UNIVERSIDADE DE CAXIAS DO SUL

ÁREA DO CONHECIMENTO DE CIÊNCIAS EXATAS E ENGENHARIAS

MARCO ANTONIO SIRTOLI

ANÁLISE COMPARATIVA DE FERRAMENTAS DE BACKUP

CAXIAS DO SUL

2022

MARCO ANTONIO SIRTOLI

ANÁLISE COMPARATIVA DE FERRAMENTAS DE BACKUP

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Orientador Prof. Giovanni Ely Rocco.

CAXIAS DO SUL

2022

MARCO ANTONIO SIRTOLI

ANÁLISE COMPARATIVA DE FERRAMENTAS DE BACKUP

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Aprovado em: __/__/__.

Banca Examinadora

_____

Prof. Giovanni Ely Rocco

Universidade de Caxias do Sul

_____

Prof. Marcos Eduardo Casa

Universidade de Caxias do Sul

_____

Prof. Dra. Maria de Fátima Webber do Prado Lima

Universidade de Caxias do Sul

AGRADECIMENTOS

Agradeço primeiramente aos meus pais e ao meu irmão, Sérgio, Vani e Sergio Júnior por sempre estarem me apoiando e acreditando em mim, sendo essencial para minha trajetória.

Agradeço aos meus amigos, familiares e demais pessoas que me apoiaram, contribuindo na concretização deste objetivo.

Agradeço também ao Prof. Giovanni Ely Rocco por ser responsável na orientação deste trabalho, dando total suporte e apoio nesta etapa. Também sou grato aos demais professores.

RESUMO

Nos dias atuais o mercado de software possui diversas ferramentas de backup gratuitas, com isso, torna-se importante a análise dessas ferramentas para avaliar se são efetivas para a utilização em empresas. O escopo deste trabalho tem como objetivo selecionar e analisar ferramentas de backup gratuitas através do método comparativo com uma ferramenta de backup paga. Para esta análise comparativa, este trabalho propõe um processo com base nas normas da série ISO/IEC 25000, realizado em duas etapas, de análise quantitativa sobre todas as ferramentas selecionadas, e de avaliação qualitativa sobre as melhores ferramentas qualificadas. As ferramentas que obtiveram destaque na avaliação quantitativa, sendo elas a Acronis, Bacula e Veeam foram selecionadas para teste na avaliação qualitativa. Nos testes realizados a ferramenta gratuita Veeam mostrou ser eficaz para utilização empresarial em comparação com a ferramenta paga Acronis.

Palavras-chave: Ferramentas de backup. Gestão de TI. Avaliação de ferramentas de backup. ISO/IEC 25040.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ISO	Organizações Internacionais de Normalização
IEC	Comissão Eletrotécnica Internacional
CID	Confidencialidade Integridade Disponibilidade
RPO	Objetivo do ponto de recuperação
RTO	Objetivo de tempo de recuperação
NAS	Armazenamento anexado à rede
AMANDA	Arquivador de disco de rede automático avançado de Maryland
TI	Tecnologia da Informação

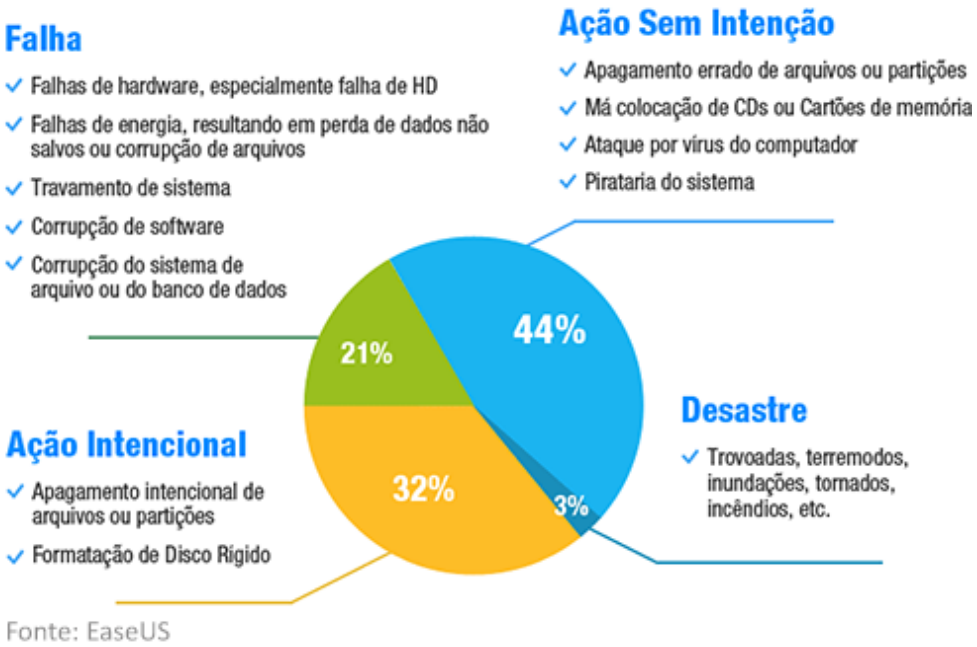
LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A tecnologia vem crescendo de forma mais rápida ao passar dos anos, gerando grande quantidade de informação pelas empresas e usuários. Com isso, tornou-se necessário atentar-se ainda mais ao salvamento das informações. Os dados de uma corporação são como ativos empresariais que demandam preservação para a continuidade da empresa, perder esses dados representa a perda de capital (FIALHO, 2007).

Figura 1 - Principais motivos de perda de dados



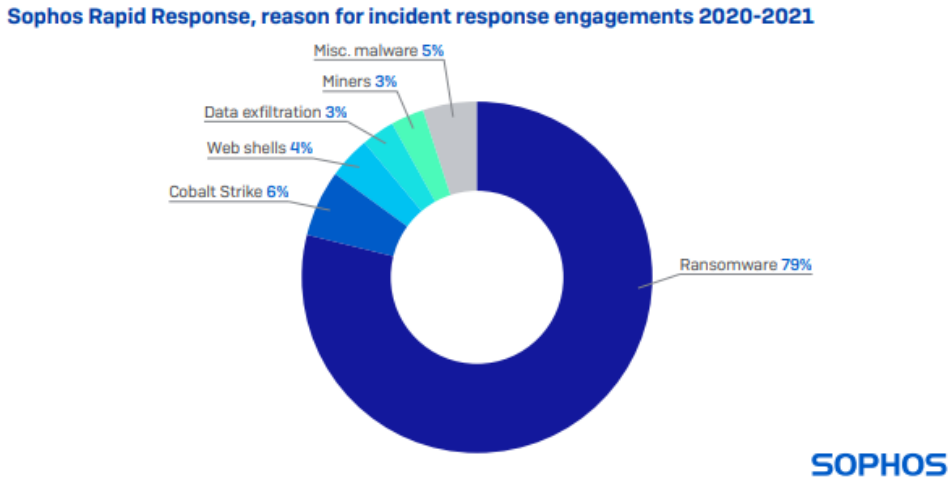
Fonte: Ease Us (2022).

Na Figura 1, uma pesquisa realizada pela empresa EaseUs mostrou que 44% das perdas de dados ocorrem por ações sem intenção, como apagar arquivos ou partições erradas, ataques por vírus ou má colocação de CDs ou cartões de memória no dispositivo; 32% em ação intencional (formatar o disco rígido, apagar intencionalmente os arquivos ou partições); 21% em falhas (hardware defeituoso, problema de energia, corrupção de software) e 3% em desastres (trovoadas, terremotos e incêndios).

A perda de dados pode causar diversos problemas financeiros e operacionais para uma empresa e há várias situações que podem causar essa perda. As principais delas são: invasões; malwares; falhas de equipamentos; desastres naturais; incêndios; falhas de usuários. Na figura 2, a empresa que presta serviços e

desenvolve ferramentas na área da segurança da informação, Sophos (2021), exibiu as principais ameaças detectadas no período de 2020 e 2021.

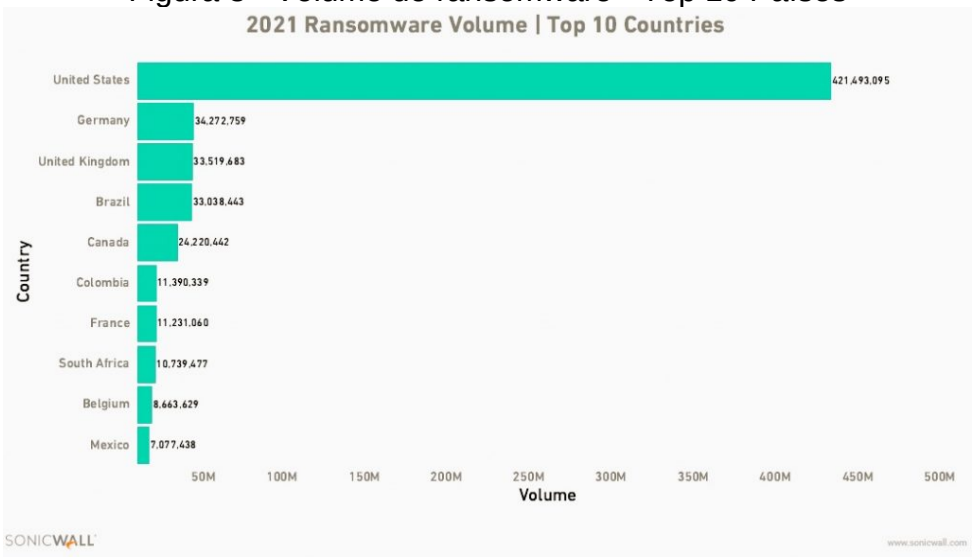
Figura 2 - Relatório de Ameaças 2020-2021



Fonte: Sophos (2021).

Conforme o relatório exibido na Figura 2, é possível identificar que no período de 2020 e 2021 houve uma grande quantidade de incidentes registrados do malware ransomware. Esse vírus criptografa os dados do computador que é infectado e realiza extorsão virtual da vítima, solicitando um valor em criptomoedas para o resgate. Conforme o relatório da SonicWall (2022), em 2021 já somam 623,3 milhões de ataques globalmente (Figura 3).

Figura 3 - Volume de ransomware - Top 10 Países



Fonte: SonicWall (2022).

Nesse contexto, ferramentas de backup são fundamentais para auxiliar as empresas na conservação e recuperação de dados que foram perdidos, em conjunto com a segurança da informação, com a finalidade de manter os dados íntegros, confiáveis e seguros. Deste modo, independentemente da forma de como ocorre a perda dos dados, um backup eficiente é aquele que minimiza os impactos causados, possibilitando a restauração do serviço no menor tempo possível e com o mínimo de defasagem em alteração de informações (FARIA, 2010).

Segundo Goodrich e Tamassia (2013), na segurança da informação, há três princípios que devem ser seguidos: confidencialidade, integridade e disponibilidade, que são definidos pelo termo C.I.D. A confidencialidade é evitar a exibição não autorizada da informação, tendo como base a proteção dos dados de quem não deve ter acesso. A integridade é a propriedade de que a informação não foi alterada de maneira não autorizada. A disponibilidade é a propriedade da informação ser acessível e modificável a aqueles que possuem acesso, no momento que for necessário sem quaisquer interrupções. Com isso, as ferramentas de backup e uma boa gestão de TI devem seguir estes princípios para minimizar as perdas de dados e assegurar que eles permanecem seguros, íntegros e disponíveis para os usuários.

1.1 PROBLEMA DE PESQUISA

Levando em consideração que ao longo do crescimento tecnológico as empresas possuem grande quantidade de dados para armazenar. Deste modo, tornou-se necessário proteger ainda mais os dados de ataques cibernéticos, desastres naturais e problemas mecânicos. Com isso, diversas desenvolvedoras de ferramentas de backup exibem suas soluções no mercado de forma gratuita, gerando dúvidas se são realmente efetivas para a aplicação em empresas, em comparação com uma ferramenta paga que se responsabiliza pela sua efetividade.

Diante deste contexto, as ferramentas de backup gratuitas serão avaliadas para comprovar sua efetividade para o uso empresarial, como uma ferramenta paga de alto nível pode proporcionar em casos de backup e recuperação de dados.

Questão de pesquisa: Existe(m) ferramenta(s) de backup gratuita(s) que possui(em) a eficácia de uma ferramenta de backup paga para uso empresarial?

1.2 OBJETIVO

O objetivo do trabalho é analisar e selecionar ferramentas de backup que sejam adequadas para o uso empresarial. No escopo deste objetivo a proposta é avaliar ferramentas gratuitas em relação à uma ferramenta paga, tendo como validação dessa avaliação comparativa o uso de critérios previamente estabelecidos com uma aplicação em um estudo de caso.

1.3 METODOLOGIA

A metodologia consiste no estudo teórico que abrange e explora a literatura disponível sobre o tema a ser estudado. No escopo deste projeto pode ser dividida em 5 etapas, sendo elas:

a) 1ª Etapa: Estudar os tipos de backup no uso empresarial, com objetivo de identificar seus benefícios e qualificações que uma ferramenta de backup precisa para realizar suas tarefas com eficiência.

b) 2ª Etapa: Definir quais ferramentas de backup disponibilizadas gratuitamente serão analisadas e testadas, e escolher o software pago para atuar como referência de comparação. Será feita a definição através de estudos de ferramentas que se adéquam a proposta do trabalho.

c) 3ª Etapa: Estabelecer um processo comparativo de avaliação das ferramentas, de acordo com a norma ISO/IEC 25040.

d) 4ª Etapa: Definir os critérios comparativos e avaliar as ferramentas de backup selecionadas em relação a ferramenta de referência.

e) 5ª Etapa: Aplicar as ferramentas selecionadas na etapa anterior em um estudo de caso a fim de validar o processo comparativo e a adequação das ferramentas selecionadas.

1.4 ESTRUTURA DO TRABALHO

O capítulo 2 apresenta um resumo sobre backup, contemplando os dispositivos de backup utilizados e seus tipos de backup. Além da seleção das ferramentas gratuitas e a seleção da ferramenta paga de backup que será utilizada como comparação.

O capítulo 3 apresenta as normas ISO que servem de fundamentação e orientação para estabelecer um processo de seleção de software, informando sobre as normas ISO/IEC 14598 (substituída pela ISO/IEC 25040) e a norma ISO/IEC 9126 (substituída pela 25010). Além de descrever o modelo de qualidade do produto de software pela sua hierarquia e as atividades de processo de seleção de software conforme a ISO/IEC 25040.

O capítulo 4 apresenta a proposta de solução do trabalho, definindo os critérios de medições em base do processo de seleção da ISO/IEC 25040 e os critérios de qualidade da ISO/IEC 25010. Sendo efetuado processo de avaliação quantitativo através do quadro de avaliações pelos critérios de qualidade e selecionando ferramentas com maior pontuação para testes na avaliação qualitativa. Com o intuito de validar se as ferramentas com maior pontuação têm a eficácia para implantação em empresas.

2 FUNDAMENTAÇÃO TEÓRICA

As cópias de segurança, ou backup, na computação são formas importantes para evitar eventuais perdas de dados. Este método é a melhor forma de recuperação, já que os dados podem voltar para o disco quando necessário. No meio corporativo, os dados são alterados com frequência e precisam ser salvos com uma determinada regularidade para que caso ocorra alguma perda o impacto seja o mínimo possível, levando em consideração a quantidade de informações a serem processadas em um sistema de pequeno, médio ou grande porte (FIALHO, 2007).

No ambiente corporativo, os gestores de TI precisam implementar uma rotina eficiente e uma infraestrutura de TI sólida para o processo de recuperação de dados ser otimizado, sem causar danos severos à produtividade da empresa em casos que necessite a paralisação. Com isso, é necessário definir um RPO e RTO adequado de acordo com a necessidade da corporação.

Segundo Gazola (2019), RPO é uma sigla em inglês para *Recovery Point Objective,* que irá definir a tolerância de dados que uma empresa pode perder em casos de um incidente de pane ou paralisação. Sendo assim, caso uma empresa possuir uma rotina de backup diário no fim do expediente (18:00 horas) e um incidente no servidor ocorrer no começo da tarde (13:00 horas), o ponto de recuperação será às 18:00 horas do dia anterior, possuindo um RPO de 19 horas.

O RTO é uma sigla em inglês para *Recovery Time Objective,* que irá definir o tempo máximo que a empresa levará para voltar operar após um incidente. Conforme a empresa de tecnologia Eveo (2021), o gestor de TI e sua equipe serão encarregados de identificar as prioridades da empresa, as perdas de lucratividade, produtividade e eficiência quando cada situação ocorrer. As prioridades da estrutura do negócio deverão ser colocadas com um RTO menor e questões menos prioritárias com o RTO maior.

Dependendo da área de negócio, as interrupções dos serviços sem um retorno esperado podem causar diversos problemas financeiros para organização. Em um estudo realizado pela Gartner (2014), o custo de inatividade dos serviços está entre US$ 5.600 por minuto, resultando em custos médios entre US$ 140.000 e US$ 540.000 por hora, dependendo da organização.

Para facilitar o cotidiano da gestão de TI, as soluções de backup transformam o procedimento massivo de salvamento dos dados em uma tarefa prática e

automatizada, poupando tempo da equipe. Uma tarefa que levaria horas a ser concluída manualmente pode ser executada com maior eficiência pelo software de backup, além disso, tendo um retorno com maior agilidade em casos de recuperações necessárias.

2.1 DISPOSITIVOS DE BACKUP

Segundo Faria (2010), os backups podem ser armazenados em diversos locais e dispositivos, sendo eles, armazenamento no mesmo servidor, armazenamento na rede e armazenamento externo. No que diz respeito ao armazenamento no mesmo servidor, é realizado o backup dentro de um disco rígido do próprio servidor a ser feito backup, com exceção da unidade onde salvará os backups. O risco da perda dos dados é alto pois, caso ocorra um malware no servidor ou um desastre, os backups podem ser afetados.

O armazenamento na rede, o backup é feito em um servidor externo dentro da mesma rede. Por exemplo, através de um dispositivo NAS (*Network Attached Storage*), que possui um firmware em operação destinado a armazenamento e gestão de backups, permitindo acoplar discos rígidos. Segundo uma empresa fabricante do dispositivo, Seagate (2022), os dispositivos NAS são importantes para pequenas empresas por serem opções de baixo custo, possuindo uma facilidade de uso elevada e permitirem crescimento. Também é possível realizar backups em um servidor físico destinado a backups, com sistema operacional Windows por exemplo.

O armazenamento externo é realizado o backup em um dispositivo externo, como HD externo na USB, fita magnética ou em um servidor remoto/nuvem. No que diz respeito a HD externo, ele é acoplado na USB do dispositivo de armazenamento, tornando possível o acesso à unidade de disco para realização dos backups. No caso das fitas magnéticas, elas são acopladas em uma unidade de fitas no dispositivo de armazenamento e são reconhecidas pelo software de backup. O servidor remoto é um servidor fora do ambiente da empresa, que os backups são enviados através de comunicação da internet, podendo ser uma filial da empresa ou um servidor terceiro, também pode ser considerado como armazenamento em nuvem.

Os backups realizados podem ser armazenados em diferentes dispositivos e locais dependendo da necessidade, diminuindo ainda mais as chances de ocorrer a perda dos dados. Contudo, é importante salientar que para evitar a perda total dos

dados da empresa em casos extremos (desastres), deve-se armazenar os backups em um local externo (nuvem ou dispositivo removível) e levar periodicamente para fora da empresa. É comum ocorrer em ambientes corporativos o descuido de deixar o HD externo no local onde foi realizado o backup, criando um risco de ser danificado em um possível desastre. Sendo assim, perdendo todas as informações mesmo com o backup realizado, por negligência do responsável ao não guardar o dispositivo longe do local afetado.

2.1.1 Fita magnética

Segundo a fabricante Dell (2021), fitas magnéticas (Figura 4) são cartuchos utilizados para armazenagem do backup. São mais resistentes a choque do que unidades de disco, pois possuem poucas peças móveis, tendo assim mais chances de estarem funcionais caso ocorra algum impacto. As fitas não possuem cabeça de unidade interna e nem eixos a serem quebrados.

Esse tipo de armazenamento possui o formato compacto e uma vantagem de estratégia de backup, o armazenamento fora do local, sendo uma ótima opção para isolar os dados como uma mídia off-line portátil. As fitas magnéticas garantem a recuperação dos dados longe do local afetado por um desastre, por exemplo, um incêndio, enchente ou furacão. Outro ponto positivo é a data de validade, sendo as atuais do mercado com data de validade de aproximadamente 20 anos, muito maior que discos rígidos que possuem mais peças móveis que se deterioram com maior facilidade. As fitas não possuem energia para ser armazenada, sendo necessário apenas no momento da restauração para o acesso aos dados armazenados (DELL, 2021).

Figura 4 - Fita Magnética Dell

Fonte: Lto Fitas e Drives LTO Ultrium (2022)

As fitas magnéticas oferecem uma forma segura e confiável de proteção de dados, onde possui uma chance maior de arquivamento criado antes da infecção, permitindo a restauração sem vírus. Além disso, caso ocorra uma cópia de um vírus em uma fita magnética, os vírus copiados não podem infectar os demais dados da fita e nem outros backups da biblioteca.

Contudo, as fitas magnéticas possuem um preço elevado na sua aquisição, podendo ser o dobro ou triplo do valor de um disco rígido, não sendo uma boa escolha para ambientes de baixo custo. No que diz respeito à velocidade de acesso, as fitas magnéticas gravam os dados do início e de forma sequencial, a pesquisa de um dado leva mais tempo pois é necessário a leitura da fita inteira para localização da informação. Para a utilização das fitas magnéticas é necessário que o servidor possua uma unidade de fita compatível com o cartucho, elevando ainda mais o custo na implantação desse mecanismo (DELL, 2021).

2.1.2 Backup em nuvem

O método de backup em nuvem é uma forma moderna de armazenamento que elimina a necessidade de investimentos de meios físicos, como fitas magnéticas, unidades de armazenamento e movimentação física dos dados. (MANDIC, 2022). Segundo a empresa Norton (2021), atualmente vem sendo a forma mais segura de armazenamento, o backup em nuvem armazena os dados em um servidor remoto, conhecido popularmente como “nuvem”.

Segundo a empresa Platon (CHAVES, 2020), este método, por enviar o backup para um servidor externo, requer que todos os dados sejam criptografados para serem exclusivos ao uso dos responsáveis da empresa, sendo assim, quem não possuir a chave criptográfica não poderá acessá-los, tornando um “arquivo morto” a um operador não autorizado, como ocorre em invasões.

A utilização do backup em nuvem tende a crescer com o passar dos anos no meio da tecnologia. Através da evolução da internet, o envio de grandes quantidades de dados para servidores remotos vem se tornando comumente realizado pelas corporações. Segundo a revista online TI Inside (2020), no Brasil, durante o ano de 2021, cerca de 56% das empresas realizaram investimentos para a proteção de dados na nuvem e a tendência é que esse investimento chegue substancialmente a 70% das empresas brasileiras até o ano de 2023.

O backup em nuvem é realizado através de uma solução de backup que possui a funcionalidade. Geralmente enviando o backup para a nuvem da empresa em que é contratado o serviço, como a Google, Dropbox, Microsoft OneDrive, Amazon, Acronis, entre outras diversas empresas que prestam serviços em nuvem. O espaço a ser utilizado cabe ao plano de serviço ofertado por cada fornecedor.

O armazenamento em nuvem requer conexão de internet para o envio dos backups. Caso a empresa possua uma conexão de internet limitada será necessário adaptar para que a rotina de backup seja realizada fora do horário de trabalho, evitando que afete a navegação e operação dos demais serviços existentes. Caso contrário, o ideal é designar um plano de internet adicional ou considerar outras opções de backup existentes.

2.2 TIPOS DE BACKUP

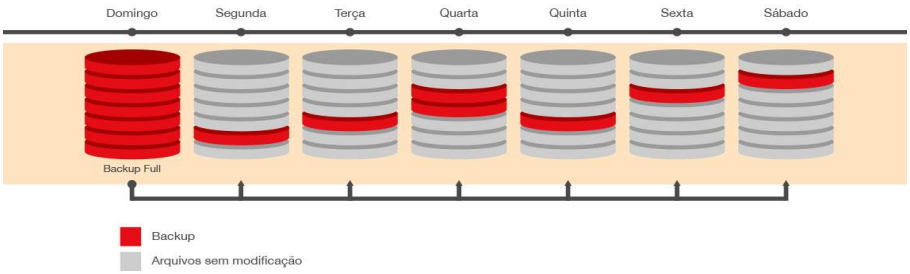
Os tipos de backup a serem utilizados dependerá da necessidade da empresa e dos RTO/RPO requeridos, sendo os principais classificados como: completo, incremental e diferencial (QNAP, 2019).

Realizar um backup completo significa efetuar a cópia de todos os dados pertencentes ao dispositivo. Os dados salvos incluem todos os arquivos de sistema, aplicativos e bibliotecas do sistema operacional em uma única operação. Este método de backup é a base para todos os outros tipos de backup, sendo através dele que outros tipos são implementados. Sua vantagem é possuir cópias idênticas do ambiente facilitando a localização dos dados que precisam ser recuperados. Em contrapartida, um backup completo tende a armazenar grandes quantidades de dados (COUGIAS, 2003).

O método de backup incremental realiza inicialmente um backup completo dos dados para que nas próximas vezes que rodar registre apenas as alterações efetuadas. Deste modo, evitando que armazene grande quantidade de dados sem a necessidade, como ocorre no método de backup completo, além de diminuir o tempo de backup que é realizado. Este método, possui como vantagem a economia de armazenamento e velocidade de compactação/gravação, porém como desvantagem caso necessite a restauração de algum arquivo perdido será exigido a restauração do último backup completo e todos os respectivos fragmentos de atualização gerados nos incrementos, aumentando risco de perda de dados (QNAP, 2019). Na Figura 5 há

uma representação de como é realizado o backup incremental, exibindo que no primeiro dia da semana é realizado o backup completo, e nos demais dias realizando o backup apenas dos incrementos.

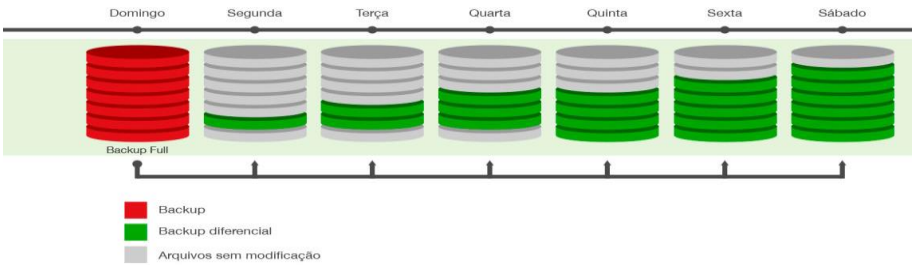
Figura 5 - Backup incremental



Fonte: QNAP (2019)

O backup diferencial tem como objetivo a minimização de riscos de perda de dados, tendo em vista a economia e velocidade. Este método inicialmente realiza um backup completo e posteriormente em cada backup diferencial compara o conteúdo com o primeiro backup efetuado, em seguida realizando as alterações necessárias. Maior quantidade de dados são gravadas a cada backup, por se tratar de fragmentos que possuem todas as diferenças entre o volume original e o atualizado. Este método é mais eficiente que o incremental, por exigir apenas o completo e o último fragmento para restauração dos dados (QNAP, 2019). Na Figura 6 há uma representação de como é realizado o backup diferencial, exibindo que no primeiro dia da semana é realizado o backup completo e nos demais dias realizando um backup apenas das diferenças.

Figura 6 - Backup diferencial



Fonte: QNAP (2019).

2.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO

O capítulo apresentou as definições gerais do backup a fim de exibir as suas funcionalidades, formas de armazenamento e ressaltar a necessidade de possuir soluções de backup no ambiente empresarial. Também foram apresentados diferentes tipos de backup que são considerados como funcionalidades essenciais em uma ferramenta de gerenciamento de backup.

3 PROCESSO DE SELEÇÃO DA FERRAMENTA DE BACKUP

Atualmente existem diversas ferramentas de backup disponíveis gratuitamente, exigindo um processo comparativo para escolha mais adequada. Para isso, é utilizado o processo de seleção da ferramenta de backup, que tem como base o estudo das normas ISO/IEC e suas orientações de avaliação. Com esse estudo, os parâmetros definidos pelas normas ISO fornecem a padronização da avaliação de software através de questões objetivas, simplificando o processo e aumentando a eficácia da seleção. Sendo utilizado modelos de aquisição e avaliação de software para aprimorar o processo de seleção, através das normas ISO/IEC 9126 (ABNT, 2003), ISO/IEC 14598 (ABNT, 2001) e o Guia de Aquisição do MPS.BR (SOFTEX, 2013).

A norma ISO/IEC 9126 estabelece um grupo de parâmetros com a finalidade de padronização e avaliação da qualidade de software. A ISO/IEC 14598, tem o objetivo de descrever o processo de avaliação de produtos de software, possuindo um modelo que diferencia três tipos de perspectivas de avaliação, sendo elas: desenvolvedor, adquirente e avaliador. O Guia de Aquisição do MPS.BR serve como um roteiro para as empresas que adquirem o Software e Serviços Correlatos (S&SC), através dele é feito um detalhamento dos processos envolvidos, representando os produtos de trabalho e contribuindo com informativos de como preencher os principais documentos.

Com o passar do tempo as normas foram atualizadas e aprimoradas, como ocorreu com a ISO/IEC 9126 e a ISO/IEC 14598, que foram substituídas pelas normas ISO/IEC 25010 (ISO/IEC; COMMISSION, 2011a) e ISO/IEC 25040 (ISO/IEC; COMMISSION, 2011b) respectivamente.

3.1 ISO/IEC 25010

A norma ISO/IEC 25010:2011 (ISO/IEC; COMMISSION, 2011a) foi lançada em 2011 através de uma atualização da norma ISO/IEC 9126-1. Foram acrescentadas novas características à ISO 25010. Sendo elas: oito características de qualidade de produto e 31 subcaracterísticas que na ISO 9126:2003 possui seis e 27, respectivamente, contendo a relação entre as propriedades de software. Além destas características adicionais foram acrescentadas compatibilidade, segurança e a

reorganização da hierarquia de características para melhor entendimento do processo.

Figura 7 - Modelo de Qualidade de Produto conforme ISO/IEC 25010:2011

Fonte: Adaptado ISO/IEC 25010.

Na Figura 7 é exibido a hierarquia do modelo de qualidade de produto, destacando que cada característica é composta por um conjunto de subcaracterísticas que se relacionam, podendo ser descritas conforme o resumo abaixo:

Adequação funcional: Possui o objetivo de representar o grau no qual um produto ou sistema fornece funções que correspondem às necessidades explícitas e implícitas, quando utilizado em condições específicas. A adequação funcional é composta por três subcaracterísticas: Integridade Funcional, Correção Funcional e Aptidão Funcional.

Eficiência de desempenho: Esta característica evidencia o desempenho em relação à quantidade de recursos utilizados em determinadas condições. É composta por três subcaracterísticas: Tempo, Utilização de Recursos e Capacidade.

Compatibilidade: Representa o nível no qual um produto, sistema ou componente possui a capacidade de trocar informações com outros, e/ou realizar funções exigidas, durante o período em que compartilha o mesmo ambiente de hardware ou software. Essa característica é composta pelas subcaracterísticas Interoperabilidade e Coexistência.

Usabilidade: É a característica que consiste na utilização de um produto ou sistema por usuários específicos para alcançar objetivos com eficácia, eficiência e

satisfação em um contexto específico. É composta por seis subcaracterísticas: Reconhecimento de Adequação, Apreensibilidade, Operabilidade, Proteção contra erro, Acessibilidade Proteção e Estética de Interface do Usuário.

Confiabilidade: Representa a execução de funções sob condições específicas em um sistema, produto ou componente, através de um período determinado. Composta pelas subcaracterísticas: Maturidade, Tolerância a Falhas, Recuperabilidade e Disponibilidade.

Segurança: Consiste na definição de proteção de informações e dados de um produto ou sistema, de modo que apenas o sujeito autorizado possa ter acesso aos dados de acordo com os níveis de autorização. Essa característica é composta pelas subcaracterísticas: Confidencialidade, Integridade, Não-repúdio, Responsabilização e Autenticação.

Manutenibilidade: Possui o objetivo de representar a efetividade no qual um produto ou sistema pode ser modificado para melhorias, correções ou adaptações de mudanças de ambiente e nos requisitos. É composta pelas seguintes subcaracterísticas: Analisabilidade, Modificabilidade, Testabilidade, Modularidade e Reutilização.

Portabilidade: Consiste na representação de efetividade no qual um produto, sistema ou componente pode ser transferido de um hardware, software ou outro ambiente operacional em uso para outro. É composta pelas subcaracterísticas: Adaptabilidade, Capacidade para ser instalado e Capacidade para substituir.

3.2 ISO/IEC 25040

A norma ISO/IEC 25000 possui uma divisão de avaliação de qualidade chamada ISO/IEC 2504n. As normas do grupo 2504n incluem os requisitos e recomendações para a avaliação de qualidade do produto de software e define os conceitos gerais, fornecendo uma descrição do processo de avaliação e estabelecendo requisitos para aplicação do presente processo. A norma ISO/IEC 25040 (ISO/IEC; COMMISSION, 2011b) é um modelo padronizado de avaliação, e fornece uma estrutura para avaliar a qualidade do produto de software para cada parte interessada, como desenvolvedores, adquirentes e avaliadores.

O método de avaliação na norma ISO/IEC 25040 é dividido em 5 atividades: estabelecer os requisitos de avaliação, especificar a avaliação, elaborar a avaliação, executar a avaliação e concluir a avaliação, conforme o Quadro 1.

Quadro 1 - Processo de seleção do software conforme ISO/IEC 25040

Estágios	Atividades	Tarefas
1º Estágio	Estabelecer os requisitos de avaliação	Determinar o objetivo da avaliação
		Obter os requisitos de qualidade do produto de software
		Identificar as partes do produto a serem incluídas na avaliação
		Determinar o rigor da avaliação
2º Estágio	Especificar a avaliação	Selecionar medidas de qualidade (módulos de avaliação)
		Determinar critérios de decisão para medidas de qualidade
		Determinar critérios de decisão para avaliação
3º Estágio	Elaborar a avaliação	Planejar atividades de avaliação
4º Estágio	Executar a avaliação	Obter as medições
		Aplicar critérios de decisão para medidas de qualidade
		Aplicar critérios de decisão para avaliação
5º Estágio	Concluir a avaliação	Analisar o resultado da avaliação
		Elaborar o relatório de avaliação
		Analisar a avaliação de qualidade e fornecer o feedback para a organização
		Realizar a disposição dos dados de avaliação

Fonte: ISO/IEC 25040 (2011), tradução do próprio autor (2022).

No primeiro estágio do quadro, é definida a atividade de estabelecer os requisitos de avaliação. Através desta atividade é determinado o objetivo da avaliação das ferramentas, obtenção dos requisitos de qualidade do produto de software, a identificação das partes do produto a serem incluídas na avaliação e a determinação do rigor da avaliação.

No segundo estágio, tem como objetivo a especificação da avaliação. Através desta atividade é selecionado as medidas de qualidade, determinado os critérios de decisão para estas medidas e a determinação dos critérios de decisão para a realização da avaliação.

No terceiro estágio, deve-se elaborar a avaliação. Através desta elaboração é definido o planejamento das atividades de avaliação para a sequência do projeto de comparação.

No quarto estágio, possui como objetivo a execução da avaliação. Nesta atividade busca-se obter as medições para avaliação, aplicar os critérios de decisão para as medidas de qualidade e os critérios de decisão para avaliação.

No quinto estágio, busca-se estabelecer a conclusão da avaliação. Esta atividade tem o objetivo de analisar o resultado da avaliação, efetuar a elaboração do relatório de avaliação, a análise da avaliação de qualidade, fornecimento do feedback para a organização e por fim a realização da disposição dos dados de avaliação.

3.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO

O capítulo apresentou as normas ISO que servem de fundamentação e orientação para estabelecer um processo de seleção de software. Através da norma ISO/IEC 25010 é possível compreender as divisões de qualidade de produto com suas características e subcaracterísticas. E através da norma ISO/IEC 25040 é feito o processo de seleção e avaliação, por estágios, atividades e tarefas para o melhor entendimento da metodologia. Por meio deste estudo é possível efetuar a definição de critérios de avaliação e a sequência de avaliação de software.

4 PROPOSTA DE SOLUÇÃO

Através do estudo realizado no capítulo anterior, a proposta de solução será guiada pelos estágios de seleção de software, conforme o Quadro 1 da ISO/IEC 25040. As atividades no primeiro estágio consistem em estabelecer os requisitos de avaliação, com as tarefas a serem seguidas: determinar o objetivo da avaliação; obter os requisitos de qualidade do produto de software; identificar as partes do produto a serem incluídas na avaliação; determinar o rigor da avaliação.

Conforme o escopo do projeto, o objetivo proposto é de analisar e selecionar as ferramentas de backup para o meio empresarial. As ferramentas que serão definidas, possuem suas distribuições de forma gratuita e será aplicado o método comparativo com uma ferramenta de backup paga. Através dessa comparação, visa-se identificar as ferramentas que possuírem maior destaque pelas suas características e serem selecionadas para o teste de aplicação de estudo de caso em relação a uma ferramenta paga.

Conforme a ISO/IEC 25010:2011, há uma série de critérios de qualidade que compõem o produto de software. Através destes critérios descritos pela norma, a ferramenta de backup precisa disponibilizar funções que satisfaçam as necessidades de acordo com o cenário requerido; necessita manter um bom nível de desempenho quando utilizada em situações específicas; precisa possuir compatibilidade com sistemas operacionais mais utilizados nas empresas; necessita possuir funcionalidades de fácil compreensão, que não necessite de longos treinamentos de equipe de TI para o entendimento da ferramenta; realizar backups e restaurações com integridade dos arquivos, além de que caso ocorra algum erro durante o seu progresso permita retomar do ponto que parou; disponibilizar a segurança das informações salvas, com senha e criptografia para evitar acesso indevido aos dados.

4.1 SELEÇÃO DE FERRAMENTAS DE BACKUP

Existem inúmeras ferramentas de backup que visam automatizar e facilitar o procedimento de backup dos dados, sendo necessário realizar uma seleção prévia antes da aplicação do processo comparativo. Em uma organização, cabe ao profissional de TI identificar e selecionar qual se adequa melhor a seu ambiente empresarial, sendo paga ou não, garantindo que os dados sejam guardados com

segurança e disponibilidade. Foi selecionado algumas ferramentas disponíveis através de publicações em sites de tecnologia, efetuando a intersecção das mais citadas. Estes sites efetuam ranqueamento de ferramentas citando as mais bem definidas pelos autores. Também localizado as ferramentas no site GetApp (2022), que realiza a recomendação de ferramentas. A ferramenta Veeam Backup & Replication Community foi escolhida devido a empresa ser referenciada no Quadrante Mágico da Gartner. Abaixo as ferramentas gratuitas escolhidas para a avaliação:

- **Cobian Backup (COBIANSOFT, 2019)**: Ferramenta gratuita utilizada no sistema operacional Windows. Permite a criação de rotinas de backup automáticas e realiza backup em HD. Segundo a CobianSoft, desenvolvedora da solução, informa que é possível executá-lo como serviço ou como aplicação regular, suportando compressão e criptografia. Ferramenta citada nos sites de tecnologia Techtudo (2022), SoftDownload (2022) e oHub (2020), como uma das melhores ferramentas de backup gratuitas.

- **Veeam Backup & Replication Community (Veeam, 2022):** Ferramenta gratuita para até 10 cargas de trabalho, sendo máquinas virtuais, Windows, Linux, laptops, NAS, entre outros. Possui funcionalidade além de backup, como proteção contra ransomware, recuperação de dados ágil e simplificada. Empresa desenvolvedora citada no quadrante mágico da Gartner de 2022, conforme exibido na Figura 9. Também citada no site GetApp (2022), em recomendações de softwares para backup de servidores.

- **Bacula (2022):** Ferramenta gratuita e de código aberto, utilizada nos sistemas operacionais Windows, Linux (baseados) e MacOS. É desenvolvido pela empresa Bacula Systems e permite a realização de backups, restauração e administração através de uma plataforma de gerenciamento web. Ferramenta citada nos sites de tecnologia oHub (2020) e Hostone (2019), como uma das melhores ferramentas de backup gratuitas. Também citada no site GetApp (2022), em recomendações de softwares para backup de servidores.

- **AMANDA (2017):** Ferramenta gratuita e de código aberto, utilizada nos sistemas operacionais Windows, Linux (baseados) e MacOS. Possui a sigla

AMANDA do inglês *Advanced Maryland Automatic Network Disk Archiver*, no português Arquivador de disco de rede automático avançado de Maryland. A solução de backup permite a configuração de um servidor mestre para fazer o backup de vários hosts em rede, para unidades de disco, fitas ou mídias ópticas. Ferramenta citada nos sites de tecnologia oHub (2020) e Hostone (2019), como uma das melhores ferramentas de backup gratuitas.

- **Iperius Backup Free (2022)**: Ferramenta gratuita utilizada no sistema operacional Windows. Oferece função de realizar backup incremental em NAS, discos, USB e rede. Realiza compactação, execução de rotinas externas e filtros avançados. A ferramenta tem a possibilidade de configurar backup automático e notificações por e-mail. Ferramenta citada no site de tecnologia SoftDownload (2019) como uma das melhores ferramentas de backup gratuitas. Também citada no site GetApp (2022), em recomendações de softwares para backup de servidores.

- **Comodo Backup (2022):** Ferramenta gratuita utilizada nos sistemas operacional Windows. Como principais características oferece até 5 GB de armazenamento online gratuito, possui opção de gravar os dados de backup em mídia ótica, HD interno, externo e computadores na rede, possui funcionalidade de backup incremental e completo, agendamentos de backup. Ferramenta citada no site de tecnologia SoftDownload (2022) e no site da fabricante de software Wondershare Technology (2018) como uma das melhores ferramentas de backup gratuitas.

As ferramentas de backup gratuitas (Cobian, Veeam, Bacula, AMANDA, Iperius e Comodo) serão comparadas com a ferramenta de backup paga Acronis Backup. Conforme a empresa Acronis (2022), o Acronis Backup é uma ferramenta de uso corporativo utilizada no sistema operacional Windows e Linux, que está há 19 anos no setor, contemplando sua atuação em mais de 150 países. A solução fornece segurança e integridade do backup com gerenciamento web, criando relatórios através de mapas de proteção de dados e fornecendo automatização das rotinas com agendamentos personalizados. Além destas funcionalidades, ela oferece recuperação segura e armazenamento personalizado, com rotinas de backup em nuvem, local ou

em rede. A seleção desta ferramenta tornou-se viável ao escopo do trabalho devido a sua exibição no Quadrante Mágico da Gartner do ano de 2022, com assunto de Soluções de Software de Backup e Recuperação Empresarial, sendo classificada como uma solução visionária para o tema (Figura 8).

Figura 8 – Quadrante Mágico da Gartner 2022

Fonte: Gartner (2022)

No segundo estágio do processo de seleção de ferramentas de software, é necessário seguir a especificação da avaliação através das seguintes tarefas: selecionar medidas de qualidade (módulos de avaliação); determinar critérios de decisão para medidas de qualidade; determinar critérios de decisão para avaliação. As medidas de qualidade são embasadas no modelo de qualidade de produto da ISO/IEC 25010 (Figura 7). A característica de manutenibilidade não será incluída nos critérios de comparação, pois suas subcaracterísticas se referem a manutenção e modificações de software, no qual não cabe ao escopo do projeto.

A característica de adequação funcional contempla as subcaracterísticas de correção funcional, aptidão funcional e integridade funcional. Esta característica define

se a ferramenta possui as funcionalidades de backup: em nuvem, rede, HD externo, local, fita e agendamento de backup. Assim como, se realiza os tipos de backup: completo, incremental e diferencial. Esta característica é essencial e de grande importância para a avaliação das ferramentas, possuindo peso de alta criticidade no processo de avaliação.

A eficiência de desempenho é uma característica composta pelas subcaracterísticas de tempo. No que diz respeito a tempo, tem como objetivo determinar o grau em que a ferramenta irá responder com eficácia, em que tempos de resposta e taxas de processamento não afetem o rendimento e a realização dos backups realizados. Esta característica possui peso de alta criticidade no processo de avaliação, por ser essencial para o funcionamento adequado da ferramenta.

A característica de compatibilidade é definida pelas subcaracterísticas de coexistência e interoperabilidade, sendo que a coexistência é a determinação de que a ferramenta de backup permite coexistir com outras ferramentas no sistema operacional sem interrupções. E a interoperabilidade é a determinação que a ferramenta atue em conjunto com o sistema operacional, trocando informações, programação de rotinas de backup. Esta característica possui peso baixo de criticidade para avaliação da ferramenta, considerando que não afeta no processo de avaliação de funcionalidades na realização de backups.

A usabilidade é uma característica de qualidade composta pelas subcaracterísticas de estética da interface do usuário, operabilidade e aprendizagem. A subcaracterística de estética da interface do usuário é o grau de definição do que será exibido para o usuário no que diz respeito a estética da ferramenta de backup. A subcaracterística de operabilidade e aprendizagem define o grau de facilidade que o usuário tenha com a ferramenta, de tarefas do dia a dia, como realização de rotinas de backup, recuperação, ajuste de armazenamentos, entre outras funcionalidades. Esta característica possui peso baixo de criticidade para avaliação da ferramenta, pois não impacta no seu objetivo de funcionamento.

A característica de portabilidade, tem como subcaracterística a capacidade de ser instalado e possui o objetivo definir o grau em que a ferramenta de backup é compatível com os sistemas operacionais Windows e Linux. Esta característica possui peso baixo de criticidade para avaliação da ferramenta, devido a não impactar nas funcionalidades da ferramenta.

A característica de confiabilidade é composta pela subcaracterística de recuperabilidade, tolerância a falhas e disponibilidade. Em recuperabilidade, é a subcaracterística de qualidade que determina o grau que a ferramenta de backup retorne ao ponto que parou ao ocorrer falhas na operação de backup. Em tolerância a falhas é a garantia de execução da tarefa em caso de falhas. E em disponibilidade é poder contar com a ferramenta quando necessário. Esta característica possui peso médio de criticidade para avaliação da ferramenta, não afetando diretamente suas funcionalidades, porém é importante para sua qualificação possuir estes critérios.

Por fim, a característica de segurança possui a subcaracterística de confidencialidade, que tem como objetivo definir o grau que a ferramenta ou o backup esteja acessível apenas para quem estiver autorizado, com utilização de criptografia e senha, além de que seja permitido apenas cópias para dispositivos autorizados. Esta característica possui peso médio de criticidade pois não afeta diretamente em suas funcionalidades, porém é importante possuir segurança para evitar que os dados sejam acessados indevidamente.

No Quadro 2 é exibido as características descritas, com suas avaliações de criticidade, para a definição com mais precisão do que possui mais importância na avaliação para o escopo do projeto. Também definido o multiplicador de criticidade, o qual é utilizado na avaliação quantitativa.

Quadro 2 – Características com avaliação de criticidade e multiplicador

Característica	**Avaliação (Criticidade)**	**Multiplicador**
Adequação Funcional	Alta	3X
Eficiência de desempenho	Alta	3X
Confiabilidade	Média	2X
Segurança	Média	2X
Compatibilidade	Baixa	1X
Usabilidade	Baixa	1X
Portabilidade	Baixa	1X

Fonte: Próprio autor (2022).

Através destas avaliações são distribuídas as notas de “0”, “0,5” e “1”. Sendo “0” não atende, “0,5” atende parcialmente e “1” atende. As subcaracterísticas selecionadas são avaliadas com grau de criticidade baixo, médio e alto para definir a sua importância na avaliação. Através desta importância obtém o grau multiplicador (baixo: resultado multiplicado por 1; médio: resultado multiplicado por 2; alto: resultado multiplicado por 3). Por fim, é aplicado o multiplicador dos critérios das medidas de qualidade e calculado o total dos valores, através deste cálculo é definido as ferramentas escolhidas para testes de aplicação.

A avaliação das ferramentas de backup é realizada através das características de qualidade: Adequação funcional (critério de funcionalidade: Backup em nuvem, rede, HD externo, local, fita, completo, incremental, diferencial e agendamento de backup); Eficiência de desempenho; Compatibilidade; Usabilidade; Portabilidade; Confiabilidade; Segurança. As informações para o preenchimento do quadro de avaliação foram coletadas no site do desenvolvedor de cada ferramenta.

A ferramenta paga, Acronis, foi definida com a nomenclatura REF no Quadro 3 por se tratar de uma ferramenta de referência para as demais que são avaliadas no modo comparativo. As ferramentas gratuitas foram definidas com a primeira letra da palavra “ferramenta” e sua sequência numérica.

Quadro 3 – Nomenclatura das ferramentas no quadro de avaliação

Abreviação	**Ferramenta**
REF	Acronis Backup
F1	Cobian Backup
F2	Veeam Backup & Replication Community
F3	Bacula
F4	AMANDA
F5	Iperius Backup Free
F6	Comodo Backup

Fonte: Próprio autor (2022).

Para a montagem do quadro avaliativo (Quadro 4), os critérios de avaliação foram organizados em linhas, enquanto as ferramentas selecionadas em colunas. Foi definido uma coluna adicional nomeada de “CRT” que retrata o grau de criticidade de cada critério. Os nomes das ferramentas foram abreviados conforme o Quadro 3 para

melhor visualização. Cada coluna de ferramenta possui duas colunas adicionais em seu interior, sendo a primeira coluna a nota recebida e a segunda o resultado da sua multiplicação pelo fator de criticidade. No final do quadro é exibido o campo “Total” que retrata a soma de todos os valores da segunda coluna de cada ferramenta. Para o critério de Eficiência de desempenho foi inserido o caractere “*”, pois o mesmo não pode ser avaliado na avaliação quantitativa.

Quadro 4 - Avaliação de ferramentas

Critério	**CRT**	**REF**		**F1**		**F2**		**F3**		**F4**		**F5**		**F6**	
Backup em Nuvem	**3**	1	3	0	0	0	0	0	0	0	0	0	0	½	1,5
Backup em Rede	**3**	1	3	1	3	1	3	1	3	1	3	1	3	1	3
Backup em HD externo	**3**	1	3	1	3	1	3	1	3	1	3	1	3	1	3
Backup Local	**3**	1	3	1	3	1	3	1	3	1	3	1	3	1	3
Backup em Fita	**3**	0	0	0	0	1	3	1	3	1	3	0	0	0	0
Backup Completo	**3**	1	3	1	3	1	3	1	3	1	3	1	3	1	3
Backup Incremental	**3**	1	3	1	3	1	3	1	3	1	3	1	3	1	3
Backup Diferencial	**3**	1	3	1	3	0	0	1	3	0	0	1	3	1	3
Agendamento de backup	**3**	1	3	1	3	1	3	1	3	1	3	1	3	1	3
Eficiência de desempenho	**3**	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Compatibilidade	**1**	1	1	1	1	1	1	0	0	0	0	0	0	0	0
Usabilidade	**1**	1	1	½	½	1	1	½	½	½	½	½	½	½	½
Portabilidade	**1**	1	1	½	½	1	1	1	1	1	1	½	½	½	½
Confiabilidade	**2**	½	1	0	0	0	0	0	0	0	0	0	0	0	0
Segurança	**2**	1	2	½	1	1	2	½	1	½	1	½	1	½	1
Total		**30**		**24**		**26**		**26,5**		**23,5**		**23**		**24,5**	

Fonte: Próprio autor (2022).

Para a avaliação da funcionalidade de backup em nuvem foi estabelecido um critério de que se a ferramenta possui a funcionalidade receberá a nota “0,5” (atende parcialmente). Conforme uma pesquisa realizada pela empresa Qualyteam (2016), em sua base de dados de pequenos clientes no setor industrial, o armazenamento médio

é de 30 GB. Portanto, caso a ferramenta possuir a quantidade de armazenamento em nuvem superior ou igual a 30 GB receberá nota 1 (atende). A ferramenta que possui a funcionalidade de armazenamento em nuvem, atendendo ao critério, foi a Acronis Backup. Por se tratar de uma ferramenta avaliada paga foi considerado a funcionalidade de backup em nuvem pago. A ferramenta que possui a funcionalidade de forma gratuita foi a Comodo Backup, porém por disponibilizar apenas 5 GB de armazenamento em nuvem foi considerado como atende parcialmente, ganhando a nota “0,5”. O restante das ferramentas não possui armazenamento de backup em nuvem gratuito. Nas funcionalidades de backup em rede, backup em HD externo e backup local todas as ferramentas atendem os critérios. Em backup em fita as ferramentas Acronis, Cobian, Iperius e Comodo não atendem o critério estabelecido, o restante das ferramentas são atendidos com a funcionalidade. As funcionalidades de backup completo, incremental e agendamento de backups são atendidos por todas as ferramentas, backup diferencial não é atendido pelas ferramentas Veeam Backup e AMANDA Backup. Em agendamento de backups foi estabelecido que as ferramentas precisam ter a funcionalidade de definir um dia e horário para rodar os backups automaticamente sem a intervenção do usuário, tornando uma tarefa prática para a gestão de TI.

O critério de eficiência de desempenho não foi possível discriminar pois será avaliado o tempo de desempenho para realização de backups. Neste caso através das documentações de cada desenvolvedora não foram possíveis definir uma média de tempo para a tarefa, por se tratar de um processo que depende de testes para ser realizado. Este critério será avaliado posteriormente sobre as ferramentas que forem selecionadas nesta etapa para a avaliação qualitativa.

Em compatibilidade, a ferramenta Acronis possui a funcionalidade de serviço operando em conjunto com sistema operacional, em contrapartida, a ferramenta Iperius, na sua versão gratuita, informa que não é possível realizar sua instalação “como serviço” tornando inviável a interoperabilidade. As fabricantes das ferramentas Comodo, Bacula e AMANDA não informaram em suas documentações se possuem a funcionalidade.

Em usabilidade, todas as ferramentas possuem um painel gráfico para gerenciamento da ferramenta, sendo o controle de rotinas de backup, configurações da aplicação, manutenção, entre outros. Porém as ferramentas Cobian, Comodo,

AMANDA, Bacula e Iperium não descrevem em sua documentação a proteção contra erros de usuário.

Na avaliação de portabilidade, apenas as ferramentas Cobian, Comodo e Iperius possuem compatibilidade com um único sistema operacional, sendo o Microsoft Windows. O restante das ferramentas é compatível com pelo menos dois sistemas operacionais, sendo eles Microsoft Windows e Linux.

Na avaliação de confiabilidade apenas a ferramenta Acronis retoma ao ponto que parou caso ocorra um erro de backup, porém se restringe a apenas backup em nuvem, neste caso foi classificado como atende parcialmente, recebendo a nota de “0,5”. O restante das ferramentas não possui em suas documentações se existe essa funcionalidade.

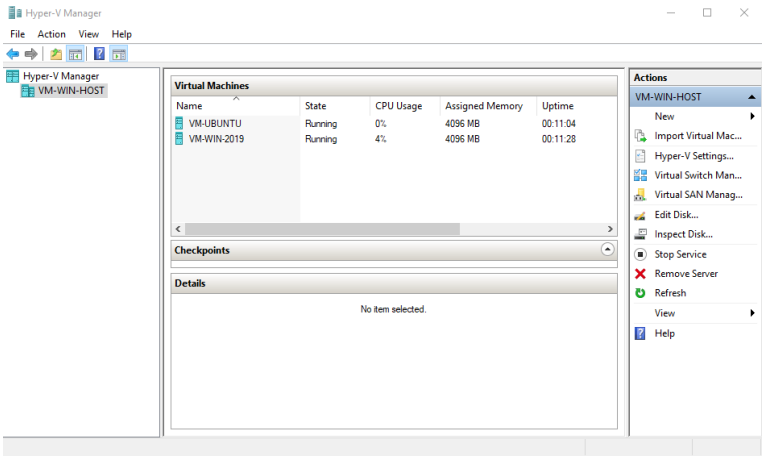
No critério de segurança, todas as ferramentas possuem um método de criptografia, porém as ferramentas Cobian, Comodo, Iperius possuem senha somente na geração do arquivo de backup, as ferramentas AMANDA e Bacula possuem senha na abertura da ferramenta. O restante possui duas camadas de segurança, sendo a primeira na aplicação e outra no arquivo de backup.

As ferramentas selecionadas para realização dos testes qualitativos foram a Acronis, Bacula e Veeam, por possuírem as maiores notas, sendo elas 30, 26.5 e 26, respectivamente. As demais ferramentas, Comodo, Cobian, AMANDA e Iperius, não foram selecionadas para os testes, pois receberam as notas 24.5, 24, 23.5 e 23, respectivamente.

4.1 PREPARAÇÃO DO AMBIENTE DE TESTES

Foi realizado a criação de duas máquinas virtuais no virtualizador Hyper-V do sistema operacional Windows Server 2019, sendo uma delas Windows Server 2019 e outra Linux Ubuntu 22.04.1 LTS (Figura 9). A máquina física utilizada possui um processador AMD Ryzen 5 2600 de 6 núcleos e 12 processadores lógicos, com velocidade base de 3,40 GHz; memória RAM de 16 GB DDR4; SSD de 240 GB para o host físico Windows Server 2019 e um disco rígido para armazenagem das máquinas virtuais de 2 TB de armazenamento.

Figura 9 – Hyper-V Manager



Fonte: Próprio autor (2022).

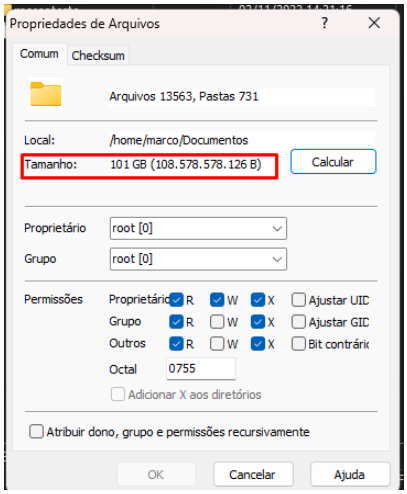
As máquinas virtuais foram definidas com uma configuração de recursos padrão para o funcionamento do sistema operacional e realização dos backups com uma base de dados definida, sendo as configurações:

- **VM-WIN-2019:**
  - Sistema operacional: Windows Server 2019 Standard;
  - Processador: 12 processadores virtuais;
  - Memória: 4096 MB;
  - Disco: 150 GB.

- **VM-UBUNTU:**
  - Sistema operacional: Linux Ubuntu 22.04.1 LTS;
  - Processador: 12 processadores virtuais;
  - Memória: 4096 MB;
  - Disco: 150 GB;

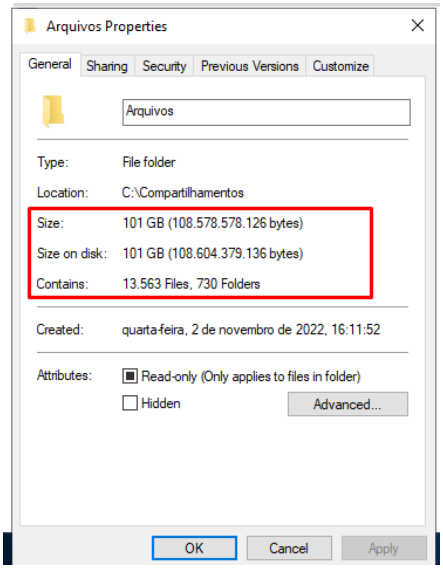
A base de dados escolhida para preencher o espaço de armazenamento das máquinas virtuais e ter dados para realização dos backups, simulando um ambiente corporativo, foram arquivos diversos de uso do próprio autor. Entre esses dados foram utilizados documentos, músicas, arquivos compactados e instaladores de software, totalizando cerca de 100 GB de armazenamento para cada máquina virtual, conforme a Figura 10 e Figura 11.

Figura 10 – Armazenamento Ubuntu



Fonte: Próprio autor (2022).

Figura 11 – Armazenamento Windows Server 2019

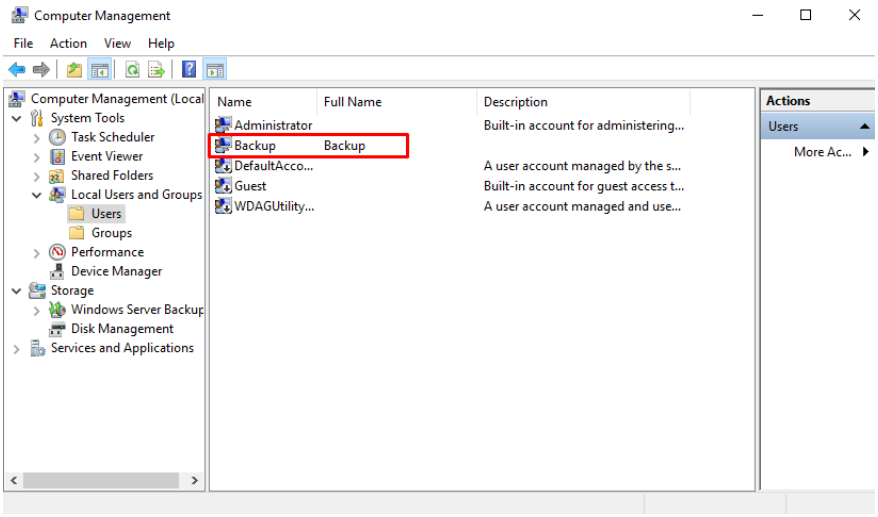


Fonte: Próprio autor (2022).

4.2 PREPARAÇÃO DO DESTINO DO BACKUP

Para a realização dos backups de forma eficiente e segura foi mantido um padrão para armazenagem dos backups realizados, sendo utilizado um HD externo de 500 GB e criado pastas compartilhadas para um usuário específico do sistema operacional. Realizado a criação de um usuário local no servidor host, nomeado de “Backup” conforme Figura 12.

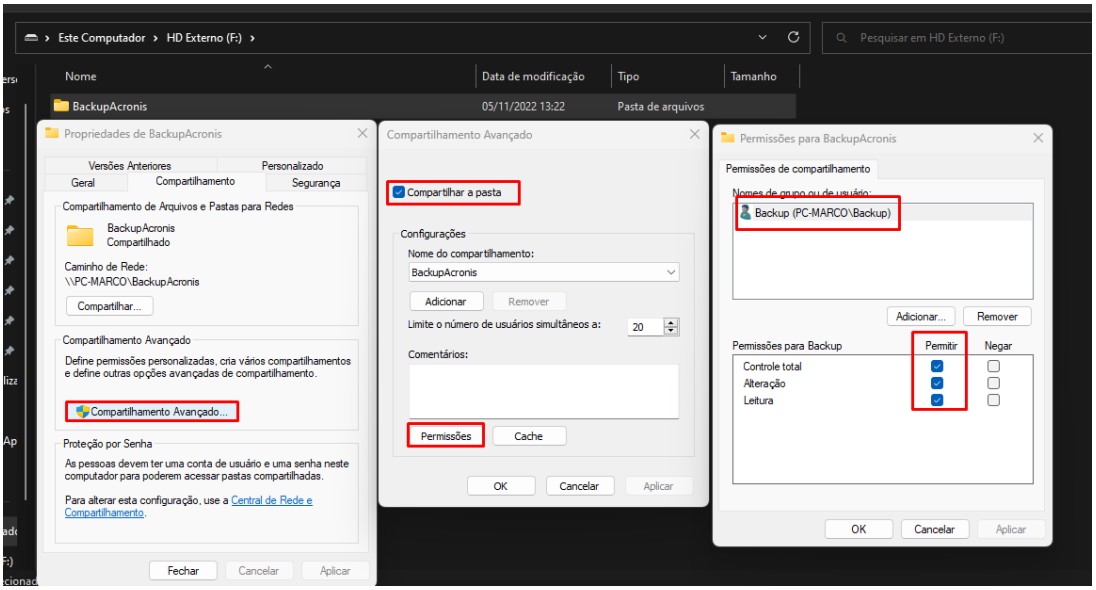
Figura 12 – Usuário backup servidor host



Fonte: Próprio autor (2022).

Realizado a criação de uma pasta chamada “BackupAcronis”, dentro do HD externo, sendo compartilhada para o usuário “Backup” criado anteriormente (Figura 13).

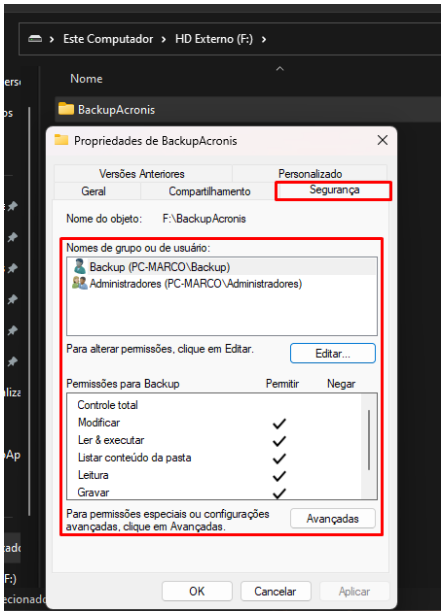
Figura 13 – Compartilhamento dos diretórios



Fonte: Próprio autor (2022).

Além disso, configurado as permissões da pasta para o usuário do backup e o grupo de administradores da máquina conforme Figura 14.

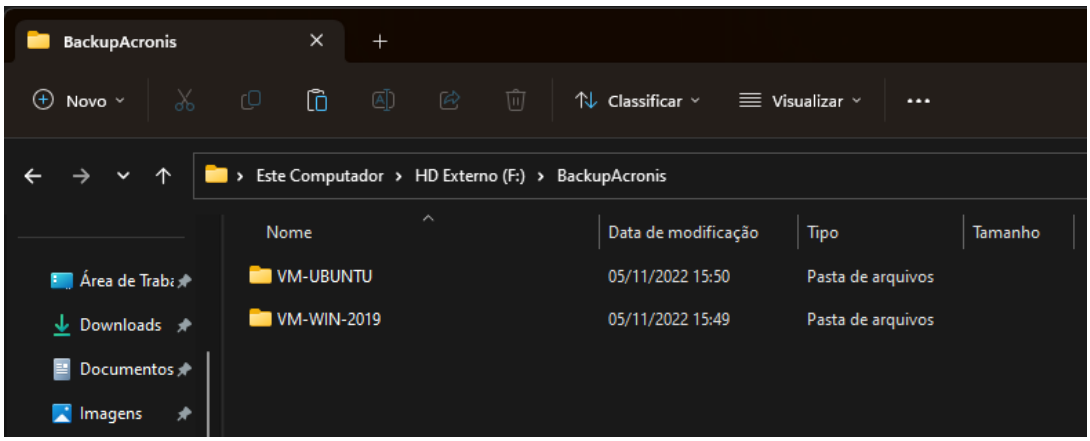
Figura 14 – Permissões de segurança pastas compartilhadas



Fonte: Próprio autor (2022).

Dentro da pasta “BackupAcronis”, criado mais duas pastas com o nome de cada máquina virtual, para organização dos backups (Figura 15).

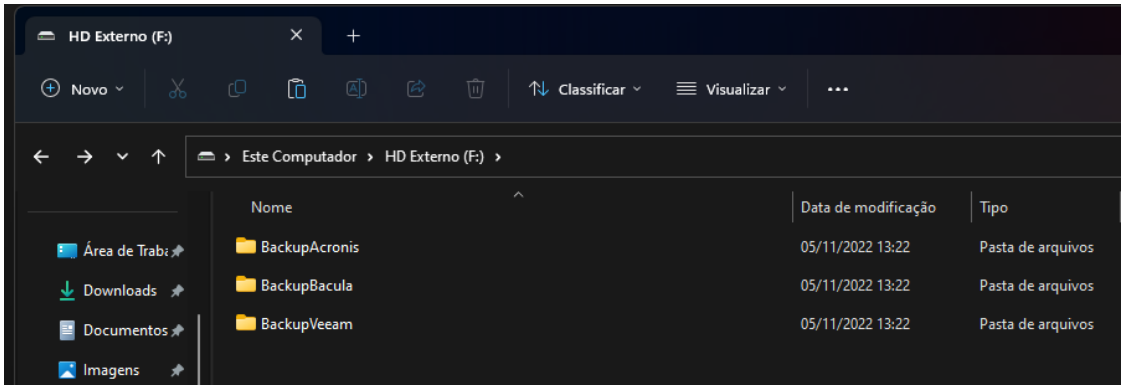
Figura 15 – Pastas criadas backup - Acronis



Fonte: Próprio autor (2022).

Este mesmo padrão de permissão e diretórios foi criado para as pastas de armazenamento de backup das ferramentas Veeam e Bácula (Figura 16).

Figura 16 – Diretório de pastas HD Externo



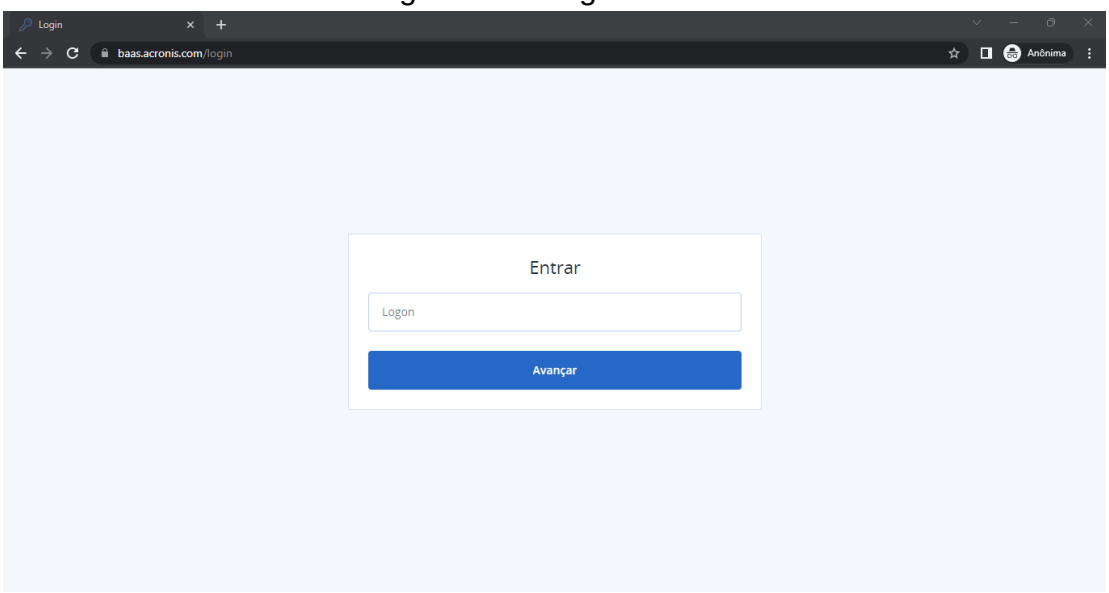
Fonte: Próprio autor (2022).

Este método de compartilhamento de pasta para um usuário de controle é uma forma eficiente de proteger os backups gerados em um ambiente de rede, pois caso uma máquina na rede seja invadida os backups não poderão ser acessados sem a permissão deste usuário.

4.3 ACRONIS CYBER PROTECTION

A ferramenta Acronis Cyber Protection, utilizada de referência, foi disponibilizada por forma de avaliação gratuita. Após a disponibilização do serviço, foi criado um acesso a console de gerenciamento web da ferramenta, com usuário e senha para autenticação (Figura 17).

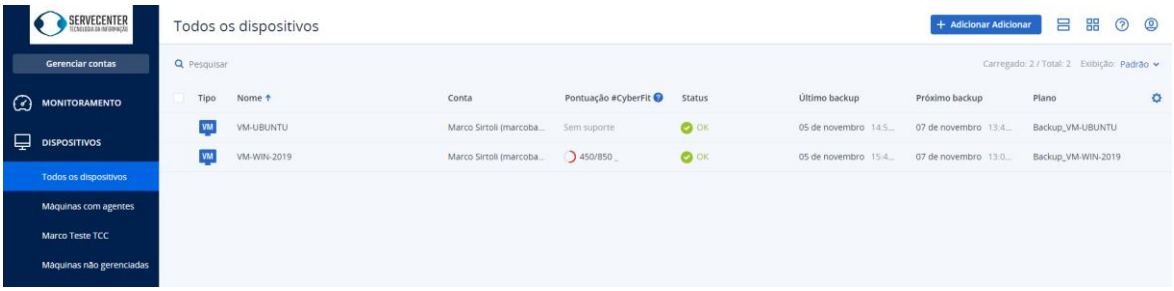
Figura 17 – Login Acronis



Fonte: Próprio autor (2022).

Após o login, foi necessário incluir as máquinas virtuais dentro do gerenciamento do portal, sendo realizado a instalação do agente de comunicação do Acronis conforme o manual do desenvolvedor. Assim que o agente de comunicação foi instalado em cada máquina virtual, elas passaram aparecer na console de gerenciamento do Acronis, conforme a Figura 18.

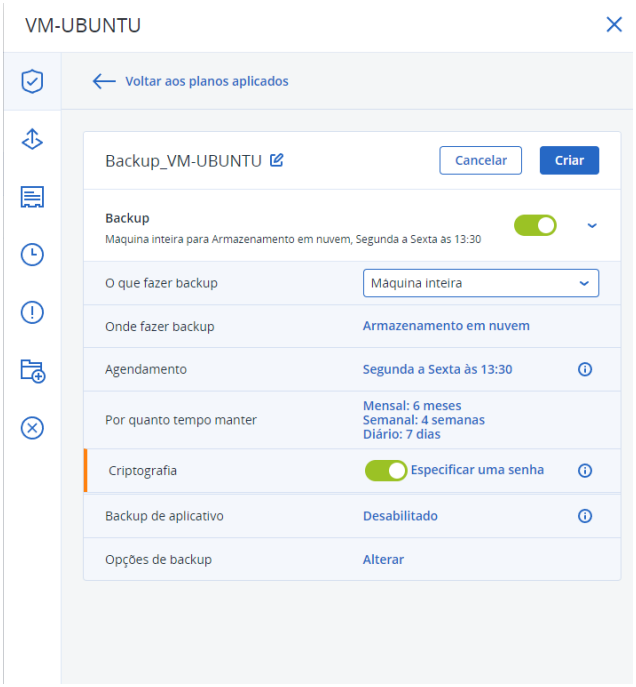
Figura 18 – Exibição dos dispositivos gerenciados no Acronis



Fonte: Próprio autor (2022).

Com as máquinas virtuais sendo exibidas na ferramenta, foi necessário realizar a criação das rotinas de backup. No menu principal de criação da rotina de backup (Figura 19) é exibido diversas opções importantes para a configuração do plano de backup, entre elas: o que fazer backup, onde fazer backup, agendamento, por quanto tempo manter, criptografia, entre outras configurações.

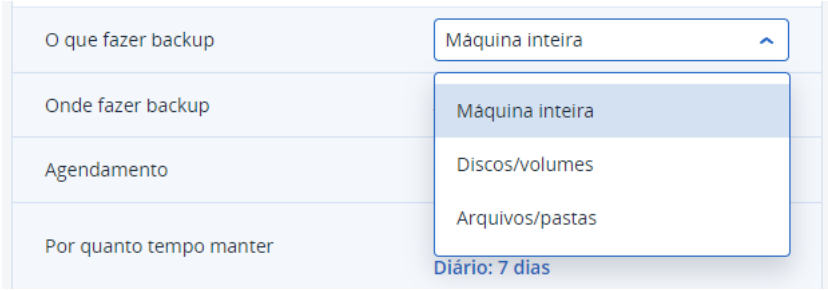
Figura 19 – Menu de criação da rotina de backup - Acronis



Fonte: Próprio autor (2022).

Na criação da rotina de backup é importante definir o que será realizado do backup, o Acronis permite três formas de realização, sendo elas: máquina inteira, discos/volumes, arquivos/pastas (Figura 20). No caso de máquina inteira, o estado de toda a máquina é gravado em um arquivo de backup, contendo todas as unidades de disco e arquivos existentes. Em discos/volumes é possível definir apenas os discos/volumes que deseja selecionar para realização do backup, a mesma lógica sendo seguida para arquivos/pastas.

Figura 20 – O que fazer backup - Acronis

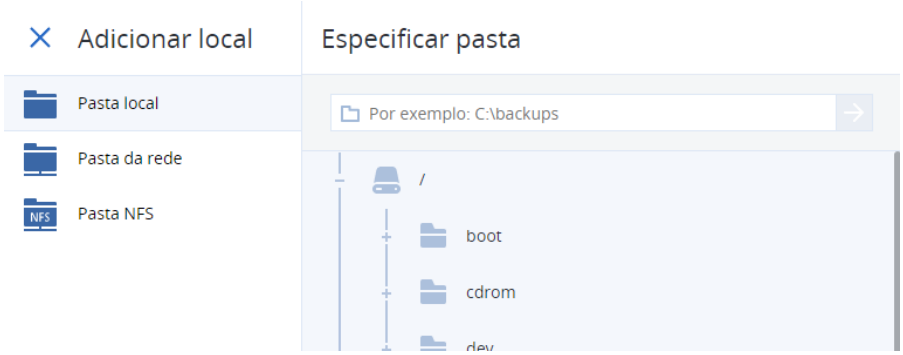


Fonte: Próprio autor (2022).

Para este teste foi definido que a máquina inteira seria o ideal a ser selecionado, pois em um ambiente corporativo é desejável que em casos de desastres tenha um backup completo do estado da máquina para recuperação. Esta configuração pode variar de acordo com o propósito da rotina de backup criada.

No campo “onde fazer backup” é exibido as opções de adicionar um local para sua realização. Conforme a Figura 21, é exibido as opções de pasta local, pasta da rede e pasta NFS. Em casos de que a máquina que será feito o backup é um servidor físico, é possível acoplar os dispositivos externos diretamente nas USBs e definir no campo “Pasta Local” do Acronis a unidade de disco onde será feito o backup, ou selecionar um HD interno para esse fim.

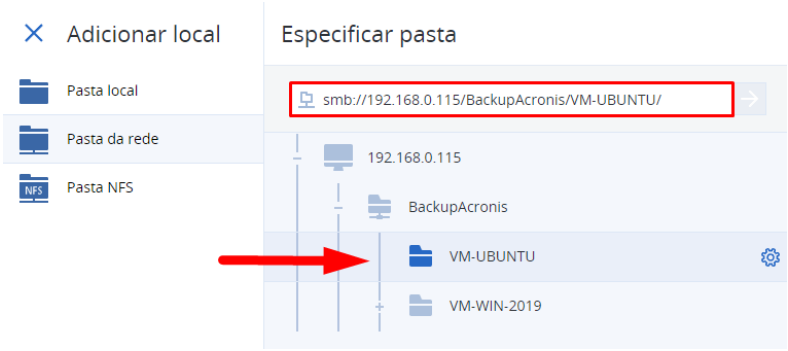
Figura 21 – Local do backup – Acronis



Fonte: Próprio autor (2022).

No caso do teste a ser realizado, é utilizado uma máquina virtual, portanto foi selecionado a opção de “pasta da rede” e selecionado o compartilhamento criado no HD externo acoplado na máquina física (Figura 22). Esta mesma opção pode ser utilizada para realizar backups em NAS ou em um outro servidor de backup disponível na rede.

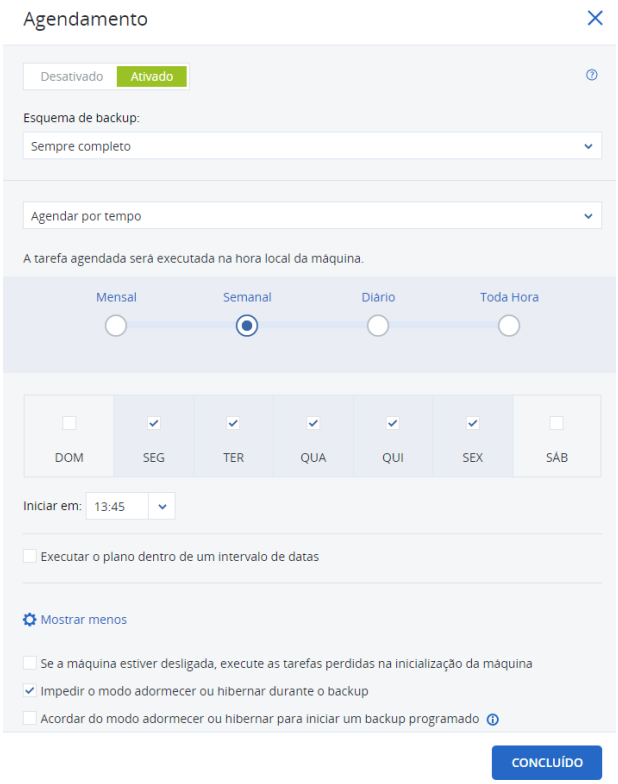
Figura 22 – Pasta da rede - Acronis



Fonte: Próprio autor (2022).

As opções de agendamento da ferramenta são flexíveis e permite criar de acordo como a gestão de TI precisar, disponibilizando esquemas de backup, forma de agendamento e datas/horas específicas para as rotinas (Figura 23).

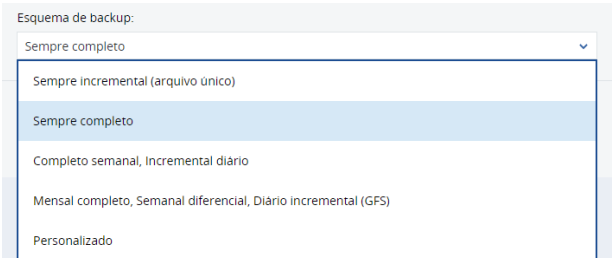
Figura 23 – Agendamento Acronis



Fonte: Próprio autor (2022).

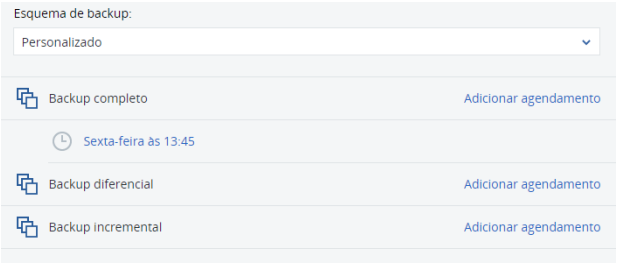
No campo de esquema de backup a ferramenta possui as opções de backup incremental, completo, diferencial ou personalizado, podendo definir da maneira que a organização precisar de forma flexível, conforme Figura 24 e Figura 25. Para este teste foi selecionado a opção de backup completo.

Figura 24 – Esquema de backup - Acronis



Fonte: Próprio autor (2022).

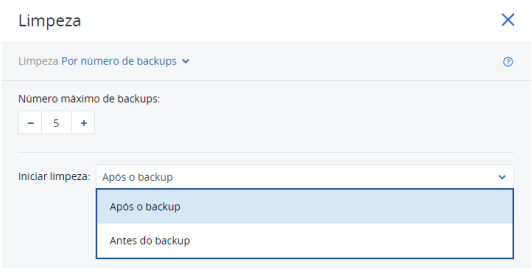
Figura 25 – Esquema de backup personalizado - Acronis



Fonte: Próprio autor (2022).

Em opções de agendamento, foi selecionado a opção de agendamento por tempo, sendo definido semanalmente entre os dias segunda-feira e sexta-feira as 13:45 conforme exibido na Figura 23. Outra opção importante a ser definida é a limpeza dos backups, podendo ser configurada no campo de “Por quanto tempo manter”. Esta opção foi definida por quantidade de backups, sendo elas 5 backups realizados, para assim ter um histórico de 5 dias de backups da máquina. Também definido a limpeza dos backups após o backup ser realizado (Figura 26).

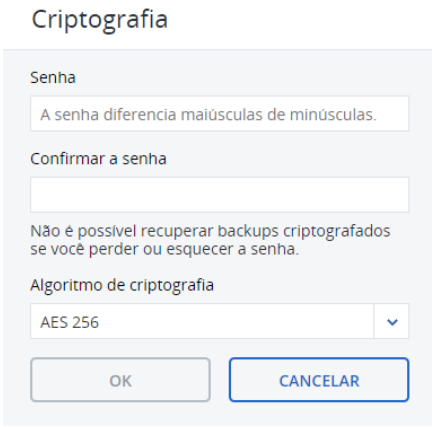
Figura 26 – Limpeza dos backups - Acronis



Fonte: Próprio autor (2022).

Por questões de segurança a ferramenta permite a configuração de uma senha para criptografar o backup, assim no momento da recuperação será solicitado a senha para sua recuperação ser efetuada (Figura 27).

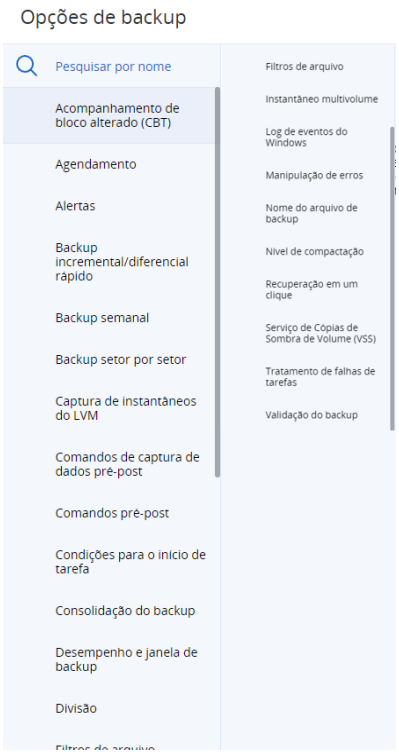
Figura 27 – Criptografia do backup - Acronis



Fonte: Próprio autor (2022).

Além destas configurações citadas, a ferramenta permite diversas outras opções de backup a serem configuradas, de acordo com o ambiente da empresa ou a necessidade da gestão de TI (Figura 28).

Figura 28 – Opções de backup - Acronis

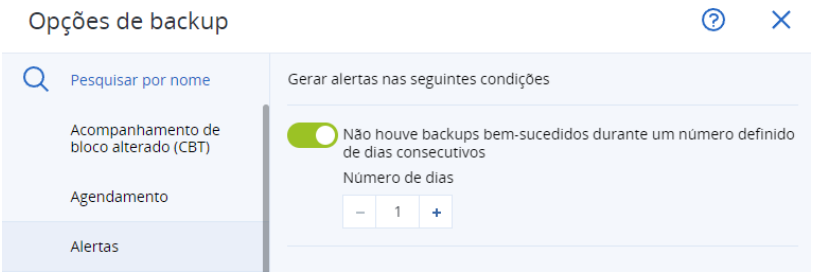


Fonte: Próprio autor (2022).

Entre todas estas configurações extras nas opções de backup é importante se atentar nas configurações de agendamento, alertas, divisão, log de eventos do Windows e tratamento de falhas de tarefas, sendo tratadas como padrão para configuração de todas as rotinas de backup na ferramenta Acronis.

Em alertas, é importante habilitar e definir o número de dias em que será gerado os alertas, assim poderá ser controlado pela console da ferramenta quando um erro ocorrer ao rodar a rotina, neste caso foi definido 1 dia, pois é uma rotina que roda dia a dia e é importante manter informado caso um dia ocorra erro (Figura 29).

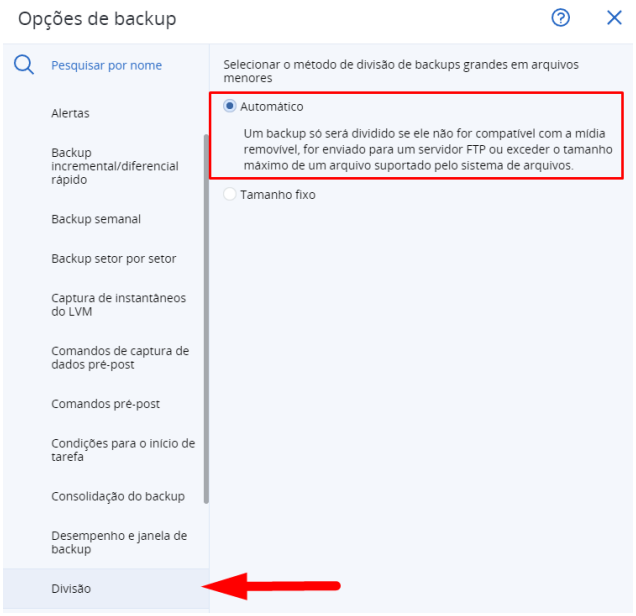
Figura 29 – Alertas de backup - Acronis



Fonte: Próprio autor (2022).

Em divisão, é importante manter em automático para manter um padrão nos backups gerados, assim sempre será criado um arquivo único, em casos que há necessidade de dividir os arquivos de backup ele fará automático, caso contrário selecionar a opção de tamanho fixo e descrever o tamanho desejado (Figura 30).

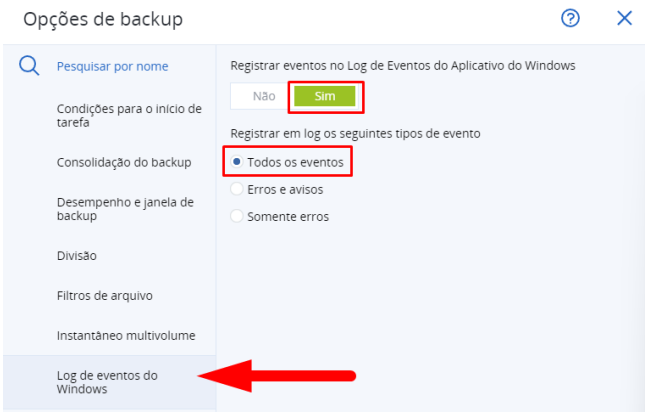
Figura 30 – Divisão de backups - Acronis



Fonte: Próprio autor (2022).

Em log de eventos do Windows manter habilitado e selecionar todos os eventos, assim quando gerar um erro será criado um log no Windows. Esta opção é fundamental quando a empresa possui uma ferramenta de monitoramento automatizada, assim o Acronis consegue atuar em conjunto com esta ferramenta para exibição de alertas de backup (Figura 31).

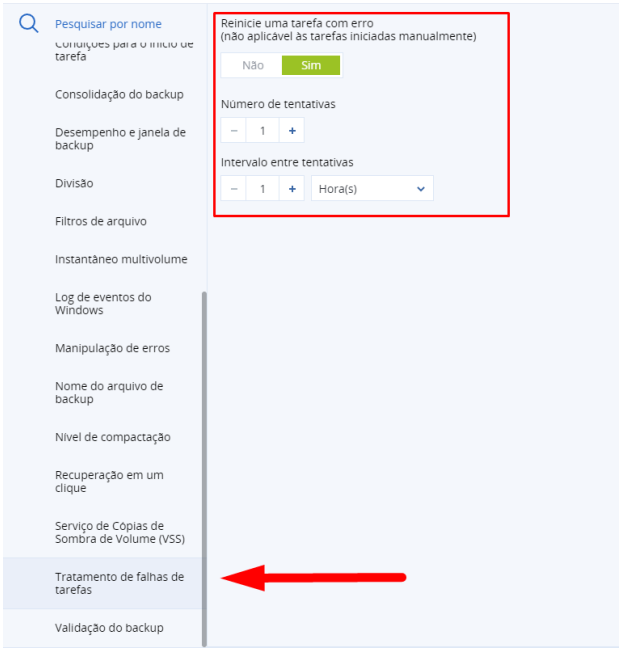
Figura 31 – Log de eventos do Windows - Acronis



Fonte: Próprio autor (2022).

Em tratamento de falhas de tarefas marcar a opção para reiniciar uma tarefa com erro em 1 tentativa em um intervalo de 1 hora. Assim que a tarefa falhar em 1 hora ela tentará rodar novamente, há casos que esse processo resolve o problema, sendo fundamental para uma recuperação automatizada da rotina de backup (Figura 32).

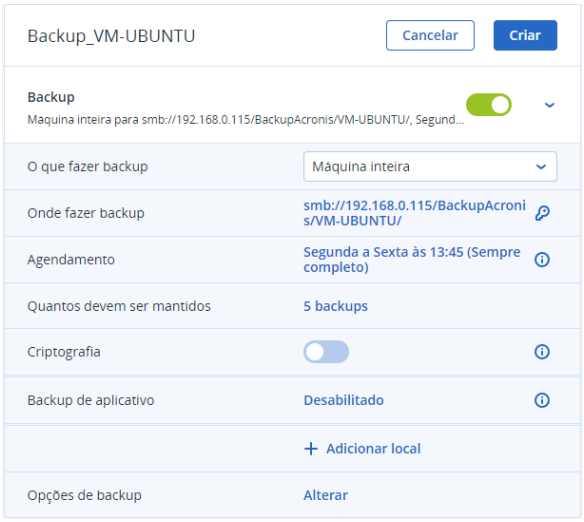
Figura 32 – Tratamento de falhas de tarefas - Acronis



Fonte: Próprio autor (2022).

A rotina de backup pronta com as definições principais inseridas é exibida na Figura 33. Para a máquina virtual Windows Server 2019 foi criado uma rotina com as mesmas definições, mudando apenas o horário de agendamento.

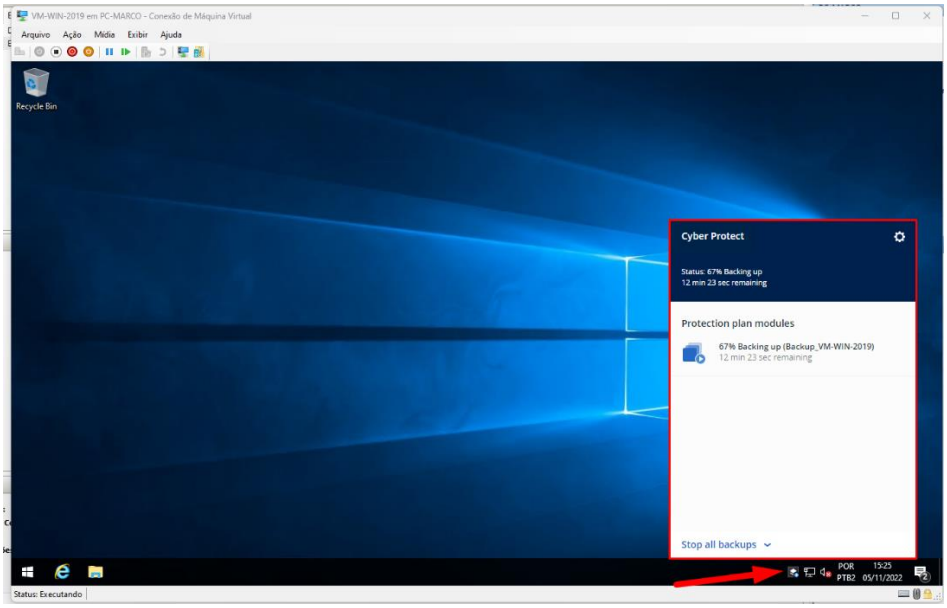
Figura 33 – Rotina de backup pronta - Acronis



Fonte: Próprio autor (2022).

No Windows Server 2019 a ferramenta exibe em modo gráfico o agente em execução na barra de tarefas, sendo possível pausar os backups que estão rodando no momento (Figura 34).

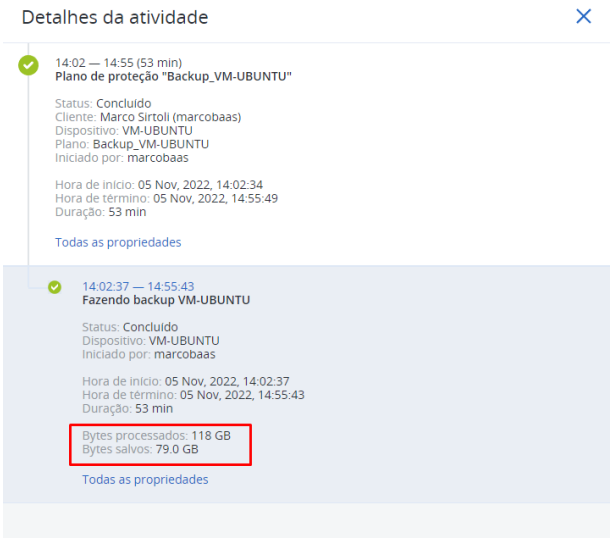
Figura 34 – Agente do Acronis Windows



Fonte: Próprio autor (2022).

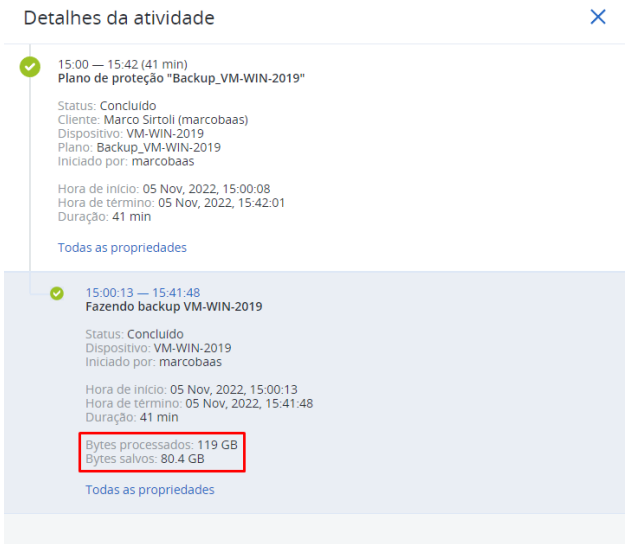
Após rodar as rotinas de backup é possível acompanhar as informações relevantes no campo de atividades dentro do gerenciamento da máquina virtual. Na Figura 35 é possível identificar que o backup realizado na máquina virtual do Linux Ubuntu demorou cerca de 53 minutos para finalizar, processando 118 GB de armazenamento total e gravando 79 GB em disco, diminuindo 39 GB na compressão do backup. Na Figura 37, é possível identificar que o backup realizado da máquina virtual Windows Server 2019 levou cerca de 41 minutos para ser realizado, processando 119 GB de armazenamento total e gravando 80.4 GB em disco, diminuindo 38,6 GB na compressão do backup.

Figura 35 – Backup completo Ubuntu - Acronis



Fonte: Próprio autor (2022).

Figura 36 – Backup completo Windows - Acronis



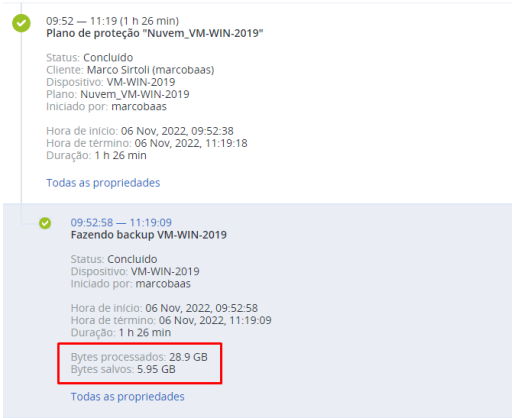
Fonte: Próprio autor (2022).

Para testes do backup em nuvem foi realizado a criação de uma rotina para armazenamento de uma única pasta da base de dados de teste. Por se tratar de um armazenamento em nuvem possui um custo para armazenagem dos dados, sendo assim, o custo aumenta na nuvem ao ser armazenado mais dados. Esta pasta escolhida contempla o total de 28,9 GB de armazenamento. Foi realizado um teste de interromper a tarefa durante seu andamento para validar se continuaria no ponto que parou, no qual é possível identificar o alerta de cancelamento na Figura 37. Na Figura 38 é possível identificar que a ferramenta finalizou o processamento dos dados e terminou de enviar para a nuvem o restante que faltava, gravando um total de 19,3 GB em nuvem (Figura 39) e diminuindo 9,6 GB de compressão de dados.

Figura 37 – Backup em nuvem andamento - Acronis

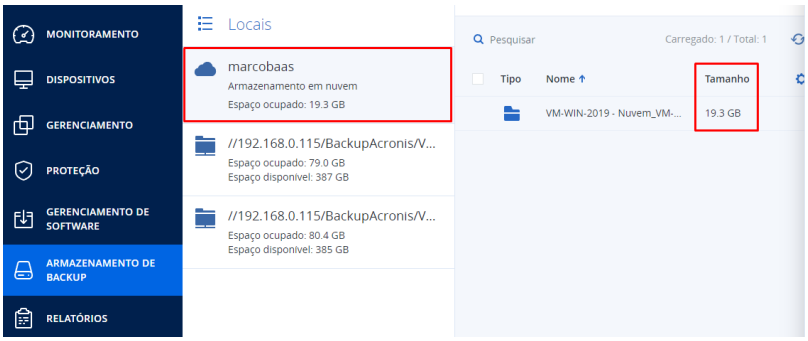
Fonte: Próprio autor (2022).

Figura 38 – Backup em nuvem final - Acronis



Fonte: Próprio autor (2022).

Figura 39 – Armazenamento na nuvem - Acronis



Fonte: Próprio autor (2022).

A ferramenta possui em sua console diversas informações importantes de seu funcionamento. Ao realizar a autenticação na console web é possível verificar informações gerais para monitoramento das rotinas no menu “Monitoramento”. Em “Visão geral” a ferramenta exibe um resumo para a gerência dos backups (Figura 40); em “Alertas” é possível visualizar informações de erro caso uma rotina apresente falha (Figura 41); em “Atividades” é possível acompanhar as informações de cada rotina, tendo seu status, descrição, dispositivo, horário de início e horário de término (Figura 42).

Figura 40 – Visão geral - Acronis

Fonte: Próprio autor (2022).

Figura 41 – Alertas - Acronis

Fonte: Próprio autor (2022).

Figura 42 – Atividades - Acronis

Fonte: Próprio autor (2022).

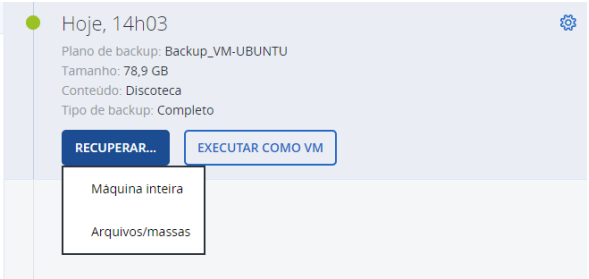
Além destas soluções abrangentes pela ferramenta de backup é possível identificar que ela possui solução antimalware, protegendo os backups de arquivos maliciosos, caso a função for habilitada na rotina de backup criada (Figura 43).

Figura 43 – Proteção - Acronis

Fonte: Próprio autor (2022).

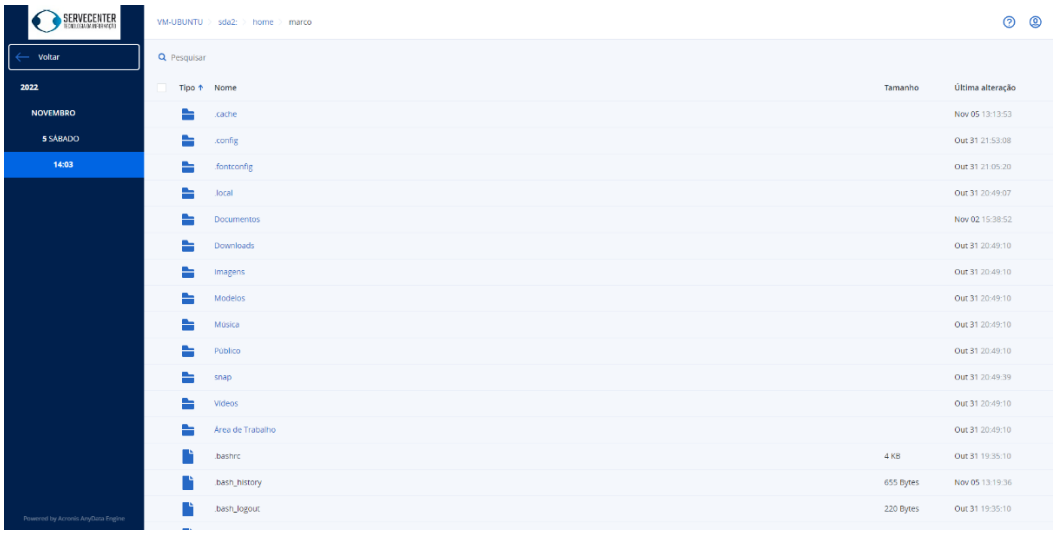
Para a recuperação dos backups realizados (Figura 44) a ferramenta se comporta de maneira flexível, permitindo o usuário a recuperar arquivos unitários, pastas, unidades (Figura 45) ou até mesmo a máquina inteira caso necessário (Figura 46).

Figura 44 – Recuperação dos dados - Acronis



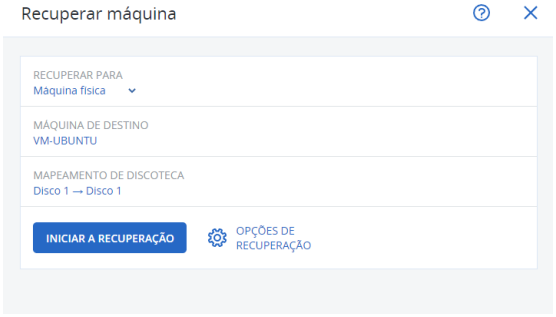
Fonte: Próprio autor (2022).

Figura 45 – Recuperação de arquivos, pastas, unidades - Acronis



Fonte: Próprio autor (2022).

Figura 46 – Recuperação máquina inteira - Acronis



Fonte: Próprio autor (2022).

Por fim, a ferramenta permite a geração de relatórios personalizados de todas as informações relevantes, com a exportação através de arquivos PDF e Excel, enviar por e-mail ou baixar localmente na máquina (Figura 47).

Figura 47 – Geração de relatórios - Acronis

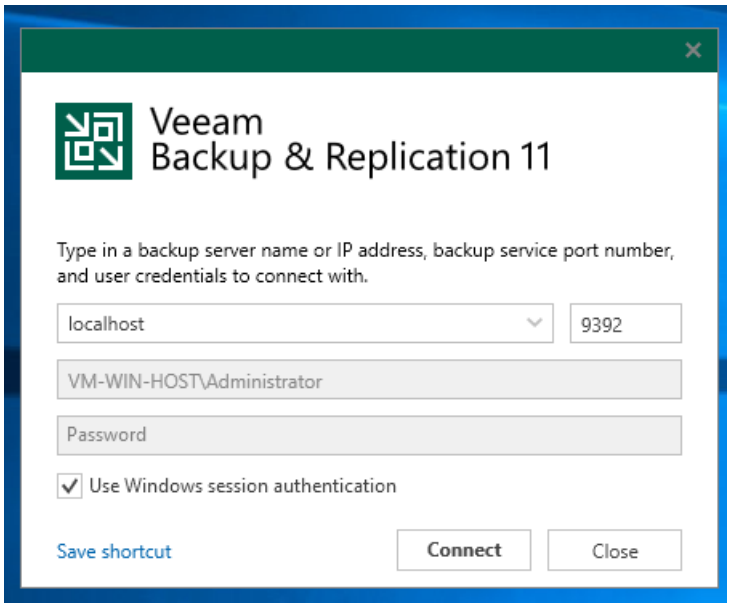
Fonte: Próprio autor (2022).

Referente ao armazenamento de backup em fita, a ferramenta Acronis em sua versão Cyber Protect não possui a funcionalidade, estando disponível apenas em sua versão Advanced. Incluída no menu de “Armazenamento de Backup”, permitindo a criação de armazenamento através de fitas magnéticas.

4.4 VEEAM BACKUP AND REPLICATION COMMUNITY EDITION

A ferramenta Veeam Backup and Replication Community Edition é distribuída sem custo através do site da desenvolvedora. Esta ferramenta é destinada para o uso em até 10 dispositivos, sendo eles, máquinas virtuais e servidores físicos. Para este teste foi realizado a instalação da ferramenta no servidor host Windows Server 2019. Após a instalação da ferramenta, conforme orientado pela desenvolvedora em seus manuais de suporte, foi realizado a inicialização, onde é solicitado a autenticação do usuário (Figura 48).

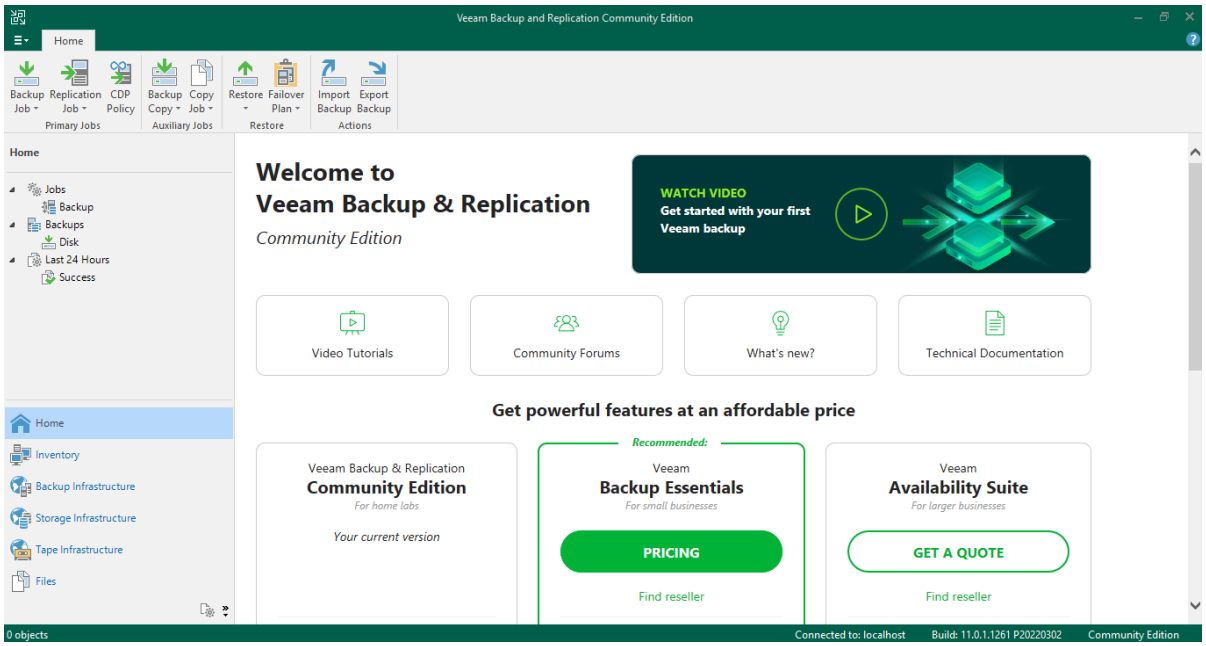
Figura 48 - Autenticação de usuário - Veeam Backup



Fonte: Próprio autor (2022).

Na abertura da ferramenta é exibido a sua interface gráfica de gerenciamento, onde o usuário possui as opções para o controle dos backups, infraestrutura, inventários e rotinas criadas (Figura 49).

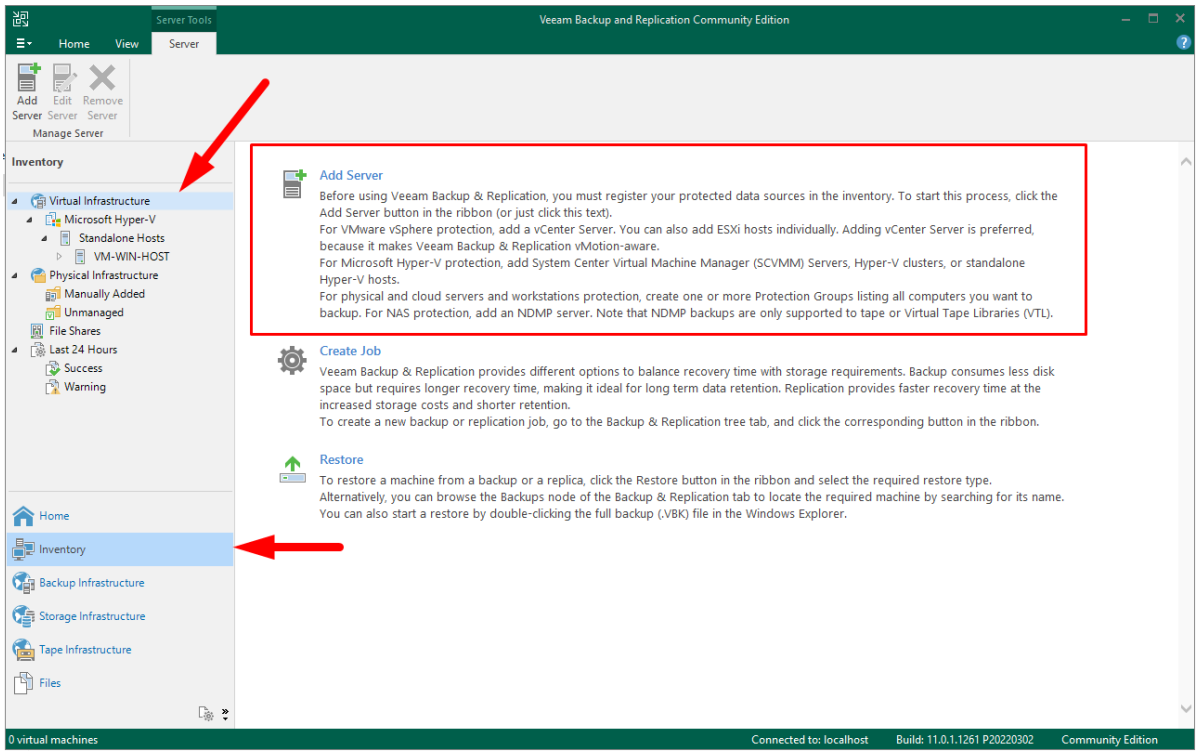
Figura 49 - Autenticação de usuário - Veeam Backup



Fonte: Próprio autor (2022).

Para a realização dos backups é necessário a inclusão das máquinas virtuais no inventário da ferramenta. Sendo necessário acessar o menu lateral, na opção de “Inventory”, “Virtual Infrastructure” e em “Add Server” (Figura 50).

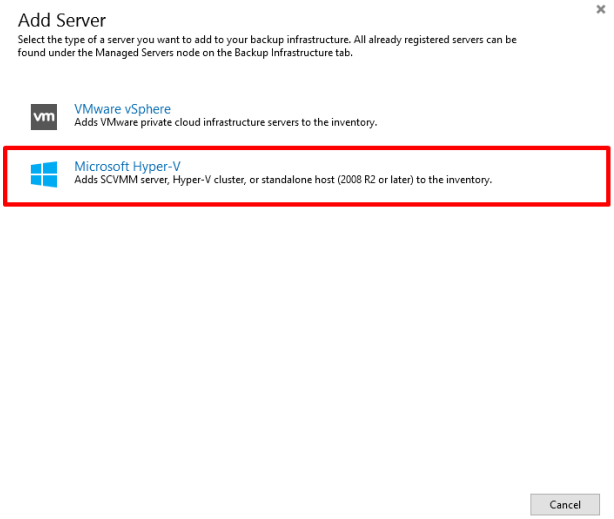
Figura 50 - Inclusão do servidor host - Veeam Backup



Fonte: Próprio autor (2022).

Dentro do menu de “Add Server” é exibido as opções de virtualizadores suportados, no caso do teste realizado será utilizado o virtualizador “Microsoft Hyper-V" (Figura 51).

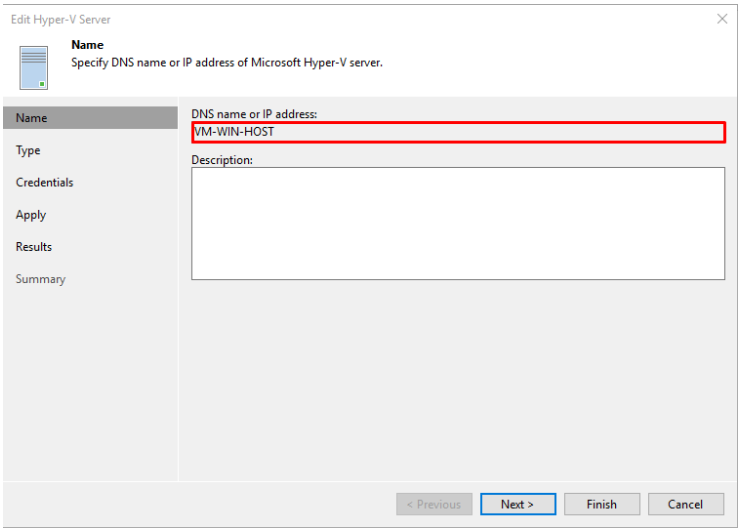
Figura 51 - Inclusão do servidor host - menu - Veeam Backup



Fonte: Próprio autor (2022).

Selecionando o Microsoft Hyper-V, será aberto uma janela de inclusão do servidor. Primeiramente deverá ser inserido o nome ou o IP do servidor, para este teste foi inserido o nome “VM-WIN-HOST”, que é o nome definido no sistema operacional Windows Server 2019 da máquina física que virtualiza as máquinas virtuais (Figura 52).

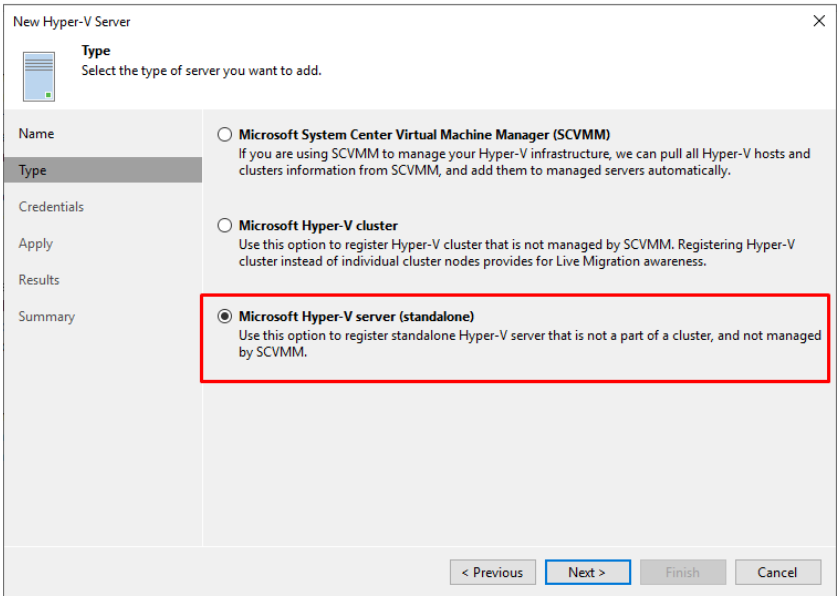
Figura 52 – Especificar nome na inclusão servidor - Veeam Backup



Fonte: Próprio autor (2022).

Na próxima tela deverá ser selecionado o modo de operação, sendo selecionado a última opção de “Microsoft Hyper-V server (standalone)” (Figura 53).

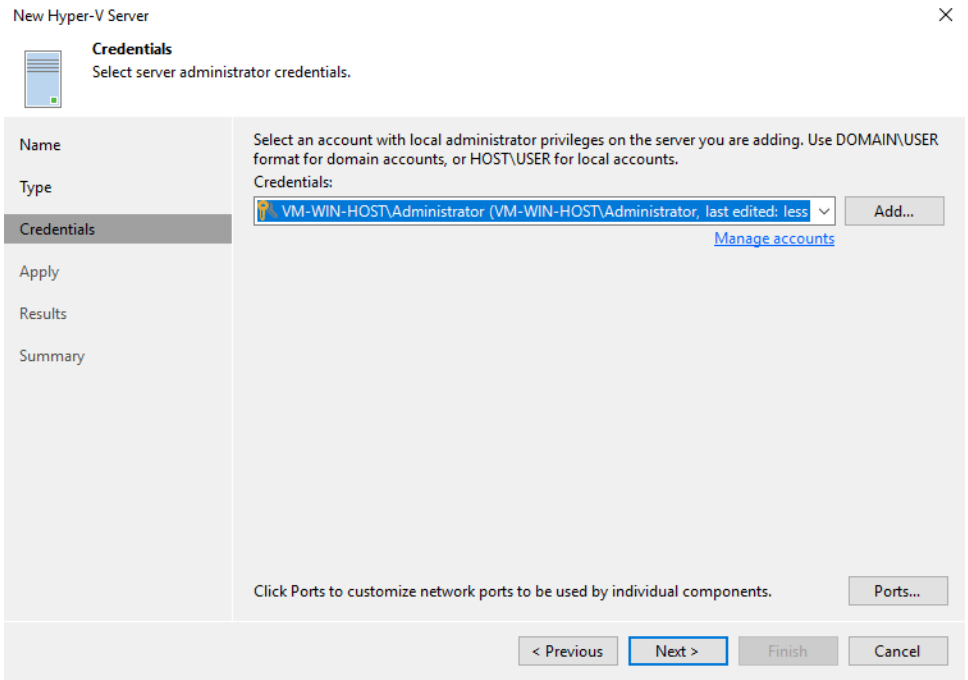
Figura 53 – Especificar tipo na inclusão servidor - Veeam Backup



Fonte: Próprio autor (2022).

Na aba de credenciais deverá ser inserido uma conta que possua privilégios de administrador no servidor, neste caso foi definido a conta local “Administrator” (Figura 54).

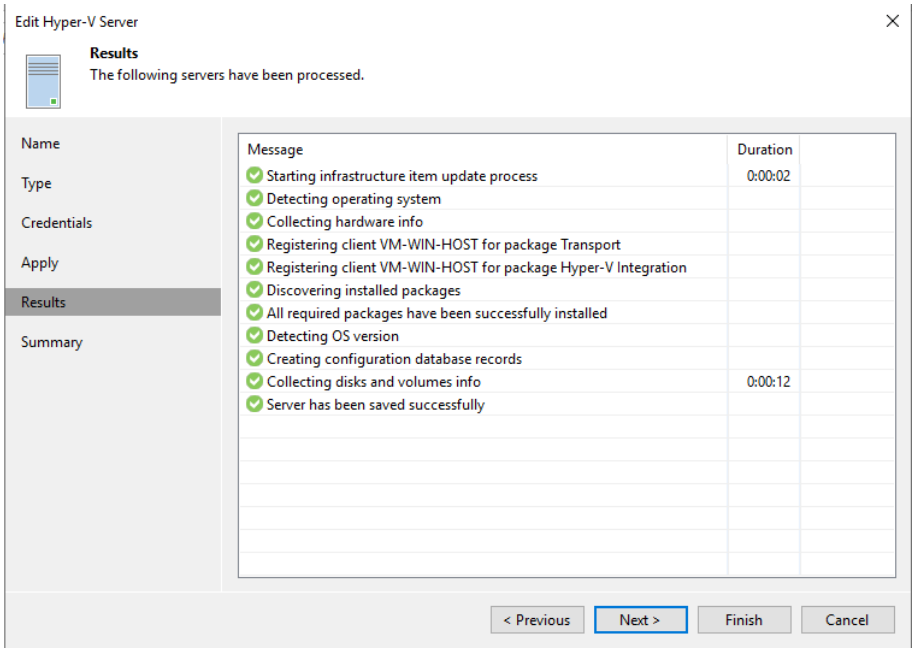
Figura 54 – Especificar credenciais na inclusão servidor - Veeam Backup



Fonte: Próprio autor (2022).

Em resultados é feito toda inclusão do registro da máquina física na ferramenta, coletando informações das máquinas virtuais que estão rodando atualmente e aplicando demais configurações (Figura 55).

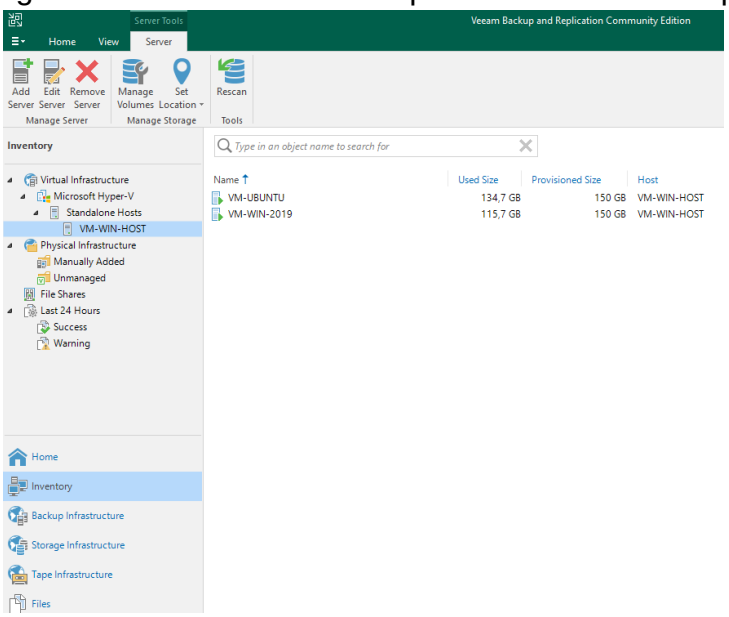
Figura 55 – Resultados na inclusão servidor - Veeam Backup



Fonte: Próprio autor (2022).

Após a inclusão da máquina física na infraestrutura, a ferramenta passa exibir as máquinas virtuais que estão sendo virtualizadas no menu de “Inventory” (Figura 56).

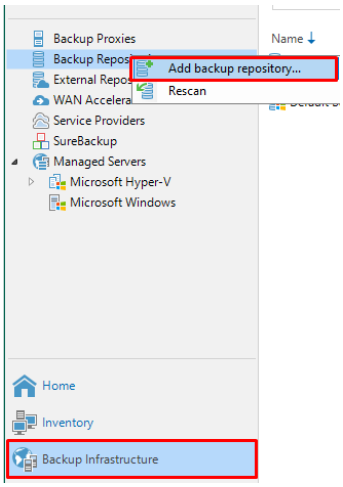
Figura 56 – Inventário de máquinas - Veeam Backup



Fonte: Próprio autor (2022).

Com o inventário de máquinas preparado, é necessário realizar a criação de um repositório de backup, onde a ferramenta irá armazenar os backups gerados pelas rotinas de backup. Na aba de “Backup Infrastructure” e na seleção “Backup Repository”, é exibido a opção para inclusão desses repositórios, com o nome de “Add backup repository...” (Figura 57).

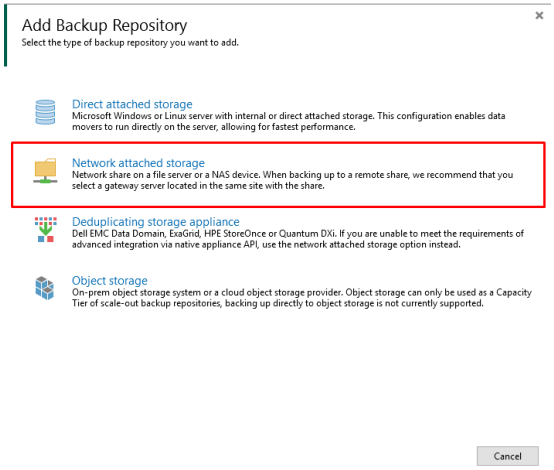
Figura 57 – Inclusão de repositório de backup - Veeam Backup



Fonte: Próprio autor (2022).

Clicando sobre esta opção, uma janela é aberta e permite ao usuário a seleção do tipo de repositório que deseja. Na primeira opção “Direct attached storage” é permitido a inclusão de pastas locais do servidor e unidades removíveis, como pen drives ou HD externos para a realização dos backups. Neste caso será selecionado a segunda opção nomeada de “Network attached storage”, para incluir a pasta compartilhada pelo servidor host, conforme configurado na seção 4.2 (Figura 58).

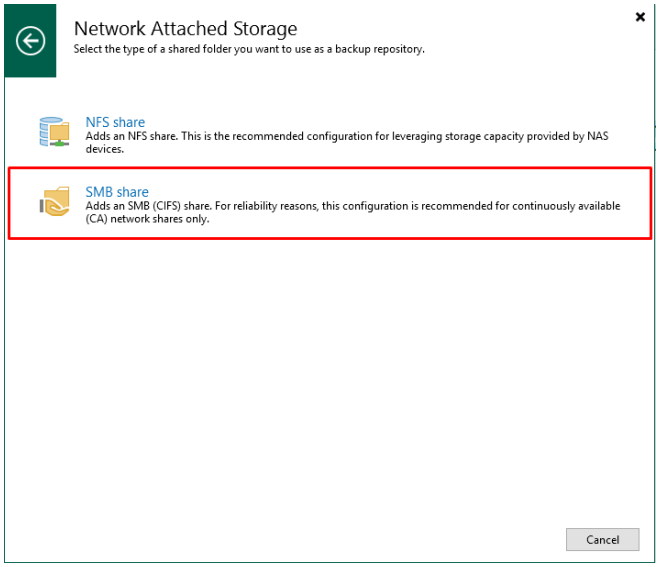
Figura 58 – Tipo de repositório de backup - Veeam Backup



Fonte: Próprio autor (2022).

Na próxima tela é exibido os protocolos de compartilhamento, “NFS share” e “SMB Share”. Sendo selecionado a opção de “SMB Share” (Figura 59).

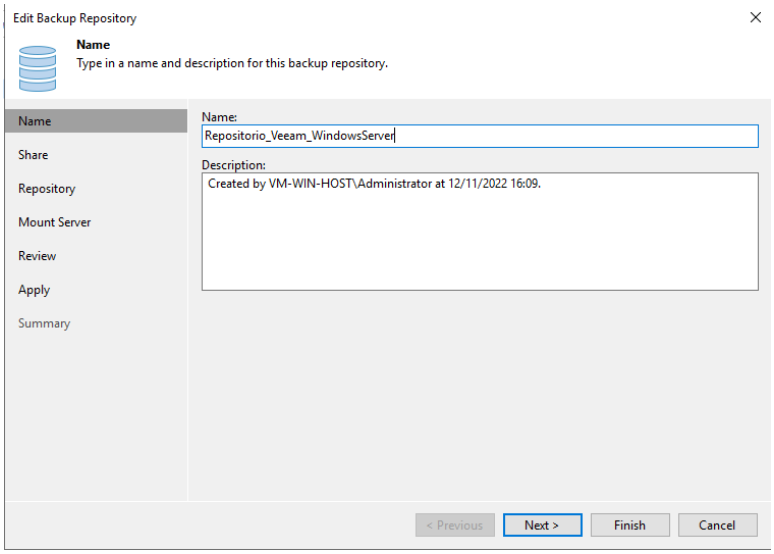
Figura 59 – Protocolo de comunicação para o compartilhamento - Veeam Backup



Fonte: Próprio autor (2022).

Após a seleção inicial é exibido a janela de criação do repositório de backup, sendo primeiramente inserido o nome do repositório (Figura 60).

Figura 60 – Nome do repositório de backup - Veeam Backup

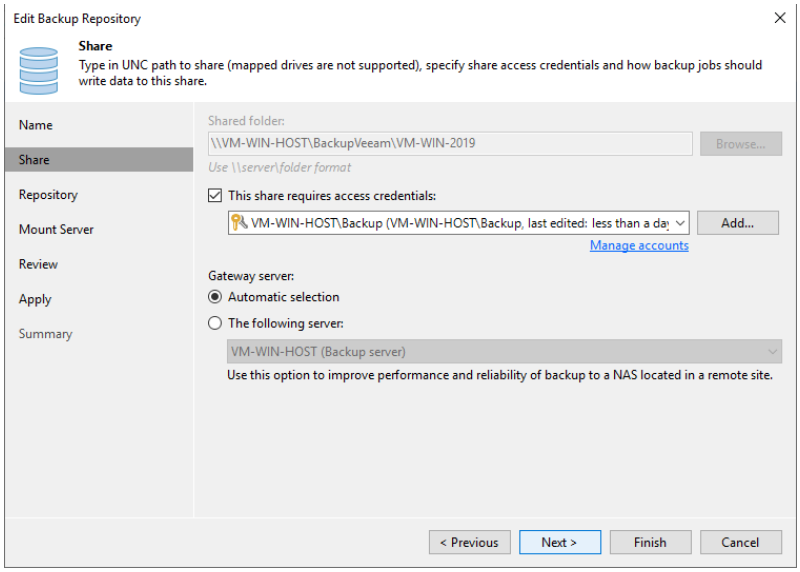


Fonte: Próprio autor (2022).

Na próxima tela, é solicitado o local de compartilhamento, onde foi definido o caminho de rede onde se encontra a pasta criada para os backups. Também exibe a opção de incluir as credenciais, onde foi informado as credenciais de acesso ao

compartilhamento, neste caso as do usuário “backup”, criado localmente no servidor host. E a opção de “Gateway server” foi mantido sua opção padrão (Figura 61).

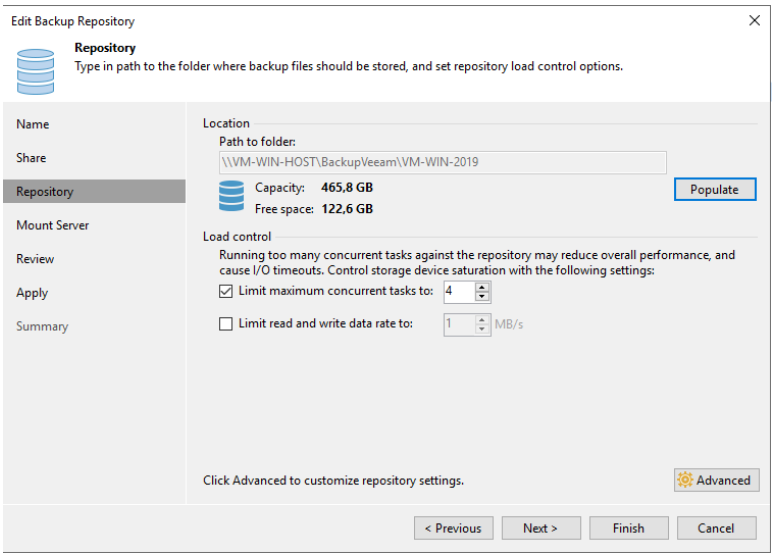
Figura 61 – Compartilhamento repositório de backup - Veeam Backup



Fonte: Próprio autor (2022).

Na próxima tela, informado o caminho do repositório e o máximo de tarefas que podem rodar simultaneamente neste repositório. Esta opção é definida pois caso houver muitas tarefas rodando simultaneamente pode causar sobrecarregamento no disco e falhar os backups (Figura 62).

Figura 62– Local do repositório de backup - Veeam Backup

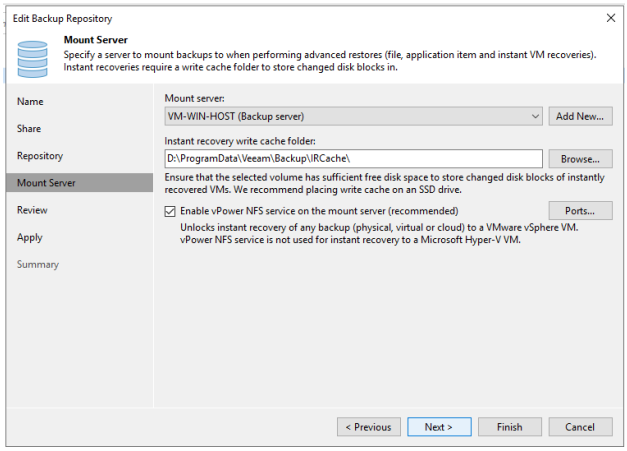


Fonte: Próprio autor (2022).

Na opção seguinte é informado o servidor de backup que será utilizado para esse repositório e onde as informações de cache serão gravadas localmente (Figura

63). As demais opções foram mantidas padrão conforme configurado pela própria ferramenta e finalizado a criação do repositório. Esta mesma configuração foi realizada para criar o repositório de armazenamento para a outra VM, no caso a Ubuntu, com seu respectivo destino de backup no HD externo.

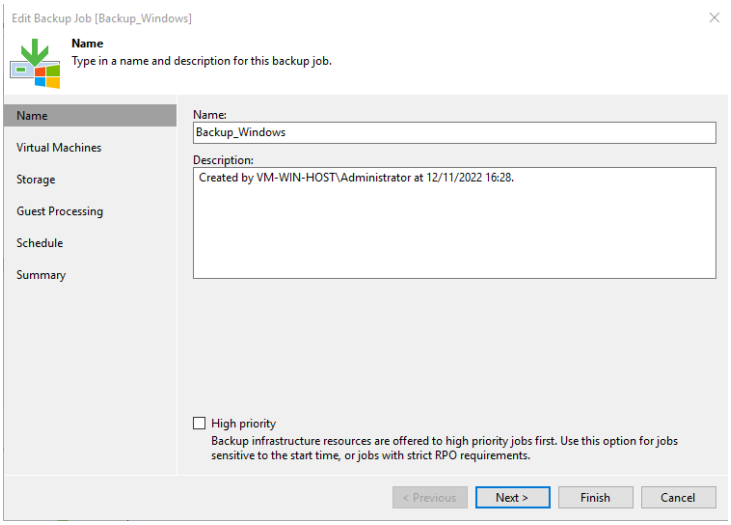
Figura 63 – Montar servidor de backup - Veeam Backup



Fonte: Próprio autor (2022).

Com a infraestrutura da ferramenta preparada para receber os backups (servidores e local de armazenamento de backups), foi necessário a criação das rotinas de backup. Na janela de criação da rotina de backup foi solicitado o nome da rotina, neste caso definido como “Backup_Windows” (Figura 64).

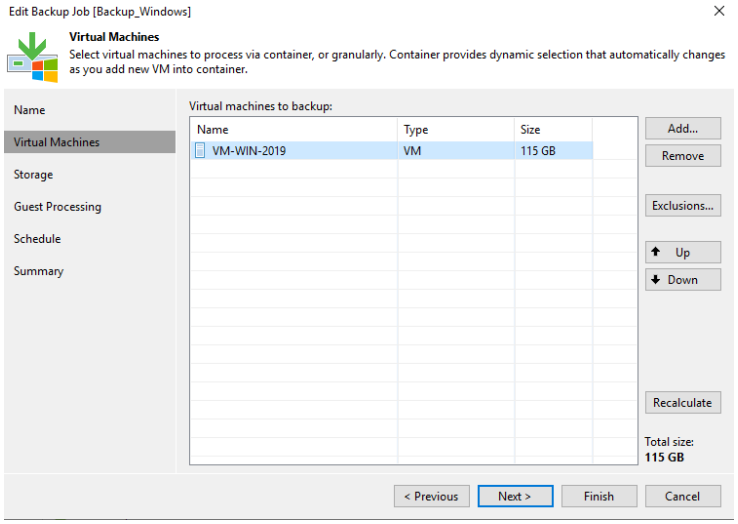
Figura 64 – Nome da rotina de backup - Veeam Backup



Fonte: Próprio autor (2022).

Na próxima tela foi solicitado a seleção de qual máquina virtual será aplicada a rotina, selecionado a “VM-WIN-2019” (Figura 65).

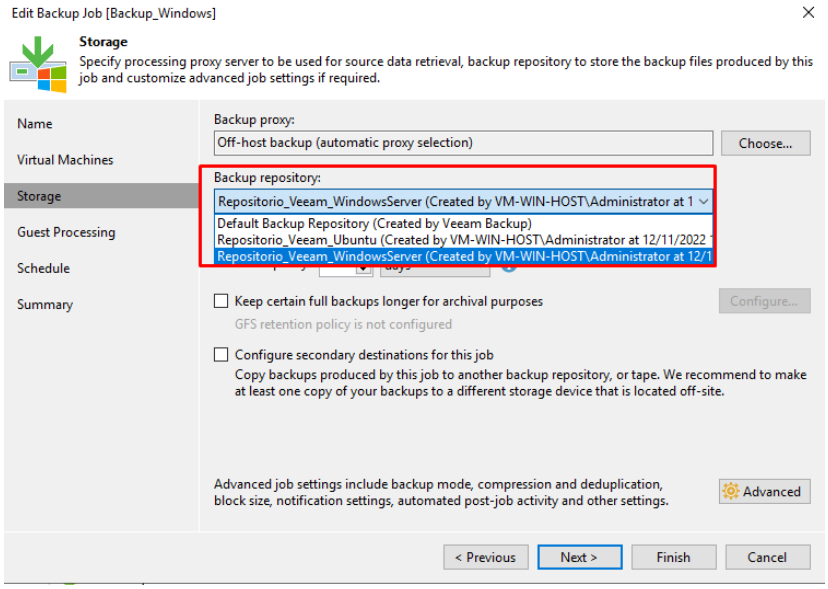
Figura 65 – Máquinas virtuais da rotina - Veeam Backup



Fonte: Próprio autor (2022).

Na próxima tela, exibido os repositórios onde será armazenado, selecionado o repositório para a máquina virtual Windows Server (Figura 66).

Figura 66 – Especificar repositório de backup - Veeam Backup

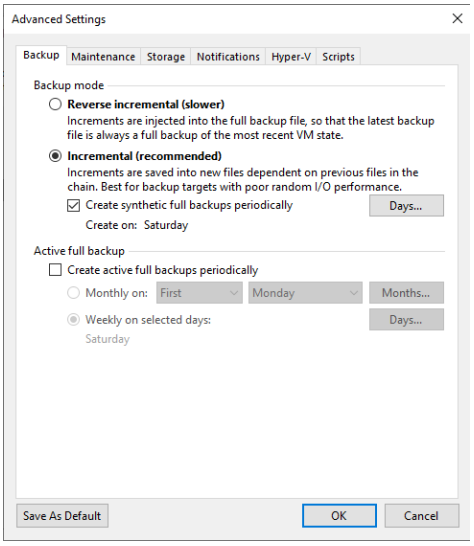


Fonte: Próprio autor (2022).

No menu avançado é exibido o modo de backup que será realizado (Figura 67). A ferramenta não possui o método de backup diferencial, porém disponibiliza dois tipos de backup. Um deles sendo o incremental reverso, onde é uma forma alternativa de backup incremental, que realiza incrementos em um backup completo, para quando for necessário a recuperação sempre ter um backup completo mais recente a disposição. E o backup incremental tradicional que realiza primeiro um backup completo e depois inclui os incrementos. Também é possível selecionar os dias em

que é realizado backups completos, aumentando a frequência deste modo de backup. Neste teste foi mantido o incremental tradicional recomendado pela ferramenta, pois a avaliação será sobre o primeiro backup completo realizado.

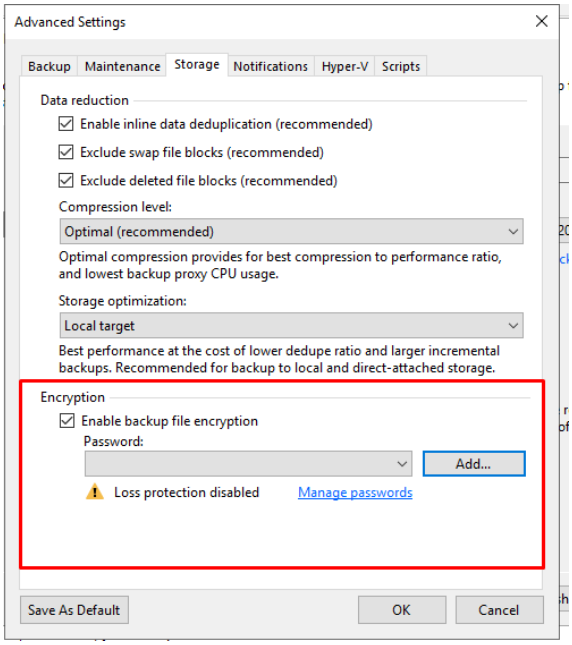
Figura 67 – Modo de backup na rotina - Veeam Backup



Fonte: Próprio autor (2022).

No menu avançado da rotina de backup e na aba de armazenamento é possível realizar a criação de uma senha de criptografia para a segurança dos backups (Figura 68).

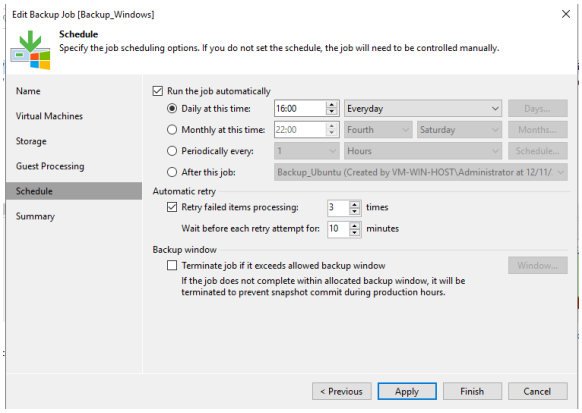
Figura 68 – Criptografia com senha - Veeam Backup



Fonte: Próprio autor (2022).

Na tela seguinte, é exibido a opção de agendamento dos backups, onde é possível configurar a automação da rotina para rodar nos dias e horários necessários. Além disso, na opção de “Automatic retry” é possível definir a quantidade de vezes que a ferramenta irá rodar a rotina de backup novamente em caso de erro e o intervalo de tempo que levará para isso ocorrer (Figura 69).

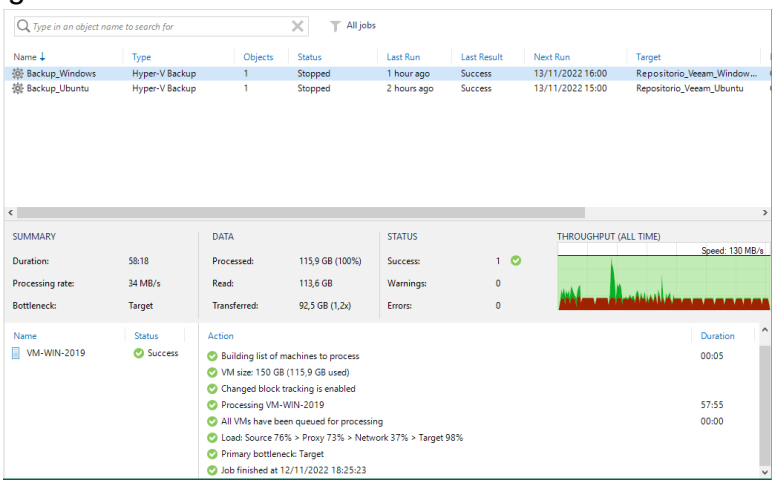
Figura 69 – Agendamento da rotina - Veeam Backup



Fonte: Próprio autor (2022).

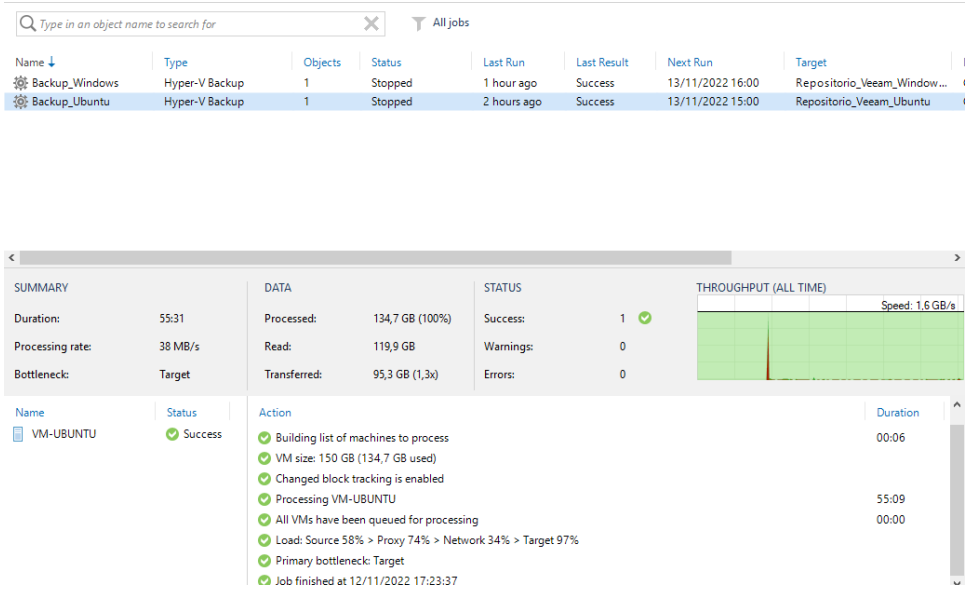
Com as rotinas de backup criadas para ambas as máquinas virtuais foi realizado sua execução. Através da execução e finalização dos backups foi identificado pontos relevantes a serem considerados, sendo eles, a rotina de backup do Windows rodou em 58 minutos, processando 115,9 GB de armazenamento e gravando 92,5 GB, tendo a compressão de 23,4 GB no armazenamento do backup (Figura 70). Para a rotina de backup do Ubuntu, é identificado que levou cerca de 55 minutos para ser concluída, processando 134,7 GB de armazenamento e gravando 95,3 GB, tendo a compressão de 39,4 GB no armazenamento do backup (Figura 71).

Figura 70 – Rotina concluída - Windows - Veeam Backup



Fonte: Próprio autor (2022).

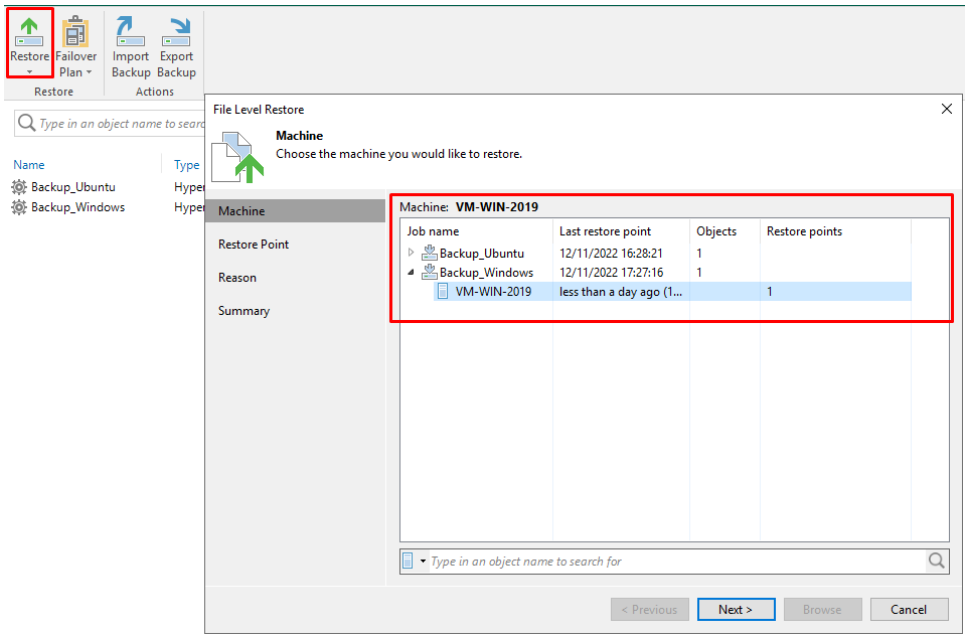
Figura 71 – Rotina concluída - Ubuntu - Veeam Backup



Fonte: Próprio autor (2022).

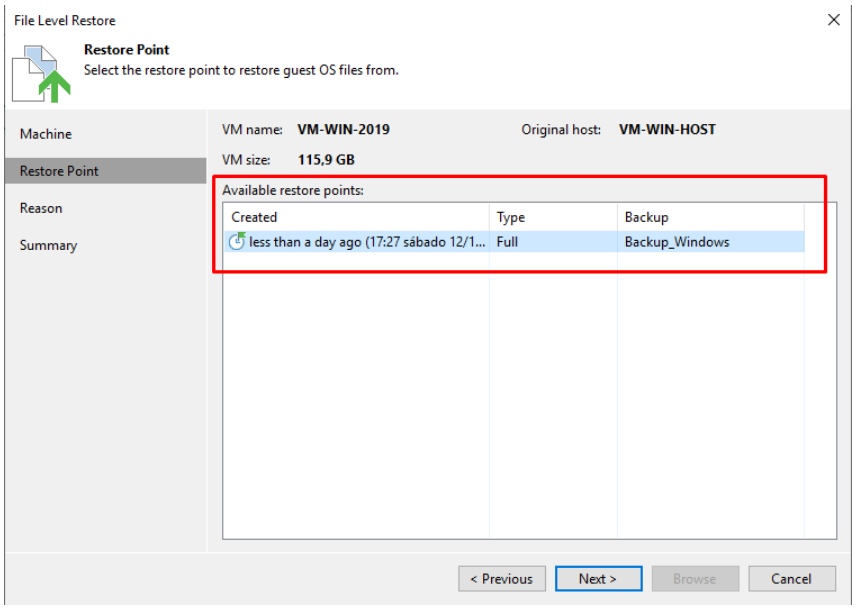
Para a restauração dos backups gerados é exibido a opção de “Restore” na tela principal da ferramenta. Com isso é permitido a restauração dos pontos de backup realizados, conforme exibidos na Figura 72 e Figura 73.

Figura 72 – Restauração do backup - Veeam Backup



Fonte: Próprio autor (2022).

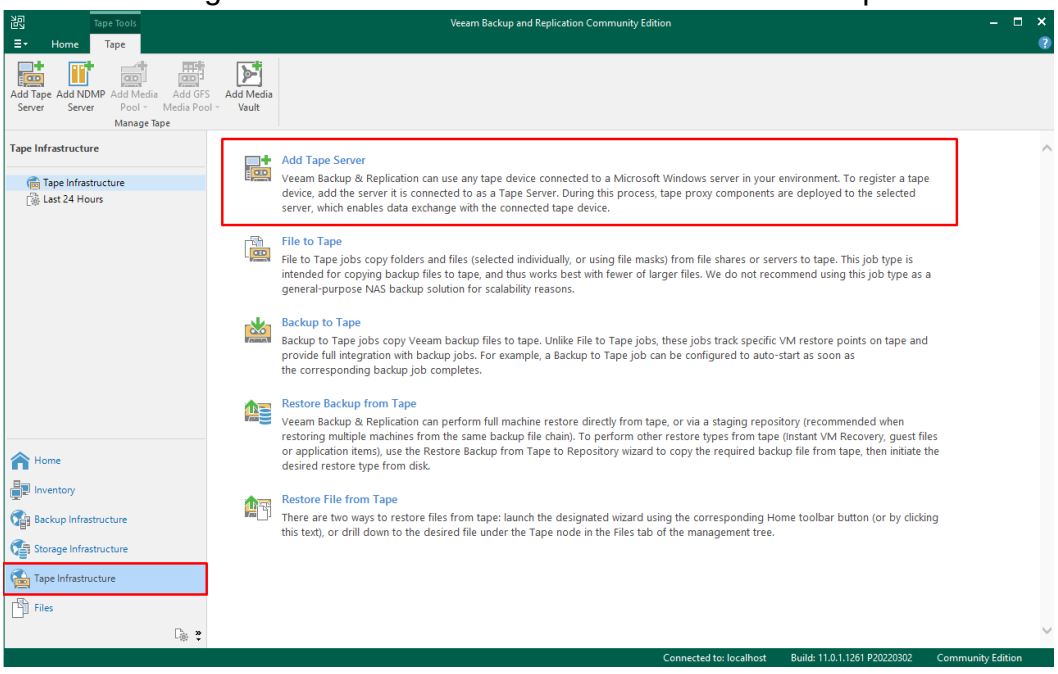
Figura 73 – Ponto de restauração de backup - Veeam Backup



Fonte: Próprio autor (2022).

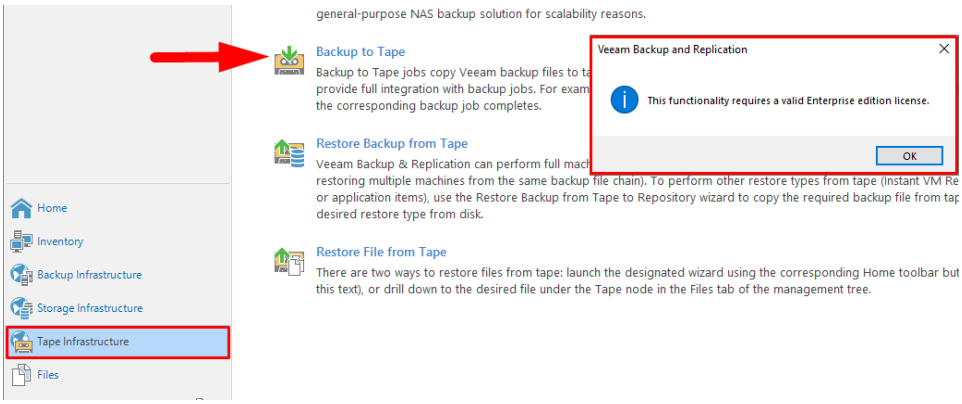
A ferramenta na sua versão gratuita permite a inclusão de servidores de fita magnética, conforme exibido na Figura 74. Através da inclusão do servidor de fita é possível realizar os backups para esse tipo de armazenamento, porém caso necessário utilizar o mesmo servidor host para integração das fitas com as rotinas de backup será preciso adquirir a licença Enterprise da ferramenta (Figura 75).

Figura 74 – Infraestrutura de fita - Veeam Backup



Fonte: Próprio autor (2022).

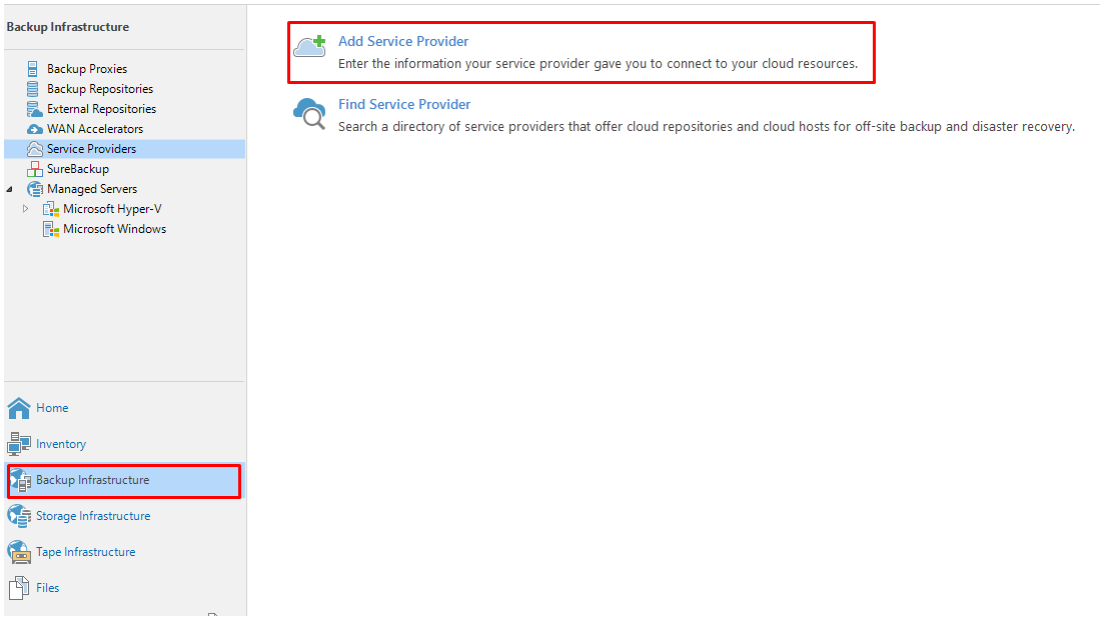
Figura 75 – Backup para fita - Veeam Backup



Fonte: Próprio autor (2022).

A ferramenta também permite a inclusão de recursos em nuvem, como um servidor para backup em nuvem caso a empresa possuir um serviço adquirido. Porém o serviço não é disponibilizado em sua versão gratuita para realização do teste (Figura 76).

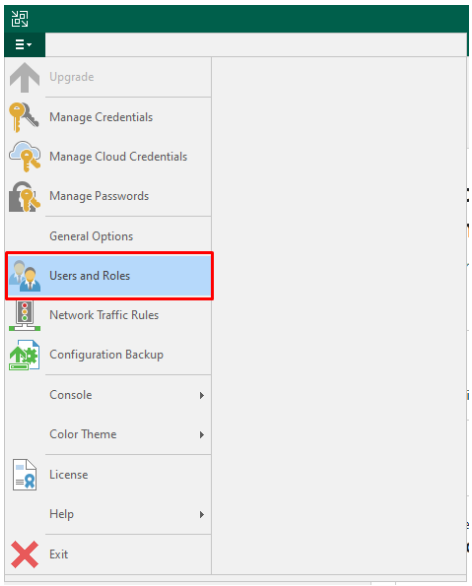
Figura 76 – Inclusão de recursos em nuvem - Veeam Backup



Fonte: Próprio autor (2022).

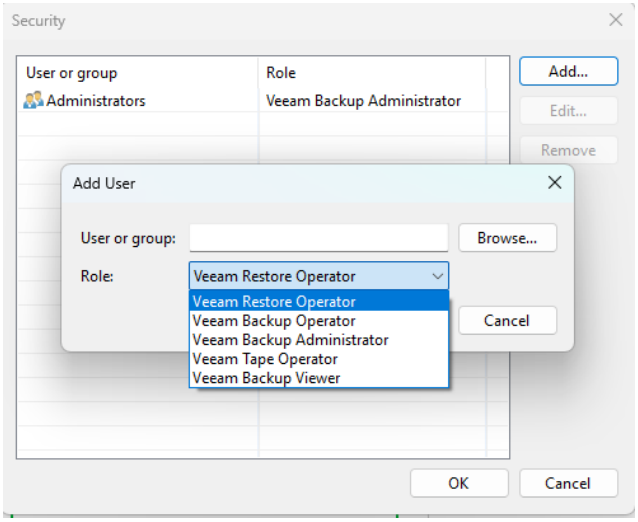
Para assegurar ainda mais o ambiente dos backups, a ferramenta possui a possibilidade de criar e gerenciar usuários para gestão da ferramenta. Para isso, é exibido no menu superior a opção de “Users and Roles”, permitindo a criação de usuário de acordo com a finalidade e permissão necessária, conforme exibido na Figura 77 e Figura 78.

Figura 77 – Usuários de segurança - Veeam Backup



Fonte: Próprio autor (2022).

Figura 78 – Criação de usuário - Veeam Backup



Fonte: Próprio autor (2022).

4.5 BACULA BACKUP COMMUNITY

A ferramenta Bacula Backup Community é oferecida sem custo no site da distribuidora e possui licenciamento de código livre. Para sua utilização foi necessário preparar um ambiente de instalação exclusivo para ferramenta, através de um servidor com a instalação dos pacotes do Bacula, a API Baculum, Apache para exibição web e o banco de dados MySQL. A instalação ocorreu com diversos empecilhos, tais como, problemas de comunicação da instalação do Bacula com a API Baculum; dificuldade

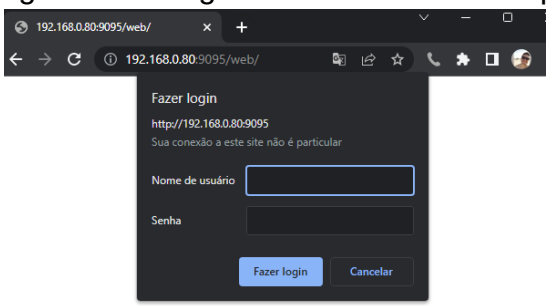
de encontrar procedimentos de instalação práticos da própria distribuidora; falha de localização dos pacotes necessários dentro dos diretórios do Linux.

Foi realizado três tentativas de instalação da ferramenta, sendo a primeira utilizando a distribuição mais recente do Ubuntu Server na versão 22.04.1 e o Bacula na última versão 13.0.1, porém ocorreu problema de comunicação entre a API Baculum com a instalação interna do Bacula. Na segunda tentativa foi realizado a instalação do Debian 11.5 e o Bacula 13.0.1, porém ocorreu problemas de localização dos diretórios da ferramenta. Por fim, foi utilizado a versão do Bacula 9.6.5 e o Ubuntu Server 20.04.5, e todos os problemas de instalação na versão servidor deixaram de ocorrer, instalando corretamente. O servidor físico selecionado para possuir a ferramenta instalada em seu modo servidor possui as seguintes configurações:

- **SRVBACULA:**
  - Sistema Operacional: Ubuntu Server 20.04.5 LTS
  - CPU: Intel Core i5-2410M
  - Disco: 120 GB SSD
  - Memória: 4096 MB

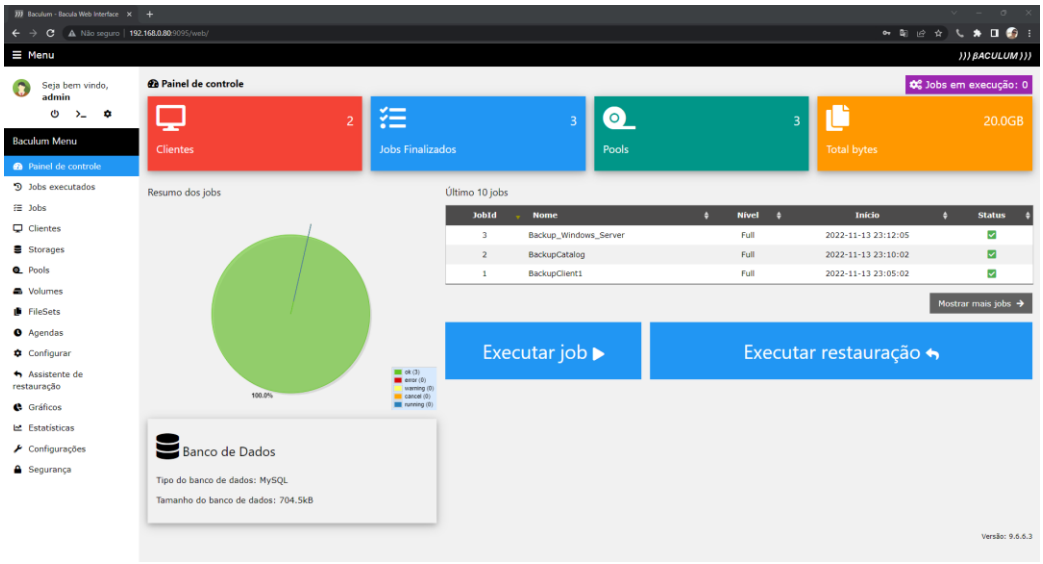
Após a ferramenta devidamente instalada, é possível acessar através do seu painel web para o gerenciamento pelo IP do servidor 192.168.0.80 e porta 9095 (Figura 80). Para acesso seguro a ferramenta requer que seja criado um usuário e senha, o qual foi criado durante a instalação da ferramenta (Figura 79).

Figura 79 – Login web – Bacula Backup



Fonte: Próprio autor (2022).

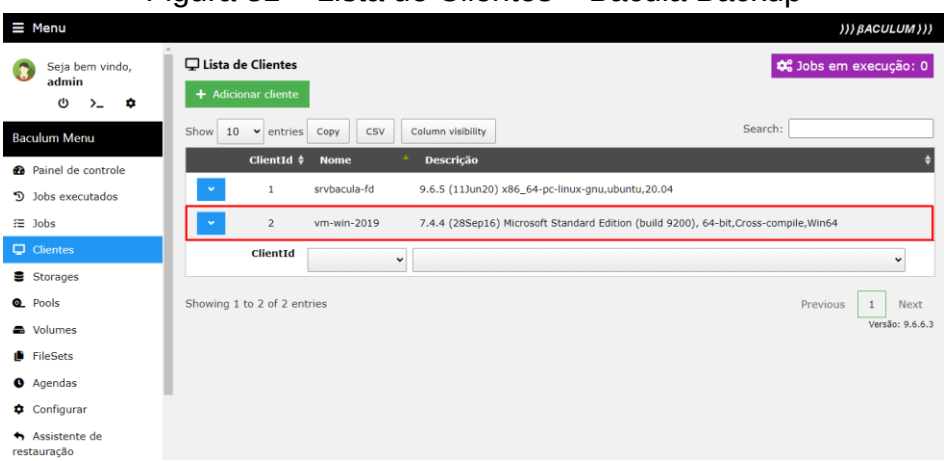
Figura 80 – Painel Web – Bacula Backup



Fonte: Próprio autor (2022).

Para a inclusão das máquinas virtuais na ferramenta é necessário instalar o software de modo cliente. Na máquina virtual Windows Server 2019 não ocorreu problemas na instalação e configuração para reconhecer na ferramenta de backup, porém na máquina virtual Ubuntu não foi possível realizar a instalação. Tentativa de instalação conforme informado nos manuais através do repositório do Linux não houve sucesso, os pacotes de instalação “bacula-client” não eram localizados no repositório do Linux, feito tentativa de instalação manual através do envio dos pacotes para dentro do Ubuntu, mas os arquivos de configuração não eram gerados corretamente. Portanto foi realizado a instalação apenas na versão Windows cliente, exibido como segundo na lista conforme a Figura 81. O servidor cliente primário “srvbacula-fd” se refere ao servidor que possui o Bacula servidor instalado.

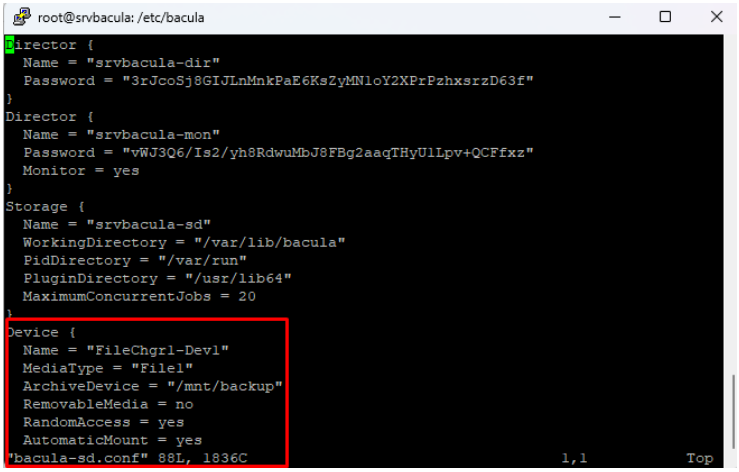
Figura 81 – Lista de Clientes – Bacula Backup



Fonte: Próprio autor (2022).

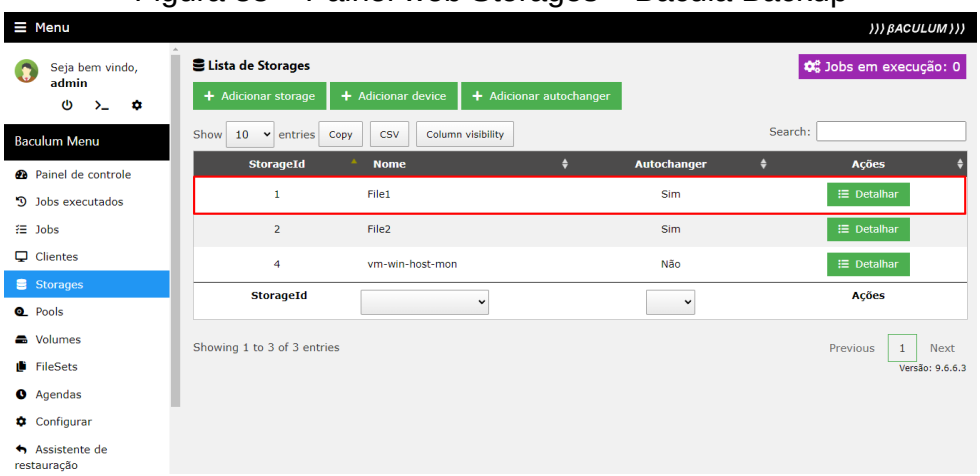
A ferramenta possui diversas configurações que podem ser realizadas, porém requer níveis avançados de conhecimento da estrutura da ferramenta para uma adequação completa dos ambientes de backup. Para a preparação do ambiente de armazenamento de backups não foi localizado opções simplificadas para sua realização, como backup em HD, em rede e uma forma prática para backups locais. A ferramenta se comporta em realização de backups por meio de “storages” e “devices”, estes dispositivos são configurados por linha de comando no Bacula servidor, realizando a comunicação através da interface web e em sua documentação informa que pode ser configurado discos locais, externos, fitas magnéticas e em rede. Por padrão a ferramenta possui configurado armazenamento “File 1”, que guarda dentro do diretório “/mnt/backup” do Bacula servidor, conforme exibido na Figura 82 e Figura 83.

Figura 82 – Srvbacula Storages – Bacula Backup



Fonte: Próprio autor (2022).

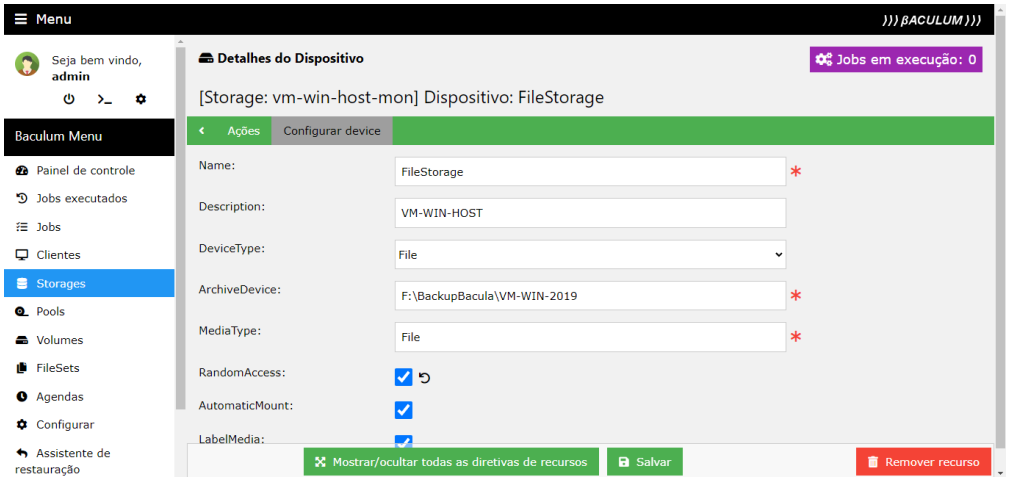
Figura 83 – Painel web Storages – Bacula Backup



Fonte: Próprio autor (2022).

Na prática, foi realizado a tentativa de incluir o armazenamento do HD externo acoplado no servidor host Windows Server 2019, através do arquivo de configuração do cliente Bacula, porém não houve sucesso (Figura 84).

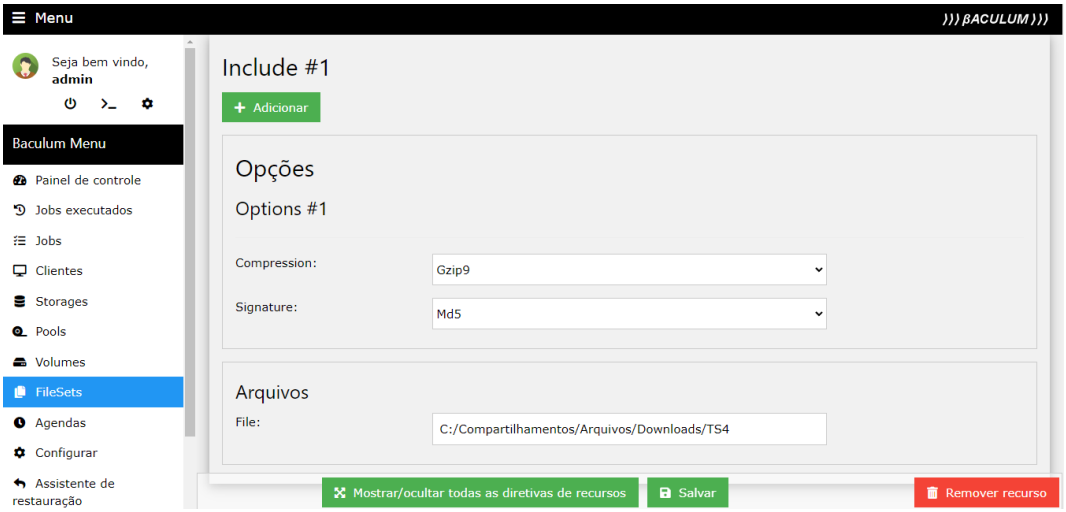
Figura 84 – Inclusão de armazenamento de backup – Bacula Backup



Fonte: Próprio autor (2022).

Para a realização de um backup foi realizado a criação de um “FileSet” que define o que será feito de backup do servidor cliente. Como não foi possível incluir o HD externo para realização dos backups, foi selecionado o armazenamento padrão do Bacula servidor e diminuído a quantidade de dados, para ser concluído o backup sem encher completamente o armazenamento do servidor. A pasta selecionada possui 28,9 GB e foi definido a opção de compressão e criptografia sugerida, Gzip9 e Md5 respectivamente (Figura 85).

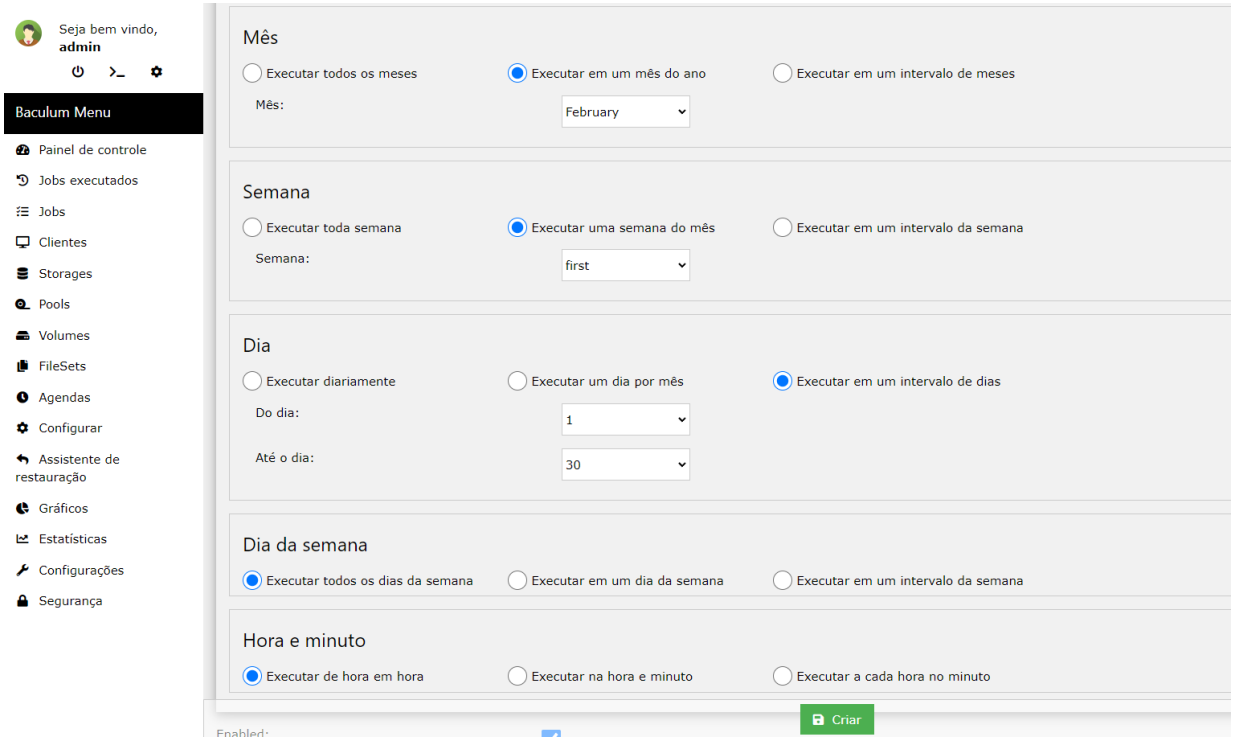
Figura 85 – Criação do FileSet – Bacula Backup



Fonte: Próprio autor (2022).

A ferramenta permite a criação de agendamentos de backup para atribuir às rotinas. Podendo definir para backups mensais, semanais, diários, dias da semana ou em hora/minuto, conforme exibido na Figura 86.

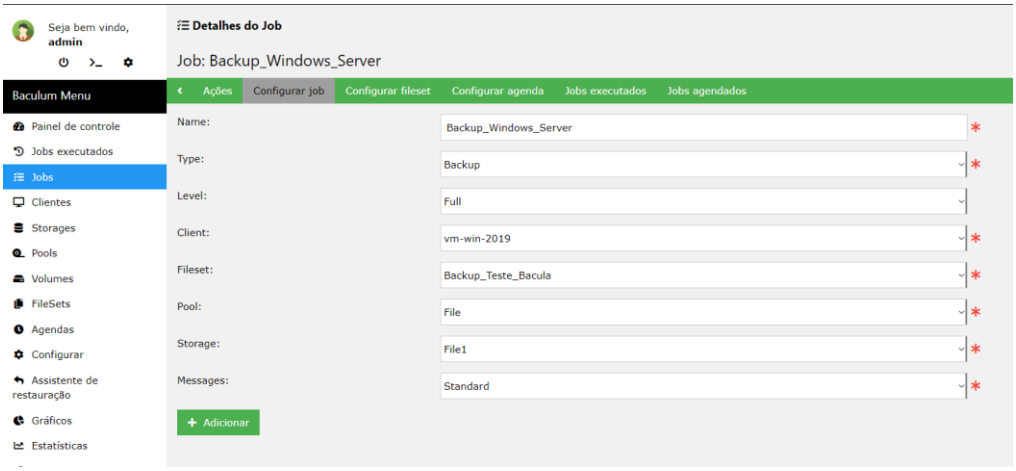
Figura 86 – Agendamentos de Backup – Bacula Backup



Fonte: Próprio autor (2022).

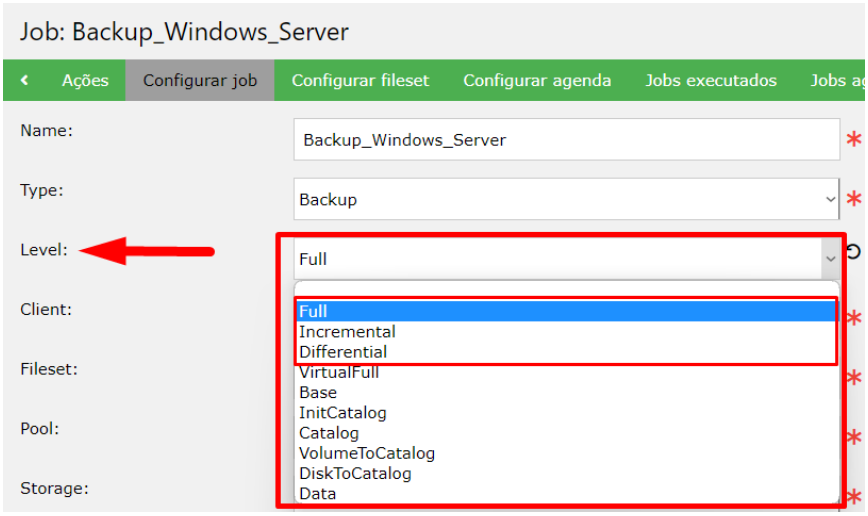
Após a criação dos agendamentos, será necessário criar a rotina de backup para execução deles. No menu de “Jobs” pode ser realizado a configuração, definindo um nome para a rotina, o tipo da rotina (backup, restauração, cópia, verificação e migração), o modo de backup (contemplando os principais modos estudados, completo, diferencial e incremental), “Pool” que é a retenção dos backups, mantido padrão como o modo “File”, o local de armazenamento (conforme definido anteriormente o padrão “File1”) e por último as mensagens, que podem ser configuradas para enviar por e-mail avisos do backup. Estas configurações são exibidas na Figura 87 e Figura 88. Além destas configurações deverá ser definido o “FileSet” criado anteriormente e caso desejar, configurar a agenda para os backups rodarem automaticamente nos horários selecionados.

Figura 87 – Rotinas – Bacula Backup



Fonte: Próprio autor (2022).

Figura 88 – Modo de backup – Bacula Backup



Fonte: Próprio autor (2022).

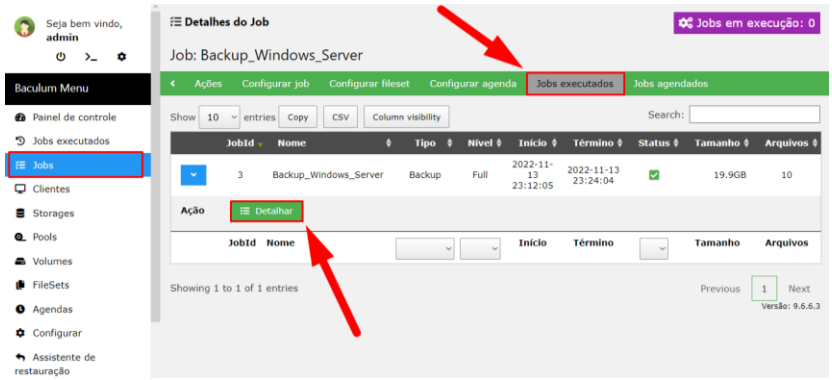
Assim que finalizado o backup, poderá ser visualizado o histórico no menu “Jobs executados”, conforme exibido na Figura 89.

Figura 89 – Histórico de backups – Bacula Backup

Fonte: Próprio autor (2022).

Para detalhar a rotina executada, deverá ser acessado o menu “Jobs”, clicar sobre a aba “Jobs executados” e na opção “Detalhar” abaixo da rotina informada, conforme exibido na Figura 90.

Figura 90 – Detalhamento de backups executados – Bacula Backup



Fonte: Próprio autor (2022).

Nos detalhes do backup realizado pode-se identificar informações relevantes, como o tempo que levou para completar a tarefa (11 minutos e 59 segundos), a compressão dos dados (35.9%), o espaço de armazenamento que utilizou (20.08 GB) e se finalizou com sucesso (Figura 91). Através da compressão, o tamanho total diminuiu cerca de 8,82 GB.

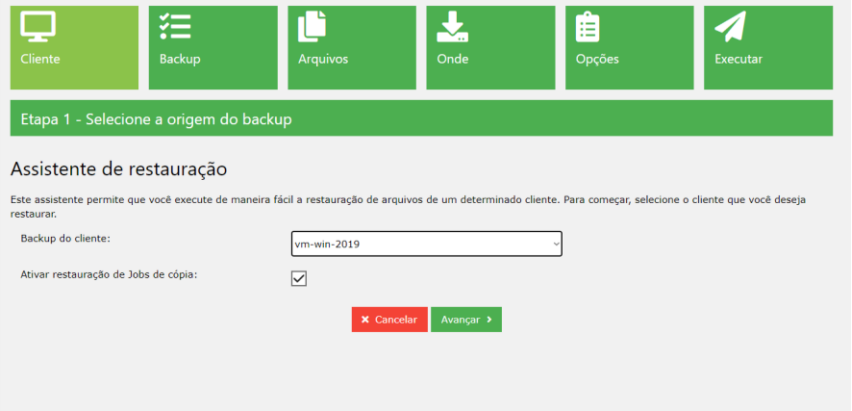
Figura 91 – Informações de backups executados – Bacula Backup

```
Build OS:               x86_64-pc-linux-gnu ubuntu 20.04
JobId:                  3
Job:                    Backup_Windows_Server.2022-11-13_23.12.03_35
Backup Level:           Full
Client:                 "vm-win-2019" 7.4.4 (28Sep16) Microsoft Standard Edition (build 9200), 64-bit,Cross-compile,Win64
FileSet:                "Backup_Teste_Bacula" 2022-11-13 23:11:37
Pool:                   "File" (From Command input)
Catalog:                "MyCatalog" (From Client resource)
Storage:                "File1" (From Command input)
Scheduled time:         13-nov-2022 23:12:03
Start time:             13-nov-2022 23:12:05
End time:               13-nov-2022 23:24:04
Elapsed time:           11 mins 59 secs
Priority:               10
FD Files Written:       10
SD Files Written:       10
FD Bytes Written:       19,956,683,246 (19.95 GB)
SD Bytes Written:       19,956,685,262 (19.95 GB)
Rate:                   27756.2 KB/s
Software Compression:   35.9% 1.6:1
Comm Line Compression:  None
Snapshot/VSS:           yes
Encryption:             no
Accurate:               no
Volume name(s):         Vol-0001
Volume Session Id:      3
Volume Session Time:    1668366971
Last Volume Bytes:      20,088,085,202 (20.08 GB)
Non-fatal FD errors:    0
SD Errors:              0
FD termination status:  OK
SD termination status:  OK
Termination:            Backup OK
```

Fonte: Próprio autor (2022).

Para realizar a recuperação dos dados armazenados deve-se acessar o campo de assistente de recuperação da ferramenta no menu principal. Após acessar o assistente irá exibir uma janela solicitando para selecionar o cliente que foi realizado o backup, no caso deste teste é selecionado o “vm-win-2019” (Figura 92).

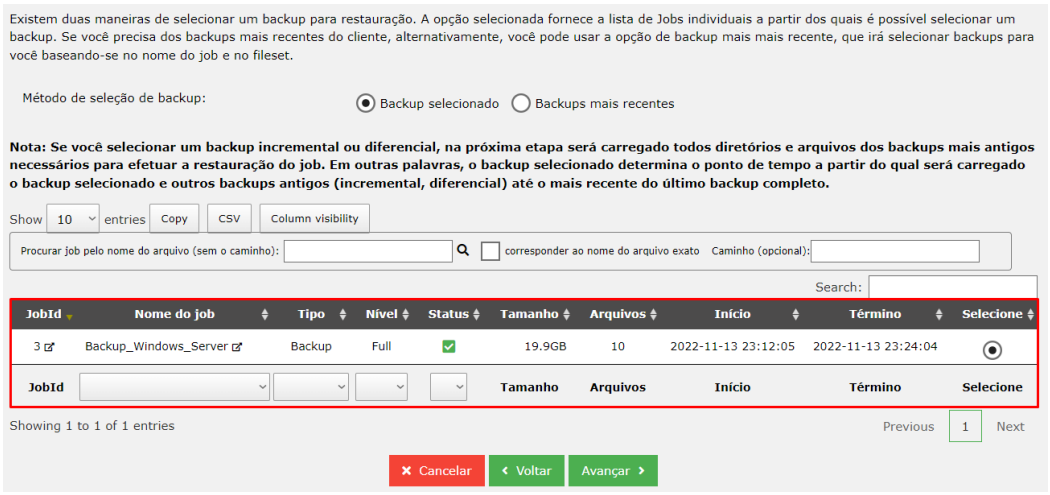
Figura 92 – Recuperação do backup – Bacula Backup



Fonte: Próprio autor (2022).

Após avançar a tela de recuperação, será solicitado o método de seleção de backup. Neste caso será mantido a opção pré-selecionada “Backup selecionado”, exibindo a rotina executada (Figura 93).

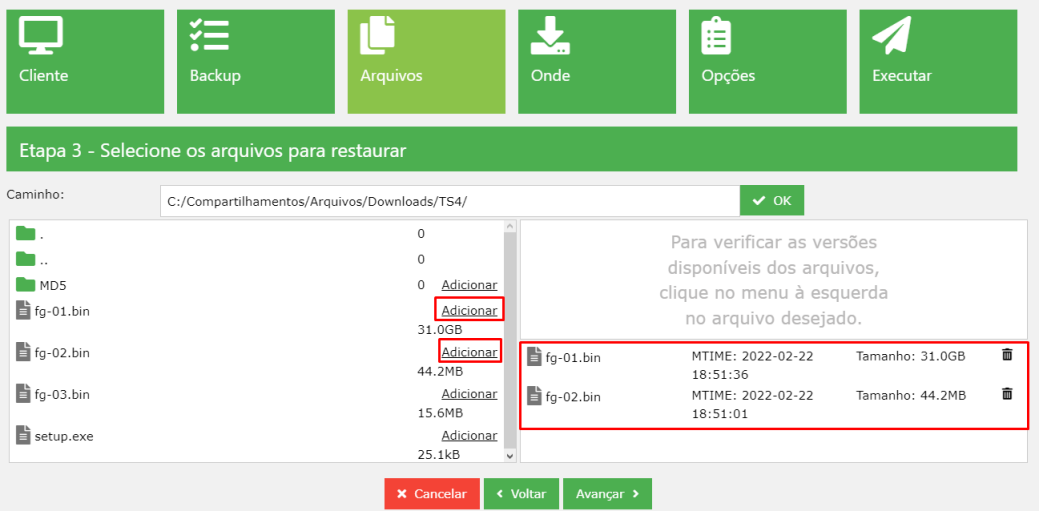
Figura 93 – Seleção para recuperação – Bacula Backup



Fonte: Próprio autor (2022).

Na próxima tela é definido os arquivos ou diretórios que serão recuperados, no teste foi selecionado dois arquivos aleatórios e foram exibidos no canto direito para restauração (Figura 94).

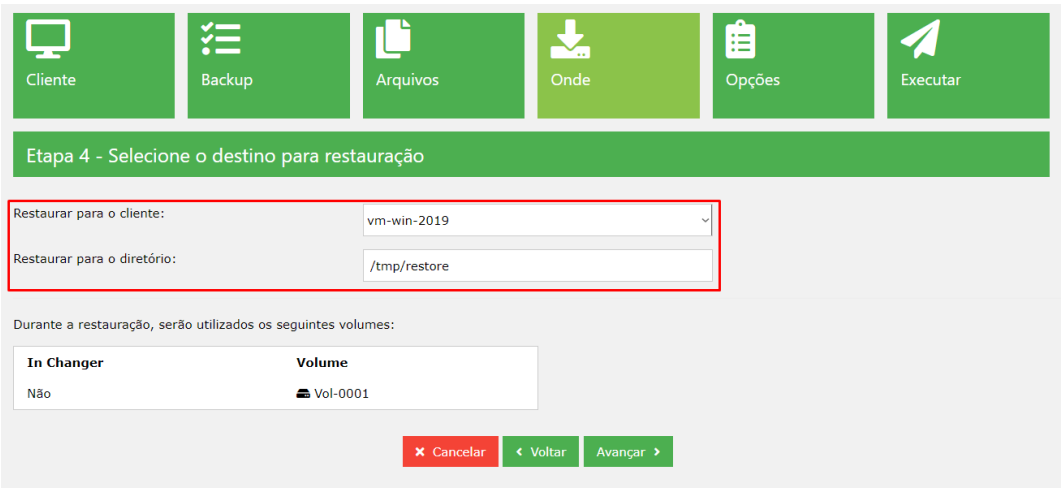
Figura 94 – Arquivos para restauração – Bacula Backup



Fonte: Próprio autor (2022).

Após a seleção dos arquivos é solicitado o local de restauração, sendo selecionado o servidor cliente “vm-win-2019” e o diretório do local “/tmp/restore” (Figura 95).

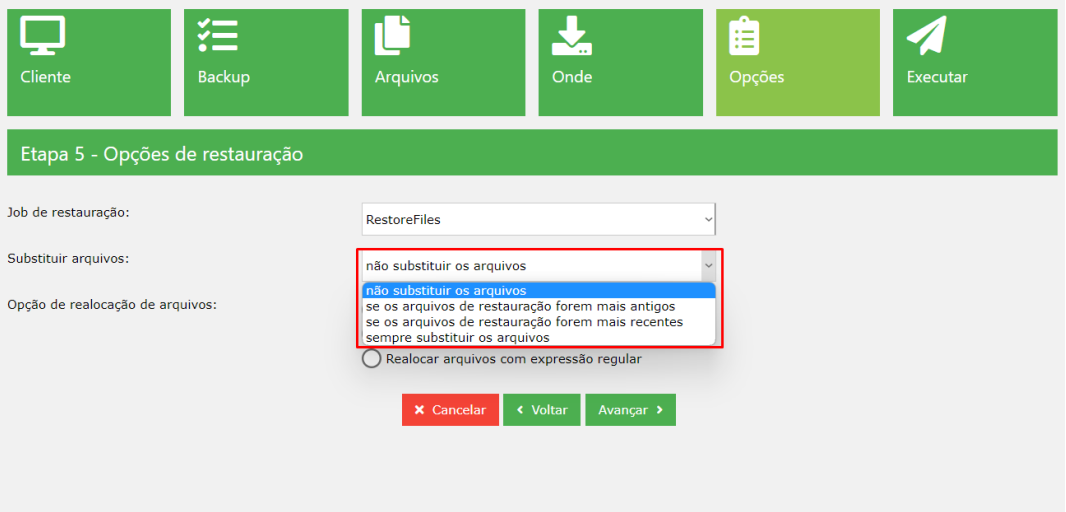
Figura 95 – Destino para restauração – Bacula Backup



Fonte: Próprio autor (2022).

Passando para as opções de restauração, é definido se deseja substituir os arquivos caso existentes no diretório, possuindo as opções de substituição se caso os arquivos existentes forem mais antigos ou mais recentes, e sempre substituir os arquivos (Figura 96).

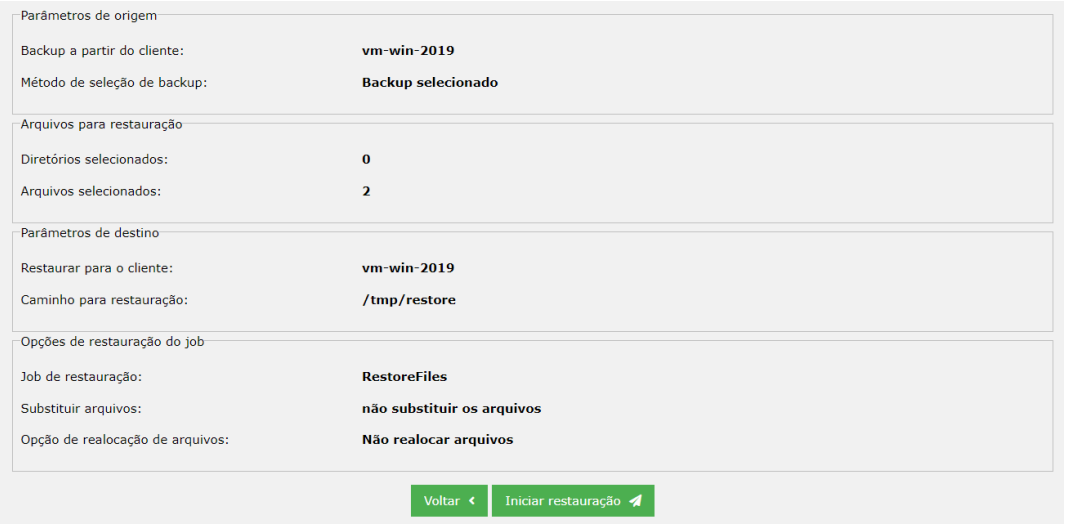
Figura 96 – Opções de restauração – Bacula Backup



Fonte: Próprio autor (2022).

Por fim, é exibido um resumo da restauração antes do usuário decidir ou não se deseja executar a tarefa, tornando assim um método contra erros do usuário (Figura 97).

Figura 97 – Resumo de restauração – Bacula Backup



Fonte: Próprio autor (2022).

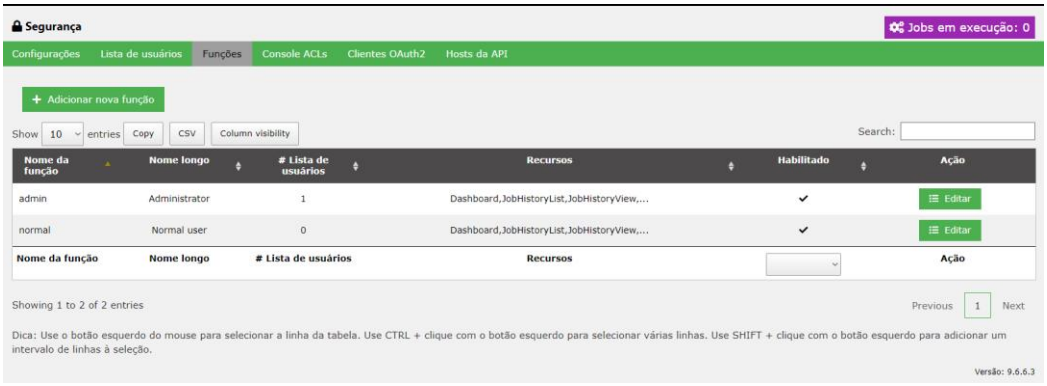
A ferramenta também exibe gráficos personalizados para relatórios, assim pode ser identificado de maneira dinâmica como as rotinas de backup rodaram (Figura 98).

Figura 98 – Gráficos – Bacula Backup

Fonte: Próprio autor (2022).

Em segurança a ferramenta permite a configuração de acesso para cada usuário que irá acessar no portal web, podendo ter vários usuários manuseando e monitorando a ferramenta, além de listá-los na aba de “Lista de Usuários” (Figura 99).

Figura 99 – Funções de segurança – Bacula Backup



Fonte: Próprio autor (2022).

4.6 COMPARATIVO DE FERRAMENTAS TESTADAS

As ferramentas de backup Acronis, Veeam e Bacula foram testadas e analisadas de acordo com os critérios definidos no processo de avaliação das ferramentas. Com isso, é possível identificar pontos relevantes que devem ser levados em consideração no processo de comparação:

- **Backup em nuvem:** A ferramenta Acronis atendeu aos critérios, possuindo sua forma de backup em nuvem paga, de acordo com a

quantidade de dados enviados a nuvem. Através dos testes foi identificado que a ferramenta disponibiliza um armazenamento nos servidores da própria empresa, sem necessidade de configuração de serviços adicionais. A ferramenta Veeam possui a funcionalidade de inclusão de um serviço em nuvem, mas não fornece de maneira gratuita em sua versão Community. Nos testes do Bacula não foi encontrado locais de configuração para um serviço em nuvem em seu painel de gerenciamento web.

- **Backup em rede:** As ferramentas Acronis e Veeam atenderam aos critérios para armazenamento em rede, permitindo a inclusão de compartilhamentos em NFS ou SMB, além da sua fácil configuração e simplicidade nas opções informadas. A ferramenta Bacula tornou o processo difícil, sem permitir configuração em seu painel de gerenciamento web, sendo necessário criar montagens dentro do servidor principal Linux, não funcionando como o esperado.

- **Backup em HD externo:** As ferramentas Acronis e Veeam atenderam aos critérios para armazenamento em HD externo, identificando as montagens dos discos no sistema operacional e permitindo a criação de backups. A ferramenta Bacula não atendeu o critério em sua configuração web.

- **Backup local:** Todas as ferramentas atenderam os critérios de backup local, permitindo o backup ser realizado localmente nas máquinas. Ressaltando que a ferramenta Bacula permitiu apenas o backup local em seu servidor principal.

- **Backup em fita:** As ferramentas Veeam e Bacula possuem a configuração de backup em fita. Sendo a Veeam necessário a configuração de um servidor de fitas e a Bacula permite o backup diretamente nas fitas. A ferramenta Acronis em sua versão testada não

permite a configuração de backup em fitas ou servidores de fitas magnéticas.

- **Backup completo, incremental e diferencial:** As ferramentas Acronis e Bacula permitem a criação de backups completos, incrementais e diferenciais. A ferramenta Veeam não possui a funcionalidade de backup diferencial.

- **Agendamento de backup:** Todas as ferramentas testadas atenderam aos critérios de agendamentos de backup.

- **Eficiência de desempenho:** As avaliações de desempenho foram definidas através da análise dos backups gerados pelas ferramentas testadas e podem ser visualizadas as informações de cada backup no Quadro 5 e Quadro 6.

Quadro 5 – Backup máquina virtual Windows - Eficiência

	Acronis	**Veeam**	**Bacula**
Tempo	41 minutos	58 minutos	11 minutos
Processamento	119 GB	115.9 GB	28.9 GB
Gravação	80.4 GB	92.5 GB	20.8 GB
Compressão	38.6 GB	23.4 GB	8.82 GB
Gravação por min.	1.96 GB/min	1.60 GB/min	1.90 GB/min
Tipo de backup	Completo	Completo	Arquivos

Fonte: Próprio autor (2022).

Quadro 6 – Backup máquina virtual Ubuntu – Eficiência

	Acronis	**Veeam**
Tempo	53 minutos	55 minutos
Processamento	118 GB	134 GB
Gravação	79 GB	95.3 GB
Compressão	39 GB	39.4 GB
Gravação por min.	1.49 GB/min	1.73 GB/min
Tipo de backup	Completo	Completo

Fonte: Próprio autor (2022).

As ferramentas de backup Acronis e Veeam realizaram um backup completo das máquinas virtuais Windows e Ubuntu. Foram levados em consideração o tempo

de execução de cada tarefa, o processamento dos dados, gravação em disco, compressão de dados, gravação por minuto e o tipo de backup. O processamento das máquinas virtuais em cada ferramenta possui informações divergentes devido ao método de backup de cada ferramenta. Por exemplo, o Acronis por possuir um agente cliente instalado na máquina virtual realiza o processamento de todos os arquivos contidos no sistema operacional, possuindo a informação mais precisa, em contrapartida a ferramenta Veeam busca as informações do virtualizador Hyper-V do Windows Server, onde analisa e processa os dados de acordo com o disco virtual da máquina virtual. A ferramenta Bacula foi desconsiderada do teste do Ubuntu por não ter sido possível efetuar a instalação cliente no sistema operacional.

A ferramenta Bacula realizou o backup de um diretório de arquivos da base de dados, gravando 1.90 GB por minuto, no total de 28.9 GB em 11 minutos de duração. O Acronis levou 41 minutos para gravar 80.4 GB do Windows, tendo uma taxa de velocidade de 1.96 GB por minuto de gravação; no Ubuntu levou 53 minutos para gravar 79 GB, tendo taxa de velocidade de gravação de 1.49 GB por minuto. O Veeam levou 58 minutos para gravar 92.5 GB do Windows, tendo uma taxa de velocidade de 1.60 GB por minuto; no Ubuntu levou 55 minutos para gravar 95.3 GB, tendo uma taxa de velocidade de 1.73 GB por minuto.

- **Compatibilidade:** As ferramentas Acronis, Veeam e Bacula possuem a aplicação que roda em conjunto com o sistema operacional, através dos seus serviços e troca de informações. A ferramenta Acronis possui uma aplicação que pode pausar os backups diretamente por dentro da máquina virtual e que realiza a comunicação com a painel web. A ferramenta Bacula possui a aplicação rodando por serviço no sistema operacional que gerencia a comunicação com o painel web, também coleta informações de arquivos locais que podem ser usados para configurações de storages e dispositivos dentro da ferramenta. A ferramenta Veeam possui a aplicação servidor que se comunica com o virtualizador e obtém as máquinas virtuais criadas nele, também é feito todo o controle da ferramenta através desta aplicação.

- **Usabilidade:** A ferramenta Acronis possui uma interface amigável e fácil de utilizar, as opções são intuitivas e práticas para usuários com menos

experiências aprender sem precisar buscar muitas informações. Seu controle é feito através da aplicação em nuvem gerenciada pela própria Acronis e depende de comunicação com a internet para acesso ao portal. Em determinados momentos ocorre lentidão no acesso e pode causar perda de conexão, precisando realizar a atualização da página do navegador para retomar o acesso. A ferramenta Veeam apresenta uma interface com mais informações na tela a primeiro momento, possui funções fáceis de utilizar e configurar, mas demanda um pouco mais de tempo para entender seu funcionamento e configurações. A ferramenta Bacula possui grande dificuldade para sua instalação e configuração, além dos manuais de apoio não serem práticos demanda tempo para aprender e resolver problemas que a própria ferramenta apresenta. Suas funções são difíceis de utilizar, não tendo clareza nas configurações e apresentando erros sem muita descrição, requer conhecimento avançado para instalação e utilização da ferramenta.

- **Portabilidade:** Todas as ferramentas testadas são compatíveis com sistemas operacionais Windows e Linux. A ferramenta Bacula apresenta problemas para instalação do modo cliente no sistema operacional Ubuntu 22.04, não sendo possível realizar a instalação para teste.

- **Confiabilidade:** Somente a ferramenta Acronis possui a funcionalidade de retomar ao ponto que parou caso ocorrer um problema no backup. Esta funcionalidade é implantada no backup em nuvem, não contemplando no backup local. As demais ferramentas não atendem esse critério e requer o processamento e gravação total após um erro na rotina de backup. As ferramentas Acronis e Veeam permitem a configuração nas rotinas de backup caso ocorra alguma falha, para rodar novamente em um período estabelecido. Não foi encontrado na ferramenta Bacula esta configuração. Todas as ferramentas estiveram disponíveis e sem interrupções no período de teste realizado.

- **Segurança:** Todas as ferramentas testadas possuem autenticação de usuário na sua inicialização, possuindo também gerenciamento de

usuários. As ferramentas Acronis e Veeam permitem a inclusão de senha na geração do backup e a utilização de usuários específicos para acesso aos compartilhamentos nos dispositivos. A ferramenta Bacula não foi localizado opção de gerenciamento de senha na geração do backup. Todas apresentam um método de criptografia para seus backups gerados.

- **Recuperação:** Todas as ferramentas realizaram recuperação total dos dados gerados no backup. A ferramenta Acronis permitiu a recuperação dos backups em modo de arquivos, pastas, unidades e máquina inteira. A ferramenta Veeam permitiu a recuperação apenas da máquina inteira, sem demais opções. A ferramenta Bacula permitiu apenas a recuperação de arquivos e pastas.

4.7 CONSIDERAÇÕES FINAIS DO CAPÍTULO

O capítulo apresentou a proposta de solução através dos critérios de avaliação definidos. Concluindo a avaliação das ferramentas no processo quantitativo, através de informações disponibilizadas no site da desenvolvedora/distribuidora das ferramentas. Através das avaliações do quadro foi possível identificar as ferramentas que se destacaram por suas funcionalidades, sendo selecionadas para o teste qualitativo, realizando um estudo de caso para comprovar sua eficácia.

Para a realização dos testes foi efetuado um processo padrão para cada ferramenta, sendo eles a preparação do ambiente de testes, instalação da ferramenta, configuração da comunicação das máquinas clientes, configuração do armazenamento, criação das rotinas de backup, realização de backup/recuperação e demais funcionalidades de cada ferramenta. Com os testes realizados, foi possível efetuar a comparação das ferramentas, através dos critérios de avaliação em relação às funcionalidades apresentadas pelas ferramentas.

5 CONCLUSÕES

Por meio dos estudos realizados sobre backup abordados neste trabalho, foram identificados vários pontos importantes que são válidos a ressaltar, como a utilização de uma ferramenta de backup em ambiente empresarial, tal como uma boa gestão de TI para o gerenciamento desses backups e a importância do salvamento de dados de backup em servidores remotos, protegendo-os de catástrofes e desastres naturais.

A utilização de ferramentas de backup é de extrema importância atualmente. Conforme os estudos realizados foram constatados grandes números de ataques de sequestros de dados que causam perdas de alto valor para as empresas. Neste contexto, a realização de backup de dados é essencial para garantir a continuidade da empresa no mercado, tendo em vista que o sigilo e integridade das informações são fundamentais para o andamento da empresa.

Atualmente há diversas ferramentas de backup gratuitas disponíveis no mercado, tornando necessário avaliar a adequação dessas ferramentas para o uso corporativo. No escopo deste trabalho foram selecionadas ferramentas de backup gratuitas com intuito de analisar e avaliar quais são adequadas para uma empresa de pequeno porte. Neste propósito, estabeleceu-se um processo comparativo entre as ferramentas gratuitas e uma ferramenta de referência, paga, a fim de avaliar a adequação de uso.

As normas ISO/IEC 25040 e ISO/IEC 25010 serviram de base para definição do processo comparativo, bem como fundamentar a escolha de critérios de avaliação das ferramentas. O processo avaliativo desenvolveu-se em duas etapas: uma quantitativa e outra qualitativa. Na etapa quantitativa foram avaliadas comparativamente as ferramentas Acronis, Cobian, Veeam, Bacula, AMANDA, Iperius e Comodo, sob alguns critérios previamente definidos. Na etapa qualitativa, as ferramentas melhores qualificadas foram testadas em um ambiente experimental a fim de efetuar-se a avaliação qualitativa em relação à ferramenta paga de referência.

Com a avaliação qualitativa foi identificado que as ferramentas gratuitas em certos pontos se igualavam a ferramenta paga de referência, como principalmente no critério de eficiência e recuperação de backups. Foi possível validar que a ferramenta de referência se sobressai em quase todos os aspectos sobre as ferramentas gratuitas, exceto por não possuir a funcionalidade de backup em fita, no qual as

ferramentas gratuitas mostraram possuir a funcionalidade. A ferramenta Veeam Backup se destacou entre as gratuitas, tendo uma facilidade em instalação e configuração e usabilidade, porém não possui a funcionalidade de backup diferencial, e em seus modos de recuperação não permitiu a recuperação de arquivos e pastas. Em contrapartida a ferramenta Bacula, que nos testes quantitativos obteve a maior nota, não representou uma boa avaliação nos testes qualitativos. Por ser difícil de instalar, configurar e utilizar, precisando de treinamentos, consultorias e preparações no ambiente, ela acaba se tornando inviável.

Portanto, pode-se definir que a ferramenta Veeam Backup and Replication Community Edition possui a eficácia para implementação em uma empresa de pequeno porte. Sua licença gratuita contemplando até 10 servidores/máquinas virtuais pode atender um ambiente corporativo pequeno que precise salvar o estado de seus servidores através de rotinas de backup personalizadas e automatizadas.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 14598-1:2001: Tecnologia de Informacao: Avaliacao de Produto de Software**. [S.l.: s.n.], 2001.

ABNT. **NBR ISO/IEC 9126-1:2003: Engenharia de Software - Qualidade de Produto**. [S.l.: s.n.], 2003.

ACRONIS. **Acronis Backup.** 2022. Disponível em: https://www.acronis.com/pt-br/. Acesso em: 20 abr. 2022.

AMANDA. **What is Amanda?** 2017. Disponível em: http://www.amanda.org. Acesso em: 24 abr. 2022.

BACULA. **Ainda não entendi: o que é o Bacula?** 2022. Disponível em: https://www.bacula.lat. Acesso em: 20 abr. 2022.

BRANDT, Andrew . Sophos. **Sophos releases the 2022 Threat Report.** 2021. Disponível em: https://news.sophos.com/en-us/2021/11/09/2022-threat-report/. Acesso em: 30 mar. 2022.

CHAVES, Vinicíus. Platon. **O que é Backup em Nuvem?** 2020. Disponível em: https://www.platon.com.br/blog/o-que-e-backup-em-nuvem/. Acesso em: 05 abr. 2022.

COBIANSOFT. **Cobian Backup/Cobian Reflector.** 2019. Disponível em: https://www.cobiansoft.com/cobianbackup.html. Acesso em: 24 abr. 2022.

COMODO. **Getting Started with Comodo Backup.** 2022. Disponível em: https://www.comodo.com/home/backup-online-storage/backup-first-time-setup.php. Acesso em: 11 out. 2022.

COUGIAS, D. J.; HEIBERGER, E. L.; KOOP, K. **The Backup Book: Disaster Recovery from Desktop to Data Center**. 3. ed. Lecanto, p. 293.

DELL. **Fita ou disco?** Escolhendo o backup ideal para a sua empresa. 2021. Disponível em: https://www.dell.com/learn/br/pt/brbsdt1/sb360/article-disk-vs-tape. Acesso em: 10 abr. 2022.

FARIA, Heitor Medrado de. **Bacula Ferramenta Livre de Backup**. Rio de Janeiro: Brasport, 2010.

FIALHO JUNIOR, Mozart. **Guia Essencial do Backup**: tudo o que você precisa saber para não perder dados vitais em seu PC!. São Paulo: Digerati Books, 2007.

GARTNER. **What is Enterprise Backup and Recovery Software Solutions?** 2022. Disponível em: https://www.gartner.com/reviews/market/enterprise-backup-and-recovery-software-solutions. Acesso em: 27 out. 2022.

GARTNER. **The Cost of Downtime.** 2014. Disponível em: https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/. Acesso em: 20 nov. 2022.

GARTNER. **Quadrante Mágico sobre soluções de software de recuperação e backup corporativas.** 2022. Disponível em: https://www.gartner.com/technology/media-products/reprints/Veeam/1-2AQ21WOX-PTB.html. Acesso em: 10 out. 2022.

GAZOLA, Rodrigo. Addee. **RTO e RPO: entenda o que são e quais são as diferenças entre eles.** 2019. Disponível em: https://addee.com.br/blog/rto-e-rpo-o-que-sao-e-quais-sao-as-diferencas/. Acesso em: 10 abr. 2022.

GETAPP. **Descubra os melhores apps para expandir sua empresa**. 2022. Disponível em: https://www.getapp.com.br/. Acesso em: 20 nov. 2022.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Porto Alegre: Bookman, 2013.

HOSTONE. **Softwares de backup gratuitos: 6 sugestões para a sua infraestrutura de TI.** 2019. Disponível em: https://blog.hostone.com.br/software-de-backup/. Acesso em: 15 out. 2022.

INFOR CHANNEL. **Ransomware somou 623,3 milhões de ataques em 2021, diz relatório.** 2022. Disponível em: https://inforchannel.com.br/2022/03/15/ransomware-somou-6233-milhoes-de-ataques-em-2021-diz-relatorio/. Acesso em: 10 abr. 2022.

INFOR CHANNEL. **SonicWall confirma que onda de ransomware dobra 2021.** 2022. Disponível em: https://inforchannel.com.br/2022/02/18/sonicwall-confirma-que-onda-de-ransomware-dobra-2021/. Acesso em: 10 abr. 2022.

IPERIUS. **Estenda a proteção para seus dados.** 2022. Disponível em: https://www.iperiusbackup.com. Acesso em: 11 out. 2022.

ISO/IEC.; **COMMISSION the I. E. ISO/IEC 25010-1:2011: Systems and Software Engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - System and Software Quality Models.** [S.l.: s.n.], 2011.

ISO/IEC. **COMMISSION the I. E. ISO/IEC 25040-1:2011:Systems and Software Engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - Evaluation Process.** [S.l.: s.n.], 2011.

LTO. **Fita LTO 7 DELL**. 2022. Disponível em: https://www.lto.com.br/fita/lto-7-dell. Acesso em: 10 abr. 2022.

MAGALHÃES, Ivan Luizio.; PINHEIRO, Walfrido Brito. **Gerenciamento de serviços de ti na prática: Uma abordagem com base na ITIL**. São Paulo: Novatec, 2007.

MANDIC. **Aplicações do Backup na Nuvem para Empresas.** 2022. Disponível em: https://www.mandic.com.br/solucoes/backup-online/. Acesso em: 07 abr. 2022.

MOTTA, Sérgio. **10 programas gratuitos de backup para Windows.** 2022. Disponível em: https://www.softdownload.com.br/10-programas-gratuitos-backup-arquivos-windows.html. Acesso em: 16 out. 2022.

NASCIMENTO, Daniel Sobral do. **A POLÍTICA DE BACKUP NAS ORGANIZAÇÕES**. 2015. 81 f. Monografia (Especialização) - Curso de Curso Superior de Tecnologia em Segurança da Informação, Faculdade de Tecnologia de Americana, Americana, 2015. Disponível em: http://ric.cps.sp.gov.br/bitstream/123456789/926/1/20152S_NASCIMENTODanielSobraldo_CD2488.pdf. Acesso em: 10 abr. 2022.

NORTON. **O que é backup na nuvem?** 2021. Disponível em: https://br.norton.com/feature/backup. Acesso em: 13 abr. 2022.

QNAP. Tipos de backup: **Completo (full), Incremental ou Diferencial - Qual é o Melhor**? 2019. Disponível em: https://www.qnapbrasil.com.br/blog/post/tipos-de-backup-completo-full-incremental-diferencial. Acesso em: 08 abr. 2022.

OHUB. **7 ferramentas de backup corporativo free e pagas.** 2022. Disponível em: https://www.ohub.com.br/ideias/ferramentas-backup-corporativo/. Acesso em: 12 out. 2022.

QUALYTEAM. **Quantos GB sua empresa precisa para armazenar dados.** 2016. Disponível em: https://qualyteam.com/pb/blog/o-que-e-armazenamento-e-quantos-gb-sua-empresa-precisa/. Acesso em: 17 out. 2022.

SEAGATE. **O que é NAS (Network Attached Storage) e por que o NAS é importante para pequenas empresas?** 2022. Disponível em: https://www.seagate.com/br/pt/tech-insights/what-is-nas-master-ti/. Acesso em: 22 abr. 2022.

SOFTEX. **MPS.BR Melhoria de Processo de Software Brasileiro: Guia de Aquisicao**. [S.l.:s.n.], 2013.

TECHTUDO (ed.). **Melhores programas para fazer backup no PC com Windows.** 2022. Disponível em: https://www.techtudo.com.br/kits/melhores-programas-para-fazer-backup-no-pc-com-windows.html. Acesso em: 12 set. 2022.

TI INSIDE. **Pesquisa: 70% das empresas desejam executar a maioria de suas aplicações na nuvem.** 2020. Disponível em: https://tiinside.com.br/26/03/2020/pesquisa-70-das-empresas-desejam-executar-a-maioria-de-suas-aplicacoes-na-nuvem/. Acesso em: 23 abr. 2022.

VEEAM. **#1 BACKUP & RECOVERY PROVIDER WORLDWIDE.** 2022. Disponível em: https://www.veeam.com. Acesso em: 10 out. 2022.

WONDERSHARE. **O melhor software de backup incremental para o sistema Windows.** 2022. Disponível em: https://recoverit.wondershare.com.br/data-backup/best-incremental-backup-software-for-windows-system.html#part1. Acesso em: 15 out. 2022.