FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

José Ricardo Pereira

GESTÃO DE *BACKUP:* UM ESTUDO DE CASO NUMA EMPRESA PRESTADORA DE SERVIÇOS DE *FULL OUTSOURCING*

Americana, SP
2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

José Ricardo Pereira

GESTÃO DE *BACKUP:* UM ESTUDO DE CASO NUMA EMPRESA PRESTADORA DE SERVIÇOS DE *FULL OUTSOURCING*

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do (a) Prof.(a) Me. Francisco Carlos Mancin.

Área de concentração: Segurança da Informação.

Americana, SP.

2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

P492g PEREIRA, José Ricardo

Gestão de backup: um estudo de caso numa empresa prestadora de serviços de full outsourcing. / José Ricardo Pereira. – Americana, 2018.

79f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Francisco Carlos Mancin

1. Segurança em sistemas de informação I. MANCIN, Francisco Carlos II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

José Ricardo Pereira

GESTÃO DE *BACKUP:* UM ESTUDO DE CASO NUMA EMPRESA PRESTADORA DE SERVIÇOS DE *FULL OUTSOURCING*

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 12 de dezembro de 2018.

Banca Examinadora:

Francisco Carlos Mancin (Presidente)
Mestre
FATEC

Clerivaldo Jose Roccia (Membro)
Mestre
FATEC

Wladimir da Costa (Membro)
Mestre
FATEC

AGRADECIMENTOS

A minha esposa por me manter no caminho mesmo quando eu já não acreditava mais que conseguiria.

Aos meus amigos de perto e de longe e aos companheiros de trabalho pelos grandes ensinamentos e direcionamentos.

A empresa pelas oportunidades que me foram concedidas e pela oportunidade de desempenhar esse trabalho.

A equipe de *Backup* da empresa pela ajuda no desenvolvimento desse trabalho.

Ao professor Mestre Francisco Carlos Mancin pelo apoio durante a elaboração desse trabalho.

Aos deuses criadores do *heavy* metal pela sua incrível criação.

DEDICATÓRIA

Aos meus pais pela vida e ensinamentos, a minha irmã por me dar um sobrinho maravilhoso e em especial a minha esposa por não me deixar desistir. A todos os professores pelos ensinamentos e conselhos, e a todos os funcionários da FATEC Americana.

RESUMO

O presente texto tem por objetivo realizar uma análise dos conceitos de *backup*, apresentando também informações a respeito dos métodos e tipos de cópias de segurança, além dos dispositivos e equipamentos utilizados nas rotinas de *backup*, é realizada também uma demonstração do uso da ferramenta ARCserve em um ambiente real. Esse trabalho procura por se amparar nos conceitos relativos a Segurança da Informação especificamente voltados para a disponibilidade dos dados e informações das organizações, está análise foi realizada por meio de uma metodologia qualitativa de estudo de caso. Esse trabalho também apresenta, conceitos sobre o Sistema de Gestão de Segurança da Informação, dados relativos ao crescimento do volume das informações, relata também a importância dos *backups* para as empresas, políticas de *backup* bem com a auditoria dessa política, contribuições realizadas pelas normas da ABNT ISO/IEC 27001 e 27002, são apresentadas também algumas medidas legais que tornam a guarda de informações obrigatória. Faz parte desse texto também, casos reais sobre a perda de dados, citando exemplos como os acontecimentos dos atentados as torres gêmeas nos Estados Unidos. Neste trabalho são apresentadas algumas ferramentas de *backup*, desde opção com custo como algumas grátis. São apresentados também, dados relativos ambiente de estudo, onde são demonstradas as informações sobre infraestrutura, volumetria de *backup* mensal, quantidade de ferramentas de *backup* instaladas no ambiente. Consta nesse trabalho, alguns guias de instalação da ferramenta ARCserve, instalação do agente de *backup*, criação de um *job* de backup e como configurar o envio de mensagens de e-mail com o status das tarefas através do ARCserve, e para finalizar esse estudo as considerações finais do autor.

Palavras Chave: Segurança da Informação; Disponibilidade; *Backup.*

ABSTRACT

The purpose of this text is accomplish an analysis of backup concepts and report information about methods and different types of backups, besides the devices and equipment used in backup routines and a use demonstration of the ARCserve tool in a real environment. This assignment is based on relative concept of Information Security, focused on the data availability and organizations information. This activity was realized through a qualitative methodology case study. Also presents concepts concerning the Information Security Management System, related data about increase of the information size, notice the importance of backups for companies, backup policies as well as the audit of this made by the norms of the ABNT ISO / IEC 27001 and 27002, some legal measures are also presented that make the information storage mandatory. It is included real cases of data loss, with examples such as the events of the attacks on the World Trade Center in the United States. Some backup tools are presented, a couple of payed and free options. Presents the data of study environment, where it is demonstrated the information about infrastructure, monthly backup measure, and number of backup tools are installed in the environment demonstrated. To complete some installation guides to ARCserve tool, installation of backup agent, creation of a backup job, how to configure the send email messages included status of jobs through ARCserve, and at the end of this study, the author's final considerations.

Keywords: *Information Security; Availability; Backup.*

Sumário

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira da Normas Técnicas
BPO	*Business Process Outsourcing*
CTN	Código Tributário Nacional
DDS	*Digital Data Storage*
DLT	*Digital Linear Tape*
LTO	*Linear Tape-open*
GRC	*Governance, Risk and Compliance*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ITO	*Information Technology Outsourcing*
SI	Segurança da Informação
SGSI	Sistema de Gestão de Segurança da Informação
SMTP	*Simple Mail Transfer Protocol*
SSD	*State Solid Disk*
TB	*Terabyte*
TI	Tecnologia da Informação
TSM	Tivoli Storage Manager
U.S	United States

1. INTRODUÇÃO

O presente trabalho tem como assunto a Segurança da Informação (SI), que basicamente visa a proteção dos dados e informações das empresas e de usuários comuns dentro da Internet. Atualmente a informação é um dos, senão o mais importante ativo dentro do ambiente corporativo (SÊMOLA, 2013). Devido a esse alto grau de importância da informação, cresceu também a necessidade e preocupação por parte das empresas em proteger tais dados. Dentro da SI podem ser encontradas diversas técnicas para elevar o grau de segurança em um ambiente. O autor considera que todas essas técnicas visam garantir a confidencialidade, integridade e disponibilidade dos dados e informações de um ambiente, organização ou usuário doméstico. Esses três itens juntos formam os pilares da SI (Figura 1). Esse trabalho abordará a disponibilidade dos dados e informações através de técnicas de *backup* muito utilizadas nas empresas atualmente.

Figura 1 - Pilares da SI

Fonte: Phonoway (2015)[1]

As implementações de rotinas de *backup* visam garantir a disponibilidade das informações ou minimizar os impactos causados diante de uma perda acidental, desastres naturais ou perdas ocasionadas por meio de ações humanas.

[1] Disponível em: https://www.phonoway.com.br/solucoes/backup-na-nuvem-e-restore> Acesso em: 13 ago, 2018.

A implementação de rotinas de *backup*, é crucial para as organizações bem como para o usuário comum, pois são através dessas técnicas que é possível garantir a recuperação das informações caso elas não estejam mais disponíveis. O *backup* não é apenas utilizado para a recuperação de um ou outro arquivo, muitas vezes um *backup* pode realizar a restauração de um ambiente todo, garantindo assim a sobrevivência de uma empresa no mercado.

O presente trabalho **justifica-se** pela importância que o *backup* tem para a disponibilidade dos dados e informações, e consequentemente para a Segurança da Informação como um todo. É de suma importância que as empresas implementem técnicas de backup afim de garantir que sejam realizadas cópias de segurança de seus dados, informações e sistemas. (SOMASUNDARAM; SHRIVASTAVA, 2011).

Como **problema** foi identificado que mesmo que as organizações possuam diversas técnicas de proteção, ainda assim existe a possibilidade de ocorrer a perda ou roubo de informações, portanto é necessário garantir que haja rotinas de *backup*, rotinas essas responsáveis por garantir a disponibilidade dos dados.

A **pergunta** que este trabalho procura responder é: Com base no ambiente de estudo, a solução de *backup* utilizada pela Empresa X, atende as necessidades da empresa e é capaz de garantir a disponibilidade de seus próprios dados e de seus clientes?

Para a presente pesquisa foram levantadas quatro **hipóteses**, a) a ferramenta de *backup* possui uma interface de instalação amigável e de fácil entendimento; b) o agente de backup precisa ser instalado manualmente em cada dispositivo que terá seus dados copiados; c) é necessário conhecimento avançado para a criação das tarefas de backup; d) a ferramenta não dispõe de um método de envio de mensagens informando o status das tarefas.

O **objetivo geral** deste trabalho é o de analisar os conceitos de *backup*, bem como o processo de instalação e implementação de uma tarefa de *backup.*

Como **objetivos específicos** tem-se: a) realizar um levantamento da infraestrutura que o ambiente estudado possui; b) acompanhar/realizar a instalação da ferramenta de *backup*; c) acompanhar/realizar a criação de um *job* de *backup*.

Este trabalho caracteriza-se quanto a sua natureza como uma **pesquisa básica,** que segundo Gil (2002), tem por objetivo conceber novos conhecimentos

que podem vir a ser utilizados para futuras pesquisas ou avanços da ciência e tecnologia.

Com relação a abordagem, este trabalho trata-se de uma **pesquisa qualitativa,** que de acordo com Goldenberg (1997), *apud* Gerhardt, Silveira (2009), esse método de abordagem não se preocupa em quantificar os resultados da pesquisa, mas sim em procurar o entendimento do objeto de estudo, e com isso responder as perguntas levantadas.

O presente trabalho, foi estruturado em seis capítulos, o segundo capítulo é responsável por conceituar assuntos acerca de dados, informação e conhecimento, além de explorar conceitos relativos ao volume de dados gerados, segurança da informação, políticas e auditorias de backup e aspectos legais e a importâncias do backup para as organizações. No terceiro capítulo é possível encontrar os conceitos quem envolvem métodos de backup, tipo de backup e suas vantagens e desvantagens e as periodicidades das rotinas. O quarto capítulo trata de explorar informações sobre alguns dispositivos de armazenamento, suas capacidades e velocidades, suas propensões a falhas e são apresentadas também algumas ferramentas de backup, gratuitas e proprietárias.

O quinto capítulo é onde são descritas as informações sobre o estudo de caso, aqui são apresentados os resultados obtidos sobre o objeto de estudo, no sexto capítulo, são apresentadas as considerações finais relativas as informações levantadas no capítulo anterior.

2. REFERENCIAL TEÓRICO

Neste capítulo serão apresentados os conceitos referentes a dados, informação, conhecimento, *backup* e seus conceitos, segurança da informação, políticas de *backup*, dispositivos de armazenamento e ferramentas de *backup*.

2.1. DADOS, INFORMAÇÃO E CONHECIMENTO

Conforme Cardoso Junior (2005) apud Dantas (2011, p.9), dado é algo bruto que sozinho não tem valor ou não faz sentido, já a informação é o dado que sofreu algum tipo de tratamento e passa a ser compreensível, o conhecimento é gerado a partir da análise da informação, gerando dessa forma valor estratégico para a empresa.

Tendo em vista as definições anteriores, é possível dizer que a relação entre dados, informação e conhecimento formam uma pirâmide conforme Figura 2, onde os dados são a base que suportam os demais níveis, fornecendo valores, métricas ou características sobre algo para o nível dois, a informação, que é o dado já processado que acaba por gerar o conhecimento, esse por sua vez possui a capacidade de fornecer algum tipo de valor ou vantagem competitiva para as organizações.

Figura 2 - Pirâmide Dados, Informação e Conhecimento

Fonte: Cursos de Informática Básica[2] (2013)

2.1.1. O VALOR DA INFORMAÇÃO PARA AS CORPORAÇÕES

Conforme Sêmola (2003), o ciclo de mudanças e inovações nas empresas é constante, pois todos os segmentos empresariais ou de pesquisas não se conformam com a mesmice, e frequentemente acabam por gerar transformações que lançam novas formas de abordagem sobre um determinado assunto já estabelecido. O autor comenta que, esse ciclo de mudanças e inovações se dão por conta de novas visões ou metodologias de uso da informação já presente nas organizações ou vindas de fora.

Fontes (2006), afirma que a informação é o motor gerador de transformação no nosso mundo, o autor ainda cita que o homem é capaz de transformar dados em valor para a vida pessoal ou profissional, ou ainda em vantagem competitiva perante a concorrência.

De acordo com Choo (2003), a informação é fator primordial dentro das organizações, e que ela é responsável pelo crescimento estratégico e auxilia diretamente na adaptação as novas demandas e tendências do mercado. O autor comenta que as empresas estão sujeitas a diversas mudanças e em curtos períodos, portanto é necessário que essas organizações estejam prontas para usar a informação a seu favor, se adaptando e moldando seus negócios a fim de criar valor a seus clientes, aumentando assim sua vantagem competitiva perante as demais.

Para Fontes (2006), todas as informações devem ser protegidas contra os diversos tipos de desastres, segundo o autor as informações possuem e geram valor para as empresas, portanto, as informações são vitais para a continuidade do negócio.

2 Disponível em: <http://www.cursosdeinformaticabasica.com.br/qual-a-diferenca-entre-dados-informacao-e-conhecimento/> Acesso em 13 ago. 2018.

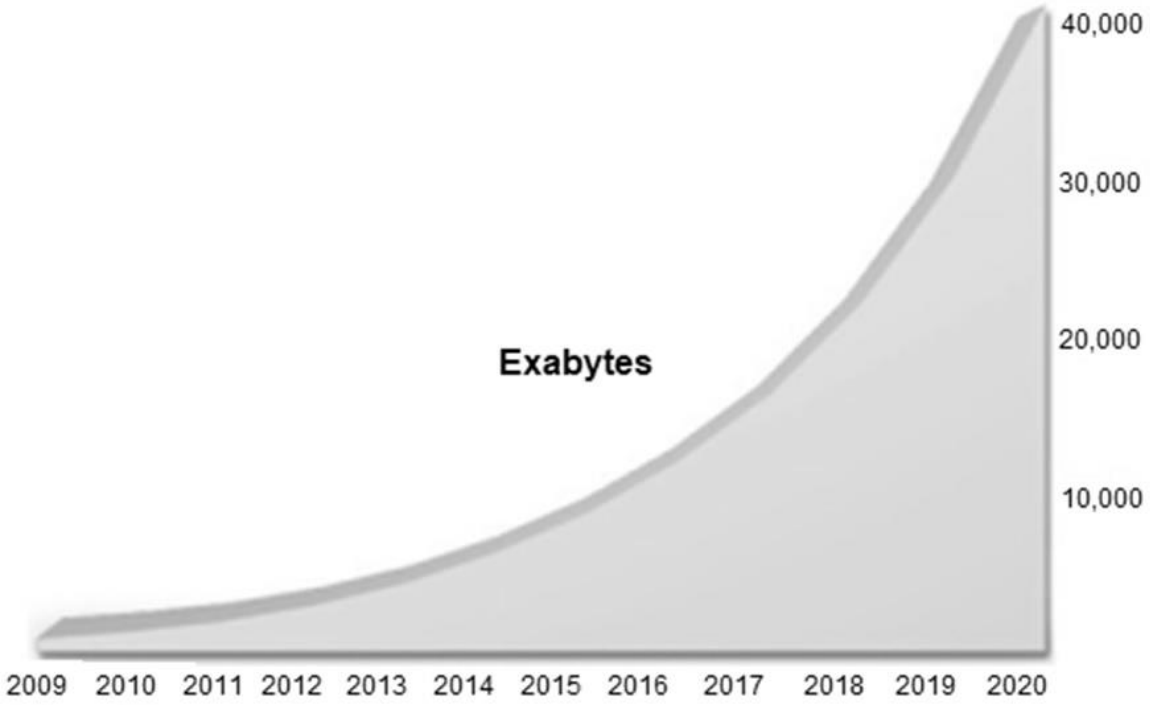
2.2. VOLUME DE DADOS GERADOS E INFRAESTRUTURA NECESSÁRIA

Eppler e Mengis (2004) apud Vick e Nagano (2012), informam que, a quantidade de informação disponível para consulta cresce a passos largos, portanto é necessário que as empresas prezem pela informação de qualidade, pois o desempenho está diretamente relacionado a qualidade da informação coletada e utilizada.

Lustosa (2001), comenta que o crescimento exponencial da informação gera um problema para sociedade moderna, tal crescimento gera uma certa dificuldade em prover informações de qualidade para os usuários e as organizações. O autor diz que a informação se faz presente em todos os níveis e setores de uma empresa e na sociedade, e que tais informações são de suma importância no crescimento de uma empresa e no desenvolvimento pessoal de cada indivíduo.

Para Ávila (2017), o crescimento do uso da internet e a popularização da tecnologia da informação, são os responsáveis pelo crescimento exponencial do volume de dados e informações gerados nos últimos anos. De acordo com o autor, conforme a necessidade por informação cresce, aumentando também a necessidade de se aprimorar as tecnologias existentes e consequentemente aumenta novamente o volume de dados e informação gerados, criando dessa forma um ciclo positivo de evolução. O autor apresenta através de um estudo desenvolvido pela EMC Corporation, "*A Universe of Opportunities and Challenges*", que em um período de 4 anos o volume de dados produzido foi de 882 *Exabytes*, foi de 166 *Exabytes* em 2006 para 988 *Exabytes* em 2010, e estimasse que esse valor pode atingir 40.000 *Exabytes* (40 trilhões de *Gigabytes*) no ano de 2020, como mostra a Figura 3.

Figura 3 - Estimativa Volume dados 2020



Fonte: *Open Knowledge* Brasil [3](2017)

2.3. SEGURANÇA DA INFORMAÇÃO COMO ESTRATÉGIA EMPRESARIAL

Conforme Jesus e Schimiguel (2018), o *backup* é uma estratégia de continuidade do negócio, com ele é possível reestabelecer as operações de uma empresa caso haja um problema, podendo ser a perda de um arquivo ou até mesmo a perda total do site da empresa ocasionados por incêndios ou uma enchente por exemplo.

O Sistema de Gestão de Segurança da Informação (SGSI), é um conjunto de medidas administrativas formada por normas, políticas e diretrizes responsáveis por diminuir os riscos à segurança da informação em uma organização (FERREIRA; ARAÚJO, 2008).

De acordo com a ABNT (2013), a norma ISO/IEC 27001:2013 tem como objetivo:

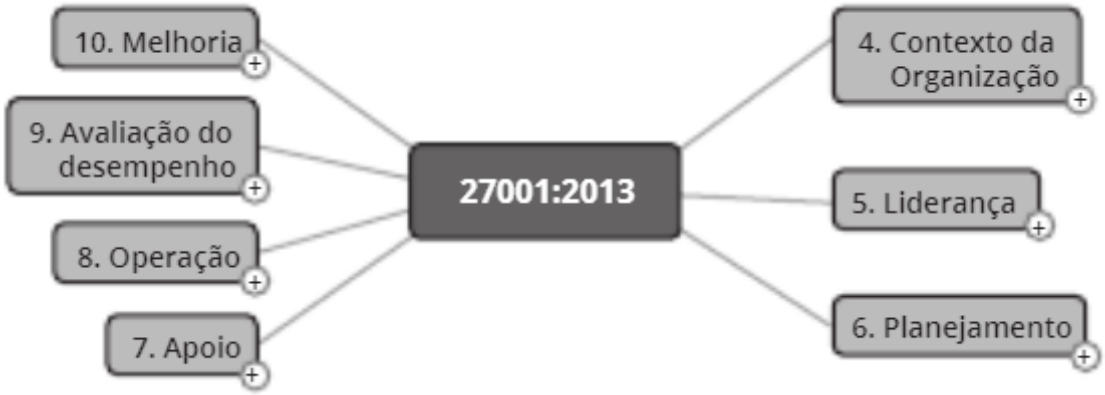
3 Disponível em: <https://br.okfn.org/2017/09/29/o-que-faremos-com-os-40-trilhoes-de-gigabytes-de-dados-disponiveis-em-2020/> Acesso em 04 set. 2018.

> "[...] prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI é uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização. São esperados que todos estes fatores de influência mudem ao longo do tempo."

Para Coelho, Araújo e Bezerra (2014), "o SGSI integra a estratégia da organização, sendo influenciado por fatores como, necessidades e objetivos, requisitos de segurança, processos e estrutura organizacional". Os autores afirmam que o SGSI, é um processo constituído de processos e diretrizes capazes de auxiliar na segurança da informação em qualquer setor de uma organização.

A norma possui em sua estrutura dez seções, onde as três primeiras tratam do escopo da mesma, enquanto as demais são responsáveis por abordar de forma direta e genérica todas as diretrizes cabíveis as empresas, independentemente de seu ramo de atuação e tamanho como mostra a Figura 4 (COELHO; ARAÚJO; BEZERRA, 2014).

Figura 4 - Seções ISO/IEC 27001:2013



Fonte: Norma ISO/IEC 27001:2013

2.4. POLÍTICA DE *BACKUP*

A política de *backup*, é fruto da política de segurança da informação, a ISO/IEC 27002:2013 (ABNT, 2013), informa que o *backup* deve possuir uma política específica capaz de apoiar a política de segurança da informação.

Bem como a política de segurança da informação, a política de *backup* também é um conjunto de normas e diretrizes responsáveis por definir como serão executadas as cópias de segurança de uma organização (FERREIRA; ARÁUJO, 2008).

Segundo a norma ISO/IEC 27002:2013, dentro de uma política de *backup*, devem ser contemplados os recursos necessários para garantir, que todas as informações e softwares necessários para uma recuperação efetiva estejam disponíveis (ABNT, 2013).

2.5. AUDITORIA DA POLÍTICA DE *BACKUP*

De acordo com a norma ISO/IEC 27001:2013 (ABNT, 2013), o SGSI solicita que as organizações implementem rotinas de auditorias a fim de verificar se os requisitos solicitados estão em conformidade com a norma e com os parâmetros impostos pela própria organização. A norma estabelece que a empresa deve levar em consideração os seguintes itens:

> a) planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores;
> b) definir os critérios e o escopo da auditoria, para cada auditoria;
> c) selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria;
> d) assegurar que os resultados das auditorias são relatados para a direção pertinente.
> e) reter a informação documentada como evidência dos programas da auditoria e dos resultados da auditoria.

Por ser derivada do SGSI, a política de *backup* também deve ser auditada, basicamente, essa auditoria tenta checar se todos os requisitos pré-estabelecidos na política estão sendo cumpridos, como por exemplo verificar se as informações estão sendo armazenados de acordo com a frequência definida, para que seja possível preservar a disponibilidade dos dados (FURLAN; ASSIS, 2015). Os autores ainda

informam que, essa auditoria não deve ser realizada pela mesma equipe que gerencia as rotinas de *backup*, pois os responsáveis pelas cópias de segurança estão sujeitos a auditoria, já o processo de auditoria deve ser realizado por pessoas que consigam se manter imparciais durante esse processo de análise.

2.6. CONTRIBUIÇÕES DA ISO/IEC 27001 E 27002

As normas ISO/IEC 27001 e 27002 (ABNT, 2013), auxiliam diretamente na implantação de diretrizes para o estabelecimento de procedimentos de cópias de segurança, enquanto a ISO/IEC 27001:2013 determina os parâmetros para a implantação de um Sistema de Gestão de Segurança da Informação, que é complementada pela ISO/IEC 27002:2013 que ajuda no estabelecimento de seleções de controles de segurança da informação. A própria norma ISO/IEC 27002:2013 (ABNT, 2013), traz em seu item 12.3.1 alguns dos parâmetros de cópias de segurança, que devem ser levados em consideração durante o desenvolvimento da política de *backup*, conforme segue abaixo.

> a) registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convém que sejam produzidos;
> b) a abrangência (por exemplo, completa ou diferencial) e a frequência da geração das cópias de segurança reflitam os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;
> c) convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;
> d) convém que seja dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança (ver 11), consistentes com as normas aplicadas na instalação principal;
> e) convém que as mídias de *backup* sejam regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial; Convém que isto seja combinado com um teste de restauração e checado contra o tempo de restauração requerido. Convém que os testes da capacidade para restaurar os dados copiados sejam realizados em uma mídia de teste dedicada, não sobrepondo a mídia original, no caso em que o processo de restauração ou *backup* falhe e cause irreparável dano ou perda dos dados;
> f) em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação. (ISO/IEC 27002:2013, 2013).

2.7. A NECESSIDADE DO *BACKUP* EM AMBIENTES CORPORATIVOS

O grau de dependências das empresas relativo ao uso da informação aumenta ano a ano e devido a isso, cresce também os cuidados relativos a garantia da disponibilidade dos dados, sistemas e informações (FERREIRA; ARAÚJO, 2008).

A norma ISO/IEC 27002:2013 (ABNT, 2013), diz que os ativos das organizações são passíveis de ameaças acidentais e deliberadas, portanto, é necessário que sejam implementadas técnicas capazes de suprimir os riscos presentes em uma organização. Para tal, é necessário que as empresas adotem técnicas de *backup*, capazes de suportar a restauração de dados e sistemas vitais de uma unidade de negócio.

Além de garantir a disponibilidade dos dados em situações de riscos que podem provocar a perda desses, a disponibilização de *backups* implica no atendimento aos requisitos legais, conforme preconiza a Legislação vigente, que determina a guarda de documentos por determinado período.

2.8. *BACKUP* PARA HISTÓRICO LEGAL E FISCAL

Castro, Victorino e Tobias (2010), afirmam que na esfera comercial e fiscal, existem inicialmente três dispositivos legais que definem prazos para guarda de documentos, sendo eles:

- art. 195, parágrafo único do CTN - Código Tributário Nacional (Lei nº 5.172, de 25 de outubro de 1966);
- Art. 37 da Lei nº 9.430 de 1996;
- Art. 4º do Decreto-Lei nº 486 de 1969.

Os artigos citados acima, determinam que:

> O art. 195 do CTN, em seu parágrafo único, determina que os livros obrigatórios de escrituração comercial e fiscal e os comprovantes dos lançamentos neles efetuados serão conservados até que ocorra a prescrição dos créditos tributários decorrentes das operações a que se refiram. Ou seja, por esse dispositivo, o prazo de guarda de documentos segue o prazo de prescrição dos tributos.
>
> O art. 37 da Lei nº 9.430 de 1996 dispõe que os comprovantes da escrituração da pessoa jurídica, relativos a fatos que repercutam em lançamentos contábeis de exercícios futuros, serão conservados até que se

> opere a decadência do direito de a Fazenda Pública constituir os créditos tributários relativos a esses exercícios.
> Por sua vez, o art. 4º do Decreto-Lei nº 486 de 1969, estipula que o comerciante é obrigado a conservar em ordem enquanto não prescritas eventuais ações que lhes sejam pertinentes, a escrituração, correspondência e demais papéis relativos à atividade, ou que se referiram atos ou operações que modifiquem ou possam vir a modificar sua situação patrimonial (CASTRO; VICTORINO; TOBIAS, 2010).

Além dos órgãos citados acima, existem outros que possuem leis, regras e normas que também determinam períodos mínimos que uma empresa terá para a guarda de documentos, algumas delas são: (CASTRO; VICTORINO; TOBIAS, 2010).

- Previdência Social
- Leis Trabalhistas
- Leis Administrativas
- Regras Excepcionais

Levando-se em consideração que o Sistema de Informação deve atender aos requisitos Legais, e considerando a existência de Leis Federal, Estadual e Municipal, sabemos que a guarda e disponibilização de todos os documentos deverão atender às Leis e como o tempo de guarda não é objeto de estudo desse, não abordaremos as especificações de cada caso.

2.9. *BACKUP* PARA CONFIGURAÇÕES DOS SISTEMAS

De Melo e Gonçalves (2004), definem o *system state* como sendo responsável por guardar informações referentes as configurações do sistema operacional, tais informações são importantes quando for necessário realizar uma restauração do sistema. Conforme os autores, são componentes do estado do sistema os seguintes itens:

- arquivos de *boot*, tais como “ntldr”, “ntdetect”, etc;
- arquivos protegidos pelo *System File Protection e Performance Counter Configuration;*
- *Active Directory* (quando for um controlador de domínio);
- pasta Sysvol (quando for um controlador de domínio);
- *Certificate Server* (quanto for uma Autoridade Certificadora);
- *Cluster Database* (quando pertencer a uma rede de clusters);
- registro;
- base de dados dos objetos COM+.

Além de realizar as cópias do *system state*, é importante que durante a restauração os dispositivos de *hardware* também sejam idênticos aos anteriores, pois é possível que a restauração não funcione se os equipamentos forem diferentes. Os diretórios e volumes, também devem permanecer com as mesma nomenclaturas e letras associadas anteriormente, com isso aumenta-se as chances de se obter sucesso na restauração do estado do sistema (DE MELO, GONÇALVES, 2004).

2.10. *BACKUP* PARA GESTÃO DE NEGÓCIOS

De acordo com Albertin (2001), a Tecnologia da Informação (TI) é crucial em diversos segmentos, tanto nas camadas de operação como nos níveis de tomada de decisão. O autor ainda comenta que, “A TI é vista como uma das maiores e mais poderosas influências no planejamento das organizações.”

Chorafas (1987) apud Albertin (2001), define que o ambiente digital realizou grandes mudanças na maneira como os negócios eram gerenciados, tanto na infraestrutura como nas tecnologias de comunicação e software e no planejamento estratégico.

A crescente valorização da informação dentro das empresas, o aumento das exigências normativas, a necessidade de se manter os dados sempre disponíveis e o crescimento acelerado dos volumes de dados, exige que sejam adotadas medidas de *backup,* cada vez melhores e com menores custos, isso faz com que esse item se torne um dos grandes recursos estratégicos de uma organização, pois, garante que os ativos mais importantes estejam protegidos contra incidentes e falhas (SOMASUNDARAM; SHRIVASTAVA, 2011).

Para Ferreira e Araújo (2008), a informação tem grande valor estratégico para as empresas, e são frutos de horas de trabalho no desenvolvimento de ativos para as organizações, portanto, as técnicas de *backup* são fundamentais para manter um ambiente no ar, e garantir que as informações possam ser recuperadas quando for necessário.

2.11. CAUSAS DE PERDA DE DADOS EM AMBIENTES CORPORATIVOS

Nenhuma empresa está livre de incidentes ligados a segurança da informação ou desastres naturais, existe uma falsa sensação de que o que aconteceu com alguma empresa não irá acontecer com as demais, e esse pensamento guia as empresas em uma direção que não procura por implementar técnicas de proteção (DAWEL, 2005). O autor, através de dados divulgados na *Insight Magazine* levantados pela U.S. *Small Business Administration* informa que, após sofrer algum tipo de incidente ou desastre, 43% das empresas de pequeno e médio porte fecham permanentemente, além disso em um período de cerca de dois anos após os desastres, 29% das empresas também fecham. Portanto, 72% das empresas não sobrevivem após sofrerem com algum tipo de incidentes ou desastre.

De acordo com Fontes (2006), qualquer empresa pode sofrer vazamento de informações, e conforme o valor que essa informação tem para a organização, pode acarretar prejuízos financeiros para as organizações além de, causar impactos negativos para a imagem da empresa perante a sociedade, clientes, acionistas e demais partes interessadas.

De acordo com a empresa EMC, pertencente ao grupo DELL (2016), através de pesquisa global intitulada Índice Global de Proteção de Dados da Dell EMC, realizada entre maio e abril de 2016 pela organização Vanson Bourne, das empresas que responderam à pesquisa, 52% delas tiveram tempos de inatividade não planejada em um período de 12 meses tendo como base o ano de 2016. Além disso, a pesquisa informa que 29% dos respondentes tiveram alguma perda de dados no mesmo período (Figura 5).

Figura 5 - Inatividade e Perda de Dados

Fonte: Dell EMC[4] (2016)

A pesquisa ainda fornece dados relativos ao montante financeiro que as empresas tiveram de prejuízo, por conta das perdas de dados ou dos tempos de inatividade. De acordo com a pesquisa as empresas que tiveram problemas por perdas de dados, tiveram prejuízos financeiros de aproximadamente 914.000 mil dólares, enquanto as empresas que apresentaram tempo de inatividade não planejado de seus sistemas, tiveram um dano financeiro de cerca de 555.000 mil dólares em um período 12 tendo como base o ano de 2016 (Figura 6).

Figura 6 - Custos Financeiros

Fonte: Dell EMC[5] (2016)

4 Disponível em: <https://brazil.emc.com/infographics/global-data-protection-index-global.htm> Acesso em 09 set. 2018.

5 Disponível em: <https://brazil.emc.com/infographics/global-data-protection-index-global.htm> Acesso em 09 set. 2018.

2.11.1. ATAQUES AO WORLD TRADE CENTER

Para Dawel (2005), nos ataques terroristas de 2001 ao World Trade Center, ninguém conseguia imaginar que isso poderia acontecer, e muito menos que haveria outro ataque que atingiria a segunda torre, para o autor se a probabilidade disso acontecer fosse calculada, ela seria muito baixa.

Muitas das empresas tinham seus escritórios em uma das torres do World Trade Center, e possuíam os *backups* e suas redundâncias de informações na segunda torre, as empresas que tinham esse tipo de configuração não conseguiram retomar suas operações após os ataques. A empresa Jun He Law sofreu grandes impactos, pois todos os dados estavam armazenados nos computadores locais e não possuíam *backups* dessas informações (OPENSPACE, 2016).

Para Spaniol (2015), o 11 de setembro mostrou as organizações que elas precisam ter uma redundância de suas informações em um local longe do site original, muitas das organizações tinham um segundo datacenter porem localizado na torre vizinha ou nas imediações que foram afetadas pela destruição, isso acabou por impactar os clientes e a continuidade dos negócios das empresas.

2.11.2. *RANSONWARE* WANNACRY

No ano de 2017 houve um grande surto do *ransonware* WannaCry, que afetou tanto, empresas privadas como institutos governamentais e pessoas em diversos países. O *ransonware* ataca computadores com sistema operacional Windows e criptografa os dados, e pedem um resgate para que os dados fossem liberados para acesso novamente, na Figura 7 segue um exemplo de uma mensagem de *ransonware* (AVAST, 2017).

Figura 7 - *Ransonware* Wannacry

Fonte: Avast[6] (2017)

2.11.3. PERDA OU ROUBO DE EQUIPAMENTOS

Além de ataques arquitetados por crackers ou desastres que acarretam na perda das informações, os dados podem cair nas mãos de terceiros através do roubo ou extravio de dispositivos de armazenamento. De acordo com Gusmão (2016), em artigo publicado no site da revista Exame, no ano de 2006 nos Estados Unidos, ocorreu o extravio de um notebook que continha informações sobre aproximadamente 26,5 milhões de veteranos e militares ativos das forças armadas americanas, segundo o autor, as informações poderiam ser facilmente acessadas pois o equipamento não dispunha de nenhum tipo de criptografia ou outras forma de segurança. O autor comenta ainda que, no ano de 2009 também nos Estados Unidos, um disco rígido contendo informações de cerca de 76 milhões de veteranos foi enviado para reparo sem que seus dados fossem apagados ou que houvesse algum método de proteção.

6 Disponível em: < https://www.avast.com/pt-br/c-wannacry> Acesso em 23 set. 2018.

3. CONCEITOS DE *BACKUP*

Ferreira e Araújo (2008), afirmam que além de recursos de *hardware*, é necessário garantir as cópias dos dados e informações lógicas, aplicando procedimentos de *backup*.

De acordo com Somasundaram e Shrivastava (2011), o *backup* possui a finalidade de guardar os dados de produção, e são utilizados unicamente caso algum desses dados sejam corrompidos ou sejam perdidos de alguma forma.

Segundo Fialho Junior (2007), as cópias de segurança não devem ser uma preocupação apenas das grandes empresas e seus profissionais da TI, mas sim de todo o profissional e dos usuários finais, pois todos estão sujeitos a uma perda de informação. Ainda conforme o autor, as perdas de dados refletem em prejuízo financeiro para as empresas, e as cópias de segurança podem reduzir esse rombo nas finanças das organizações.

Faria (2014), diz que as copias de segurança assertivas, são aquelas capazes de reduzir ao máximo os impactos causados por uma perda de informação e garantem o retorno de um serviço de forma ágil e sem discrepância entre o dado perdido e o dado restaurado.

O processo de se implementar rotinas de *backup* exige que alguns pontos sejam previamente definidos, como por exemplo, granularidade do *backup*, método de *backup*, tempo de retenção, tipo de armazenamento e rotulação da mídia (FERREIRA; ARÁUJO, 2008).

3.1. MÉTODOS DE *BACKUP*

De acordo com Somasundaram e Shrivastava (2011), o método de *backup* está relacionado ao estado em que se encontram os arquivos ou programas que estão sendo copiados, onde são classificados em duas modalidades, *online* (em uso) e *off-line* (fora de uso).

3.1.1. BACKUP ONLINE

No *online*, as rotinas de *backup* são executadas com o ambiente em produção, esse método de *backup* é mais complexo já que diversos arquivos podem estar em uso durante a cópia, e o sistema operacional bloqueia a cópia de arquivos que estão abertos ou em uso (SOMASUNDARAM; SHRIVASTAVA, 2011).

3.1.2. *BACKUP* OFF-LINE

O *backup off-line* é realizado com o ambiente "parado" ou sejam, sem arquivos e dados sendo usados por usuários ou sistemas (SOMASUNDARAM; SHRIVASTAVA, 2011).
Esses dois métodos de *backup* também são conhecidos como *backup* quente (*online*) e *backup* frio (*off-line*) (MCDOWALL, 2011 *apud* SILVA, 2015).

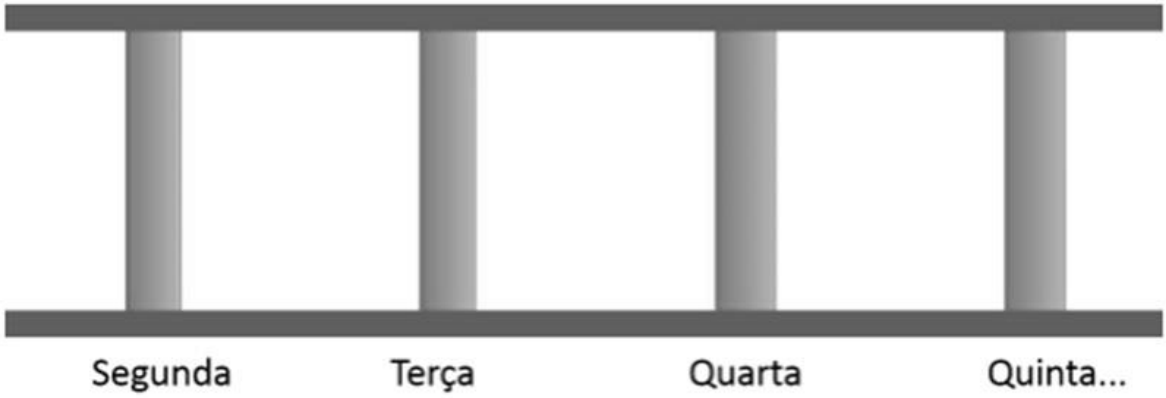
3.1.3. TIPOS DE *BACKUP*

De acordo com Somasundaram e Shrivastava (2011), a granularidade do *backup*, ou tipo de *backup* depende das necessidades apresentadas pela empresa, mas geralmente acabam por optar por uma mescla entre *backup* completo (*full*), incremental ou o cumulativo (incremental).

3.1.4. *BACKUP* TOTAL OU COMPLETO

O *backup* completo consiste na cópia exata dos dados presentes nos diretórios ou dispositivos que são necessários, (CA TECHNOLOGIES, 2014). Basicamente, todos os dados gerados em produção são enviados para o dispositivo de armazenamento todas as vezes que a rotina de *backup* é executada (Figura 8).

Figura 8 - Cópia Completa



Fonte: Aliança Tecnologia da Informação [7](2015)

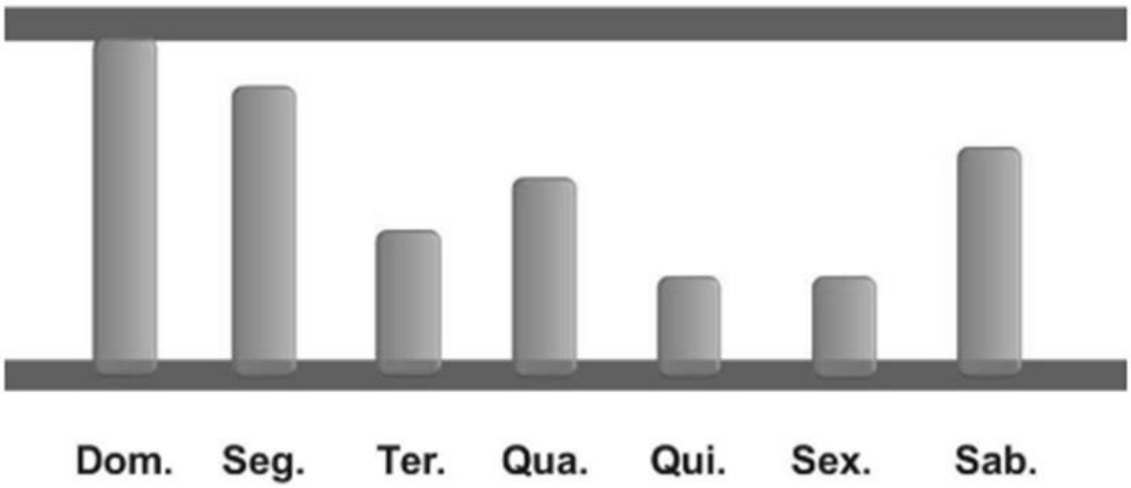
Na cópia completa, o ponto positivo é com relação a integridade dos dados, já que teremos a disposição o arquivo completo, porém esse tipo de *backup* gera um alto volume de espaço ocupado e o tempo de execução que a cópia *full* leva para concluir é superior as outras (SPANIOL, 2016).

3.1.5. *BACKUP* INCREMENTAL

No *backup* incremental são copiados apenas os arquivos alterados desde a última cópia completa ou incremental (CA TECHNOLOGIES, 2014). Em um primeiro momento é necessário que haja um *backup full* e na sequência pode-se iniciar a cópia incremental conforme mostra a Figura 9.

7 Disponível em: <http://www.aliancatecnologia.com/conteudo/2015/05/quatro-tipos-de- backup/> Acesso em: 16 ago, 2018.

Figura 9 - Cópia Incremental



Fonte: Aliança Tecnologia da Informação[8] (2015)

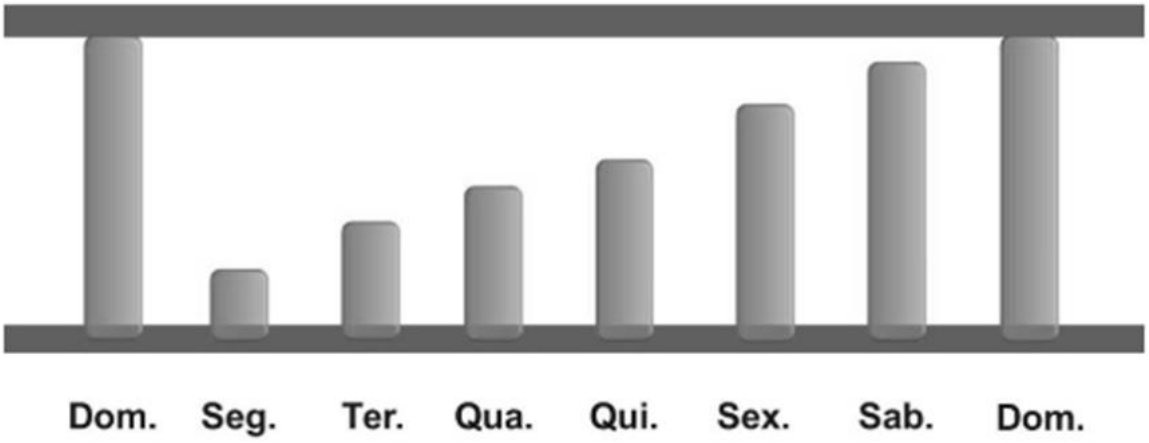
Devido a esse *backup* copiar apenas os arquivos que sofreram alterações, o volume de dados será menor e consequentemente o tempo de execução da tarefa de cópia também será curto, além disso será necessário um espaço menor para armazenar esse *backup* (CA TECHNOLOGIES, 2014).

3.1.6. *BACKUP* DIFERENCIAL

O *backup* diferencial, é muito similar ao incremental, a diferença é que o diferencial armazena apenas os arquivos alterados após o *backup full* (CA TECHNOLOGIES, 2014). Essa forma de *backup* leva mais tempo que o modo incremental, pois ele realiza uma cópia completo dos dados alterados desde o último *backup* completo (Figura 10). Porém sua restauração é mais rápida e é necessário apenas o conjunto de armazenamento completo e o conjunto incremental (SOMASUNDARAM; SHRIVASTAVA, 2011).

8 Disponível em: <http://www.aliancatecnologia.com/conteudo/2015/05/quatro-tipos-de-backup/> Acesso em: 16 ago, 2018.

Figura 10 - *Backup* Diferencial



Fonte: Aliança Tecnologia da Informação[9] (2015)

3.2. VANTAGENS E DESVANTAGENS ENTRE *BACKUP* TOTAL X DIFERENCIAL X INCREMENTAL

Na Tabela 1 que segue abaixo, é possível identificar algumas das vantagens e desvantagens dos três tipos de *backup* mais comuns (ROSA, et al., 2015).

Tabela 1 - Vantagens x Desvantagens Tipos *Backup*

Tipo de *Backup*	Vantagem	Desvantagem
Total	Cópia total dos dados escolhidos ou da mídia inteira	Dados redundantes
Incremental	Uso eficiente do tempo, pois cópia apenas os dados alterados no último *backup*	Restauração complexa, pois necessita do conjunto de fitas para completa restauração.
Diferencial	Rápida Restauração	Necessita sempre de dois *backups* (Um total e o último diferencial)

Fonte: Tecnologia e Redes de Computadores[10] (2015)

9 Disponível em: <http://www.aliancatecnologia.com/conteudo/2015/05/quatro-tipos-de-backup/> Acesso em: 29 ago. 2018.

10 Disponível em: < http://redes.sombrio.ifc.edu.br/wp-content/uploads/sites/7/2015/12/Livro-Tecnologia-e-Redes-de-Computadores-2015.pdf#page=93>. Acesso em: 07 out. 2018

3.3. PERIODICIDADE E RETENÇÃO DE *BACKUP*

Para Fialho Junior (2007), a frequência das cópias de segurança, estão ligadas diretamente com a importância que a informação tem para a empresa e a quantidade de informação que será armazenada. O autor comenta que existem situações em que as rotinas de backup são diárias, pois as informações são alteradas continuamente, em outros casos existem rotinas semanais, quinzenais e até mesmo mensais.

Ferreira e Araújo (2008), dizem que, o período retenção de um backup é definido levando-se em consideração dois fatores, a velocidade da informação, que está relacionada ao tempo em que a informação é atualizada, e a volatilidade da informação que é o período que uma informação se mantém utilizável ou atual.

O período de retenção está ligado ao tempo em que a cópia de segurança não poderá ser excluída, por exemplo, quando é definido que a retenção de uma mídia de backup é de quinze dias, a mesma só poderá ser apagada ao fim dessas duas semanas (FARIA, 2010).

4. EQUIPAMENTOS DE *BACKUP* - DISPOSITIVOS DE ARMAZENAMENTO DE DADOS

Existem disponíveis diversas tecnologias capazes de realizar o armazenamento das informações provenientes das rotinas de *backup*, dentro eles estão as fitas e discos que são os dispositivos mais utilizados (SOMASUNDARAM; SHRIVASTAVA, 2011).

A computação em nuvem adicionou mais uma opção para o armazenamento de *backup*, onde as cópias de segurança são realizadas diretamente pelas ferramentas na nuvem.

4.1. DISPOSITIVOS ÓPTICOS

Fazem parte dos dispositivos ópticos, os Minidiscos, CD’s, DVD’s, esses dispositivos de armazenamento foram, e em alguns locais ainda são utilizados

devido ao baixo custo das mídias e dos dispositivos de gravação, e ao tempo relativamente alto de duração de suas mídias (FIALHO JUNIOR, 2007).

De acordo com a IBM Knowledge Center (2018), “[...] armazenamento ótico é qualquer método de armazenamento que utiliza laser para armazenar e recuperar dados de mídia ótica”.

4.2. DISPOSITIVOS MAGNÉTICOS

Segundo Somasundaram e Shrivastava (2011), as fitas magnéticas são conhecidas por serem tecnologias de acesso sequencial, pois as informações são gravadas e lidas de forma sequencial. É grande a variedade de cartuchos de fitas magnéticas disponíveis no mercado, eles variam de tamanho físico, capacidade de armazenamento, velocidade etc. O autor comenta que, as fitas são muito usadas devido ao seu armazenamento a longo prazo e por possuírem baixos custos.

As fitas magnéticas geralmente possuem duas formas de apresentação de sua capacidade, em sua rotulação pode constar o valor de armazenamento de forma compactada ou não compactada, essa compactação pode ser realizada via software, ou via hardware, esse último por sua vez possui uma maior taxa de compactação com relação ao outro (FARIA, 2010). De acordo com o autor são exemplos de fitas magnéticas as fitas Digital Data Storage (DDS), Digital Linear Tape (DLT) e Linear Tape-open (LTO).

Os discos também são exemplos de dispositivos magnéticos para armazenamento, devido ao seu desempenho, seu baixo custo e a facilidade de manuseio e implementação, eles vêm pouco a pouco substituindo as fitas magnéticas, pois também possuem um melhor desempenho para a recuperação dos dados se comparado as fitas (SOMASUNDARAM; SHRIVASTAVA, 2011).

4.3. DISPOSITIVOS ELETRÔNICOS

São exemplos de dispositivos eletrônicos, *pendrives*, cartões de memória e os discos de estado sólido (SSD-*state solid disk*), os *pendrives* e cartões de memória não são indicados para realizar cópias, eles são muito utilizados por usuários

domésticos no transporte diário de arquivos entre computadores (FIALHO JUNIOR, 2007).

O fator agravante que impediu a popularização dos discos SSD foi o seu alto valor de venda, pois sua performance é superior aos discos magnéticos, além de ser mais resistente e ser muito mais leve que um *hard disk* tradicional. Ultimamente, as empresas estão notando que as vantagens da adoção de disco SSD junto a estratégias corretas, podem a longo prazo superar seus custos se comprados aos disco magnéticos (FERRAZ, 2018).

4.4. ARMAZENAMENTO NA NUVEM

O armazenamento em nuvem vem trazendo vantagens se comparados com os métodos tradicionais disponíveis, onde possui um custo inferior e escalável, ou seja, você paga conforme sua demanda de uso, além de oferecer resiliência, confiabilidade e agilidade. O *backup* em nuvem vem se popularizando e se tornando uma tendência para empresas que visam deixar as antigas soluções de *backup* para traz, e querem adotar uma solução única capaz de garantir a proteção física e virtual das informações (AMADO; MARCONDES, 2014).

4.5. DISPOSITIVOS DE ARMAZENAMENTO – CAPACIDADES E VELOCIDADES

Os dispositivos de armazenamento possuem tamanhos de armazenamento e taxas de transferências distintas, na Tabela 1 é possível ver alguns dispositivos e suas características.

Tabela 2 - Relação Capacidade e Velocidade

Dispositivo	Capacidade	Velocidade Leitura	Velocidade Escrita
Blu-ray	Até 128 GB	até 216Mbit/s	até 432Mbit/s
Pendrive	Até 1 TB	240 MB/s	160 MB/s
Cartão de Memória	Até 512 GB	80 Mb/s	10 MB/s
Disco Rígido	Até 4 TB	200 Mb/s	200 Mb/s
SSD	Até 1 TB	550 Mb/s	550 Mb/s

Fitas Magnéticas	Até 15 TB	Até 750 Mb/s	Até 750 Mb/s
Nuvem	Escalonavel	Sem Informação	Sem Informação

Fonte: O autor

4.6. PROPENSÃO À FALHA

Segundo Picovsky (2013), as intermitências relacionadas à tecnologia da informação (TI), tem gerado incômodos aos donos de empresas, pois interferem diretamente na continuidade dos negócios. O autor cita que problemas relacionados a roubo de fitas de *backup*, erro em servidores de *backup* e problemas relacionados as mídias de armazenamento são os mais comuns.

A empresa fabricante de fitas magnéticas para *backup* Hewllet Packard Enterprise (HP, 2013), fornece um guia de recomendações para o uso adequado de mídias magnéticas de armazenamento, onde orienta aos detentores de fitas de *backup* quais são os cuidados que devem tomar para prolongar a vida útil das fitas. Segundo as recomendações da HP, as mídias são sensíveis ao calor, portanto, seus locais de manuseio e operação devem oferecer condições confortáveis de temperatura e não se deve sujeitar as mídias a condições de umidade extremas. A HP (2013), ainda traz outras recomendações sobre o manuseio adequado das fitas magnéticas, seguem abaixo algumas delas:

- Não deixe o cartucho cair nem tente abri-lo.
- Nunca toque a superfície da mídia nem tente limpar os componentes do cartucho, como o caminho da fita ou as guias da fita.
- Sempre armazene a mídia em um ambiente limpo, longe de copiadoras e impressoras para evitar a contaminação pelo toner e partículas de papel.
- Não exponha a mídia ao calor, frio ou umidade extrema, próximo a extintores de incêndio, portas, entradas, campos magnéticos e fontes de calor.
- Não fume, coma nem beba onde a mídia está sendo usada ou armazenada.
- Certifique-se de que os rótulos ficaram na área de rótulos.
- Sempre use uma proteção contra gravação para evitar que a mídia seja sobre gravada acidentalmente (quando você está lendo fitas de arquivo, por exemplo).

A fabricante de discos rígidos Western Digital (WD, [s.d.]), orienta aos usuários de seus produtos quais são as melhores práticas para manusear seus discos. A WD alerta que, os discos são instrumentos frágeis e quem precisam de cuidados especiais, pois podem ser danificados através do uso de força física ou de

descargas elétricas. Abaixo segue algumas recomendações que a WD passa a seus usuários para garantir a integridade de seus discos.

- Antes de remover o disco rígido da embalagem, prepare as ferramentas e cabos para a instalação.
- Mantenha o disco rígido dentro da embalagem até que esteja pronto para instalá-lo fisicamente no sistema do computador.
- Use uma pulseira de aterramento, se disponível – especialmente quando estiver próximo a dispositivos sensíveis como memórias, placas controladoras ou outras placas eletrônicas.
- Com o computador desligado (mais ainda plugado na fonte de alimentação), toque na unidade no gabinete do computador e desligue o cabo de alimentação. *
- Não deixe que outras pessoas encostem na unidade.
- Segure os discos rígidos pelas laterais, com cuidado para não encostar nos conectores ou na montagem da placa de circuito impresso.
- Ao instalar a unidade, não caminhe sobre carpetes nem se movimente de maneira a gerar eletricidade estática.
- Não solte nem agite o disco rígido. Esta ação poderia danificar os componentes internos da unidade.
- Evite expor a unidade a temperaturas extremas.
- Não empilhe os discos rígidos.
- Não posicione os discos sobre suas laterais.
- Não coloque nada em cima de um disco rígido.
- Não force o disco rígido dentro do gabinete do computador.
- Seja cuidadoso ao instalar conectores de alimentação e de dados para evitar danos nos pinos do conector.
- Não obstrua nem tampe os orifícios de filtragem de ar das unidades.

4.7. EQUIPAMENTOS DE *BACKUP* - FERRAMENTAS DE *BACKUP*

Existem no mercado, diversas ferramentas para a realização de *backups*, com opções *opensource* (código aberto), estas não possuem custos para quem quiser usá-las, e opções que precisam ser pagas para obter licenças de uso.

4.8. FERRAMENTAS GRATUITAS

São ferramentas que não precisam de licença para uso, muitas são desenvolvidas e mantidas por grupos que desejam ajudar a comunidade, ou ainda, empresas lançam versões gratuitas de suas versões pagas, essas versões sem custo possuem um número limitado de funcionalidades se comparadas as versões com custo.

4.8.1. VEEAM BACKUP AND REPLICATION

A empresa Veeam surgiu no mercado no ano de 2006 com o lançamento de um monitor para máquinas virtuais baseadas na plataforma VMWARE. No ano de 2009 ela lançou sua ferramenta de *backup*, naquela época, exclusiva para máquinas virtuais. Em 2015 sua solução para *backup* estendeu-se para servidores físicos, atendendo a demanda para sistemas Linux e Windows. Devido à grande popularização da virtualização de servidores, a Veeam Backup and Replication ganhou muita visibilidade, e de acordo com a Gartner Group (2017), ocupa a quarta posição no quesito faturamento (CAMPOS, 2017).

De acordo com Rocha *et al* (2015), a Veeam Backup and Replication, foi desenvolvido para realizar cópias de máquinas virtuais completas de um servidor para outro, tais cópias são usadas para reduzir o tempo que um serviço ou servidor fica indisponível em um ambiente.

4.8.2. BACULA

Faria (2010), descreve o Bacula como sendo um conjunto de vários programas, que auxiliam na criação e administração de rotinas de *backup*, o Bacula roda em sistema operacional Linux, e é capaz de realizar *backups* de outros sistemas. O autor comenta que o Bacula funciona em módulos, e que esses módulos não precisam necessariamente estar em um mesmo servidor, e ainda podem rodar em sistemas operacionais diferentes.

Os módulos do Bacula são (FARIA, 2010):

- ***Director's Daemon:*** módulo responsável pela administração dos *backup*s e restaurações;
- ***Console Manager:*** esse módulo realiza a comunicação com o *director's daemon*, pode ser executado em qualquer máquina da rede e em sistemas operacionais diferentes, esse módulo possui três versões, sendo elas em modo texto, modo gráfico e *Widgets* para Unix ou Windows.
- ***File Daemon:*** esse é cliente do Bacula, é instalado nas máquinas que serão copiadas e enviam os dados através da rede para *director's daemon*, possui

versões para diversos sistemas operacionais (Linux, *BSD, Unix, Windows e Macintosh).

- ***Catalog:*** é responsável por armazenar as informações relativas as cópias, funciona como uma base de dados para pesquisa, quando necessário realizar uma restauração ele agiliza a busca por arquivos.

4.8.3. AMANDA

Amanda é um acrônimo para *Advanced* Maryland *Automatic Network Disk Archiver*, é um *software* em Linux para o gerenciamento de *backup* que foi desenvolvido por James da Silva na universidade de Maryland nos Estados Unidos. Esse programa é capaz de realizar cópias em diversas mídias como por exemplo, HD, fitas magnéticas, CD's e outros, assim como o Bacula ele realiza *backups* em diversos sistemas operacionais e de várias estações de trabalho (DA ROSA; et al, 2015).

Faria (2010) comenta que o desde 2006 o Bacula já superou o Amanda, o autor comenta que os principais fatores responsáveis por isso foram:

- Amanda não possui cliente nativo para Windows;
- Sua operação é pouco intuitiva;
- Dificuldade para customizar um esquema para rotação de fitas.

4.9. FERRAMENTAS PROPRIETÁRIAS

São ferramentas que necessitam da compra uma licença para uso, são produtos desenvolvidos e mantidos por empresas com o intuito de lucrar com a comercialização de seu *software*.

4.9.1. CA ARCSERVE BACKUP

A CA Technologies (2014), descreve o CA ARCserve Backup como sendo:

> [...] uma solução de gerenciamento de armazenamento distribuído abrangente para ambientes distribuídos e de várias plataformas. O aplicativo pode fazer o *backup* dos dados e restaurá-los de todos os computadores da rede (inclusive daqueles que executam Windows, UNIX e Linux) usando os agentes clientes opcionais. O CA ARCserve Backup também fornece utilitários de gerenciamento de dispositivos e mídia.

O CA ARCserve Backup oferece controle a partir de um console de gerenciamento. Ele pode oferecer suporte a ambientes de empresas de pequeno e grande porte, que compreendem um ou vários computadores em diferentes plataformas e organizações (CA TECHNOLOGIES, 2014).

Faria (2010), comenta que as licenças da ferramenta Arcserve possuem um valor elevado e que uma licença para um determinado sistema operacional serve exclusivamente para aquele sistema, ou seja, caso haja uma troca ou upgrade de sistema operacional, a licença não atendera a nova demanda. O autor diz que para um desempenho adequado, o Arcserve necessita de um servidor com boas configurações e uma boa largura de banda para que o desempenho da ferramenta seja adequado.

4.9.2. COMMVAULT

A Commvault é uma empresa que surgiu nos anos 90 e está na vanguarda da tecnologia de proteção e recuperação de dados. Seu software de *backup* anteriormente era conhecido como Simpana, e por uma decisão estratégica resolveram por rebatizá-lo com o nome da empresa. O Commvault é uma ferramenta que suporta diversos sistemas operacionais e bancos de dados de diversos fabricantes além de suportar vários serviços de nuvem e ser compatível com muitos sistemas de virtualização. Uma das desvantagens que a ferramenta apresenta é possuir uma dinâmica de implantação e administração um pouco complexa, o que exige por parte da equipe que irá manuseá-lo a participação em cursos e treinamentos oficiais (CAMPOS, 2017).

4.9.3. VERITAS BACKUP EXEC

O Backup Exec é uma ferramenta de proteção de dados com *backup* simples e compatível com ambientes virtuais, físicos e nuvem. Oferece 3 níveis de licenciamento sendo eles, Bronze que é a opção mais barata, Silver que acompanha os recursos mais utilizados e a opção Gold que habilita todas as funções disponíveis pela ferramenta. O Backup Exec oferece integração total com o Azure Recovery, possui compatibilidade com diversas versões de sistemas operacionais e sistemas

de virtualização além de realizar as cópias de segurança em diversos tipos de mídias de armazenamento (VERITAS TECHNOLOGIES LLC, 2018).

4.10. OUTRAS FERRAMENTAS DE *BACKUP*

Além das ferramentas apresentadas anteriormente, que segundo a Gartner Group (2017) apud Campos (2017), são as com maior número de uso. Além dessas, existem outras ferramentas para realizar cópias de segurança, capazes de atender as demandas de pequenas, médias e grandes empresas, tendo opções com ou sem custos.

4.10.1. BSN (BACKUP SEGURO NA NUVEM)

O BSN é uma ferramenta desenvolvida pela empresa SiplamControl.M junto com a Microsoft, com a visão de atender a crescente procura por armazenamento em nuvem, agilidade e segurança dos dados. O BSN possui total integração com a Microsoft Azure, que possibilita que os dados estejam armazenados no território nacional, garantido assim que em caso de desastre os dados estejam preservados (AMADO; MARCONDES, 2014).

4.10.2. HPE DATA PROTECTOR

De acordo com Philereno (2017), é uma ferramenta cliente/servidor, escalável e capaz de se ajustar as necessidades do negócio. O autor comenta que ela é compatível com sistemas operacionais Linux e Windows e com a tecnologias SAP, Oracle, SQL e tecnologias de virtualização além de realizar cópias em diversos tipos de mídias de armazenamento.

4.10.3. TSM (TIVOLI STORAGE MANAGER)

De acordo com Faria (2010), o TSM é uma ferramenta que oferece muitos recursos, e chega a ser similar ao Bacula, porém carece de documentação a respeito o que acarreta a dificuldade de operação e na necessidade de capacitação dos usuários. O autor comenta que é uma ferramenta que acompanha a *storage* da IBM, como se fosse uma compra combinada, à medida que essa ferramenta é

utilizada, cria-se um legado de *backup* que “obriga” a empresa a comprar a licença para continuar usando após o primeiro ano.

5. GESTÃO DE *BACKUP*: UM ESTUDO DE CASO NUMA EMPRESA PRESTADORA DE SERVIÇOS DE *FULL OUTSOURCING*

5.1. CONTEXTUALIZAÇÃO DO ESTUDO DE CADO

O desenvolvimento desse estudo foi realizado na empresa X, a fim de apresentar a viabilidade de um ambiente de backup capaz de atender a demanda interna e a de clientes. O estudo foi desenvolvido entre os meses de julho de 2018 a novembro de 2018.

Para se desenvolver e estabelecer as atividades de backup de dados, seja para uma demanda interna ou para um cliente novo ou já existente, existe a necessidade de se levantar as informações acerca da infraestrutura, esses dados contemplam servidores, equipamentos de *backup* (bibliotecas ou *stand alone*), mídias de armazenamento, meio de comunicação entre outros, além disso é necessário também que seja realizada a elaboração da política de *backup* de acordo com as informações acordadas com o cliente, como por exemplo, quais dados serão copiados, forma de armazenamento, períodos de retenção, método e tipo de *backup*. Essas informações, devem ser definidas previamente ao início das implementações das rotinas de *backup*, a fim de atender a todas as necessidades do cliente e garantir a proteção de seus dados.

5.1.1. HISTÓRIA DA EMPRESA

Fundada em meados de 1999 na cidade de São Paulo, passou por uma remodelação em 2005 para redesenhar todos os seus processos, tendo inclusive mudado a sua localização, que passou de São Paulo, na vila Olímpia, para a cidade de Americana – SP.

Hoje já situado na cidade de Americana, conta com cerca de 500 funcionários e atua com a execução de processos relacionados a nove áreas: Contabilidade, Tesouraria, Jurídico-Tributária, Seguros, Jurídico-Trabalhista, Saúde, Administração, Tecnologia da Informação e Suprimentos.

No final de 2016 a empresa optou por se lançar no mercado e deixar de atender apenas as empresas do grupo ao qual pertence, e passou a oferecer serviços de *Full Outsourcing*.

A empresa, atua no segmento de *full outsourcing,* tendo atendido cerca de 120 clientes, tanto nacionais como internacionais. A principais atividades desenvolvidas pela X são:

- **BPO**
    - *Finance* - Suporte completo com processos automatizados que garantem Segurança e *Compliance* para suas operações financeiras e administrativas.
    - *Accounting & Tax* - Sistemas integrados de ponta e sistemas auxiliares aliados à nossa experiência global de apoio nas operações contábeis e tributárias para garantir o melhor suporte fiscal e contábil à sua empresa.
    - *Strategic Sourcing & Procurement* - Criado para compras compartilhadas. Oferece à sua empresa ganhos de escala e redução de custos unitários, com suporte especialista, abrangente e próximo.
    - *Human Resources* - Contribui para as operações da sua área de Recursos Humanos, possibilitando ganhos a partir do nosso apoio técnico na gestão de contratos e constante atualização dos processos conforme Legislação e Acordos Coletivos de Trabalho.
    - Legal - Gestão de operações jurídicas que garante alto índice de êxito nas ações e suporte tributário e contratual, com custos competitivos.
- **ITO**
    - *Application Management Services* - Sustentação de diferentes aplicações e tecnologias de sistemas e a flexibilidade do atendimento de uma equipe na medida exata da sua necessidade, com total aproveitamento do seu investimento.
    - *Infrastructure* - Serviço *nonstop* que busca a estabilidade e a segurança dos ambientes. Parcerias estratégicas, conhecimento multidisciplinar e uma consultoria em segurança de informações garantem o pleno funcionamento de sua infraestrutura.
    - Telecom - Somos um provedor de serviços e soluções de comunicação. Com foco em tecnologias inovadoras e ampla experiência em Integração,

temos alianças com os principais fornecedores de tecnologia e agregamos a essas parcerias a nossa capacidade em Consultoria Tecnológica, Gestão de Projetos e Serviços Profissionais e Gerenciados, oferecendo soluções completas com foco no seu negócio.

- ***Consulting***
    - *Consulting* - Há 10 anos absorvendo processos de negócios em segmentos diversos. Entendimento das especificidades dos clientes com profissionais atuando presencialmente para apoiar as equipes internas. Metodologias devidamente adaptadas ao porte dos projetos e clientes.
- **GRC**
    - *Governance, Risk And Compliance* - Soluções customizadas aplicadas por uma equipe sênior, do Diagnóstico à Implementação, levando em conta as suas características e necessidades e oferecendo custos competitivos.

5.1.2. INFRAESTRUTURA E SISTEMAS

De acordo com o sistema de inventário da empresa X, durante os meses em que o estudo foi desenvolvido, as quantidades relativas a estações de trabalho, servidores físicos, servidores virtuais, bancos de dados, *database* e aplicações constam na Tabela 3.

Essas informações, não representam a real quantidade de equipamentos e sistemas ao qual a Empresa X suporta ou administra, são dados coletados através da ferramenta Microsoft System Center Configuration Manager (SCCM), esses números representam as quantidades de equipamentos e sistemas que estão inseridos no domínio da Empresa X. Quando um novo dispositivo é inserido no domínio o SCCM coleta os dados e alimenta o sistema de inventário. Equipamentos de clientes que não estão no domínio da Empresa X, podem não constar no inventário até que ele seja cadastrado manualmente, por conta disso a quantidade de dispositivos e sistemas pode variar.

Tabela 3 - Quantidades de Equipamentos e Sistemas

Dispositivo	Quantidade Ativos	Total Ativos e Desativados
Estações de trabalho	786 registradas	6732 registros
Servidores Físicos	162	817
Servidores Virtuais	234	551
Servidor em Nuvem	7	8
Storage	14	34
Bibliotecas de *backup*	19	19
Dispositivos de *backup stand alone*	7	N/A
Aplicações e Sistemas	645	1182
Servidores da Banco de Dados	124	139
Database	909	1081

Fonte: O autor

5.2. INFRAESTRUTURA DE *BACKUP*

A Empresa X possui uma infraestrutura de *backup* capaz de atender a demanda dos clientes internos e externos, além de possuir uma empresa parceira que, é capaz de disponibilizar equipamentos a pronta entrega para novos clientes, e ainda, realiza todas as manutenções e trocas de equipamentos e peças quando necessário.

5.2.1. EQUIPAMENTOS DE *BACKUP* – LIBRARY

Nos meses de elaboração desse estudo, foram levantadas as informações relativas a infraestrutura de *backup,* disponível pela empresa para atendimentos de seus clientes, na Tabela 4 é possível conferir as informações referente as *libraries* de *backup* (bibliotecas de backup), esses são equipamentos que são de responsabilidade ou de propriedade da Empresa X. Existem ainda os dispositivos que são da contratante, e a responsabilidade sobre eles é do próprio cliente.

Tabela 4 - Libraries de Backup

Dispositivo	Marca	Modelo	Tecnologia	Capacidade da Fita	Quantidade
Library de *Backup*	Hewlett Packard (HP)	MSL G3 SERIES	Linear Tape-Open 4 (LTO4)	800 GB	2
	International Business Machines (IBM)	TS3200			1
	Dell	TL2000	Linear Tape-Open 5 (LTO5)	1.5 TB	8
		TL1000			1
	Hewlett Packard (HP)	MSL G3 SERIES			3
		StoreEver 1/8 G2			2
	Hewlett Packard (HP)	StoreEver 1/8 G2	Linear Tape-Open 6 (LTO6)	2.5 TB	1
	Dell	TL2000		2.5 TB	1
				Total	**19**

Fonte: O autor

5.2.2. EQUIPAMENTOS DE *BACKUP – STAND ALONE*

Além das bibliotecas de *backup*, alguns clientes aos quais a Empresa X presta serviço, utilizam equipamentos *stand alone* para realizarem suas rotinas de *backup.* Atualmente existem 7 em operação. A Empresa X realiza a gestão dos *backups,* mas se isenta das responsabilidades sobre a manutenção, pois esses equipamentos geralmente são do próprio cliente e muitos estão fora da garantia.

5.2.3. EQUIPAMENTOS DE *BACKUP* – SERVIDORES

Durante o desenvolvimento desse trabalho, foram levantadas as quantidades de servidores utilizados para *backup,* na Tabela 5 é possível conferir esses números. Durante a coleta dessas informações, foi possível constatar que a Empresa X possui servidores dedicados a *backup,* bem como servidores mistos, ou seja, que possuem outros serviços e aplicações. Isso ocorre em clientes onde os *backups* são menores e não ocupam uma janela muito grande, que poderiam invadir o horário comercial, portanto os recursos podem ser compartilhados com outras necessidades.

Tabela 5 - Servidores de Backup

Sistema Operacional	Versão	Quantidade
Windows Server 2008	*ENTERPRISE*	2
Windows Server 2008	R2 *STANDARD*	12
	R2 *ENTERPRISE*	1
Windows Server 2012	R2 *STANDARD*	17
	Total	**32**

Fonte: O autor

5.2.4. EQUIPAMENTOS DE *BACKUP* – FERRAMENTA

A empresa Empresa X, faz uso da ferramenta CA ArcServe Backup para implementar suas rotinas de *backup*. Na Tabela 6, é possível ver as informações referente as versões do ARCserve em uso hoje pela Empresa X. Existe um projeto interno de estudo na Empresa X, sobre a possibilidade da implementação de um *software* livre para a realização das rotinas de *backup.*

Tabela 6 - Ferramentas de *Backup*

Ferramenta	Versão	Quantidade
CA ArcServe Backup	12.5	3
	14.0	1
	15.0	2
	15.1	1
	16.0	6
	16.5	19
	Total	**32**

Fonte: O autor

5.3. VOLUMETRIA DE *BACKUP*

Durante os meses de elaboração desse estudo, a equipe de *backup* realizou o levantamento das informações relativas a volumetria mensal de *backup*. Foi realizado também, o levantamento individual por empresa, e realizado o cálculo de

soma total da quantidade de dados em *terabyte* (TB). Na Tabela 7 é possível checar os dados levantados referente as volumetrias de *backup.*

Tabela 7 - Volumetria de *Backup*

Cliente	Volume em (GB)
1	10100
2	106217
3	64044
4	48852
5	306771
Total em TB	**523,422**

Fonte: O autor

Em média por mês, são realizados 523,422 TB de *backup,* que são copiados em fitas ou discos rígidos. São executadas, aproximadamente 324 tarefas de *backup* todos os meses, tarefas essas, responsáveis por garantir essa volumetria citada anteriormente.

5.4. POLÍTICA DE TESTES DE RESTAURAÇÃO

A Empresa X, estabelece um processo de auditoria para realizar testes regulares anuais, a fim de testar a integridade das restaurações do *backup's.* Anualmente são testados aproximadamente de 40 a 50% das cópias realizadas para os servidores administrados.

Esse processo é realizado pela equipe de operações da empresa, todos os meses são abertos chamados para o teste de diferentes servidores. A equipe de *backup* auxilia na execução, mas não age diretamente na execução dos testes, todas as evidências geradas são salvas no chamado, e os servidores que foram testados são inseridos em uma planilha de controle.

5.5. POLÍTICA DE ARMAZENAMENTO DE FITAS DE *BACKUP*

A Empresa X, oferta serviços de guarda de dispositivos de armazenamento de *backup*, caso o cliente opte por realizar a guarda fora de seu *site*, que é a opção mais segura, a empresa X realiza o gerenciamento desse processo de coleta e envio

para empresa parceira credenciada para realizar esse armazenamento e guarda das mídias de *backup*.

5.6. FERRAMENTA DE *BACKUP* - ARCSERVE

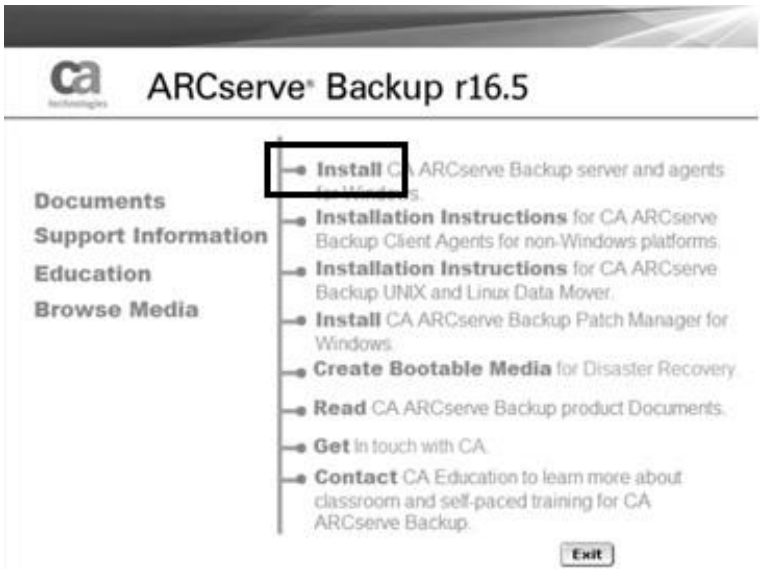
Durante o desenvolvimento dos estudos, foi realizado pela equipe de *backup* da Empresa X, a instalação da ferramenta ARCserve em um novo servidor, para o atendimento de uma nova demanda, solicitada por um cliente. No capítulo seguinte, é possível acompanhar o procedimento de instalação dessa ferramenta.

5.6.1. INSTALAÇÃO ARCSERVE BACKUP

Para essa instalação, foi utilizada a versão r16.5 da ferramenta de *backup* ARCserve, em um servidor dedicado, com o Windows Server 2012. Esse novo servidor foi criado para atender um projeto, onde foi solicitada a atualização do sistema operacional do servidor, que anteriormente operava com o Windows 2008 R2 Standard, após a atualização do sistema operacional do servidor, a equipe de *backup* realizou a instalação do *software* de *backup.* A seguir é possível acompanhar o passo-a-passo da instalação realizada.

- Clicar na opção "*INSTALL*" (Figura 11).

Figura 11 - Instalação ARCserve Backup



Fonte: O autor

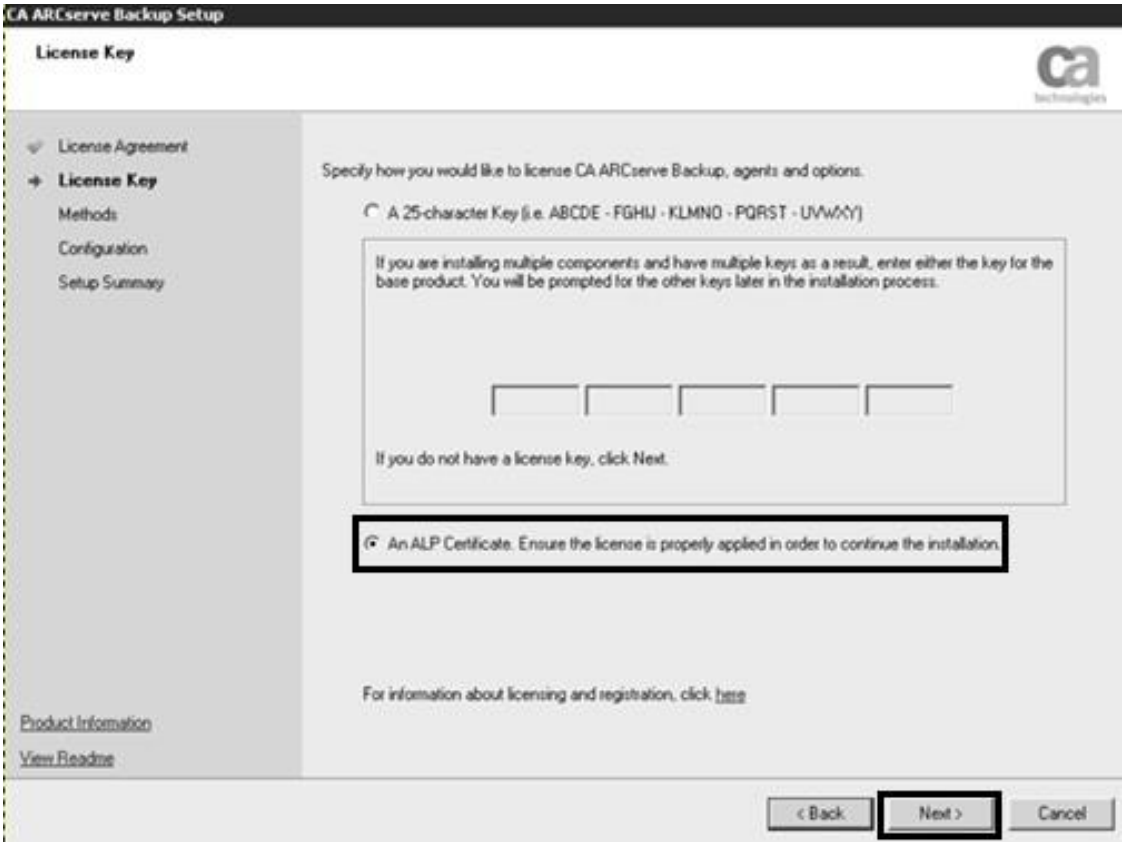
- Correr a barra de rolagem até o final do texto e clicar em "*I Agree*" e em seguida em *"Next"* (Figura 12).

Figura 12 - Instalação ARCserve Backup

Fonte: O autor

- Em seguida, escolher a opção "*An ALP Certificate*" e clicar em *"Next"* (Figura 13).

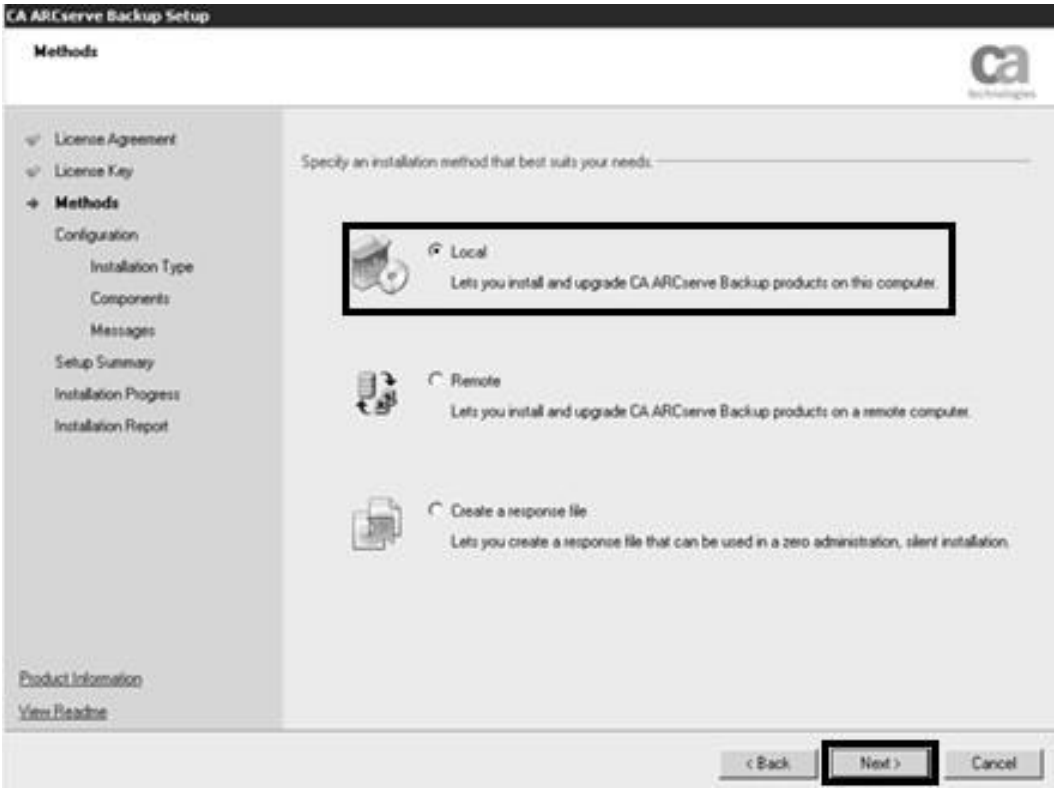
Figura 13 - Instalação ARCserve Backup



Fonte: O autor

- Nesse caso, a instalação está sendo executada localmente, portanto escolher a opção “Local” em em seguida clicar em *“Next”* (Figura 14).

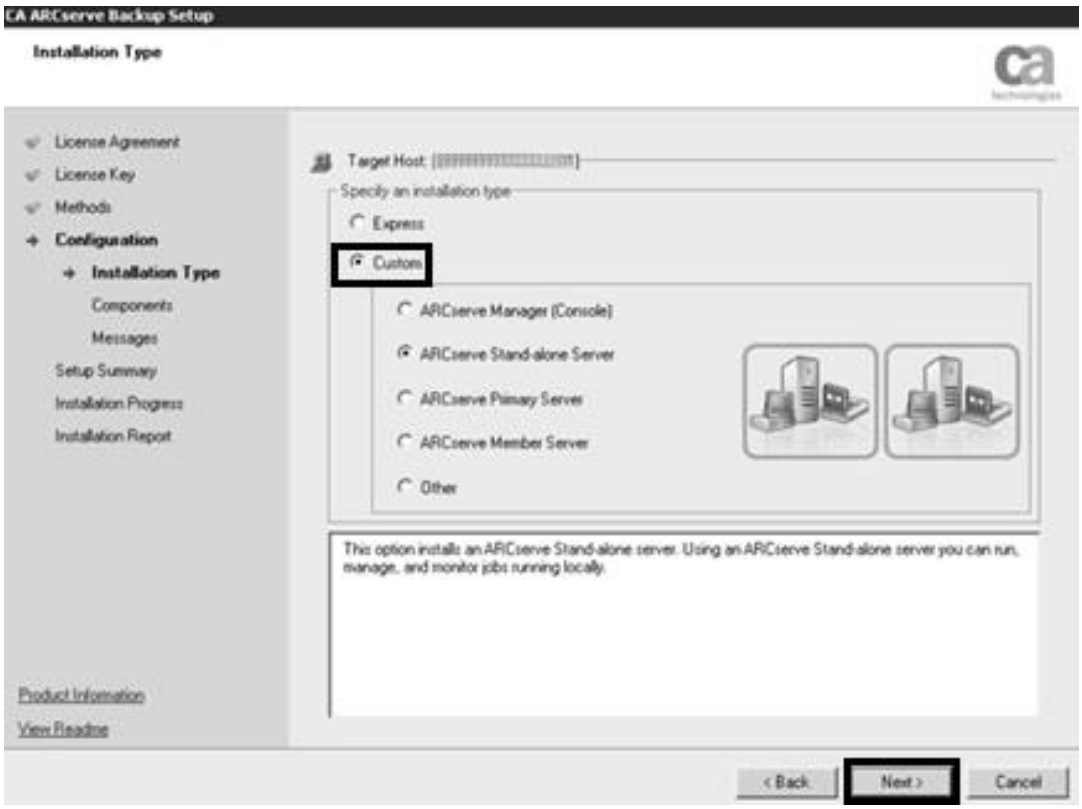
Figura 14 - Instalação ARCserve Backup



Fonte: O autor

- Escolher a opção “*Custom*”, neste caso o equipamento será uma *stand-alone*, portanto, selecionar a opção “ARCserve *Stand-alone Server*” e clicar em “*Next”* (Figura 15).

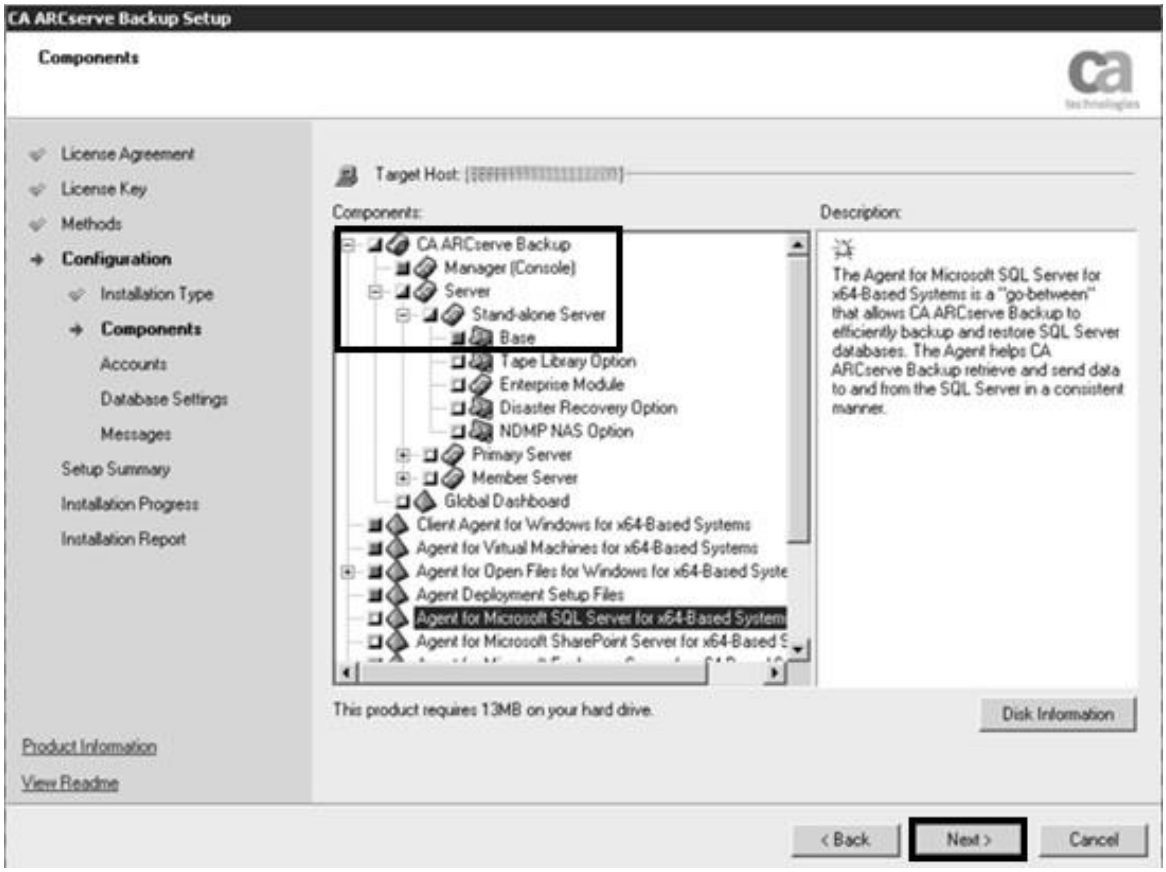
Figura 15 - Instalação ARCserve Backup



Fonte: O autor

- Em “*Components*”, navergar nos menus até encontrar a opção “*Base*”, selecionar essa opção e clicar em “*Next*”. Algumas das opções abaixo necessitam de licença específica. Caso a instalação seja realizada em um equipamento *Library* com dois drives de gravação, selecionar a opção *Tape Library Option* (Figura 16).

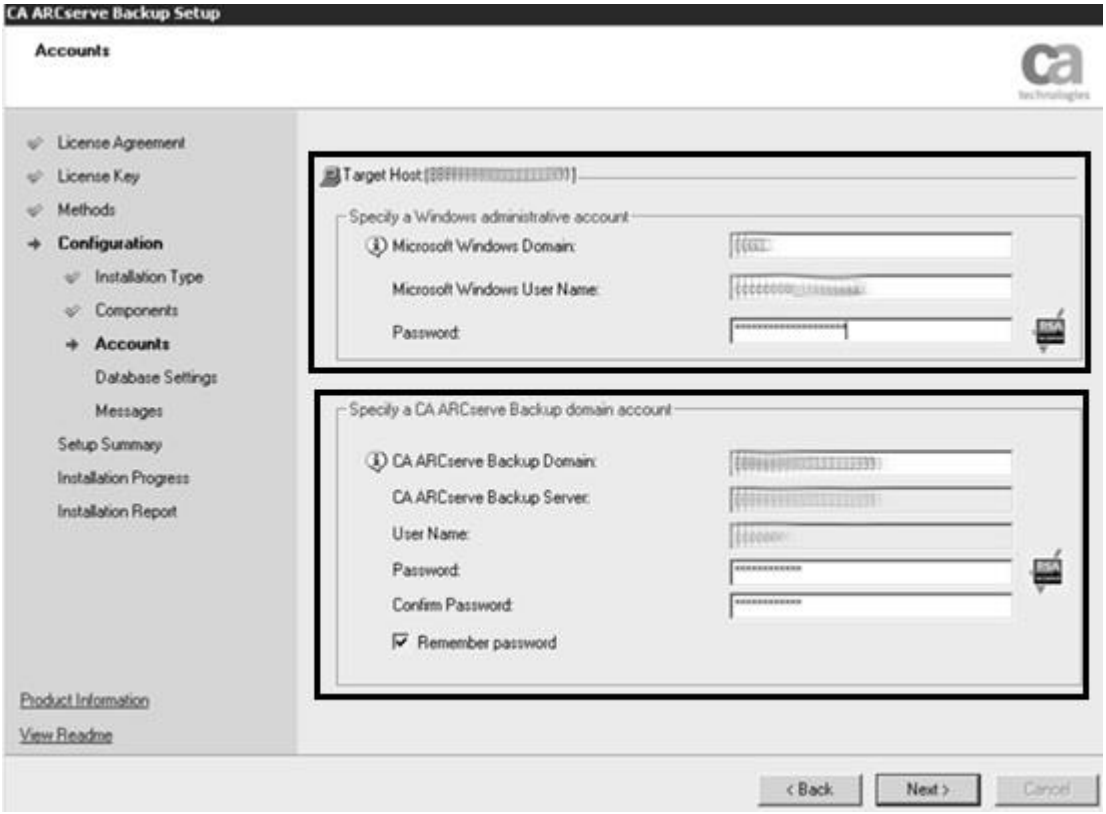
Figura 16 - Instalação ARCserve Backup



Fonte: O autor

- Em “*Accounts”,* inserir as credenciais das contas de administrador local e a conta de *backup* do domínio. Essa conta do *backup* deve ter os privilégios de administrador e deve ser usada apenas pela ferramenta de *backup,* clicar em *“Next”* para prosseguir (Figura 17).

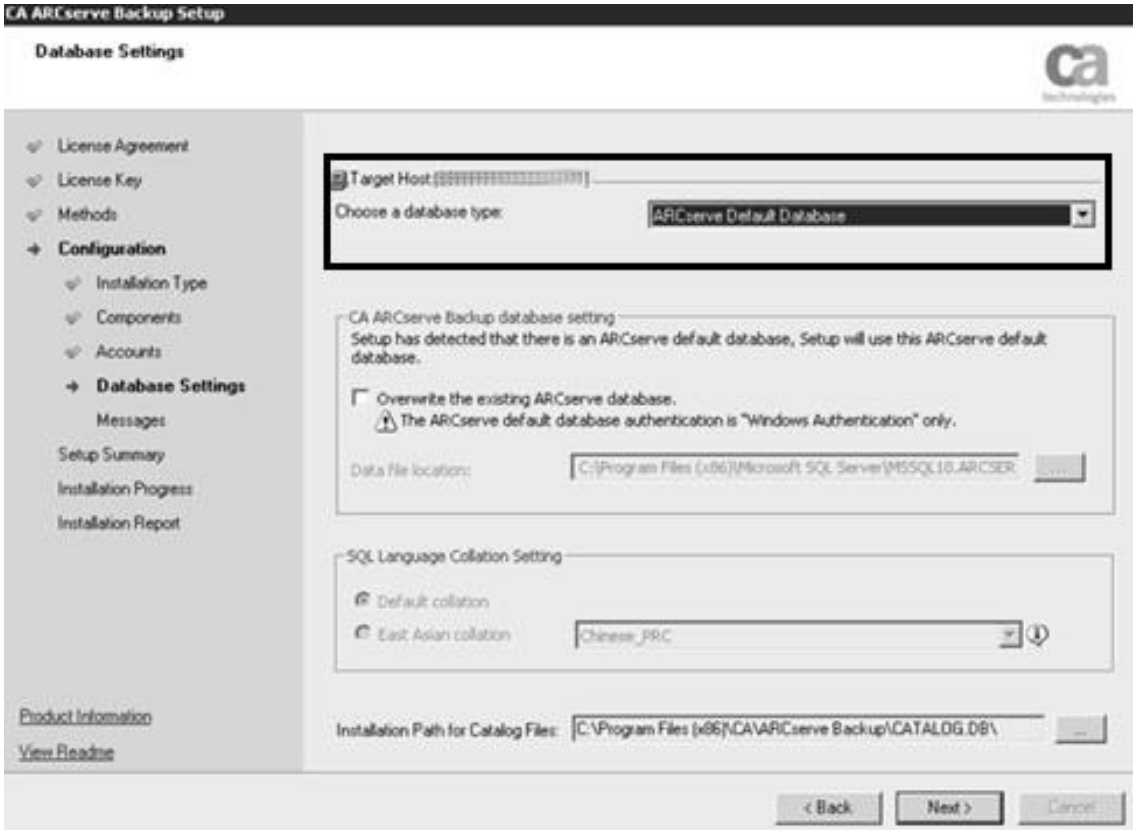
Figura 17 - Instalação ARCserve Backup



Fonte: O autor

Na Figura 18, o ARCServe irá criar um banco de dados SQL *Express* no *Backup Server* ou o administrador pode colocar o banco de dados da ferramenta de *backup* em outro servidor dedicado de banco de dados. O banco de dados SQL *Express* suporta um grande volume de dados de *backup*, não se faz necessário a criação de um SQL dedicado.

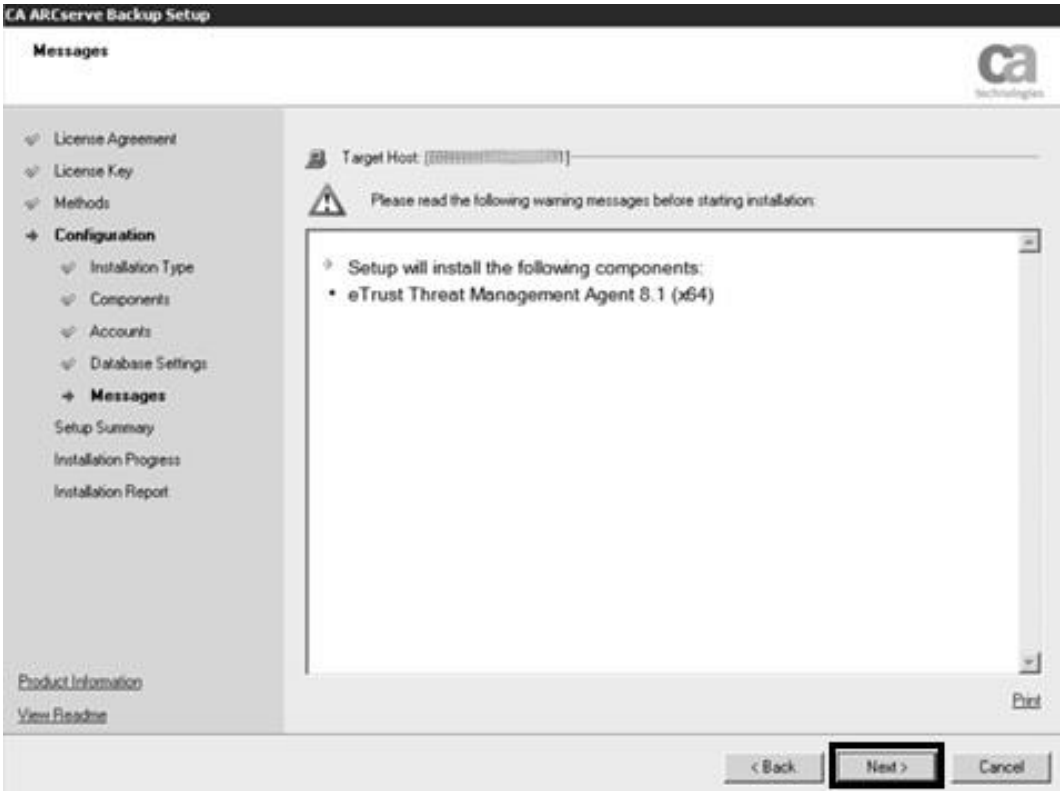
Figura 18 - Instalação ARCserve Backup



Fonte: O autor

- Na etapa seguinte, em "*Messages*", uma mensagem será apresentada, informando o que será instalado. Clicar em *"Next"* para prosseguir (Figura 19).

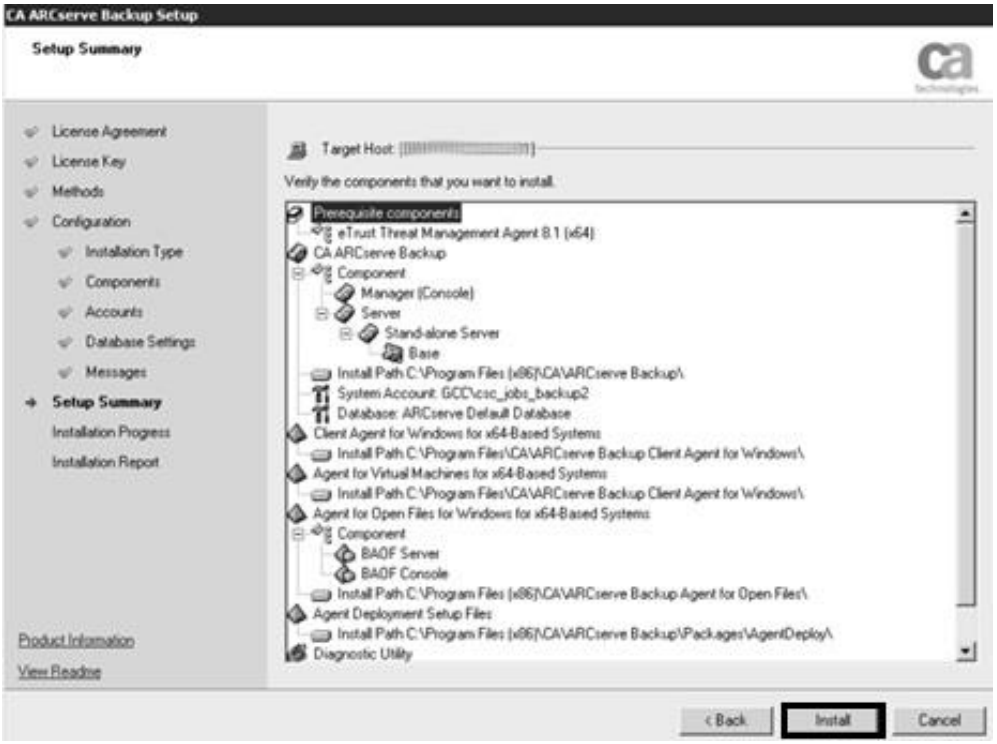
Figura 19 - Instalação ARCserve Backup



Fonte: O autor

- Após realizar as configurações anteriores, clicar em "*Install"* e aguardar a instalação (Figura 20).

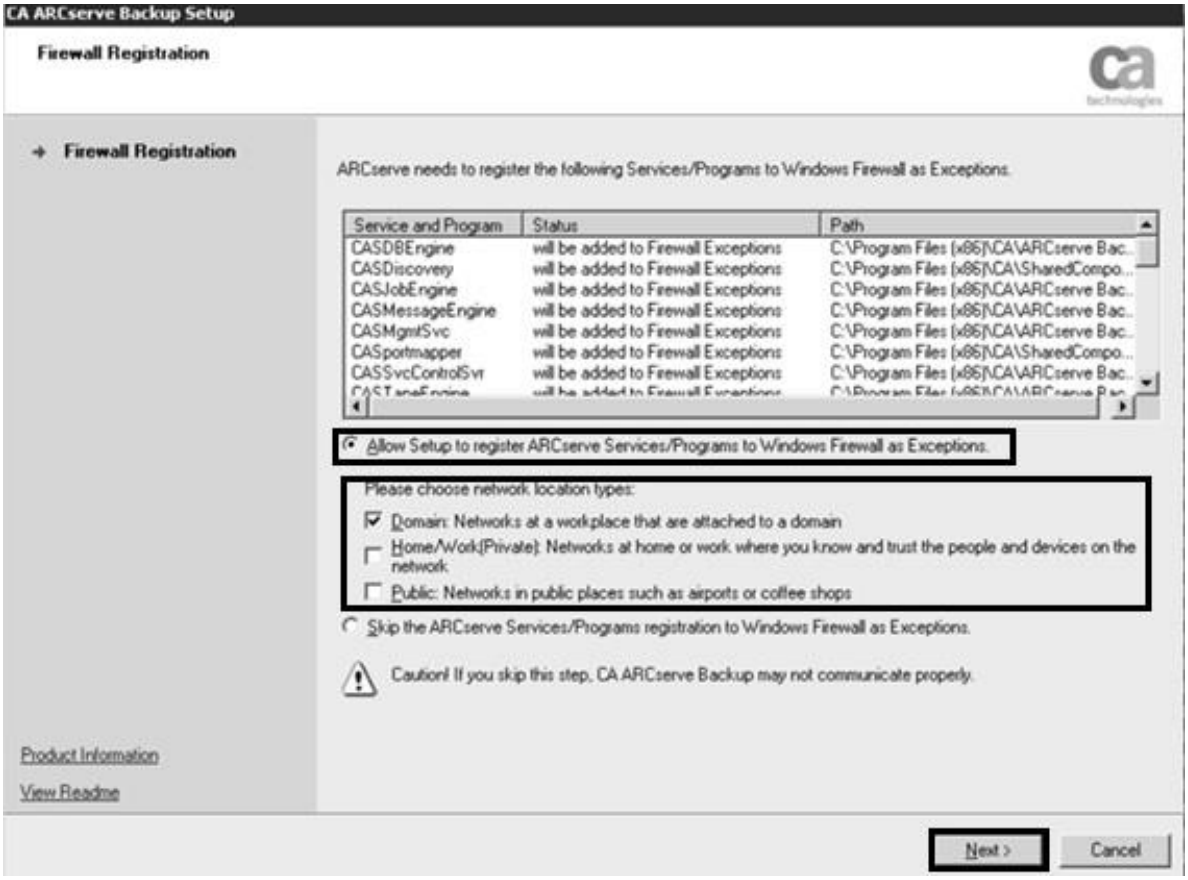
Figura 20 - Instalação ARCserve Backup



Fonte: O autor

- Na janela seguinte, o assistente de instalação solicita o registro das exceções dos serviços do ARCserve no *Firewall* do Windows. Selecionar a opção *"Allow Setup to register..."*, marcar a opção referente localização de rede e clicar em "*Next*" (Figura 21).

Figura 21 - Instalação ARCserve Backup

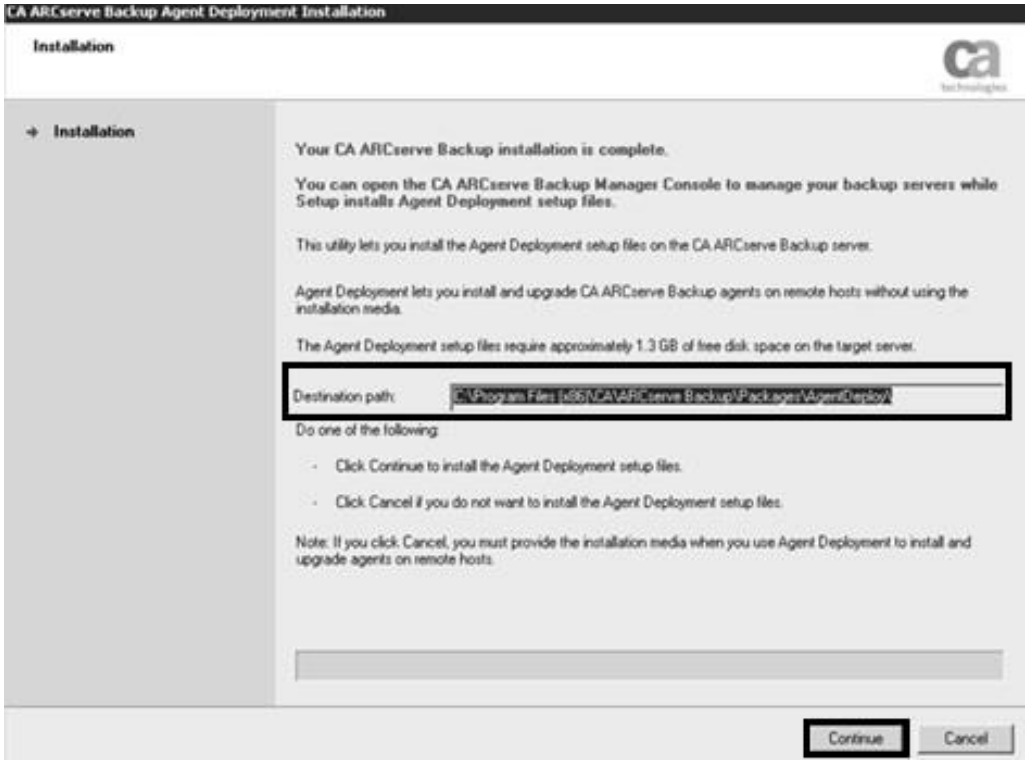


Fonte: O autor

Após a instalação do Arcserve será solicitado a instalação do pacote de *Agent* via *Deploy* (essa opção serve para instalar agentes direto da ferramenta de *backup*).

- Na janela que segue, basta selecionar o caminho onde quiser instalar o pacote, caso vá manter no diretório de instalação padrão, basta clicar em “C*ontinue”* (Figura 22).

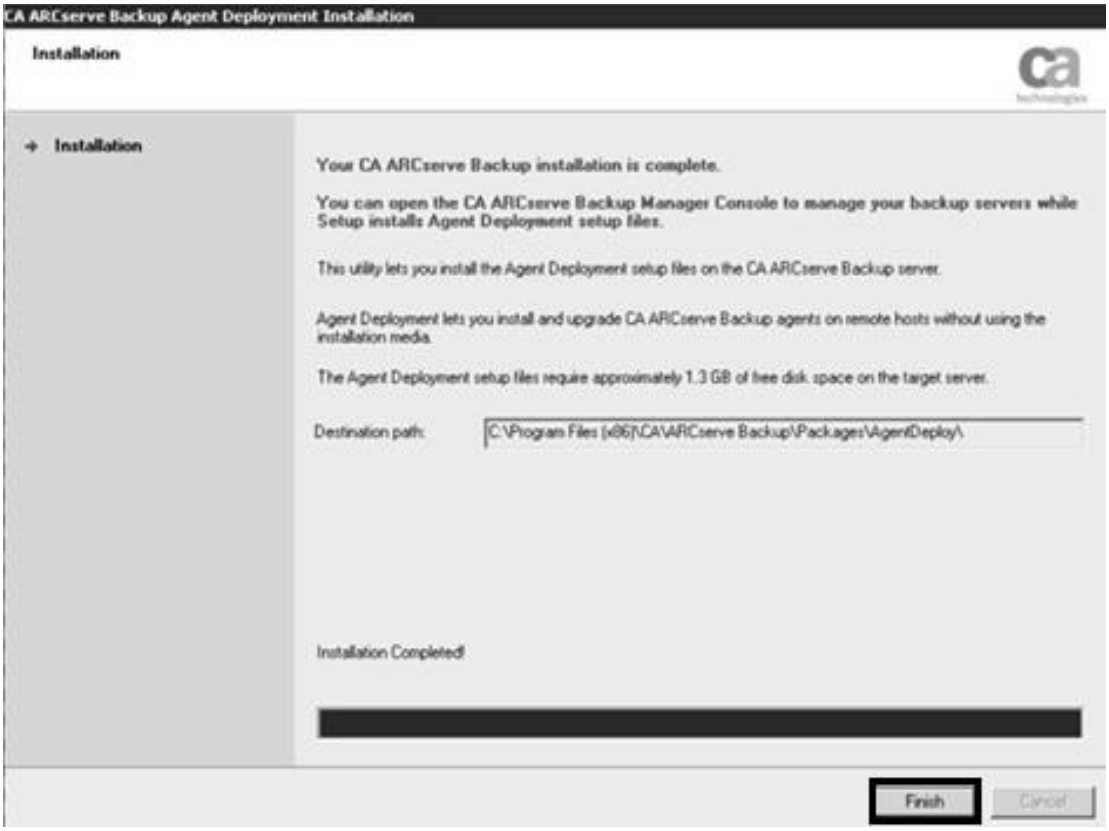
Figura 22 - Instalação ARCserve Backup



Fonte: O autor

- Ao fim da instalação clicar na opção "*Finish"*, e a instalação estará concluida (Figura 23).

Figura 23 - Instalação ARCserve Backup

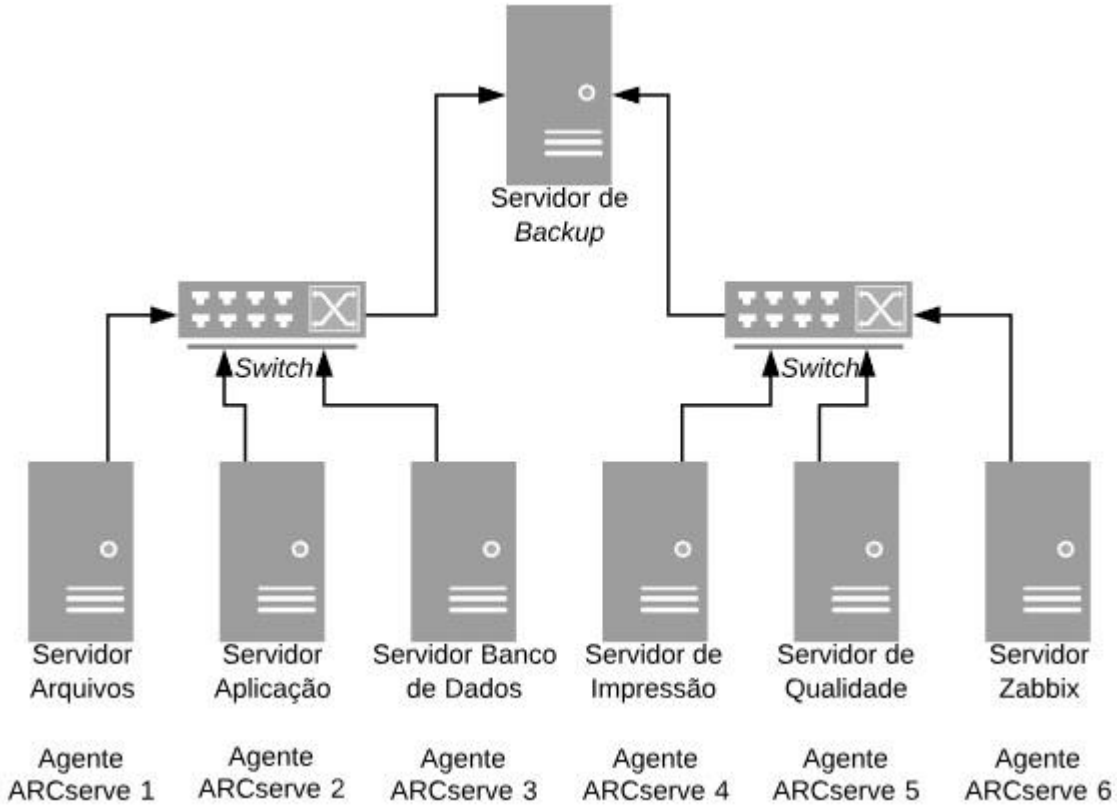


Fonte: O autor

5.7. INSTALAÇÃO AGENTE DE *BACKUP* ATRAVÉS DA OPÇÃO *AGENT DEPLOYMENT*

Após concluir a instalação do ARCserve Backup, é necessário realizar a instalação do agente no servidor onde os dados serão copiados. Para tal, será utilizada a opção de instalação via *Agent Deployment*. É importante ressaltar que, para todo servidor que terá seus dados copiados, é necessário que seja instalado um agente do *software* ARCserve, na Figura 24 é possível constatar que para realizar *backup* dos seis servidores do ambiente tomado como exemplo, é necessária a instalação de seis agentes, uma para cada servidor.

Figura 24 - Agente de Backup



Fonte: O autor

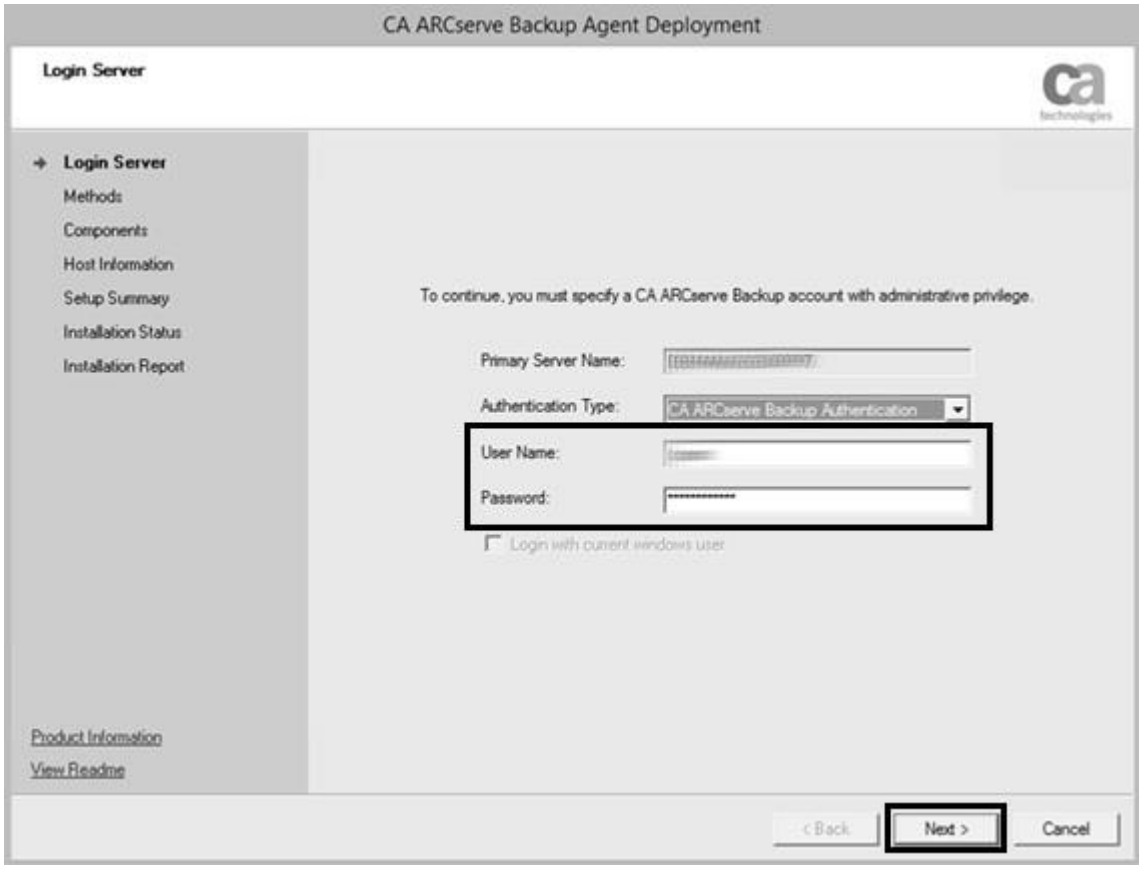
- Para iniciar a instalação do agente de backup, é necessário acessar a ferramenta de *backup* expandir a aba *Administrator* em seguida selecionar a opção *Agent Deployment* (Figura 25).

Figura 25 - Instalação Agente de *Backup*

Fonte: O autor

- Informar as credenciais da conta de *backup* cadastradas na instalação e clicar em “*Next*” (Figura 26).

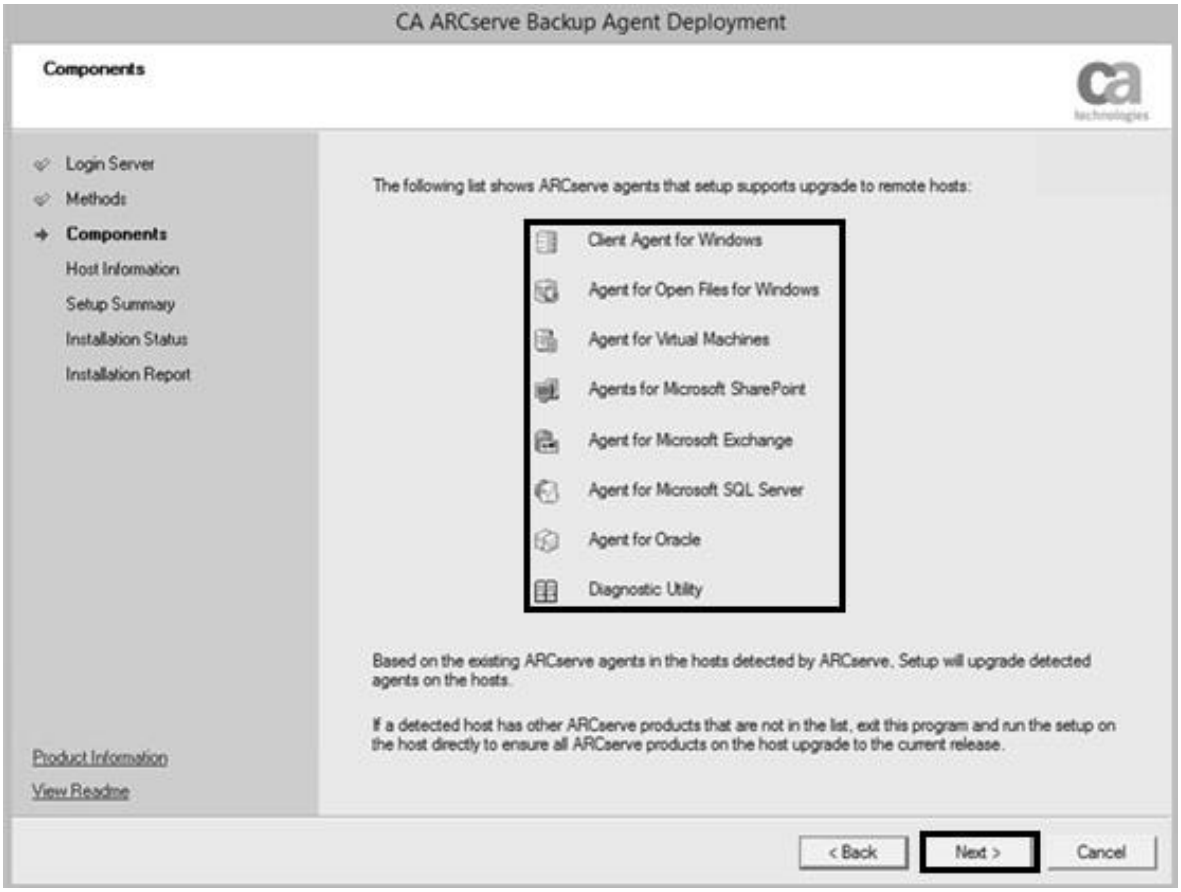
Figura 26 - Instalação Agente de *Backup*



Fonte: O autor

- Escolher a opção de instalação de acordo com as características do *host* onde o agente será instalado, servidor físico, máquina virtual, servidor SQL etc., em seguida clicar em "*Next".* (Figura 27).

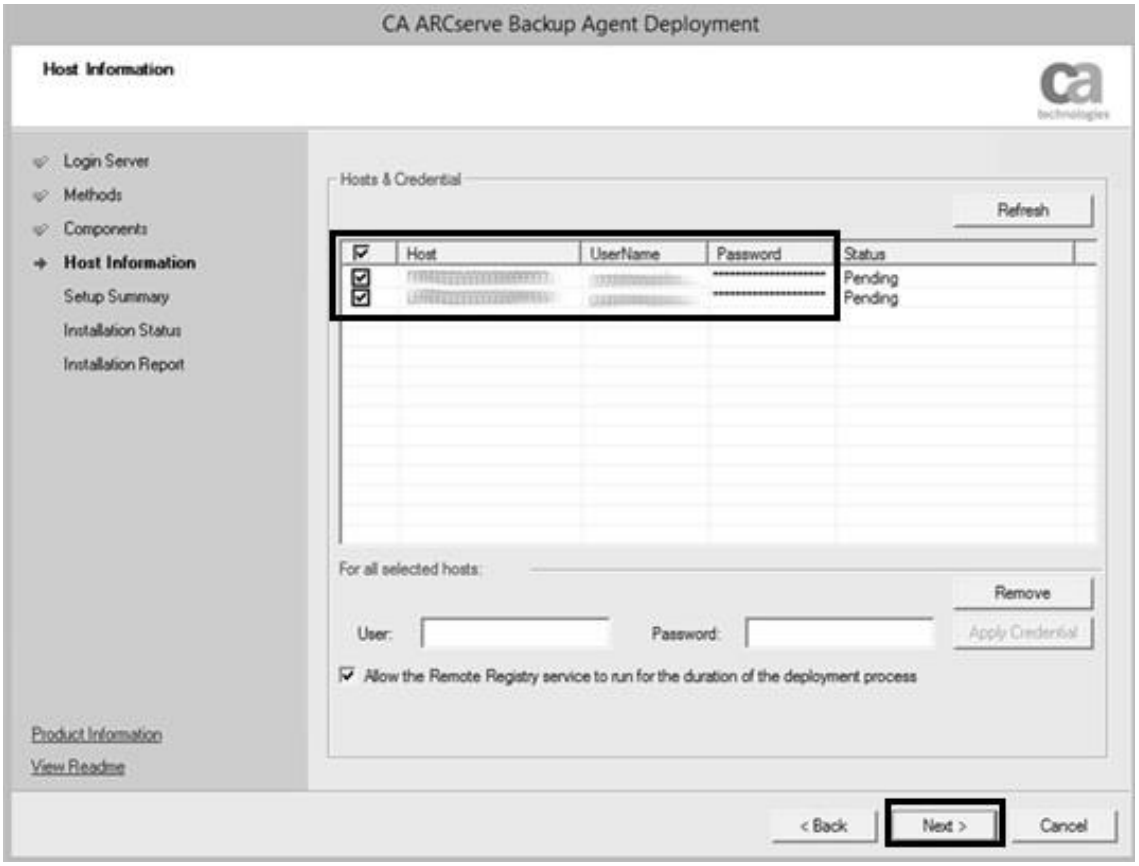
Figura 27 - Instalação Agente de *Backup*



Fonte: O autor

- Informar o *hostname* dos servidores que receberão o agente ou a atualização do agente, e inserir as credenciais da conta administrativa de *backup,* clicar em "*Next*" para prosseguir (Figura 28).

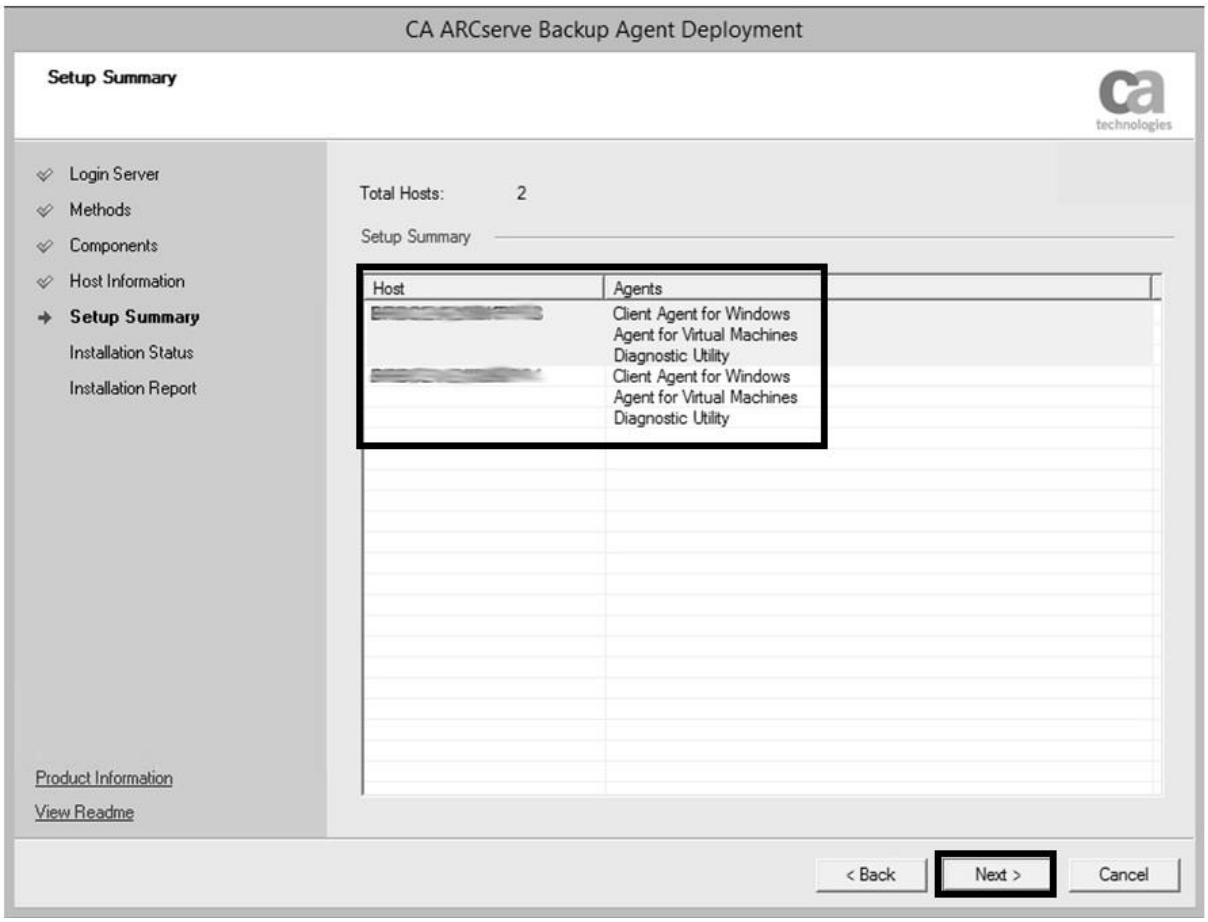
Figura 28 - Instalação Agente de *Backup*



Fonte: O autor

- Na janela seguinte, confirmar os nomes dos servidores e os componentes que serão instalados, se estiver tudo OK, clicar em "*Next*" (Figura 29).

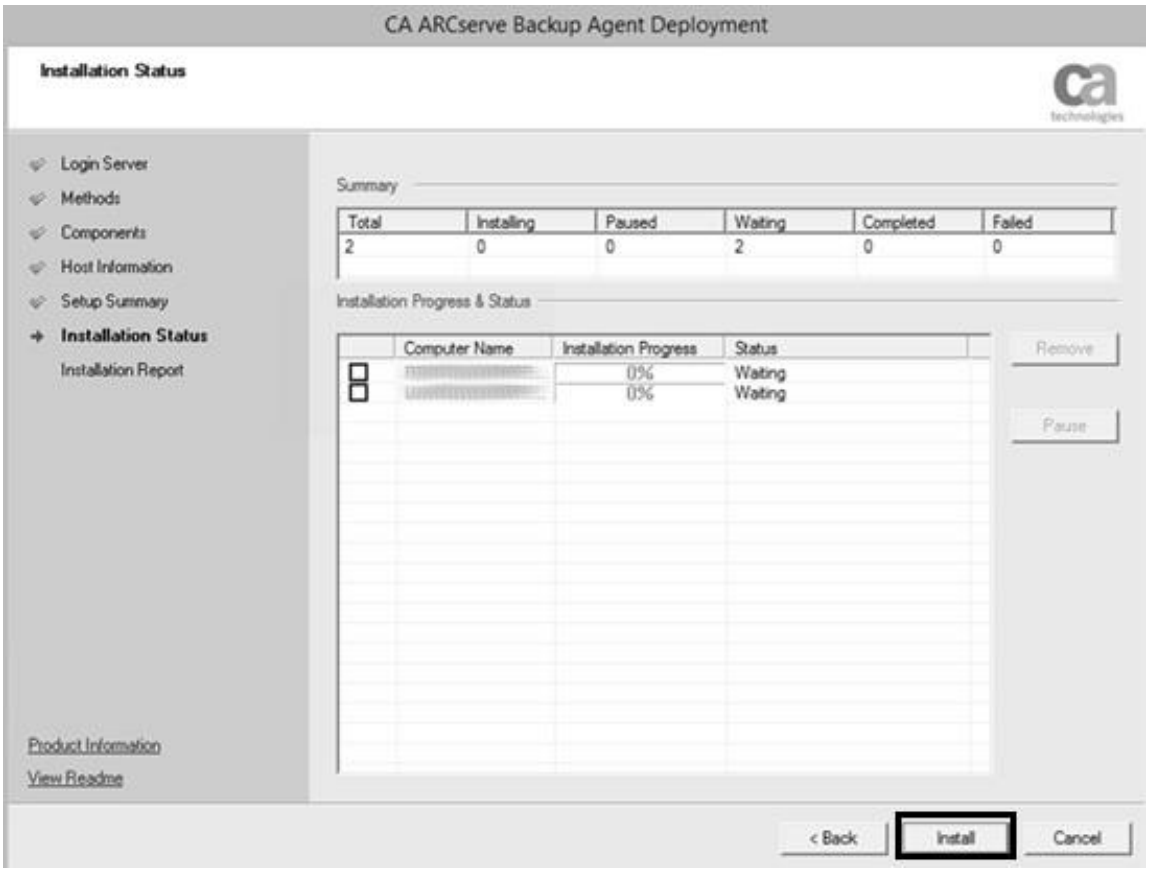
Figura 29 - Instalação Agente de *Backup*



Fonte: O autor

- A seguir, basta clicar em "*install"* e aguardar a conclusão (Figura 30).

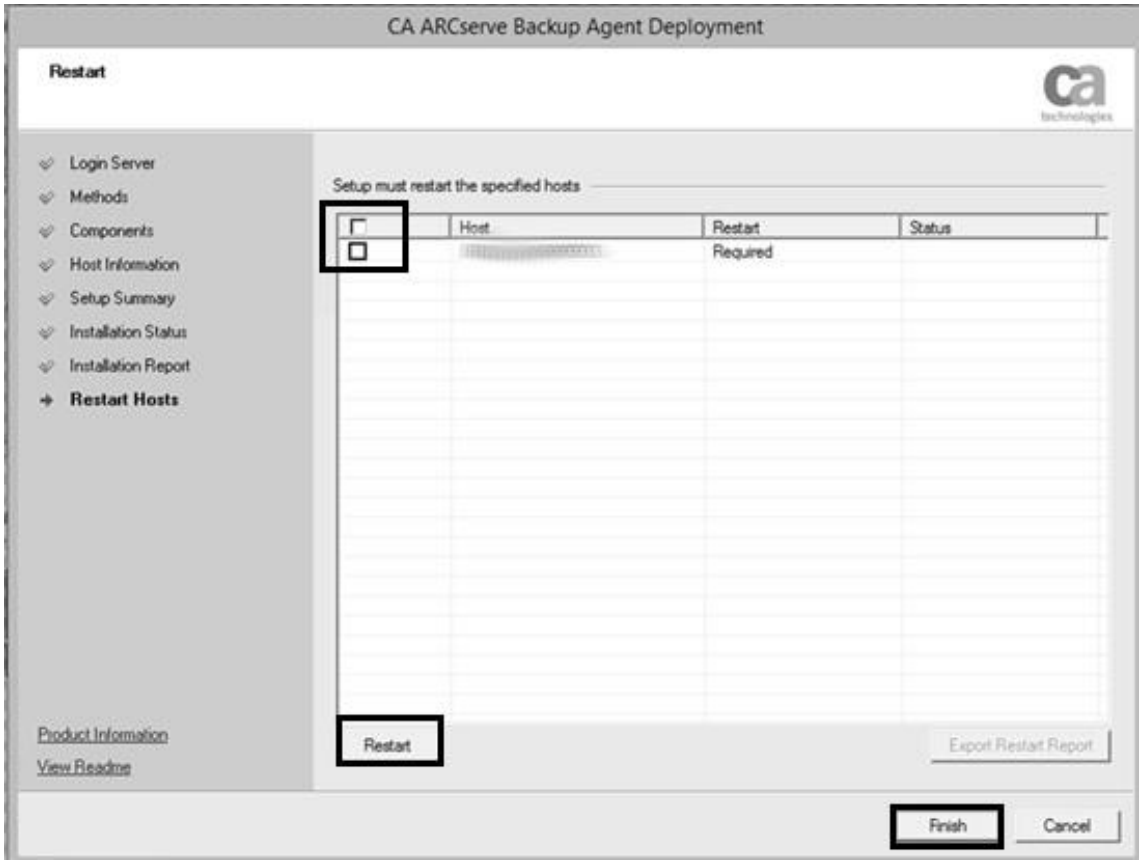
Figura 30 - Instalação Agente de *Backup*



Fonte: O autor

- Confirmar se a instalação/atualização foi aplicada com sucesso, e clicar em "*Next*". Caso seja solicitada a reinicialização do *host,* marcar o *box* e em seguida no botão "*Restart*" e finalizar a instalação no botão "*Finish"* (Figura 31)

Figura 31 - Instalação Agente de *Backup*



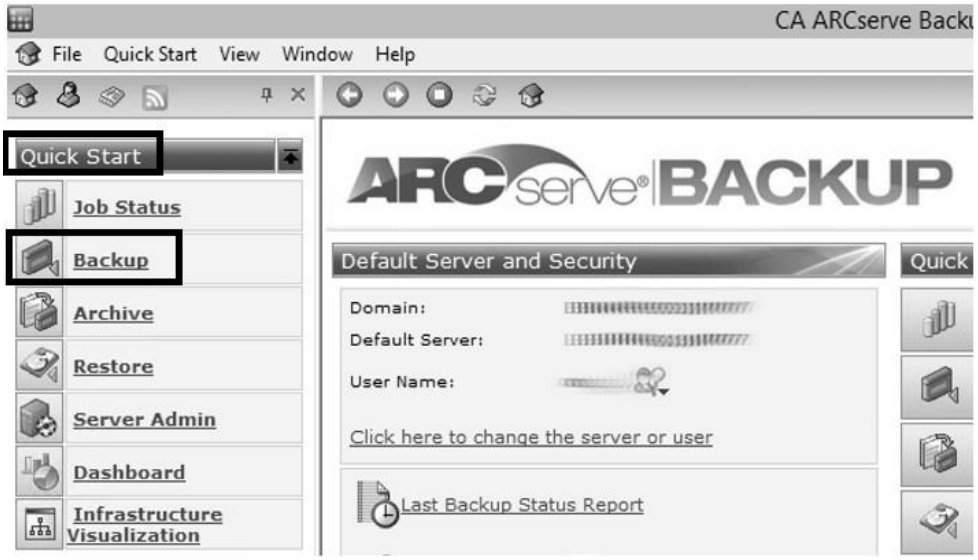
Fonte: O autor

5.8. CRIAÇÃO DE UMA TAREFA DE *BACKUP*

Durante o desenvolvimento desse trabalho, junto a equipe de *backup* da Empresa X, foi realizada a criação de um *job* de *backup* na ferramenta ARCserve. Segue abaixo o guia de implementação de uma nova rotina de cópia.

- Acessar a ferramenta ARCserve, no painel esquerdo, expandir a opção *Quick Start* e em seguida clicar na opção *Backup* (Figura 32).

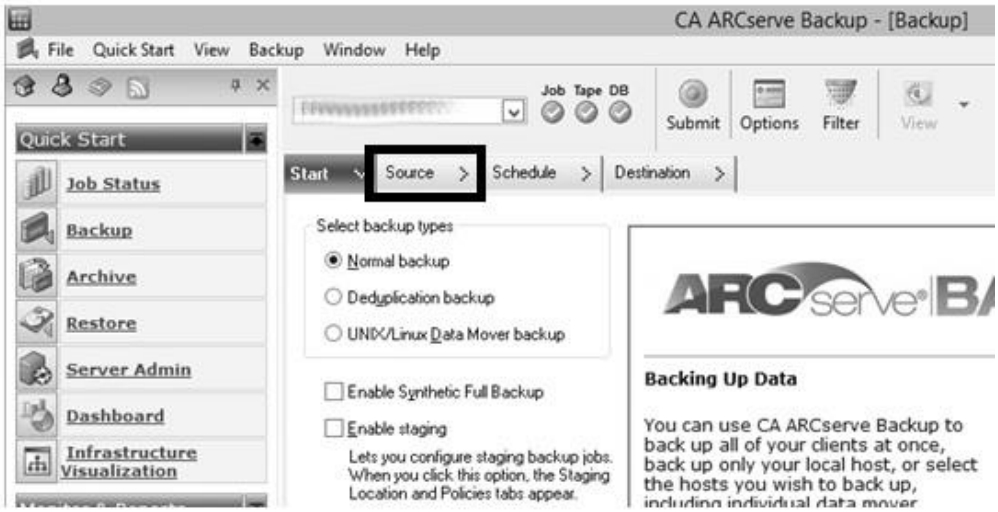
Figura 32 - Criação Job de *Backup*



Fonte: O autor

- Em seguida, clicar em *Source* (Figura 33).

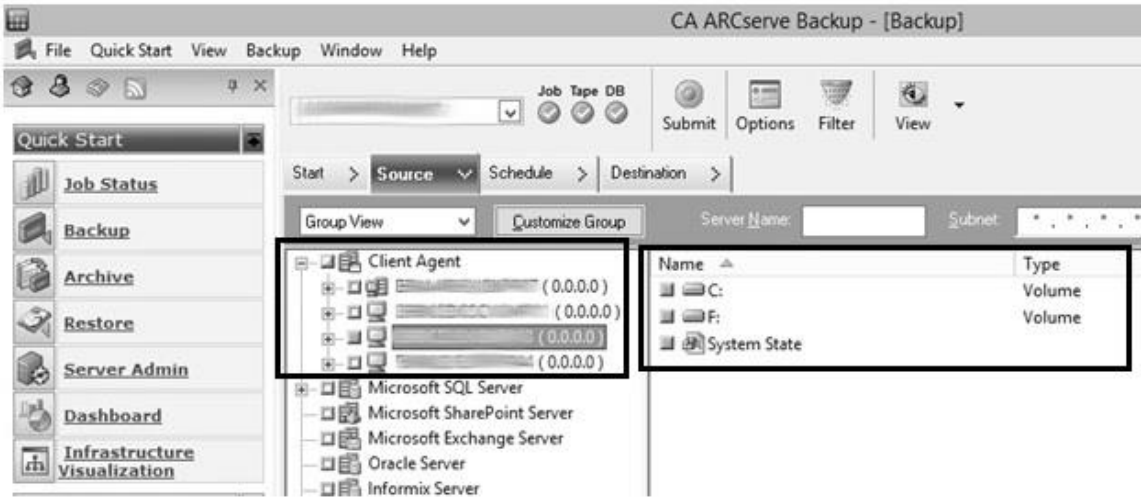
Figura 33 - Criação *Job* de *Backup*



Fonte: O autor

- Em *Source,* selecionar o host e os discos que devem ser copiados (Figura 34).

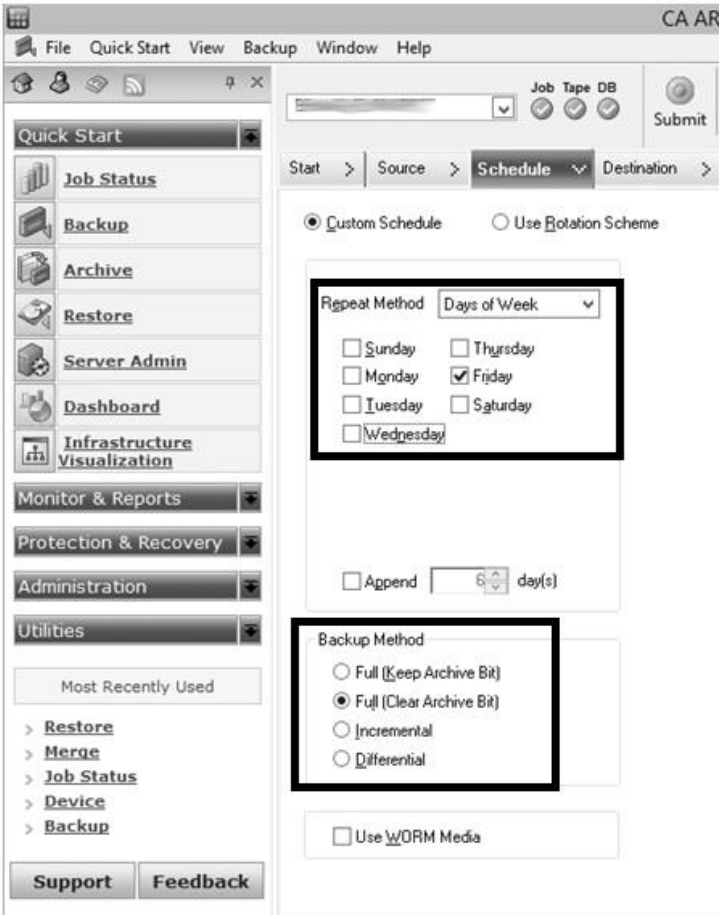
Figura 34 - Criação *Job* de *Backup*



Fonte: O autor

- Na sequência, é necessário inserir as informações referente a periodicidade do *job*, se irá executar todos os dias ou apenas um dia da semana, deve-se informar também, qual será o tipo do *backup*, incremental, completo ou diferencial (Figura 35).

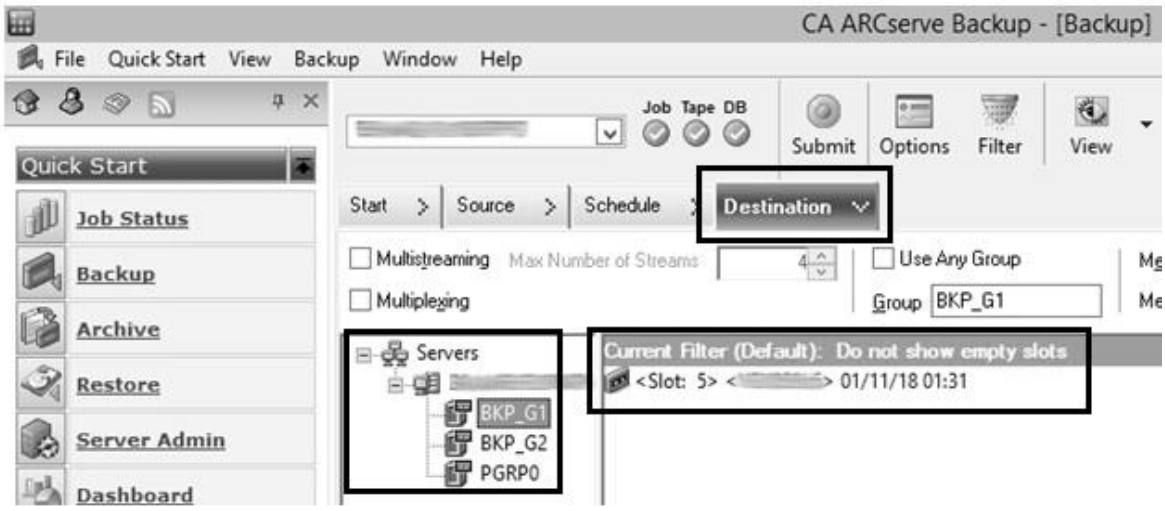
Figura 35 - Criação *Job* de *Backup*



Fonte: O autor

- Na aba *Destination,* selecionar em qual mídia será executado o *backup*, nuvem, HD ou fita, neste caso as cópias serão executadas em fita (Figura 36).

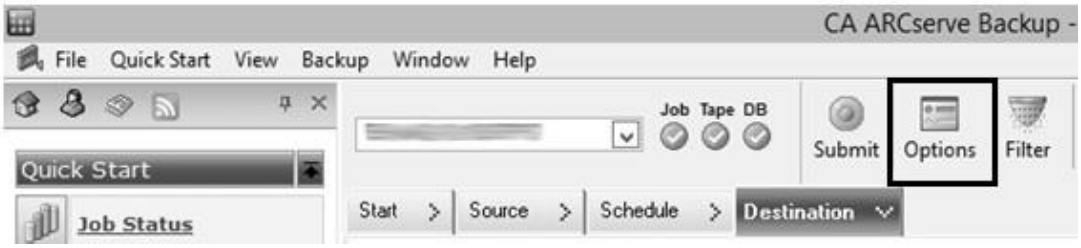
Figura 36 - Criação *Job* de *Backup*



Fonte: O autor

- Abra a opção *Options* (Figura 37).

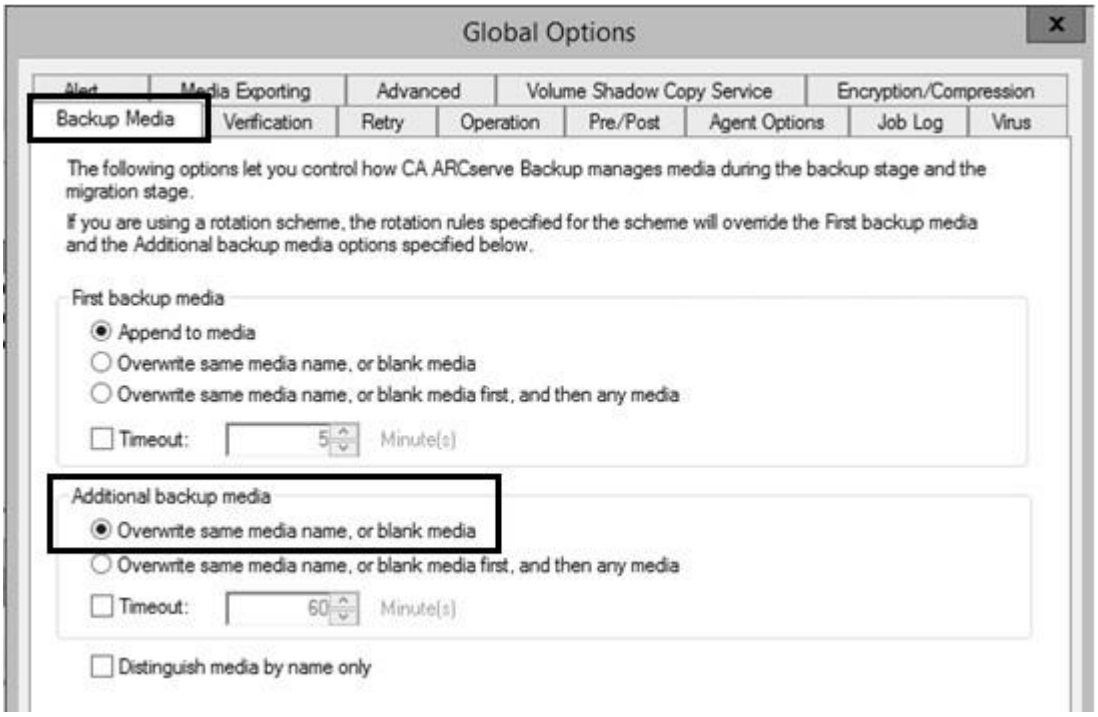
Figura 37 - Criação *Job* de *Backup*



Fonte: O autor

- Na aba *Backup Media,* configurar o tempo que a tarefa irá esperar para montar a outra fita caso seja necessário, para essa configuração não há *"time out*", ele fica esperando até a próxima fita ser montada (Figura 38).

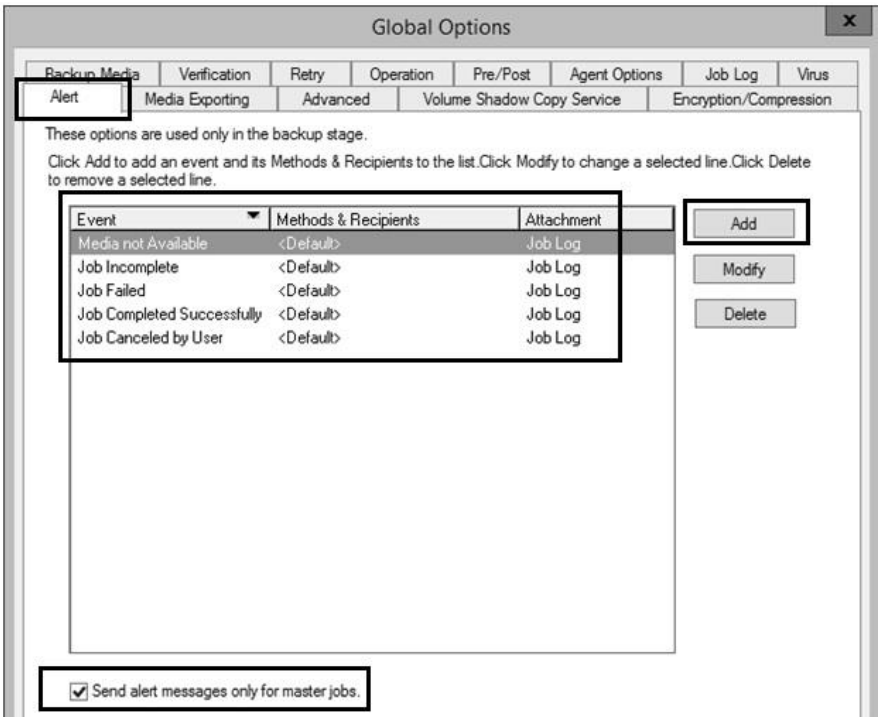
Figura 38 - Criação *Job* de *Backup*



Fonte: O autor

- Na aba *Alert* é possível configurar os eventos que serão notificados via e-mail, basta clicar em *Add* e selecionar conforme necessidade, marcar a opção "*Send alert messages only for master Jobs",* assim os alertas serão enviados para as tarefas principais, clicar em "OK" para concluir ().

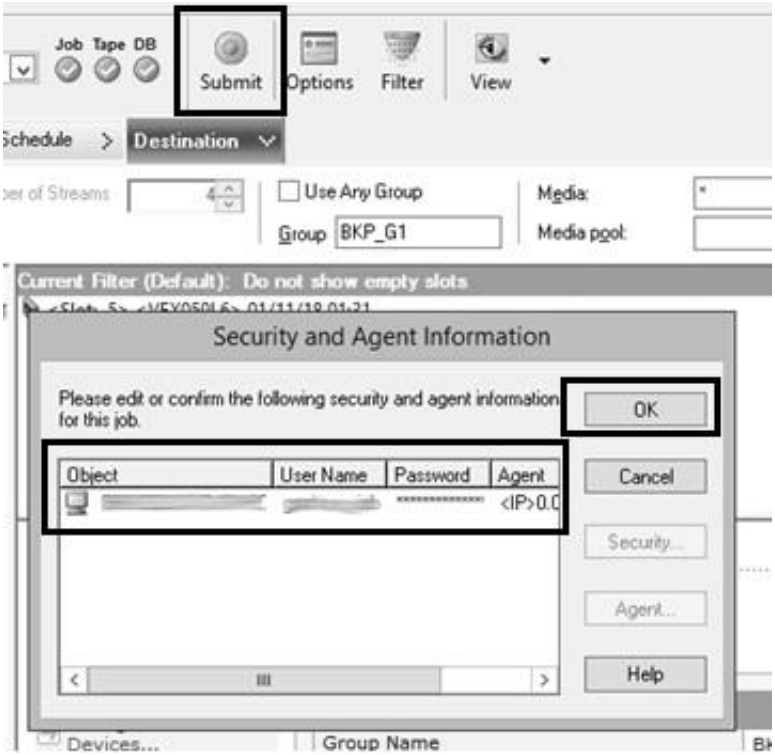
Figura 39 - Criação *Job* de *Backup*



Fonte: O autor

- Após realizar as configurações na aba *Options* clicar em S*ubmit,* na janela que irá abrir, confirmar as informações do agente e de segurança para a tarefa criada, se estiver tudo correto clicar em “OK” (Figura 40).

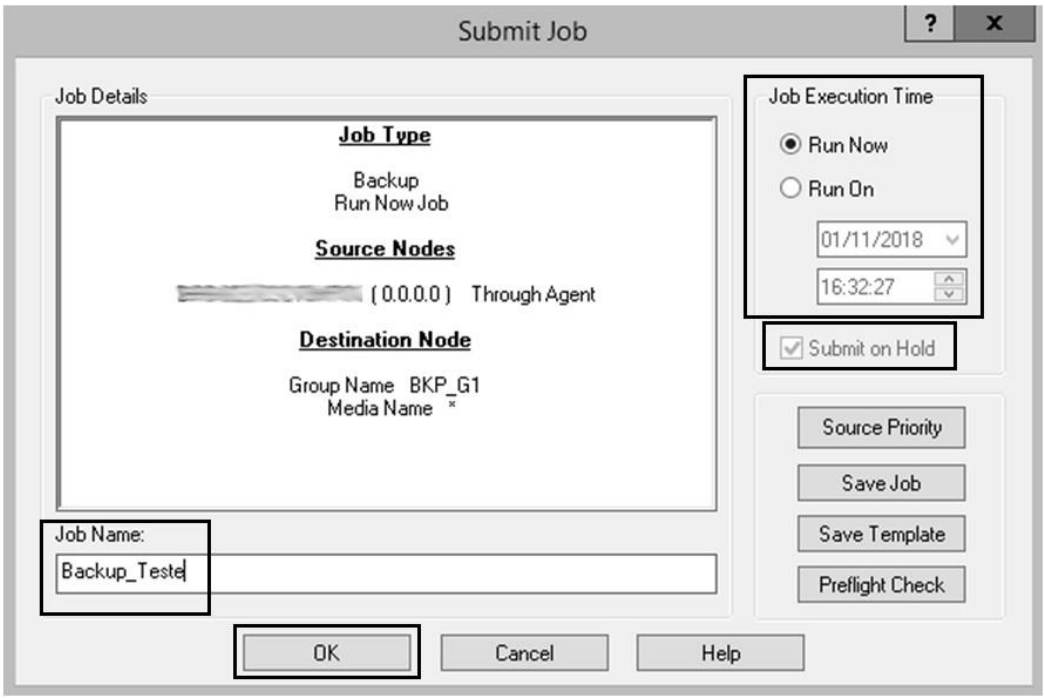
Figura 40 - Criação *Job* de *Backup*



Fonte: O autor

- Para finalizar a criação da tarefa, é necessário inserir um nome para a mesma e selecionar se o *job* irá executar imediatamente ou terá início em uma data específica, se a opção *Submit on Hold* estiver marcada, a tarefa será criada e ficara com o status de aguardando, portanto para ela iniciar será necessário que ela seja colocada em execução manualmente, por fim clicar em “OK” e o *job* estará criado (Figura 41).

Figura 41 - Criação *Job* de *Backup*



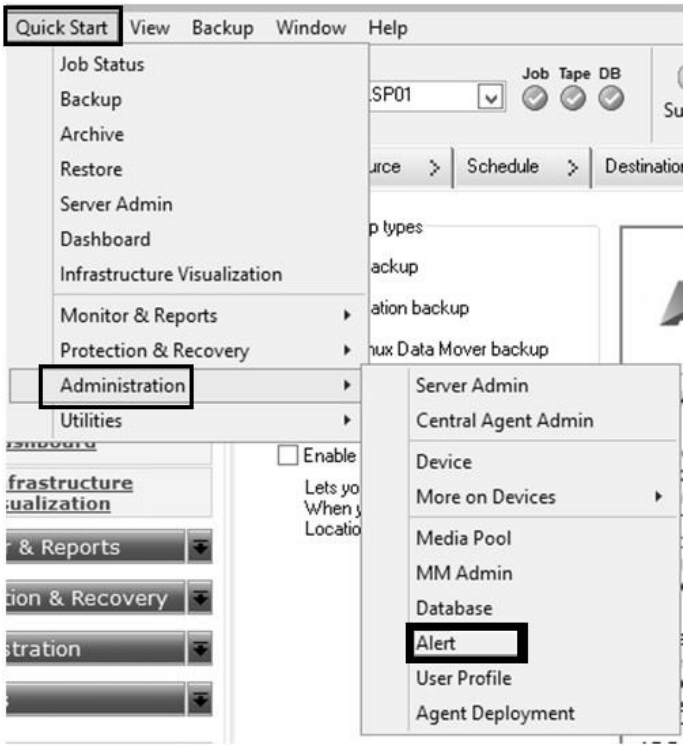
Fonte: O autor

5.9. INSERIR E-MAIL DE ALERTA NO ARCSERVE

A ferramenta de *backup* ARCserve, possibilita o envio de e-mail com os *status* das tarefas, isso auxilia no monitoramento dos *backups* em ambientes onde existem diversas tarefas sendo executadas diariamente. Segue o passo-a-passo da configuração.

- Abrir o ARCserve, na aba *Quick Start,* ir até *Administration* e em seguida clicar na opção *Alert* (Figura 42)

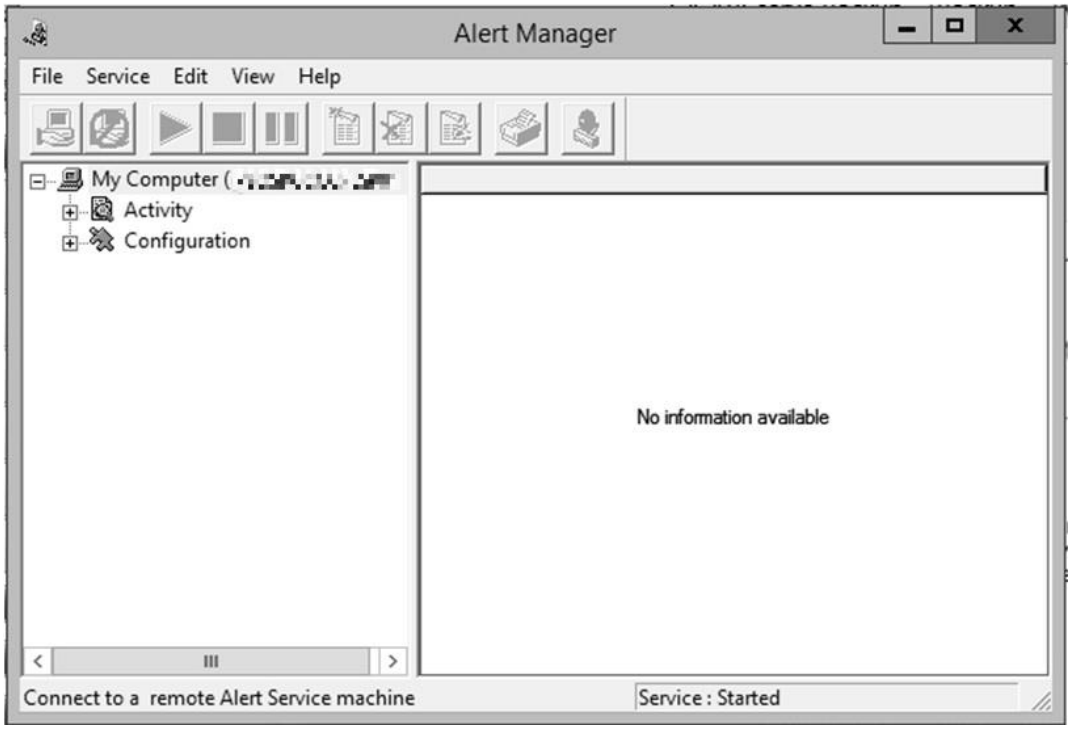
Figura 42 - Configurar E-Mail de Alerta



Fonte: O autor

- Em seguida, será aberta uma nova janela conforme mostra a Figura 43, talvez seja necessário inserir o domínio e as credenciais da conta de administrador usada para as tarefas de *backup.*

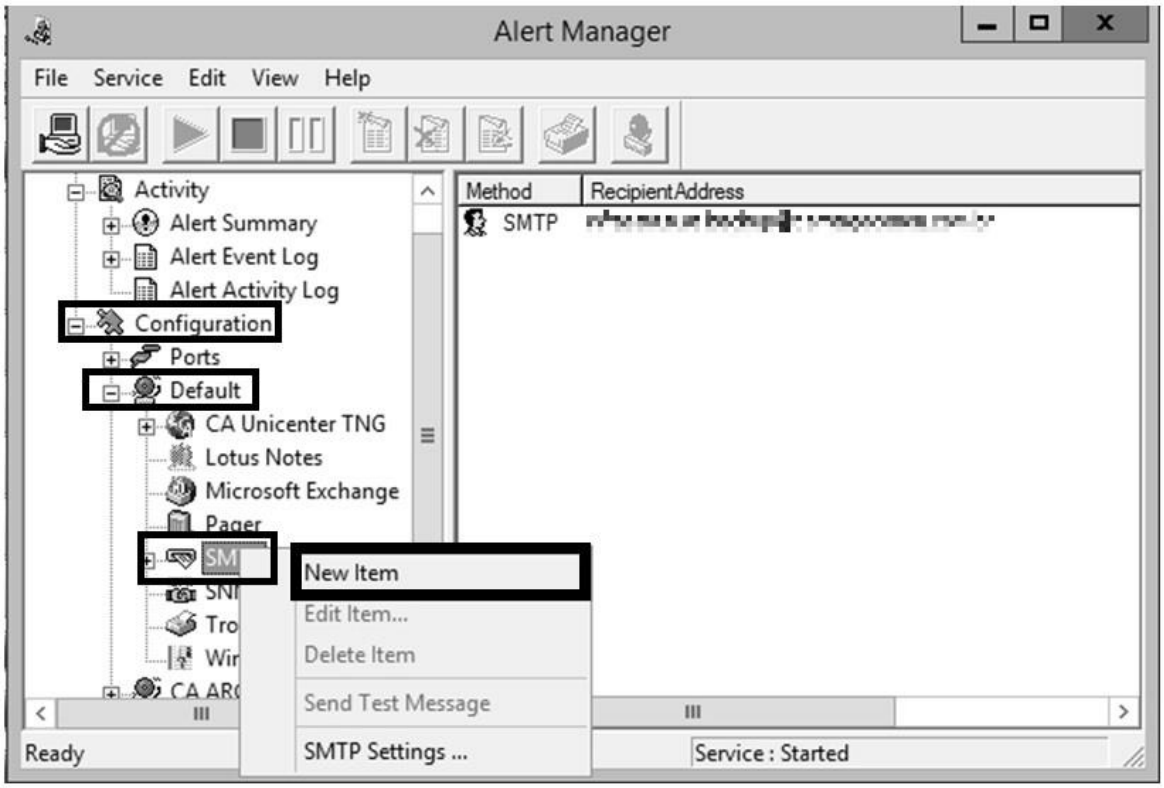
Figura 43 - Configurar E-Mail de Alerta



Fonte: O autor

- Expandir a opção *Configuration,* em seguida *Default*, e na opção SMTP, clicar com o botão direito e selecionar a opção *New Item* (Figura 44).

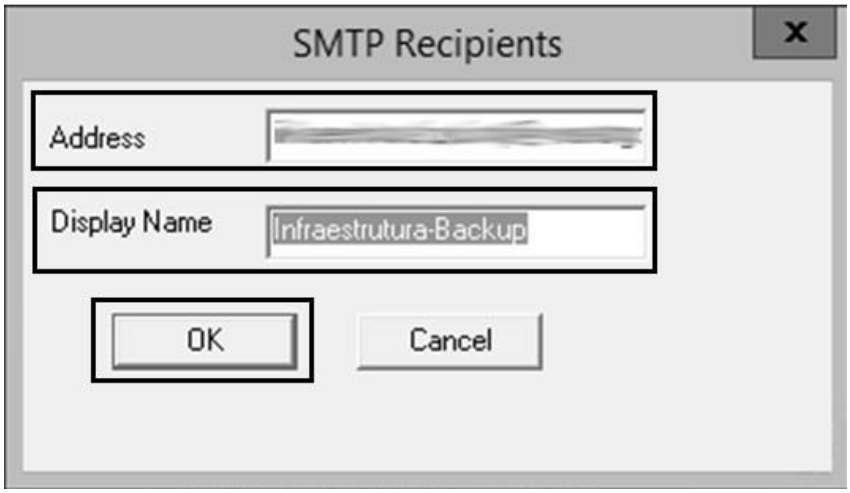
Figura 44 - Configurar E-Mail de Alerta



Fonte: O autor

- Na janela que será aberta, inserir a conta de e-mail que receberá os alertas e um nome para exibição e clique em “OK” para confirmar (Figura 45).

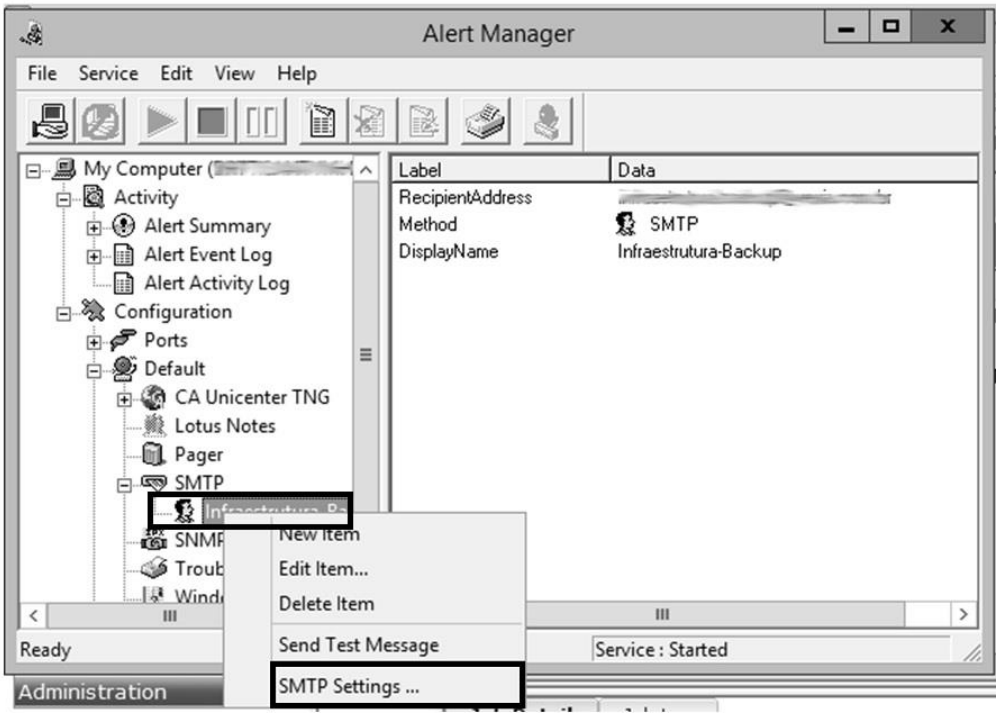
Figura 45 - Configurar E-Mail de Alerta



Fonte: O autor

- A seguir, clicar com o botão direito em cima do novo objeto criado e selecionar a opção SMTP *Settings* (Figura 46).

Figura 46 - Configurar E-Mail de Alerta



Fonte: O autor

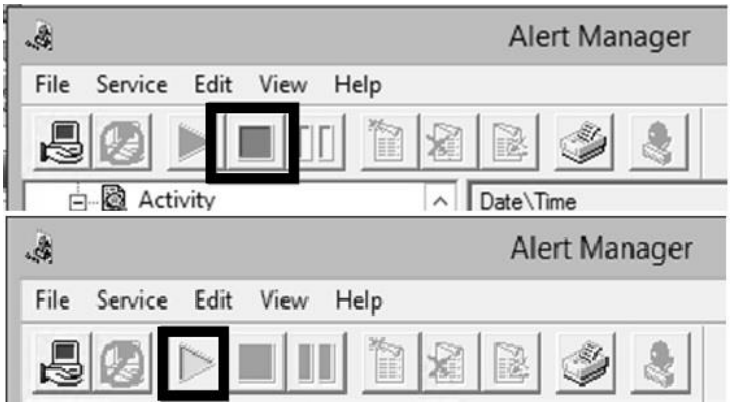
- Na janela que irá abrir, adicionar as informações referente ao e-mail que irá enviar as mensagens, o assunto do e-mail e o SMTP do servidor de e-mail e clicar em “OK” (Figura 47).

Figura 47 - Configurar E-Mail de Alerta

Fonte: O autor

- Após realizar os procedimentos anteriores, é necessário parar e reiniciar o serviço de alerta do ARCserve (Figura 48).

Figura 48 - Configurar E-Mail de Alerta



Fonte: O autor

- Após concluir a configuração, é possível realizar o envio de um e-mail de teste clicando no ícone conforme mostra a Figura 49.

Figura 49 - Configurar E-Mail de Alerta

Fonte: O autor

6. CONSIDERAÇÕES FINAIS

A informação vem se tornando um dos ativos mais importantes e valiosos para as organizações modernas, levando isso em consideração e adicionando o fator que o volume de dados gerados cresce em ritmo acelerado, é necessário atentar-se aos riscos que esse crescimento junto ao valor da informação pode gerar.

É importante ressaltar que o mercado da segurança da informação vem crescendo, e cresce também a procura por novas tecnologias de proteção além é claro, de reformulações em métodos já largamente utilizados bem como a extinção de outros.

Levando em consideração os riscos reais ao qual uma empresa está sujeita, este trabalho buscou por apresentar conceitos relativos as cópias de segurança, bem como a instalação e configuração de uma ferramenta de *backup,* em um ambiente real e que manipula um volume alto de dados mensalmente, isso com o intuito de garantir que em um caso de perda ou roubo de informações, a mesma possa ser recuperada garantindo assim a disponibilidade dos dados e a continuidade dos negócios.

A resposta para a pergunta desse trabalho é, sim, a ferramenta ARCserve atende as necessidades da Empresa X, os recursos disponibilizado pela ferramenta, vão de encontro com as necessidades que a empresa apresenta, pois a ferramenta é capaz de atender altas demandas, bem como demandas menores, ou seja ela pode se ajustar ao volume de informações que serão copiados. Essa característica é muito importante para a Empresa X, já que ela possui grandes clientes, que demandam um grande volume de dados para serem copiados, assim como clientes com um volume menor de informações a serem guardadas.

Com relação as hipóteses levantadas, seguem as constatações realizadas, sobre casa uma delas.

a) A ferramenta possui uma interface de instalação amigável e de fácil entendimento;

Durante as atividades desse trabalho, foi possível verificar que a ferramenta ARCserve, oferece uma interface amigável e muito intuitiva, sua instalação é bem simples e não exige conhecimentos avançados para essa etapa.

b) O agente de *backup* precisa ser instalado manualmente em cada dispositivo que terá seus dados copiados;

A ferramenta possui um módulo de gerenciamento das instalações de agentes de *backup* (*Agent Deployment),* como podemos ver nesse trabalho, com ele não é necessário realizar a instalação manual em cada novo equipamento, o instalador dos agentes, também possui uma interface simples, onde o usuário que necessitar inserir novas rotinas de *backup* para um novo servidor, não encontrara dificuldades para tal.

c) É necessário conhecimento avançado para a criação das tarefas de *backup;*

A configuração de uma tarefa de *backup* se mostrou muito rápida e fácil, mesmo a ferramenta dispondo de diversos recursos para se criar uma nova rotina de *backup*, se o objetivo do administrador for criar um novo *job* em poucos minutos, com o ARCserve isso é possível, já que as opções são muito claras e não fogem dos conceitos comuns a cerca de *backup*.

d) A ferramenta não dispõe de um método de envio de mensagens informando o *status* das tarefas.

O recurso oferecido pelo ARCserve de alertas via e-mail, é muito interessante e útil, em ambientes onde há um volume de rotinas de *backup* muito grande, esse recuso auxilia muito no gerenciamento de sucessos e falhas, já que não seria necessário ficar realizando "*login*" em cada servidor que hospeda o ARCserve. Através dos e-mails de alerta trata-se apenas os *jobs* com falhas, cancelados ou incompletos, isso gera uma economia de tempo para a equipe de *backup,* tempo esse que pode ser empregado em melhorias para o processo.

Com a realização desse trabalho, foi possível ampliar a visão sobre as rotinas de *backup,* e sobre sua importância. Dentre os diversos conceitos vivenciados, é possível citar, disponibilidade de dados, tipos de *backup*, política de *backup*, a importância do *backup* para as empresas. Além disso, foi possível conhecer a ferramenta ARCserve, e constatar sua viabilidade em um ambiente que gerencia um grande volume de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTIN, Alberto Luiz. **Valor Estratégico dos Projetos de Tecnologia de Informação**. Revista de Administração de Empresas: São Paulo/SP, vol. 41, n. 3, p. 42-50, 2001.

AMADO, Wesley Ricardo; MARCONDES, Cesar Augusto Cavalheiro. **Análise do Software BSN para a Realização de Backups na Nuvem**. Revista T.I.S: São Carlos/SP, vol.3, n3, p. 244-253, 2014. Disponível em: < www.revistatis.dc.ufscar.br/index.php/revista/article/download/180/88>. Acesso em: 07 out. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2013: **Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos**. São Paulo/SP. 2013. 32p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013: **Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação**. São Paulo/SP. 2013. 112p.

AVAST. **WannaCry.** Avast, Praga/República Checa. Disponível em: <https://www.avast.com/pt-br/c-wannacry>. Acesso em: 12 ago. 2018.

AVILA, Thiago. **O que faremos com os 40 trilhões de gigabytes de dados disponíveis em 2020?.** Cambridge/França: Open Knowledge Brasil, 29 setembro 2017. Disponível em: < https://br.okfn.org/2017/09/29/o-que-faremos-com-os-40-trilhoes-de-gigabytes-de-dados-disponiveis-em-2020/>. Acesso em 15 ago. 2018.

BARROS, E. **Entendendo os conceitos de *backup*:** *Restore* e recuperação de desastres. 1ª.ed. Rio de Janeiro: LCM. 2007. 80p.

CAMPOS, Rafael de Moura. **Gerenciamento E Proteção De Dados "On Premise" E "Cloud"**. Tubarão/SC: Unisul Virtual, 2017. p. 6-7. Disponível em:< https://riuni.unisul.br/handle/12345/3151?show=full>. Acesso em: 06 out. 2018.

CA TECHNOLOGIES. **CA ARCserve Backup para Windows:** Guia de administração. Nova Iorque/Estado Unidos. Disponível em: < http://documentation.arcserve.com/Arcserve-Backup/Available/R16-5/PTB/Bookshelf_Files/PDF/AB_ADMIN_W_PTB.pdf>. Acesso em 20 ago. 2018.

CASTRO, Carlos José de Lima; VICTORINO, Carlos Roberto; TOBIAS, Josué José. **Guarda e Manutenção de Documentos Fiscais**. Brasília: FiscoSoft, 2010. p. 10-13. (Três capítulos)

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br.** 2018. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 09 set, 2018.

CHOO, C. W. **A organização do conhecimento:** como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: Senac, 2003. 426p

COELHO, F. E. S.; ARAÚJO, L. G. S.; BEZERRA, E. K.; **Gestão da Segurança da Informação:** NBR 27001 e NBR 27002. 1ª edição. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa-RNP, 2014. p. 70-72. Disponível em: <https://www.passeidireto.com/arquivo/16870037/gestao-da-seguranca-da-informacao---nbr-27001-e-nbr-27002>. Acesso em: 16 de set. 2018.

DANTAS, Marcus Leal. **Segurança da Informação:** uma abordagem focada em gestão de riscos. Olinda/PE: Livro Rápido, 2011. p. 9-11. Disponível em: < http://www.marcusdantas.com.br/files/seguranca_informacao.pdf>. Acesso em 15 ago. 2018.

DA ROSA, Mateus Gonzaga et al. **Comparativo entre Softwares de Backup em Ambiente Organizacional**. Organizadores Vanderlei Freitas Junior Lucyene Lopes da Silva Todesco Nunes Thales do Nascimento da Silva Gerson Luis da Luz, v. 88960, p. 93. Disponível em: <http://redes.sombrio.ifc.edu.br/wp-content/uploads/sites/7/2015/12/Livro-Tecnologia-e-Redes-de-Computadores-2015.pdf#page=93>. Acesso em: 06 out. 2018.

DAWEL, George. **Segurança da Informação nas Empresas:** Ampliando Horizontes Além da Tecnologia. 1ª.ed. Rio de Janeiro: Editora Ciência Moderna. 2005. 136p.

DE MELO, Marco A. M.; GONÇALVES, Fernando S. P. **S.O.S. Backup Database**. Florianópolis/SC: Virtus Infomática LTDA. 2004, p. 1-4. Disponível em: < http://www.virtos.com.br/pt/documentacao/S.O.S_Backup_Database.pdf>. Acesso em: 07 out. 2018.

DELL EMC. **Índice global de proteção de dados da EMC:** resultados globais. 2016. Disponível em: <https://brazil.emc.com/infographics/global-data-protection-index-global.htm>. Acesso em: 9 set, 2018.

FARIA, H. M. **Bacula:** Ferramenta livre de backup. São Paulo: BRASPORT. 2014. 318p.

FERNANDES, J. H. C. **Gestão da segurança da informação e comunicações.** v.1. Brasília: Editado pela Faculdade de Ciência da Informação da Universidade de Brasília. 2010. 125p.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Políticas de segurança da informação:** Guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2008.

FERRAZ, Gilnei. **Principais meios de armazenamento de dados utilizados em datacenters modernos.** Tubarão/SC: Unisul Virtual, 2018. p. 1-3. Disponível em: < https://www.riuni.unisul.br/bitstream/handle/12345/4812/AD6_Principais_meios_de_armazenamento_de_dados_utilizados_em_datacenters_modernos_v2.pdf?sequence=5&isAllowed=y>. Acesso em 13 ago. 2018.

FIALHO JR, M. **Guia essencial do *backup***. São Paulo: Universo dos Livros. 2007. 128 p. Disponível em: <https://books.google.com.br/books?id=RP8R90IysJQC&pg=PP1&lpg=PP1&dq=Guia+essencial+do+*Backup*+-+Mozart+Fialho+Jr.&source=bl&ots=dUTbfWAnbp&sig=ZKA3Gn-GtjlE27fltP4ohkyaIlM&hl=pt-BR&sa=X&ved=0ahUKEwjMvqnDgvTWAhWIDJAKHZv3Cv0Q6AEIQTAF#v=onepage&q=Guia%20essencial%20do%20*Backup*%20-%20Mozart%20Fialho%20Jr.&f=false>. Acesso em 01 set. 2017.

FONTES, E. **Segurança da informação:** O usuário faz a diferença. São Paulo: Saraiva. 2006. 168p.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa.** 1ª.ed. Porto Alegre: Editora UFRGS. 2009. p. 31-41.

GIL. Antonio Carlos. **Como elaborar projetos de pesquisa.** 4ª.ed. São Paulo: Atlas. 2002. p. 41-55.

Hewlett Packard Enterprise Centro de Suporte. **Mídia HP LTO Ultrium - Recomendações de uso de mídia.** Palo Alto/Estados Unidos. Disponível em: < https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c03756648&docLocale=pt_BR>. Acesso em 18 de ago. 2018.

IBM Knowledge Center. **Armazenamento Ótico**. Armonk/Estado Unidos. Disponível em <https://www.ibm.com/support/knowledgecenter/pt-br/ssw_ibm_i_73/rzam4/rzam4optical.htm>. Acesso em: 12 ago. 2018.

JESUS, Guilherme Bindi Alencar; SCHIMIGUEL, Juliano. **Implementação De Backup Como Processo de Segurança da Informação.** Revista Atlante: Cuadernos de Educación y Desarrollo. p. 2-3. Disponível em: <https://www.eumed.net/rev/atlante/2018/02/backup-seguranca-informacao.html>. Acesso em 16 ago. 2018.

LUSTOSA, J. G. **O comportamento informacional de gerentes e pesquisadores do centro de Pesquisa Agropecuária do Meio-Norte**. Embrapa Meio-Norte. 2001. 123 f. Dissertação de Metrado – Universidade Federal de Minas Gerais. Belo Horizonte, 2001. Disponível em: < http://www.bibliotecadigital.ufmg.br/dspace/handle/1843/EARM-7HARNY>. Acesso em: 04 set. 2018.

MARCONI, Mariana de Andrade; LAKATOS. Eva Maria. **Fundamentos da metodologia cientifica.** 5ª.ed. São Paulo: Atlas. 2003. p. 217-226.

OPENSPACE. **O 11 de Setembro e os modelos de Continuidade dos Negócios.** OpenSpace, São Paulo/SP, 21 dezembro 2016. Disponível em: <http://ospace.com.br/o-11-de-setembro-e-os-modelos-de-continuidade-dos-negocios/>. Acesso em: 9 ago. 2018.

PICOVSKY, José. **Análise De Gestão De Riscos E Impactos Da Tecnologia Da Informação Nos Negócios**. Revista Brasileira de Inovação Tecnológica em Saúde - ISSN:2236-1103, v. 3, n. 1, 20 maio 2013. Disponível em: <//doi.org/10.18816/r-bits.v3i1.3439>. Acesso em: 06 out. 2018.

PHILERENO, Eduardo. **Backup, Restore E Armazenamento:** Conceitos E Práticas Aplicados A Solução HPE Data Protector. Tubarão/SC: Unisul Virtual, 2017. p. 19-22. Disponível em: <https://www.riuni.unisul.br/handle/12345/4666>. Acesso em: 07 out. 2018.

ROCHA, Clécio Teixeira *et al*. **Plano de Recuperação de Desastres utilizando ferramenta Veeam Backup & Replication em falha do Active Directory.** Jaboatão dos Guararapes/PE: Unibratec, 2015. p. 4-5. Disponível em: < http://www.unibratec.edu.br/tecnologus/wp-content/uploads/2015/12/tecnologus_edicao_09_artigo_02.pdf>. Acesso em: 06 out. 2018.

SÊMOLA, M. **Gestão da segurança da informação:** Uma visão executiva. Rio de Janeiro: Campus. 2003. 184p.

SOMASUNDARAM, G.; SHRIVASTAVA, A. **Armazenamento e gerenciamento de informações**: Como armazenar, gerenciar e proteger informações digitais. Acauan Pereira Fernandes. Porto Alegre: Artmed. 2011. P. 273-305. Disponível em: <https://books.google.com.br/books?id=d8uCfC46hwsC&pg=PA3&lpg=PA3&dq=Armazenamento+e+Gerenciamento+de+Informa%C3%A7%C3%B5es:+Como+armazenar,+gerenciar+e+proteger+informa%C3%A7%C3%B5es+digitais+-+G.+Somasundaram,Alok+Shrivastava&source=bl&ots=v-d21WWCoM&sig=aScvEUb3bj7t49kU7oJmPDMoabo&hl=pt-BR&sa=X&ved=0ahUKEwjugIWU5fPWAhVBhZAKHWV9CWcQ6AEIOzAE#v=onepage&q=*Backup*&f=false>. Acesso em: 04 set. 2017.
SPAIOL, Bruna. **Como o 11/9 Mudou a trajetória da proteção de dados.** Aliança Tecnologia da Informação, Natal/RN, 11 setembro 2015. Disponível em: <http://www.aliancatecnologia.com/conteudo/2015/09/como-o-119-mudou-a-protecao-de-dados/>. Acesso em: 9 ago. 2018.

VERITAS TECHNOLOGIES LLC. **Veritas Backup Exec**. Califórnia/Estado Unidos. Disponível em: < https://www.veritas.com/content/dam/Veritas/docs/data-sheets/backup_exec_data_sheet.pdf>. Acesso em: 19 ago. 2018.

VICK, Thais Elaine; NAGANO, Marcelo Seido. **Processos dependentes de informação em empresas incubadas e graduadas de base tecnológica:** um estudo comparativo de casos. Perspectivas em Ciência da Informação, v. 17, n. 3, p. 67-81, 2012. Disponível em: <http://www.brapci.inf.br/v/a/12721>. Acesso em: 04 set. 2018.

Western Digital Suport. **Como lidar apropriadamente com discos rígidos da Western Digital**. San José/Estados Unidos. Disponível em: <https://support.wdc.com/knowledgebase/answer.aspx?ID=4479&lang=bp>. Acesso em 16 ago. 2018.