CÓDIGO 31

Short Paper

SEGURANÇA DA INFORMAÇÃO: PESQUISA APLICADA DE UMA POLÍTICA DE BACKUP EM UMA EMPRESA DE ENGENHARIA METALÚRGICA

INFORMATION SECURITY: APPLIED RESEARCH OF A BACKUP POLICY IN A METALLURGICAL ENGINEERING COMPANY

Data de Submissão: 03/07/2023
Data de Aprovação: 23/08/2023

Presleyson Plínio de Lima[1]
presleyson.lima@academico.domhelder.edu.br

Thiago Oliveira Pereira[2]
e00844@academico.domhelder.edu.br

RESUMO

Introdução: Este trabalho busca acompanhar o desenvolvimento de uma política de backup a ser acordada entre a governança de TI e a governança da empresa de engenharia metalúrgica no Brasil, complementando assim as tecnologias de *backup* e ferramentas de armazenamento já utilizadas pelo software *Backup Exec* desenvolvido pela Veritas Technologies, empresa americana sediada em Santa Clara, Califórnia, presta serviços no ramo de gerência de dados internacionais incluindo: gerenciamento de dados em multinuvem, proteção de dados, otimização do armazenamento, preparação para conformidade e portabilidade de cargas de trabalho, sem dependerem de um único fornecedor de nuvem. **Objetivos:** O principal objetivo deste trabalho é fornecer diretrizes para a implementação de boas práticas relacionadas à retenção, replicação e criação de cópias de segurança, seguindo as normas estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT). Já os objetivos específicos são desenvolver uma política de *backup* em uma empresa focada em engenharia metalúrgica no Brasil que está passando pelo período de expansão de mercado e busca formalizar o procedimento de armazenamento das cópias de segurança; identificar melhorias acarretadas pela implementação da política desenvolvida em conjunto com a necessidade do negócio e aplicar a política desenvolvida na ferramenta de backup utilizada pela empresa: software Veritas *Backup Exec*. **Metodologia:** O presente trabalho conta com a pesquisa bibliográfica e aplicada sobre a implementação de uma solução de *backup* englobando software e política de retenção. **Resultados:** Os resultados desse estudo de caso são apresentados no Anexo A que ilustra a política de backup desenvolvida considerando fatores e limitações apresentados nessa seção. **Conclusão:** Após realizar o mapeamento e classificação das informações em conjunto com as áreas de negócio, levando em consideração a localização nos servidores de arquivos, bem como identificar o cluster de máquinas virtuais responsáveis pelos programas utilizados em toda a empresa, é possível concluir que a política de backup não é um mero documento do departamento de Tecnologia da Informação (TI), mas sim um documento de interesse amplo da organização. Essa política garante o alinhamento estratégico entre as governanças de TI e do negócio, além de proporcionar o fator essencial que agrega valor a essa política: a segurança de todas as informações necessárias para a continuidade dos negócios em caso de perda.

Palavras-chave: Política de *backup*. Governança. Continuidade. Segurança e Informação.

1 Escola Superior Dom Helder, Belo Horizonte, Brasil
https://orcid.org/0000-0002-6850-3638
presleyson.lima@academico.domhelder.edu.br
Mestre em Sistemas de Informação e Gestão do Conhecimento

2 Escola Superior Dom Helder, Belo Horizonte, Brasil
https://orcid.org/0009-0002-4818-5414
e00844@academico.domhelder.edu.br
Bacharel em Ciência da Computação

ABSTRACT

Introduction: *This work seeks to monitor the development of a backup policy to be agreed between IT governance and the governance of the metallurgical engineering company in Brazil, thus complementing the backup technologies and storage tools already used by the Backup Exec software developed by Veritas Technologies, an American company headquartered in Santa Clara, California, provides international data management services including: multi-cloud data management, data protection, storage optimization, compliance preparation and workload portability, without relying on a single cloud provider.* ***Objectives:*** *The main objective of this work is to provide guidelines for the implementation of good practices related to retention, replication and creation of backup copies, following the standards established by the Brazilian Association of Technical Standards (ABNT). The specific objectives are to develop a backup policy in a company focused on metallurgical engineering in Brazil that is going through a period of market expansion and seeks to formalize the backup storage procedure; identify improvements brought about by the implementation of the policy developed in conjunction with business needs and apply the policy developed in the backup tool used by the company: Veritas Backup Exec software.* ***Methodology:*** *This work relies on bibliographic and applied research on the implementation of a backup solution encompassing software and retention policy.* ***Results:*** *The results of this case study are presented in Appendix A, which illustrates the backup policy developed considering factors and limitations presented in this section.* ***Conclusion:*** *After mapping and classifying the information together with the business areas, taking into account the location on the file servers, as well as identifying the cluster of virtual machines responsible for the programs used throughout the company, it is possible to conclude that the Backup policy is not a mere document from the Information Technology (IT) department, but rather a document of broad interest to the organization. This policy ensures strategic alignment between IT and business governance, in addition to providing the essential factor that adds value to this policy: the security of all information necessary for business continuity in the event of loss.*

Keywords: *Backup Policy, Governance, Continuity, Security and Information.*

1 INTRODUÇÃO

Em uma sociedade globalmente interconectada, a informação e seus processos associados, assim como outros ativos essenciais, possuem um valor significativo para o sucesso dos negócios de uma organização. Esse valor transcende meras palavras escritas, números e imagens, abrangendo também conhecimento, conceitos, ideias e marcas, os quais constituem diversas formas de informação que devem ser protegidas contra uma variedade de riscos (ABNT, 2013).

De acordo com Campos (2007) é preciso entender a relação entre a segurança da informação e sua relevância para os negócios da organização, complementando conforme Gillenson (2006), para manter conteúdos confidenciais fora de riscos de exposição, é importante realizar cópias de segurança dos arquivos que contém informações da organização e manter registrado de todas as ações realizadas na manipulação desses arquivos. Dessa forma, é possível evitar a destruição de arquivos, os erros de atualização e corrigir erros de sincronização dos arquivos e dados armazenados.

Segundo Purvis (2011) uma série de regulamentos obrigam que os dados sejam armazenados por anos até mesmo décadas, além disso, cada vez mais as empresas buscam guardar a maior quantidade de dados possíveis pelo motivo de que podem ter valor algum dia.

Este trabalho busca acompanhar o desenvolvimento de uma política de backup a ser acordada entre a governança de TI e a governança da empresa de engenharia metalúrgica no Brasil, complementando assim as tecnologias de *backup* e ferramentas de armazenamento já utilizadas pelo software *Backup Exec* desenvolvido pela Veritas Technologies, empresa americana sediada em Santa Clara, Califórnia, presta serviços no ramo de gerência de dados internacionais incluindo: gerenciamento de dados em multinuvem, proteção de dados, otimização do armazenamento, preparação para conformidade e portabilidade de cargas de trabalho, sem dependerem de um único fornecedor de nuvem.

1.1 OBJETIVOS

1.1.1 *Objetivo Geral*

O principal objetivo deste trabalho é fornecer diretrizes para a implementação de boas práticas relacionadas à retenção, replicação e criação de cópias de segurança, seguindo as normas estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT).

1.1.2 *Objetivo Específicos*

- Desenvolver uma política de *backup* em uma empresa focada em engenharia metalúrgica no Brasil que está passando pelo período de expansão de mercado e busca formalizar o procedimento de armazenamento das cópias de segurança.
- Identificar melhorias acarretadas pela implementação da política desenvolvida em conjunto com a necessidade do negócio.
- Aplicar a política desenvolvida na ferramenta de backup utilizada pela empresa: software Veritas *Backup Exec*.

1.2 Justificativa

Atualmente os *backups* da empresa de engenharia metalúrgica não seguem uma política de retenção e recuperação de desastre, além de existir um histórico de perdas de arquivos que impactaram a produção da empresa. Devido ao histórico de perdas e o momento de crescimento

no mercado com aquisição de outras empresas, surgiu a necessidade de desenvolvimento de uma política de *backup* e recuperação de desastres alinhado com sua governança.

Essa seção se divide em quatro etapas, a primeira aborda o conceito de política de *backup* e suas recomendações e definições para o ambiente que está sendo escrita, a segunda etapa bem como as etapas que a seguem tratam sobre os tipos de *backup* e suas particularidades que impactam diretamente na retenção das cópias de segurança e consequentemente na política a ser escrita.

1.3 Política de *backup*

Cabe à companhia definir uma política de *backup* que define os dados a serem copiados, buscando garantir a possibilidade de recuperação completa ou o mais próximo possível do ponto de falha do ambiente, e que garanta a proteção dos dados importantes para continuidade do negócio.

Segundo ABNT (2013), na política de *backup* é definida a regularidade das execuções de cada cópia de segurança, o que exige uma análise de relevância dos dados contidos no ambiente a ser copiado, possibilitando assim maior organização em caso de necessidade de recuperação dos dados.

Ainda conforme ABNT (2013), outro ponto a ser definido pela política é o tempo de retenção das cópias realizadas, assim como a replicação delas, garantindo assim uma segunda cópia de segurança em outro ambiente físico, reduzindo o risco de falhas ou perdas. Entretanto, mesmo buscando reduzir a possibilidade de perdas ou falhas, é impossível extinguir por completo esse risco, tomando como exemplo o atentado às torres gêmeas em 11 de setembro de 2001, onde o datacenter de uma das torres realiza *backup* na torre vizinha.

1.4 *Backup* Completo

Conhecido como *backup full*, este modelo de *backup* consiste na cópia de todas as informações existentes no ambiente em que a cópia está sendo realizada. Por ser uma cópia completa, a restauração dos dados se torna mais simples quando necessária, todos os dados copiados são restaurados, porém, o tempo gasto para recuperação dos dados desse modelo é maior devido ao volume de dados copiados.

De acordo com Rodrigues (2017), o volume de dados a serem copiados e o tempo necessário para realização do *backup* acarreta uma limitação para realizar e restaurar o *backup*.

1.5 *Backup* Diferencial

Com seu volume consideravelmente menor, o *backup* diferencial realiza a cópia dos dados que foram modificados depois do último *backup* completo, que por sua vez serve como um ponto de referência e comparação do estado dos dados para realização de uma tarefa diferencial.

Segundo Santos et al. (2018), o tempo de execução e volume do *backup* diferencial é consideravelmente menor em relação ao *backup* completo, porém, ele apresenta um aumento de volume e tempo de execução conforme o número de arquivos modificados, criados ou excluídos desde a última execução do *backup* completo.

Por ser cumulativo, o *backup* diferencial sempre realizará uma cópia de todo e qualquer arquivo que foi alterado, criado ou apagado depois da realização do *backup* completo.

Segundo Rodrigues (2017), com o emprego do *backup* diferencial, a restauração dos dados em caso de algum incidente necessita somente do último *backup* completo e o *backup* diferencial que contenha a informação desejada.

1.6 *Backup* Incremental

Segundo Philereno (2017), o *backup* incremental realiza a cópia de qualquer dado que foi criado ou modificado desde a última execução da tarefa.

Para poder ser executado o *backup* incremental necessita que em algum momento anterior um *backup* completo tenha sido realizado, da mesma forma como no *backup* diferencial o *backup* completo é usado como ponto de referência para comparar se dados foram criados ou modificados. A grande diferença do *backup* incremental para o *backup* diferencial está na forma em que o ponto de referência é usado, quando executado, o *backup* incremental se torna o ponto de referência para o próximo *backup* incremental, ou seja, somente os dados que foram criados ou alterados do *backup* completo são copiados pelo primeiro *backup* incremental e apenas os dados que sofreram mudanças ou foram criados após essa tarefa são copiados pelo segundo *backup* incremental.

Segundo Philereno (2017), esse modelo de *backup* tem o tempo de execução menor assim como o volume de dados copiados, porém, a tarefa de recuperação dos dados se torna mais complexa devido à necessidade de restaurar não só o último *backup* completo, mas todos os *backups* incrementais subsequentes até o momento do incidente.

2 METODOLOGIA

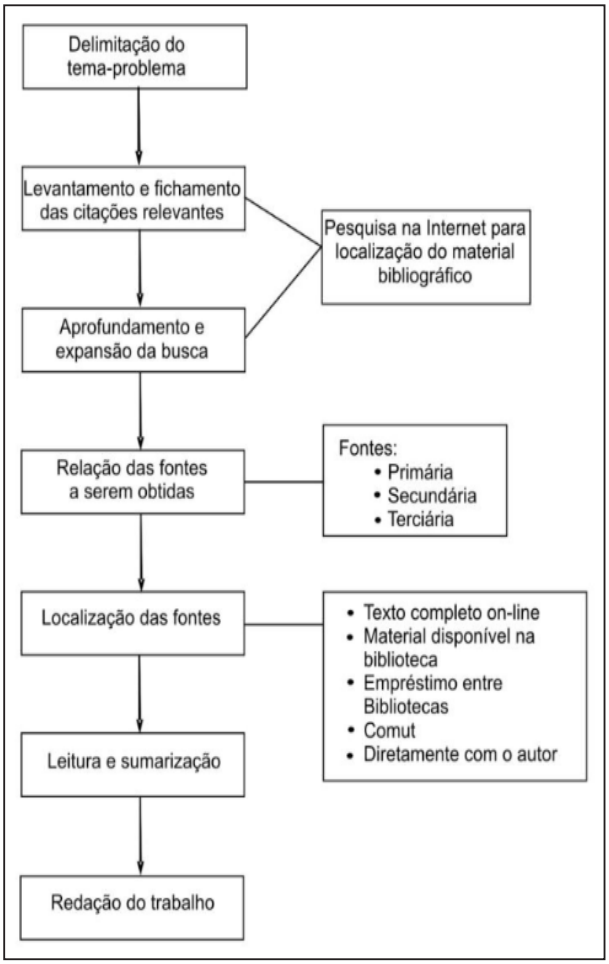
Além da pesquisa bibliográfica, o presente trabalho conta com a pesquisa aplicada sobre a implementação de uma solução de *backup* englobando software e política de retenção.

2.1 Pesquisa Bibliográfica

Segundo Pizzani (2012), a pesquisa bibliográfica pode ser entendida como a revisão da literatura sobre as principais teorias que norteiam o trabalho científico e é base fundamental de uma pesquisa, a mesma pode ser realizada em livros, periódicos, artigos de jornais, sites da internet entre outras fontes.

Conforme ilustrado por Pizzani (2012), para ser realizada com sucesso, alguns passos podem ser seguidos para facilitar a dinâmica para se obter a informação necessária durante a pesquisa bibliográfica, conforme ilustra a Figura 1.

Figura 1 - Processo de coleta da informação para pesquisa bibliográfica.



Fonte: Pizzani (2012).

2.2 Pesquisa Aplicada

A pesquisa aplicada concentra-se em torno dos problemas presentes nas atividades das instituições, organizações, grupos ou atores sociais. Ela está empenhada na elaboração de diagnósticos, identificação de problemas e busca de soluções. Responde a uma demanda formulada por "clientes, atores sociais ou instituições" (THIOLLENT, 2009). Segundo Fleury (2016) a pesquisa aplicada pode ser definida como conjunto de atividades nas quais conhecimentos previamente adquiridos são utilizados para coletar, selecionar e processar fatos e dados, a fim de se obter e confirmar resultados, e se gerar impacto.

Baseado em Philereno (2017) o quadro 1 ilustra quais serão as ferramentas utilizadas durante o processo de coleta dos dados.

Quadro 1 - Instrumento de coleta de dados.

Instrumento de coleta de dados	Universo pesquisado	Finalidade do Instrumento
Observação Direta ou dos participantes	Definir conceitos e a arquitetura do ambiente de *backup* e armazenamento.	Obter um ambiente de *backup* funcional alinhado com a política implantada.
Documentos	Políticas de *Backup* anterior, caso exista, e procedimentos operacionais.	Documentos úteis para fins de auditoria e entendimento e operação do cenário de *backup* na empresa.

Fonte: Elaborado pelo autor (PHILERENO, 2017)

3 RESULTADOS E DISCUSSÃO

Os resultados desse estudo de caso são apresentados no Anexo A que ilustra a política de backup desenvolvida considerando fatores e limitações apresentados nessa seção.

3.1 Mapeamentos necessários

A abrangência e a frequência dos serviços de backup devem estar conforme os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, conforme instrui a norma NBR 27002 (ABNT, 2013).

Baseada nessa instrução, a governança de TI mapeia com as áreas do negócio toda a informação gerada levando em consideração a criticidade da informação e o tempo necessário de retenção para esses dados. Após a definição do tempo de retenção e de quais informações as cópias de segurança devem ser realizadas, a TI mapeia seu ambiente ilustrando seus servidores responsáveis por aplicações do negócio, servidores de arquivos, servidor responsável por alocar a ferramenta de *backup*, dispositivo de armazenamento local (*local storage*) e armazenamento em nuvem (*cloud storage*).

Por fim, são detalhados os serviços de *backup* configurados na ferramenta seguindo o acordo feito entre as governanças visando continuidade do negócio.

4 CONSIDERAÇOES FINAIS

Após realizar o mapeamento e classificação das informações em conjunto com as áreas de negócio, levando em consideração a localização nos servidores de arquivos, bem como identificar o cluster de máquinas virtuais responsáveis pelos programas utilizados em toda a empresa, é possível concluir que a política de backup não é um mero documento do departamento de Tecnologia da Informação (TI), mas sim um documento de interesse amplo da organização.

Essa política garante o alinhamento estratégico entre as governanças de TI e do negócio, além de proporcionar o fator essencial que agrega valor a essa política: a segurança de todas as informações necessárias para a continuidade dos negócios em caso de perda.

4.1 Trabalhos futuros

A política de backup desenvolvida e implementada no presente artigo, conforme ilustrado no Anexo A, atende exclusivamente às necessidades do negócio no ambiente mapeado e apresentado no documento. No entanto, em caso de qualquer alteração no escopo mencionado, seja no âmbito do negócio, nos clusters de máquinas virtuais, nos dispositivos e tecnologias de armazenamento das cópias de segurança ou na ferramenta escolhida para gerenciar os backups gerados, torna-se necessário revisar e ajustar a política de backup com a aprovação das governanças envolvidas.

REFERÊNCIAS

ABNT, N. Iec 27002. (2013). Tecnologia da informação-Técnicas de segurança--Código de prática para controles de segurança da informação, 2013.

CAMPOS, André. **Sistema de Segurança da Informação**: controlando os riscos. 2 ed. Florianópolis: Visual Books, 2007.

FLEURY, Maria Tereza Leme; DA COSTA WERLANG, Sergio Ribeiro. Pesquisa aplicada: conceitos e abordagens. **Anuário de Pesquisa GV Pesquisa**, 2016. Disponível em: https://periodicos.fgv.br/apgvpesquisa/article/view/72796. Acesso em:7 de setembro de 2023.

GILLENSON, Mark L. **Fundamentos de sistemas de gerência de banco de dados**. Rio de Janeiro: LTC, 2006.

PHILERENO, Eduardo. *Backup*, *restore* e armazenamento: conceitos e práticas aplicados a solução hpe data *protector*. **Tecnologia em Gestão da Tecnologia da Informação-Unisul Virtual**, 2017. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/8978/1/Estudo%20de%20Caso%20-%20Avalia%c3%a7%c3%a3o%20Final.pdf. Acesso em: 7 de setembro de 2023.

PIZZANI, Luciana et al. A arte da pesquisa bibliográfica na busca do conhecimento. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 10, n. 2, p. 53-66, 2012.

PURVIS, Walt. The hot new storage technology for 2011 is... tape? **Research Note**, Data Mobility Group, March, v. 1, 2011.

RODRIGUES, Wilson Flávio. **Análise dos procedimentos de *backup* dos institutos federais**. 2017. Dissertação de Mestrado. Universidade Federal de Pernambuco. Disponível em: https://repositorio.ufpe.br/handle/123456789/25612. Acesso em: 7 de setembro de 2023.

SANTOS, B. B. A. d. et al. ***Backup* corporativo com alta retenção:** subsídios para construção da arquitetura. Universidade Católica de Brasília, 2018. Disponível em: https://bdtd.ucb.br:8443/jspui/handle/tede/2616. Acesso em: 7 de setembro de 2023.

THIOLLENT, M. **Metodologia de Pesquisa--ação**. São Paulo: Saraiva. 2009

VENTURA, Magda Maria. O estudo de caso como modalidade de pesquisa. **Revista SoCERJ**, v. 20, n. 5, p. 383-386, 2007.

ANEXO A

1 OBJETIVO

O objetivo deste procedimento é estabelecer orientações para a elaboração de cópias de segurança sob a responsabilidade do departamento de Tecnologia da Informação dá, bem como estabelecer definições para circulação, acondicionamento e restauração em caso de desastre.

2 APLICAÇÃO

Este procedimento aplica-se ao processo acima descrito, bem como aos colaboradores responsáveis pela execução do mesmo em todas as empresas vinculadas a Paul Wurth do Brasil.

3 DOCUMENTOS ASSOCIADOS

Não é aplicável.

4 DEFINIÇÕES

Desastre

Um evento de causa natural e/ou tecnológica que afeta a normalidade do funcionamento de ecossistemas provocando danos à infraestrutura de TI.

Políticas de Backup

Conjunto de orientações que indicam a localização e periodicidade dos trabalhos de Backup.

5 PROCESSO OPERACIONAL

5.1 Elaboração das Cópias de Segurança (Backups)

As cópias de segurança são executadas automaticamente por uma ferramenta (*Backup Exec* ou equivalente), que controla a consistência das seguranças e avisa ao profissional de tecnologia operador da ferramenta das anomalias detectadas.

Face à característica do sistema existem três tipos de políticas de armazenamento e retenção da informação:

Backup em Disco

- **R**etenção Semanal

2 Backups diários incrementais;

- **R**etenção Mensal

Backups totais de todo o servidor.

A retenção semanal garante a possibilidade de recuperação de informação num período de quatro semanas, de forma contínua, ou seja, as mídias são retidas por um período de um mês.

No primeiro e último finais de semana de cada mês é feita uma cópia de segurança total dos servidores, de forma que possibilite a recuperação total do servidor, sendo as cópias guardadas por um período de dois meses.

O serviço de restauração dos dados (*restore*) contidos no backup em disco deve ser testado a cada quinze dias, garantindo confiabilidade em caso de uso emergencial, visando evitar que processo de restauração ou backup falhe e cause irreparável dano ou perda dos dados.

***Backup* em Nuvem**

- **R**etenção Anual

Backups totais de todo o servidor.

- **R**etenção Mensal

Backups mensais incrementais;

No último final de semana do ano é feita uma cópia de segurança total do servidor, de forma que possibilite a recuperação total dos arquivos, sendo as cópias guardadas por um período que poderá variar de doze a sessenta meses, ou seja, de 1 a 5 anos.

A retenção Mensal garante a possibilidade de recuperação de informação em um período de um a 5 anos, de forma contínua, ou seja, as mídias incrementais serão retidas por um período de um ano ou até o próximo *backup* anual em nuvem.

O serviço de restauração dos dados (*restore*) contidos no *backup* em nuvem deve ser testado a cada trinta dias, garantindo confiabilidade em caso de uso emergencial, visando evitar que processo de restauração ou backup falhe e cause irreparável dano ou perda dos dados.

Disaster Recovery

- Retenção Semestral

Backups semestrais de imagens de todas as máquinas virtuais (VM's).

Na segunda sexta-feira de janeiro e na segunda sexta-feira de julho é feita cópia de segurança de todo o ambiente de máquinas virtuais de forma que possibilite a recuperação do ambiente em cenários de desastre. As imagens serão retidas por um período de seis (6) meses em que poderão ser substituídas por uma cópia de segurança mais recente.

O registo da execução das cópias de segurança encontra-se no sistema servidor de backups.

Os servidores alvo de cópia de segurança automática, estão identificados no próprio sistema de execução de *backup*.

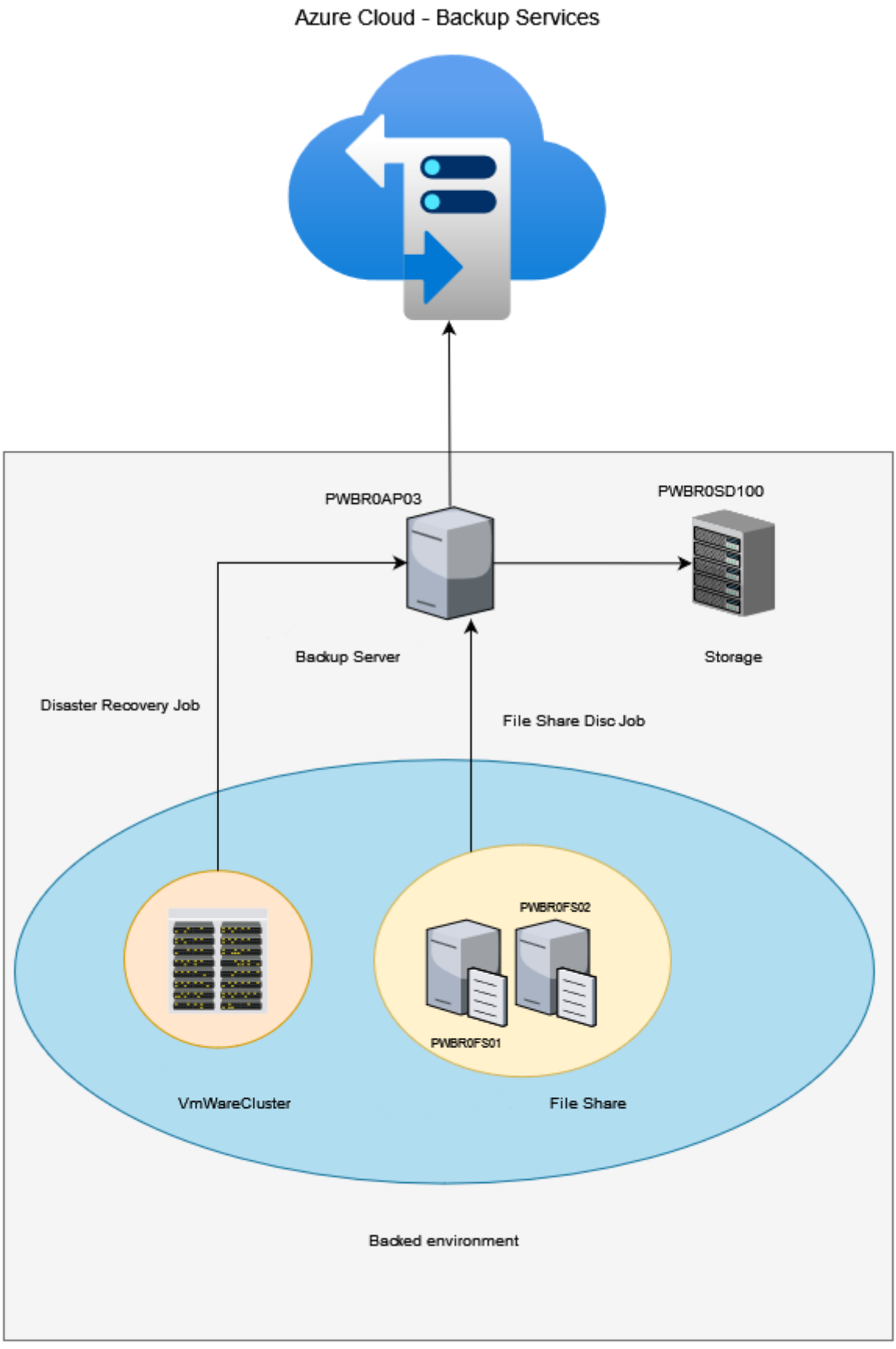
5.2 Acondicionamento e Circulação de Backups

Todos os Backups dos Servidores de cada um dos locais deverá ser armazenado em discos configurados com o devido sistema de redundâncias (RAID) em *data centers* apropriados.

Os Backups Mensais em disco são executados no primeiro fim de semana de cada mês, e logo em seguida replicados para o ambiente em nuvem por meio de *backups* incrementais ao último *backup* total em nuvem, permanecendo retido pelo período de 12 meses ou até o próximo backup total.

A figura seguinte, ilustra o processo de circulação e armazenamento dos backups:

Figura 2 – Processo de circulação e armazenamento dos backups



Fonte: autoria própria

5.3 Descrição das Políticas e trabalhos de Backup

A ferramenta responsável por executar e administrar as cópias de segurança, irá trabalhar rotineiramente com tarefas pré-configuradas chamadas de "políticas" ou "*Polices*". Cada Política poderá conter um ou mais "trabalhos" ou "*Job*" que irão conter as configurações de periodicidade, retenção e armazenamento das cópias de segurança.

Abaixo a relação atual de Políticas e Trabalhos e seus respectivos períodos de retenção.

Polices	Jobs	Storage Retention
PBR - Filesystem - SSMA		
	PBR SSMA Full	3 Meses
	PBR SSMA Incremental	4 Semanas
	PBR SSMA Full Cloud	5 Anos
	PBR SSMA Incremental Cloud	1 Ano
PBR - Filesystem - DP		
	PBR DP Full	3 Meses
	PBR DP Incremental	4 Semanas
	PBR DP Full Cloud	5 Anos
	PBR DP Incremental Cloud	1 Ano
PBR - Filesystem - GFC		
	PBR GFC Full	3 Meses
	PBR GFC Incremental	4 Semanas
	PBR GFC Full Cloud	5 Anos
	PBR GFC Incremental Cloud	1 Ano
PBR - Filesystem - Contratos		
	PBR Contratos Full	3 Meses
	PBR Contratos Incremental	4 Semanas
	PBR Contratos Full Cloud	1 Ano
	PBR Contratos Incremental Cloud	1 Ano
PBR - Filesystem - Proposta		
	PBR Propostas Full	3 Meses
	PBR Propostas Incremental	4 Semanas
	PBR Propostas Full Cloud	1 Ano
	PBR Propostas Incremental Cloud	1 Ano
PBR - Filesystem - AVEVA		
	PBR AVEVA Full	3 Meses
	PBR AVEVA Incremental	4 Semanas
	PBR AVEVA Full Cloud	1 Ano
	PBR AVEVA Incremental Cloud	1 Ano
PBR - Filesystem - Engineering		
	PBR Engineering Full	3 Meses
	PBR Engineering Incremental	4 Semanas
	PBR Engineering Full Cloud	1 Ano
	PBR Engineering Incremental Cloud	1 Ano
PBR - Filesystem - Legacy		
	PBR Legacy Full	N/A
	PBR Legacy Incremental	N/A
	PBR Legacy Full Cloud	1 Ano
	PBR Legacy Incremental Cloud	1 Ano
PBR - Filesystem - General		
	PBR General Full	3 Meses
	PBR General Incremental	4 Semanas
	PBR General Full Cloud	1 Ano
	PBR General Incremental Cloud	1 Ano
PBR - Filesystem - Userdata$		
	PBR Userdata$ Full	3 Meses
	PBR Userdata$ Incremental	4 Semanas
	PBR Userdata$ Full Cloud	1 Ano
	PBR Userdata$ Incremental Cloud	1 Ano

PBM - Filesystem - DP		
	PBM DP Full	3 Meses
	PBM DP Incremental	4 Semanas
	PBM DP Full Cloud	5 Anos
	PBM DP Incremental Cloud	1 Ano
PBM - Filesystem - SST		
	PBM SST Full	3 Meses
	PBM SST Incremental	4 Semanas
	PBM SST Full Cloud	5 Anos
	PBM SST Incremental Cloud	1 Ano
PBM - Filesystem - Controladoria		
	PBM Controladoria Full	3 Meses
	PBM controladoria Incremental	4 Semanas
	PBM Controladoria Full Cloud	5 Anos
	PBM Controladoria Incremental Cloud	1 Ano
PBM - Filesystem - Propostas		
	PBM Propostas Full	3 Meses
	PBM Propostas Incremental	4 Semanas
	PBM Propostas Full Cloud	1 Ano
	PBM Propostas Incremental Cloud	1 Ano
PBM - Filesystem - Contratos		
	PBM Contratos Full	3 Meses
	PBM Contratos Incremental	4 Semanas
	PBM Contratos Full Cloud	1 Ano
	PBM Contratos Incremental Cloud	1 Ano
PBM - Filesystem - General		
	PBM General Full	3 Meses
	PBM General Incremental	4 Semanas
	PBM General Full Cloud	1 Ano
	PBM General Incremental Cloud	1 Ano
PBR - Disaster Recovery		