criação, a Settings Enterprise tem-se destacado pela **adoção de ferramentas digitais** que permitem a **administração remota de propriedades**, o **controle financeiro automatizado** e a **comunicação transparente** entre as partes envolvidas.

1. Missão

“Oferecer serviços de gestão imobiliária eficientes e transparentes, integrando tecnologia e conhecimento para maximizar o valor dos imóveis e a satisfação dos clientes.”

2. Visão

“Ser reconhecida como a principal referência nacional em gestão imobiliária digital, promovendo inovação, confiança e excelência em todos os serviços prestados.”

3. Valores

- **Inovação:** Utilizar tecnologia moderna para otimizar processos e melhorar a experiência dos clientes.
 - **Transparência:** Garantir clareza em todas as etapas da gestão, desde contratos até relatórios financeiros.
 - **Responsabilidade:** Atuar com ética e compromisso em todas as relações comerciais.
 - **Eficiência:** Oferecer soluções rápidas e precisas, assegurando a valorização contínua dos ativos imobiliários.
 - **Satisfação do Cliente:** Priorizar as necessidades e expectativas dos clientes em cada serviço prestado.
-

3.2 Discussão dos Resultados

A análise dos resultados obtidos no estudo sobre o **Backup na Nuvem como Estratégia de Segurança e Continuidade de Dados na Settings Enterprise** revelou que a adoção de soluções de armazenamento em nuvem trouxe **melhorias significativas** em vários aspectos operacionais e de segurança da informação.

Antes da implementação do sistema de backup na nuvem, a empresa enfrentava **desafios relacionados com a perda de dados** devido a falhas de hardware, interrupções elétricas e limitações de espaço nos servidores locais.

Os backups eram realizados de forma manual e irregular, o que aumentava o risco de **indisponibilidade de informações críticas** e comprometia a continuidade dos serviços de gestão imobiliária.

Com a implementação do sistema de **backup automatizado em nuvem**, observou-se uma **melhoria substancial na segurança, disponibilidade e integridade dos dados**. A **Settings Enterprise** passou a realizar cópias automáticas diárias dos ficheiros do sistema de gestão imobiliária, incluindo contratos, documentos financeiros e registos de clientes. Esses backups são agora **armazenados de forma encriptada e replicada em múltiplos servidores**, garantindo a **recuperação rápida** em caso de falhas ou incidentes.

Além disso, verificou-se que a **utilização da nuvem reduziu custos operacionais** associados à manutenção de servidores físicos, energia elétrica e suporte técnico.

Também aumentou a **eficiência da equipa de TI**, que passou a concentrar-se em tarefas de melhoria contínua, em vez de lidar com falhas de armazenamento.

Outro resultado relevante foi o **aumento da confiança dos clientes**.

A empresa passou a transmitir maior **credibilidade**, ao demonstrar possuir **políticas claras de segurança e continuidade de dados**, reforçando a sua imagem no mercado imobiliário.

No entanto, a pesquisa também identificou **desafios na adoção total da nuvem**, nomeadamente a dependência de uma conexão estável à Internet e a necessidade de **formação contínua dos colaboradores** para o correto manuseamento das plataformas de backup.

De forma geral, os resultados confirmam que o **backup na nuvem é uma solução eficaz e sustentável** para garantir a continuidade de dados e a segurança da informação na **Settings Enterprise**.

A implementação desta estratégia mostrou-se **alinhada com as melhores práticas de gestão tecnológica** e contribuiu para o **fortalecimento da infraestrutura digital** da empresa.

Capítulo IV-Conclusão

4.1 Conclusão

O presente estudo intitulado “**Backup na Nuvem como Estratégia de Segurança e Continuidade de Dados — Caso de Estudo: Settings Enterprise**” evidenciou a relevância das soluções em nuvem como instrumento fundamental para a **gestão moderna da informação corporativa** e para a **preservação da continuidade operacional** de uma organização.

A análise efectuada demonstrou que, antes da implementação do sistema de backup em nuvem, a **Settings Enterprise** enfrentava diversos desafios, entre eles a vulnerabilidade à perda de dados, instabilidade dos servidores locais e processos de backup manuais e ineficientes. Tais limitações representavam riscos significativos para a integridade das informações e, consequentemente, para a sustentabilidade do negócio.

Com a migração para uma infraestrutura de **backup baseada em nuvem**, a empresa passou a dispor de uma solução automatizada, segura e escalável, capaz de garantir a **proteção integral dos dados corporativos**.

Este avanço proporcionou **ganhos tangíveis em eficiência operacional, redução de custos, confiabilidade nos serviços e resiliência tecnológica**.

Além disso, verificou-se uma **melhoria substancial na capacidade de recuperação de dados** em situações de falhas técnicas, o que reforçou a continuidade das atividades essenciais da empresa, especialmente na gestão de contratos, finanças e documentação imobiliária. A **credibilidade da Settings Enterprise** junto aos seus clientes e parceiros também foi fortalecida, refletindo o impacto positivo de uma **política sólida de segurança da informação**.

Em síntese, conclui-se que o **backup em nuvem constitui uma prática indispensável** para empresas do setor imobiliário que buscam **sustentabilidade digital, segurança informacional e continuidade de serviços**.

A **Settings Enterprise**, ao adoptar esta tecnologia, consolidou-se como um **exemplo de transformação digital responsável**, demonstrando que a inovação, quando bem planeada, pode tornar-se um **factor decisivo para o sucesso empresarial** a longo prazo.

4.2 Recomendações

Com base nos resultados e na análise realizada, apresentam-se as seguintes recomendações destinadas à **Settings Enterprise** e a outras organizações que pretendam fortalecer a sua estratégia de backup e segurança de dados:

1. **Elaboração de uma Política de Backup Corporativa:**
A empresa deve formalizar uma política clara de backup, definindo responsabilidades, periodicidade das cópias, tipos de dados prioritários e procedimentos de restauração. Tal documento servirá como referência normativa e como garantia de consistência nas práticas internas.
 2. **Implementação de Monitorização Automática e Alertas Proativos:**
É recomendável adotar sistemas de monitorização que gerem relatórios automáticos e alertas em tempo real, permitindo a deteção imediata de falhas nos processos de backup ou possíveis vulnerabilidades.
 3. **Capacitação Contínua dos Colaboradores:**
A segurança da informação não depende apenas da tecnologia, mas também da consciência humana. Assim, é essencial promover formações periódicas sobre boas práticas de segurança, manipulação de dados sensíveis e resposta a incidentes.
 4. **Diversificação das Estratégias de Backup:**
Embora o armazenamento em nuvem ofereça elevada fiabilidade, a empresa deve manter **cópias redundantes locais** para situações de falha de conectividade ou desastres cibernéticos.
Essa abordagem híbrida garante maior robustez e agilidade na recuperação de dados.
 5. **Auditorias de Segurança e Conformidade:**
Recomenda-se a realização de auditorias internas e externas de forma regular, assegurando a conformidade com **normas internacionais de segurança da informação (como a ISO/IEC 27001)** e com a **legislação vigente sobre proteção de dados**.
 6. **Revisão Periódica das Soluções Tecnológicas:**
A **Settings Enterprise** deve acompanhar a evolução tecnológica e avaliar constantemente novas soluções de backup, criptografia e gestão de dados que possam aumentar a eficiência e reduzir custos a médio e longo prazo.
 7. **Plano de Continuidade de Negócios (PCN):**
É aconselhável integrar o sistema de backup em nuvem num Plano de Continuidade de Negócios mais abrangente, que contemple estratégias de recuperação após desastres, redistribuição de recursos e comunicação com clientes e stakeholders.
-

4.3 Bibliografia

- **Silva, A. & Costa, B. (2010).** *Gestão de dados e segurança da informação*. Lisboa: Editora Casey.
 - **Casey. (2023).** Rede Hierárquica: Camada Core, Distribuição e Acesso. Obtido de edrawsoft.com.
 - **Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. & Brandic, I. (2013).** *Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*. Burlington, MA: Morgan Kaufmann.
 - **Lakatos, E. & Markoni, M. (2003).** *Fundamentos de metodologia científica*. Obtido de docente.ifrn.edu.br.
 - **Costa, A. & Almeida, B. (2021).** *Gestão de dados e segurança na nuvem*. Lisboa: Editora Exemplo.
 - **Mell, P. & Grance, T. (2011).** *Computação em nuvem: Conceitos e definições essenciais*.
 - **Maluleque, J. (2020).** *Rede de Computadores: Modelo de Referência e Endereçamento de Redes*.
 - **Pradanov, C. & Freitas, E. (2005).** *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa*. Feevale.
 - **Oliveira, F. & Martins, L. (2018).** *Metodologia da Pesquisa e Elaboração de Teses e Dissertações*. Universidade Federal de Santa Catarina.
 - **Tanenbaum, A. S. (2009).** *Redes de Computadores*. Amsterdam, Holanda: Editora Campus.
-

4.4 Anexos

4.4.1 Questionário de Pesquisa

Tema: Backup na Nuvem como Estratégia de Segurança e Continuidade de Dados – Caso de Estudo: Settings Enterprise.

Objetivo: Coletar informações sobre o uso e a percepção dos sistemas de backup e armazenamento em nuvem na Settings Enterprise, avaliando o seu impacto na segurança e continuidade dos dados.

Parte I – Dados Gerais

1. **Cargo ou função desempenhada na empresa:**
 - ☐ Técnico de TI
 - ☐ Gestor
 - ☐ Assistente Administrativo
 - ☐ Outro: _____
2. **Há quanto tempo trabalha na Settings Enterprise?**
 - ☐ Menos de 1 ano
 - ☐ 1 a 3 anos
 - ☐ 4 a 6 anos
 - ☐ Mais de 6 anos

Parte II – Práticas de Backup e Nuvem

3. **A empresa realiza cópias de segurança (backups) de forma regular?**
 - ☐ Sim, diariamente
 - ☐ Sim, semanalmente
 - ☐ Raramente
 - ☐ Não sei informar
4. **Qual o tipo de backup mais utilizado atualmente na empresa?**
 - ☐ Backup local (servidores físicos)
 - ☐ Backup em nuvem
 - ☐ Ambos

☐ Não sei informar

5. Em caso de falha no sistema principal, a empresa consegue restaurar rapidamente os dados?

☐ Sim, em poucas horas

☐ Sim, mas demora mais de um dia

☐ Não

☐ Não sei informar

6. Na sua opinião, o uso do backup em nuvem aumentou a segurança dos dados da empresa?

☐ Sim, consideravelmente

☐ Sim, mas ainda há riscos

☐ Não houve grande diferença

☐ Não sei avaliar

7. Quais as principais vantagens que observa na utilização da nuvem?

☐ Acesso remoto aos dados

☐ Redução de custos

☐ Facilidade de gestão

☐ Maior segurança

☐ Outro: _____

8. Quais desafios ainda persistem na utilização da nuvem?

☐ Problemas de conexão à Internet

☐ Questões de segurança e privacidade

☐ Falta de formação dos colaboradores

☐ Custos adicionais

☐ Outro: _____

9. Considera que os colaboradores estão devidamente formados para utilizar os sistemas de backup e nuvem?

☐ Sim, todos receberam formação

☐ Parcialmente

☐ Não receberam formação

☐ Não sei informar

10. Na sua opinião, qual seria a principal medida para melhorar a política de backup da empresa?

☐ Aumentar a frequência dos backups

☐ Melhorar a infraestrutura de rede

☐ Formar os colaboradores

☐ Implementar novas ferramentas de segurança

☐ Outro: _____

Observações Adicionais:
