CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
CAMPUS TIMÓTEO

Guilherme Augusto Biagio Spadotto

SEGURANÇA EM REDE: ESTUDO E ANÁLISE PARA UM PROCEDIMENTO SEGURO EM UM AMBIENTE CLIENTE/SERVIDOR

Timóteo

2017

Guilherme Augusto Biagio Spadotto

SEGURANÇA EM REDE: ESTUDO E ANÁLISE PARA UM PROCEDIMENTO SEGURO EM UM AMBIENTE CLIENTE/SERVIDOR

Monografia apresentada à Coordenação de Engenharia de Computação do Campus Timóteo do Centro Federal de Educação Tecnológica de Minas Gerais para obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Prof. Me. Adilson Mendes Ricardo

Timóteo

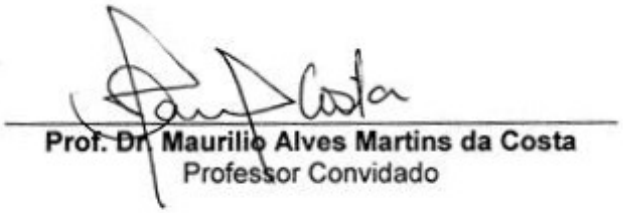
2017

Guilherme Augusto Biagio Spadotto

SEGURANÇA EM REDE: ESTUDO E ANÁLISE PARA UM PROCEDIMENTO SEGURO EM UM AMBIENTE CLIENTE/SERVIDOR

Monografia apresentada à Coordenação de Engenharia de Computação do Campus Timóteo do Centro Federal de Educação Tecnológica de Minas Gerais para obtenção do grau de Bacharel em Engenharia de Computação.

Prof. Me. Adilson Mendes Ricardo
Orientador



Prof. Dr. Maurilio Alves Martins da Costa
Professor Convidado

Prof. Me. Odilon Corrêa da Silva
Professor Convidado

Timóteo
2017

Dedico esse trabalho à minha família
por todo apoio e incentivo.

Agradecimentos

Agradeço primeiramente a minha família, que é o que tenho de mais valioso e minha base para a vida. Meu pai Cláudio e minha mãe Marinizia pelo apoio, carinho, incentivo e a consciência da importância dos estudos, minha irmão Mayara, minha companheira Jordana, uma pessoa especial e sem igual. Agradeço também aos meus avós, tios, primos e padrinhos pelo incentivo mesmo que distante. Aos meus amigos que sempre caminharam junto comigo, os vários colegas que fiz durante a graduação que também almejavam a formação e os amigos de estágio que contribuíram imensamente.

Agradeço ao CEFET, a todos os professores que dê alguma forma conseguiram passar algo valioso que levarei para toda a vida, o conhecimento. Agradeço também a equipe administrativa e os demais funcionários por proporcionarem um ambiente agradável e propício para o meu crescimento pessoal e intelectual.

Agradeço em especial ao professor Adilson Mendes Ricardo que foi de extrema importância para o desenvolvimento deste trabalho, contribuindo não só com seus inestimáveis conhecimentos mas também com todo incentivo necessário para alcançar o objetivo final.

Agradeço principalmente a Deus que me guiou, capacitou, abençoou e colocou todas essas pessoas incríveis no meu caminho. Que ele continue me guiando por toda minha vida.

“A imaginação é mais importante que a ciência, porque a ciência é limitada, ao passo que a imaginação abrange o mundo inteiro”.

Albert Einstein

Resumo

O MASC (Método Alternativo de Segurança Corporativa) foi um método criado com o objetivo de reduzir as vulnerabilidades nas quais um sistema está exposto, independentemente dessas ameaças serem por códigos maliciosos ou por engenharia social, consistindo em alguns procedimentos e configurações que devem ser executados que culminarão em um aditivo extra de segurança. Para tal, foram levantadas situações que corriqueiramente ocorrem nas corporações e representam riscos para a mesma e, posteriormente, proposto estratégias para diminuir, ou se possível, eliminar essas ameaças. Foi simulado um ambiente cliente/servidor próximo aos dessas instituições e realizadas algumas baterias de testes comparativos entre um servidor com as configurações padrões e um outro caracterizado de acordo com o método MASC, e os resultados demonstraram que o método proposto no trabalho gera sim um aditivo na segurança da informação de quem o aplica.

Palavras-chave: Riscos. Segurança. Servidor. Proteção.

Abstract

MASC (Alternative Enterprise Security Method) was a method designed to decrease the vulnerabilities to which a system is exposed, regardless of whether these threats are malicious code or social engineering, consisting of some procedures and configurations that must be performed an additional safety element. To this end, situations that occur in corporations and pose risks to them have been raised and, subsequently, strategies have been proposed to reduce or, if possible, eliminate these threats. A client/server environment was simulated next to these institutions and some comparative test batteries were carried out between a server with the standard configurations and another one characterized according to the MASC method, and the results demonstrated that the method proposed in the work generates an increase in the security level of the information of those who apply it.

Keywords: Risks. Security. Server. Protection.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ENIAC - *Electronic Numerical Integrator and Computer*
ARPA - *Advanced Research Projects Agency*
ARPANET - *Advanced Research Projects Agency Network*
ONU - Organização das Nações Unidas
TI – Tecnologia da Informação
DDOS - *Distribuited Deny of Service*
DMZ – *Demilitarized Zone*
IDS - *Intrusion Detection System*
SGSI – Sistema de Gestão de Segurança da Informação
PSI - Política de Segurança da Informação
ACL – *Access Control List*
IP - *Internet Protocol*
IPv4 -*Internet Protocol Version*4
RFID – *Radio Frequency Identification*
RF – *Radio Frequency*
CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
MASC – Método Alternativo de Segurança Corporativa
NBR – Norma Brasileira
ISO – *International Organization of Standardization*
IEC - *International Electrotechnical Commission*
ABNT – Associação Brasileira de Normas e Técnicas
DNS - *Domain Name System*
USB - *Universal Serial Bus*
AES - *Advanced Encryption Standard*
HD – *Hard Disk*
AGDLP - *Acount, Global, Domain Local, Permission*
RAID - *Redundant Array of Independent Disks*
BIOS - *Basic Input/Output System*
FTP - *File Transfer Protocol*
HTTP – *HyperText Transfer Protocol*
NT - *New Technology*
UAL – *User Access Logging*

Sumário

1 Introdução

O computador é uma máquina capaz de efetuar cálculos em grandes escalas, processar enormes quantidades de dados, grande armazenamento de informações, tratamento de vídeos e imagens, realidade virtual e também utilizado para assistir filmes, jogar, escutar músicas, realizar videoconferência, estudos, pesquisas entre outras utilizações. Porém, essa máquina na qual usufruímos de inúmeros recursos, não possui propriamente um inventor, sendo o resultado de uma evolução ao longo da história.

Charles Babbage produziu o primeiro conceito de uma máquina programável, fazendo uso para isso apenas de partes mecânicas, denominada *Difference Engine*, o também inglês Alan Turing é reconhecido por seu pioneirismo na programação lógica, sendo o criador da Máquina de Turing, invento essencial para a computação que conhecemos atualmente (FILHO, 2007).

O computador é o resultado do progresso de outras máquinas tais como o Ábaco, a calculadora e o ENIAC (*Electronic Numerical Integrator and Computer*), que foi o primeiro computador digital eletrônico programável e pesava cerca de 30 toneladas, ocupando um espaço de aproximadamente 180m^2. Seu processo evolutivo é tão significante quanto à importância que este possui para a sociedade atualmente, principalmente após a criação da Internet (FILHO, 2007).

A rede mundial de computadores, conhecida como Internet, em seu início era bem particular. Criada em meados de 1960 pela ARPA (*Advanced Research Projects Agency*), órgão do governo americano responsável pelos avanços tecnológicos dos Estados Unidos e batizada de ARPANET (*Advanced Research Projects Agency Network*), em seu início o acesso à rede só era permitido aos militares do governo norte americano. O projeto tinha como único objetivo a proteção da comunicação dos Estados Unidos, pois o país encontrava-se em meio a Guerra Fria e a ARPANET era a forma mais eficaz e ágil de comunicação em meio aos conflitos. Posteriormente essa tecnologia chegou às universidades, o que possibilitou o desenvolvimento de novos *hardwares*, *softwares* e protocolos e contribuiu muito para a popularização da rede, que nos anos seguintes alcançou o ambiente corporativo e mais adiante os lares das pessoas, passando a ser chamada de Internet (FILHO, 2007).

Com o passar dos anos, porém, para ter acesso e essa rede, não era mais preciso apenas estar no ambiente de trabalho, universitário ou doméstico. Com o surgimento dos dispositivos móveis, tais como celulares, *tablets*, *notebooks* juntamente com a Internet móvel e *wi-fi*, o utilizador ganhou em ergonomia e facilidade de ingresso. Com essa praticidade, o número de usuários com acesso à Internet subiu radicalmente, segundo o relatório da ONU (Organizações das Nações Unidas) de 2014, quase 3 bilhões de pessoas, cerca de 40% da população mundial, usufruem do serviço.

Com essa quantidade de usuários é esperado que a quantidade de dados que trafeguem na rede sejam descomunais, segundo a companhia *Cisco Systems*, de acordo com um

relatório da empresa em 2011, chegaria a incríveis 966 *exabytes* no ano de 2015, com uma tendência de crescimento para os anos seguintes.

Com tanta troca de informações é natural que surjam preocupações quanto à segurança dos dados, já que uma falha nesse quesito pode acarretar em fracassos, por exemplo, se houver planos confidenciais, perdas financeiras e danos morais. Segurança é proteger as informações, sistemas, recursos e serviços contra erros, manipulação não autorizada e desastres para garantir a redução do impacto e diminuir a probabilidade de incidentes de segurança (DIAS, 2000).

Com o intuito de proteger esses dados, temos o conceito de segurança da informação, uma área da TI (Tecnologia da Informação) que visa à proteção dos dados das organizações e dos indivíduos. A segurança da informação nas grandes empresas adquiriu importância prioritária, sendo peça chave para as decisões e investimentos no mercado. Segundo Fontes (2006), a segurança da informação possui três pilares como alicerces:

- Confidencialidade
- Integridade
- Disponibilidade

Já Forouzan (2006) além de considerar os três conceitos como pilares, ele ainda acrescenta a autenticação e o não repúdio como medidas de segurança aplicadas à informação.

O uso de alguns *softwares*, em conjunto com algumas técnicas podem deixar seu computador seguro e seus dados protegidos e é isto que buscamos mostrar ao longo desse trabalho. A elaboração de um procedimento seguro, o qual minimize a exposição do computador aos perigos da rede é o nosso intuito. Para isso é necessário conhecer o conceito de segurança da informação, os riscos oferecidos pela Internet, como os invasores se comportam para usufruir das vulnerabilidades do sistema, entender as ferramentas que contribuem para a proteção e validar mecanismos que possibilitem a montagem de uma rede considerada segura, seguindo os procedimentos operacionais estudados e propostos.

1.1 Objetivos

1.1.1 Objetivo Geral

Desenvolvimento de um procedimento operacional para avaliação da segurança em uma rede, envolvendo os mecanismos de proteção no acesso à mesma e políticas de acesso a recursos dos servidores.

1.1.2 Objetivo Específico

Tendo como intuito a segurança da informação, este trabalho tem como propósito o desenvolvimento de um procedimento operacional capaz de qualificar a confiança em uma rede de computadores. Para que isso se realize, teremos como meta estudar as disciplinas da

segurança da informação e verificar suas implicações em um ambiente corporativo; estudar, instalar e configurar um sistema operacional servidor de rede para identificar procedimentos que o tornem seguro para um ambiente corporativo.

1.2 Motivação

Com as ameaças existentes atualmente, em se tratando de Internet, é necessário um procedimento operacional no qual diminua a exposição dos computadores, principalmente os servidores, aos riscos e aumente a segurança das informações armazenadas, enviadas e recebidas.

1.3 Organização do Trabalho

O presente trabalho está organizado em 6 capítulos. O segundo capítulo nos coloca a par dos conceitos, pesquisas e técnicas utilizadas para a elaboração deste projeto.

O terceiro capítulo relaciona trabalhos desenvolvidos na área e o estágio em que se encontram.

O objeto do quarto capítulo é informar sobre os métodos e ferramentas utilizadas.

No quinto capítulo é realizado a implementação do ambiente e analisado os resultados.

Por fim, no sexto capitulo é feita a conclusão dos testes, o significado que este representa para o trabalho e expostas algumas idéias de futuros trabalhos.

2 Fundamentação Teórica

A informação é um ativo, que como qualquer outro, é de grande valia para os negócios de corporações, empresas e outras organizações, sendo assim necessitam de proteção adequada. É necessário lembrar que a informação pode existir de diversas formas, armazenada eletronicamente, impressa, transmitida por meios físicos ou eletrônicos, falada, entre outros. Seja a forma que for, sabemos que é recomendável que ela esteja sempre protegida (ABNT, 2005).

A seguir serão apresentados alguns conceitos que são a base para o desenvolvimento do presente trabalho.

2.1 Segurança da Informação

A segurança da informação é a prática de garantir que os recursos gerem, armazenem ou proliferem informações e estas sejam protegidas contra a quebra de confidencialidade, comprometimento da integridade e contra a indisponibilidade que asseguram acesso aos recursos. Independente de qual seja o plano de segurança da informação, esse deverá cobrir os conceitos de: confidencialidade, integridade e disponibilidade (DIOGENES; MAUSER, 2013).

- **Confidencialidade:** Refere-se à precaução do vazamento da informação para usuários ou sistemas que não estão autorizados a ter acesso a tal informação.
- **Integridade:** Refere-se à preservação/manutenção dos dados na sua forma original, ou seja, sem sofrer modificações através de fontes ou usuários não autorizados.
- **Disponibilidade:** Refere-se à manutenção da disponibilidade da informação, ou seja, a informação precisa estar disponível quando se necessita.

Além dos três conceitos supracitados, ainda inclui como base da segurança da informação a autenticação e o não repúdio como medidas necessárias (FOROUZAN, 2006).

- **Autenticação:** É um serviço que vai além da integridade da mensagem: o receptor precisa estar certo da identidade do emissor e que um impostor não enviou a mensagem.
- **Não repúdio:** Significa que um emissor não deve ser capaz de rejeitar uma mensagem que ele, de fato, enviou. O ônus da prova recai sobre o receptor.

2.2 Política de segurança da informação

A PSI (Política de Segurança da Informação) é um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando

mudanças se fizerem necessárias. É o SGSI (Sistema de Gestão de Segurança da Informação) que vai garantir a viabilidade e o uso dos ativos somente por pessoas autorizadas e que realmente necessitam delas para realizar suas funções dentro da empresa (FONTES, 2006).

É importante salientar que ao elaborar uma PSI deve-se levar em conta a NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação para empresas e organizações, contendo informações sobre a implementação da rede, a seleção e o gerenciamento de controles, sempre com o objetivo de minimizar os riscos aos quais o ambiente está exposto (ABNT, 2013).

A NBR (Norma Brasileira) é a sigla para a norma aprovada pela ABNT (Associação Brasileira de Normas e Técnicas). Geralmente são normas técnicas aprovadas de acordo com um consenso entre pesquisadores e profissionais da área. Para a norma atingir um alcance internacional, ela precisa ser publicada pela ISO (*International Organization of Standardization*). Caso seja uma norma relacionada a tecnologias elétricas e eletrônicas, deve ser publicada pela IEC (*International Electrotechnical Commission*).

2.3 Vulnerabilidades

Os invasores fazem uso das vulnerabilidades presentes no sistema para alcançarem seus objetivos e, conseqüentemente, deixar o computador em risco. De acordo com Araujo (2005), elas assim são definidas:

- **Naturais:** Computadores que guardam as informações importantes são susceptíveis a desastres naturais, acúmulo de poeira nos barramentos de comunicação da placa-mãe que pode causar falhas nos sistemas;
- **Físicas:** Instalações prediais fora do padrão; riscos de explosões ou incêndios; controle de acesso precário às instalações;
- ***Software:*** Possíveis erros na configuração ou na própria instalação podem acarretas acessos indevidos;
- **Humanas:** As ações humanas também podem acarretar certas vulnerabilidades, como a falta de treinamento em segurança que faz com que muitos funcionários sejam alvos em potencial ataque de engenharia social. Outros exemplos também podem ser observados, como sabotagens, vandalismo e roubo.

2.3.1 Engenharia Social

Técnica que se aproveita da inocência, desatenção ou desconhecimento do usuário. O objetivo da engenharia social é similar aos de outras técnicas de um grupo específico de usuários denominados *crackers*. Estes possuem vasto conhecimento em informática, assim como os *hackers*, porém, agem para prejudicar financeiramente alguém ou em benefício próprio, sendo considerados criminosos cibernéticos (DUMONT, 2006)

A engenharia social pode ser considerada um tipo de ataque *hacker*, no qual o instrumento utilizado é a habilidade de lidar com pessoas persuadindo-as a fazer coisas de interesse dos *crackers*. Estes ataques podem ser feitos por sala de bate-papo, espaço que reúne virtualmente as pessoas para conversarem e trocarem fotos, telefone, e-mails falsos, cujo o emissor pode ser desconhecido ou a mensagem incluir conteúdo suspeito ou até mesmo pessoalmente (SARAIVA, 2012)

2.3.2 Códigos Maliciosos

Conhecidos também por *malware* incluem vários tipos de códigos maliciosos e representam o mais alto risco dentre as vulnerabilidades, resultado de sua fácil disseminação e o poder de estrago que possuem. Dentre os vários tipos, Diogenes e Mauser (2013) os classificam assim:

- **Vírus:** O vírus computacional é um programa que é secretamente anexado ao computador da vítima através de um ‘’transportador”, que neste caso pode ser um documento ou programa qualquer. Quando estes são iniciados, o vírus entra em execução. Este tipo de código malicioso possui alta capacidade de replicação, procurando meios para infectar, tais como outros arquivos, documentos e até mesmo computadores.

- **Cavalo de Tróia:** Também conhecidos por *trojan*, são programas que entram no sistema escondidos junto com outros programas. O usuário recebe o programa imaginando que este é designado para uma determinada função, mas na realidade ele carrega outras instruções maliciosas. Daí a analogia à lenda grega associada à tomada de Tróia pela Grécia, onde um cavalo de madeira oco foi ocupado por soldados gregos. Muitas vezes o cavalo de tróia abre uma brecha no sistema para que o autor invada a máquina ou usufrua de informações privadas do usuário.

- ***Worms:*** A segunda maior categoria de *malware* é conhecida como *worm*. Este código malicioso é concebido para tirar vantagem de uma vulnerabilidade em uma aplicação ou sistema operacional para entrar no computador. Uma vez que o *worm* compromete o sistema através da exploração da vulnerabilidade, ele inicia a procura por outro sistema com a mesma vulnerabilidade, ou seja, o *worm* usa a rede para se copiar para outros computadores.

- ***Spyware:*** O *spyware* é um termo geral utilizado para descrever *softwares* que violam a privacidade das informações do usuário. A presença do *spyware* é normalmente escondida do usuário, ou seja, este *software* é secretamente instalado sem consentimento ou conhecimento do usuário. Entretanto, algumas vezes o *spyware* é instalado em computadores compartilhados, com funções de captura de teclado (*keylogging*) para secretamente monitorar as atividades do usuário. A atividade do *spyware* vai além de simplesmente monitorar as atividades do usuário, pois tais programas coletam diversas informações pessoais do usuário, de simples hábitos de navegação, tais como os sites visitados pelo usuário, para mais sofisticadas, como instalar outros *softwares* maliciosos para redirecionar o tráfego de navegação da Internet.

- ***Rootkits:*** É uma forma de *malware* recente e vem se popularizando principalmente por sua efetividade e dificuldade de detecção. O *rootkit* pode fazer praticamente o que quiser devido à forma com que se acopla ao sistema operacional tomando vantagem na realização de tarefas de modo privilegiado. Historicamente, o termo *rootkit* era referenciado como um conjunto de ferramentas recompiladas para sistemas operacionais *Unix*. O *root* é o maior nível de privilégio disponível no sistema *Unix*, sendo *rootkit* o termo usado para que tais programas fossem utilizados pelo usuário malicioso para ganhar privilégios de *root* e ocultar o próprio *software* malicioso.
- ***Botnet:*** É um termo genérico para um conjunto de *softwares* "robotizados", apelidados de *bots*, que são executados automaticamente e de forma anônima. Este termo também é utilizado quando um grupo de computadores, tipicamente vinte ou mais, são comprometidos (chamados computadores zumbis) por um conjunto de *softwares* maliciosos tais como: vírus, cavalos de tróia, *worms* ou *backdoors* – os autores dos ataques fazem isso de forma distribuída com intuito de burlar a identificação da origem dos ataques bem como DDOS (*Distribuited Deny of Service*) desestabilizando serviços de Internet, como os serviços de correios.
- ***Backdoor:*** Este tipo de *malware* tem o objetivo de prover acesso remoto à máquina. Após ser instalado no computador da vítima, este *malware* é capaz de verificar e criar vulnerabilidades internas, permitindo que o *cracker* acesse de forma irrestrita o sistema a qualquer hora.

2.4 A Proteção Lógica da Informação

Após conhecer os invasores e os ataques, é de suma importância conhecer os *softwares* e técnicas que auxiliam na defesa, minimizando as vulnerabilidades dos computadores. Na sequência será apresentada algumas ferramentas que auxiliam na proteção das informações.

2.4.1 *Firewall*

A tradução literal da palavra para o português é "parede de fogo", passando a idéia de isolar as ameaças, tal qual um muro em uma residência, resguardando a segurança interna nas empresas em um ambiente de rede. Um *firewall* é um sistema de segurança que impõe política de controle de acesso entre duas redes, tendo as seguintes propriedades (SARAIVA, 2012).

- Todo tráfego de dentro para fora de uma rede, e vice-versa, deve passar pelo *firewall*.
- Apenas tráfego autorizado, como definido pela política de segurança local, terá permissão de passar.
- O próprio *firewall* deve ser imune a penetrações.

Apenas a instalação de um *firewall* não garante que uma rede esteja segura contra invasores e ataques. Sendo assim, um *firewall* não pode ser a única linha de defesa, ele é

mais um dentre os diversos mecanismos e procedimentos que aumentam a segurança de um sistema. Outra limitação dos *firewalls* é que eles protegem apenas contra-ataques externos ao mesmo, nada podendo fazer contra ataques que partem de dentro do sistema por ele protegido (SARAIVA, 2012).

2.4.2 Antivírus

Podemos prever a sua utilização de acordo com o significado do seu nome. Na etimologia da palavra, antivírus significa “aversão aos vírus”, ou seja, sua função é eliminar os vírus presentes no computador. Ele funciona monitorando todos os arquivos executados no computador e faz uma comparação automática dos códigos presentes nos arquivos com aqueles que compõem a coleção de vacinas, particular a cada antivírus. Caso haja partes parecidas entre eles, o antivírus julga aquele arquivo contaminado e tenta devolver o documento ao seu formato original.

2.4.3 IDS

O IDS (*Intrusion Detection System*) é um sistema que tem como função avaliar e detectar se o sistema sofreu alguma tentativa para explorar a sua vulnerabilidade e, em caso afirmativo, mandar um alerta ao sistema. Qualquer atividade que coloque em risco os pilares da segurança da informação (confiabilidade, disponibilidade e integridade) é considerada como uma tentativa de intrusão e, desse modo, reportada ao sistema (DIOGENES; MAUSER, 2013).

2.4.4 DMZ

DMZ (*Demilitarized Zone*) é a forma clássica de segmentação com objetivos de segurança, também conhecida como rede de perímetro. Ao criar-se um DMZ, deve-se ter como objetivo adicionar uma camada extra de segurança para as redes corporativas, pois se houver uma ameaça de algum agente externo, este será direcionado para os recursos publicados na DMZ ao invés de atacar diretamente a rede local (DIOGENES; MAUSER, 2013).

2.4.5 Senhas

Constituída por uma sequência de caracteres, as senhas, também chamadas de *passwords* possuem o objetivo de restringir o acesso a ambientes e processos, permitindo o ingresso apenas aos usuários que se dispõem das mesmas. Entretanto, os sistemas de autenticação por senha não oferecem um grau de segurança elevado de acordo com Beal (2005), isso porque os usuários não seguem as recomendações da PSI, especialmente por atribuírem palavras de fácil adivinhação para suas senhas. Temos como *passwords* considerados inseguros o nome ou sobrenome do próprio usuário ou de entes queridos pelo mesmo, datas festivas, tais como aniversário, casamento, admissão no serviço. Outras características das senhas ineficazes são sequências de números, como “123456” ou até mesmo sequência do teclado, como “asdfgh”, “qwerty”, entre outras. Também não se recomenda a utilização de palavras do dicionário, pois são as mais utilizadas em ataques de força bruta. No entender

de Saraiva (2012) as senhas devem ser elaboradas com ao menos 8 caracteres, envolvendo letras, números e símbolos, para aumentar a sua complexidade. Também aconselha a usar senhas diferentes para cada serviço, evitando que o atacante, outra denominação dada aos invasores, caso descubra uma senha, tenha acesso a todos os serviços do usuário. E por fim, o autor recomenda alterar a senha com frequência, dificultando assim o trabalho dos invasores.

2.4.6 Criptografia

Originada das palavras gregas *kriptós* (escondido, obscuro, oculto) e *grápho* (escrita, grafia), criptografia é a técnica de segurança na qual há uma codificação do conteúdo e o mesmo só pode ser restaurado ao seu estado original por quem possui a chave criptográfica correta, assegurando assim a integridade da informação. A criptografia é utilizada quando se deseja um alto nível de proteção, pois dependendo da quantidade de *bits* das chaves, a quebra da senha, fazendo uso de ataques por força bruta, pode demorar milhares de ano para ter sucesso (SILVA, 2008). Essa técnica subdivide-se nos seguintes tipos:

2.4.6.1 Criptografia de chave simétrica

Comumente chamada de criptografia de chave única ou secreta, essa técnica consiste em utilizar a mesma chave tanto para codificar como para decodificar os dados, garantindo assim a confidencialidade dos mesmos. Possui uma implementação rápida e fácil e seus algoritmos são menos complexos que os de chaves assimétricas. Segundo Silva (2008), esses algoritmos apresentam como pontos falhos o fato de não permitir a assinatura nem a certificação digital, não contemplando assim o serviço de segurança e não-repúdio, pois a chave simétrica é de conhecimento de mais de uma pessoa.

2.4.6.2 Criptografia de chave assimétrica

Também chamada de criptografia de chave pública, esta técnica faz uso de duas chaves complementares entre si para atingir o objetivo proposto: uma chave pública para cifrar os dados e outra privada para decifrá-los. No entender de Silva (2008) ao contrário dos algoritmos de chave simétrica, possui uma implementação bem mais demorada e algoritmos complexos, sendo assim, são cerca de 60 a 70 vezes mais lentos e necessitam de maior poder de processamento para a sua execução, porém possuem como maior vantagem um nível bem mais alto de segurança, quando comparados aos de chave secreta.

2.4.7 *Backup*

A cada dia que passa, os serviços de *backups* vêm se tornando essenciais para as corporações, pois são eles os responsáveis por restaurar posteriormente aquilo que já foi desenvolvido em caso de catástrofes, tragédias ou incidentes que possam vir a acontecer. Os *backups* funcionam armazenando cópias e segundo Borba (2014) podem ser efetuados de duas formas:

- **Frio:** O sistema precisa ficar *off-line*, sem a intervenção de qualquer usuário para que a cópia de dados seja efetuada com sucesso.
- **Quente:** Nessa forma de *backup*, o sistema pode permanecer ativo enquanto ocorre a cópia dos dados.

Além das formas como são feitas as cópias de segurança, Borba (2014) informa também que os *backups* se diferem pelo seu tipo e no meio corporativo geralmente apenas os quatro a seguir que são utilizados:

2.4.7.1 *Backup Full*

Também conhecido como *backup* completo, é uma cópia completa de todos os arquivos do sistema e costuma ser o primeiro *backup* realizado justamente por ser mais amplo, sendo o *backup* inicial de todos os arquivos e dados no sistema. Devido a sua complexidade e totalidade, exige mais disco e banda para ser efetuado. Outra característica deste tipo é que também marca os arquivos que passaram por *backup*, o que é importante para o controle (BORBA, 2014).

2.4.7.2 *Backup* Incremental

Este tipo de *backup* cópia apenas os arquivos que sofreram alteração ou foram criados após o último *backup* completo ou incremental. Por copiar apenas arquivos modificados ou novos, este tipo de cópia de segurança é a mais rápida e a que mais economiza a banda do sistema, porém para recuperar os arquivos é necessário combinar o *backup* completo e todos os *backups* incrementais, o que pode demandar um bom tempo. Este tipo também marca os arquivos que passaram por *backup* (BORBA, 2014).

2.4.7.3 *Backup* Diferencial

Este tipo de *backup* funciona de forma parecida com o Incremental, copiando apenas os arquivos que sofreram alteração desde o último *backup* completo ou os arquivos novos que foram criados. Diferentemente do Incremental, não marca os arquivos que passaram por *backup*. É necessário a combinação com o *backup* completo para a recuperação dos arquivos, o que pode tornar o processo um quanto custoso e demorado (BORBA, 2014).

2.4.7.4 *Backup* Diário

Este tipo de *backup* copia todos os arquivos selecionados que foram modificados no dia da execução do *backup* diário. Nesta categoria os arquivos não são marcados como arquivos que passaram por *backup* (BORBA, 2014).

2.5 Sistemas de Proteção ao Acesso Físico

A segurança lógica da informação é de extrema importância, principalmente considerando um ambiente cada vez mais conectado à rede mundial de computadores e os riscos que

isto pode acarretar a um sistema. Porém, a proteção ao acesso físico não pode e nem deve ser deixada de lado, tendo em conta as tecnologias existentes que auxiliam no resguardo do ambiente. De acordo com Galhardo (2011), esse controle de acesso pode ser compreendido como uma atividade que controla a circulação de pessoas ou veículos à uma determinada instituição fazendo uso de barreiras físicas que dificultem ou retardem e controlem toda a movimentação. Temos como sistemas de proteção que se adequam a esse conceito:

2.5.1 Câmeras de Monitoramento

Dispositivos para a captura de imagens e gravação de vídeos, capaz de guardar momentos e identificar equipamentos presentes no local e pessoas com acesso ao mesmo. A filmagem costuma ser armazenada por 30 dias em uma central, podendo esse tempo ser postergado de acordo com as necessidades do cliente. Atualmente os dispositivos mais usados de acordo com Segurança (2017) são:

- **Infravermelho:** Característica presente em algumas câmeras, permite a obtenção de imagens mesmo em ambientes sem iluminação, graças aos *leds* emissores de sinais infravermelho presente no equipamento, que acendem quando o sensor capta ausência mínima de luminosidade.
- **IP:** Esta tecnologia tem ganhado cada vez mais adeptos pelo fato de possibilitar o envio das imagens diretamente para a Internet, graças a um servidor interno presente na câmera, possibilitando assim assisti-las em tempo real.
- **Alta Capacidade de Resolução:** Relacionada a capacidade de fragmentação da imagem, quanto maior a resolução mais nítida a imagem e, consequentemente, mais caro o equipamento. Atualmente a maior resolução presente em câmeras de segurança é a de 4K, também conhecida como ultra HD, que garante imagens de 3840 x 2160 pixels.
- **Camêra *Bullet*:** Considerada a câmera mais utilizada do mercado, possui esse nome por causa de seu formato. Caracterizadas pelo seu tamanho pequeno, são indicadas para ambientes externos e pequenos, gravando a movimentação nos arredores de onde se encontra instalada.
- **Camêra *Dome*:** Câmeras bastantes utilizadas no mercado, possui esse nome por terem a forma de um dome. Indicadas para ambientes internos, apesar de já haver modelos com vedação apropriada para poeira e chuva, deve-se ser instalada preferencialmente no teto, para facilitar a mudança de direção da lente.
- **Mini Camêra:** De dimensões reduzidas, essa categoria de câmera é indicada quando não há espaço suficiente para o funcionamento de câmeras maiores, quando precisa de objetos pequenos ou nas vezes em que se deseja discrição. Possuem como vantagem a possibilidade de serem instaladas em qualquer lugar, porém possuem baixa resolução.
- **Camêra *Speed Dome*:** Considerada as câmeras mais completas e caras, essa categoria é comumente encontrada em locais públicos, tais como aeroportos, estádios, *shoppings*

e centros comerciais, por possuírem grande capacidade de resolução, movimentação da mesma e a possibilidade de dar *zoom* a qualquer hora.

2.5.2 Dispositivos de Bloqueio

De acordo com Galhardo (2011), esses dispositivos podem ser definidos como barreiras físicas utilizadas para segregar as áreas controladas das de uso comum. Se enquadram nesta categoria os seguintes dispositivos de bloqueio:

2.5.2.1 Portas, Portões e Portais

São as mais utilizadas por necessitarem de menor investimento e treinamento, sendo a porta utilizada internamente na corporação e os portões e portais tendo um uso externo. Segundo Galhardo (2011), para que uma porta funcione em um sistema de controle de acesso é necessário apenas uma pequena modificação na mesma, substituindo a fechadura existente por uma outra eletromagnética, aumentando assim sua segurança.

2.5.2.2 Cancelas Automáticas

Utilizadas principalmente em condomínios, *shoppings*, mercados e outros estabelecimentos que há grande fluxo de automóveis, as cancelas são a melhor escolha para gerir o controle de acesso em estacionamentos de empresas, pois consegue a liberação do fluxo de forma mais rápida que os portões por exemplo.

2.5.2.3 Catracas Eletrônicas

Diferentemente do foco das cancelas automáticas que são veículos, as catracas eletrônicas já são direcionadas ao controle do fluxo de pessoas. Geralmente são instalados em portarias e recepções afim de já restringir o acesso de pessoas no início. Galhardo (2011) cita que a maior vantagem das catracas eletrônicas é que por ter um controle de acesso giratório, permite a passagem de apenas uma pessoa por vez, evitando que pessoas não autorizadas tirem vantagem para adentrar junto de alguém habilitado.

2.5.3 Identificação

Controlar o acesso físico da sala onde se encontra os servidores e cópias de *backups* é de extrema importância e segurança, restringindo a circulação de pessoas para um menor número e apenas pessoas autorizadas, impedindo que pessoas sem conhecimento e/ou que possam colocar em risco a segurança dos dados e informações adentrem ao local. Esse controle pode ser feito de várias formas, desde as mais simples e usuais, até maneiras tecnológicas que oferecem menor risco, porém necessitam de um maior investimento. Dentre as tecnologias citadas por Galhardo (2011) destacam-se:

2.5.3.1 Crachás

É a forma de identificação mais presente em empresas, escolas e universidades pois sua implantação é de baixo custo quando comparada as outras formas de reconhecimento

do usuário. Não oferece um nível de segurança alto pois geralmente é composto apenas pelo nome da pessoa, uma foto e a função do mesmo na instituição, o que pode ser facilmente burlado.

2.5.3.2 Cartões

Bastante utilizado, de acordo com Galhardo (2011) os cartões podem ser de contato ou proximidade, para leitura de códigos de barra ou tarjas magnéticas, sendo que os dois últimos caíram em desuso nos últimos anos pois eram fáceis de serem clonados. Os cartões de proximidade utilizam um protocolo de codificação em cartões de 26 ou 32 *bits*, o que torna praticamente impossível a cópia desses dispositivos. São considerados seguros a não ser que por perda, roubo, furto ou extravio sejam usados por pessoas não autorizadas.

2.5.3.3 Teclados

Esse sistema requer a digitação de uma senha de acesso por parte do usuário para que o dispositivo de bloqueio seja liberado. Não possui um grau elevado de segurança pois, caso o indivíduo divulgue sua senha, qualquer pessoa de posse da mesma conseguirá acesso as áreas restritas nas quais o teclado ajuda a limitar o acesso.

2.5.3.4 Biometria

Oriunda das palavras *bio* (vida) e *metria* (medida), segundo Galhardo (2011) é o estudo estatístico das características físicas ou comportamentais dos seres vivos. Também é uma forma única de identificação do ser humano, já que cada um apresenta traços exclusivos que o diferem de todos os demais. Por essa razão a biometria cada vez mais vem sendo usada, devido ao seu alto grau de confiabilidade, exatidão e segurança apresentada. Essa técnica funciona com um *software* responsável por recolher as informações e imagens necessárias, de acordo com a biometria desejada, para em sequência comparar com os dados armazenados em seu banco de dados, verificando se trata de uma pessoa conhecida e autorizada a acessar áreas e informações privadas. Para ter acesso aos dados biométricos das pessoas existem vários sistemas, sendo que os principais são:

2.5.3.4.1 Impressões Digitais

O modelo de biometria mais utilizado, presente em bancos que possuem o sistema de segurança como referência, a biometria por impressão digital utilizar um dispositivo óptico com um sensor de impressão digital que digitaliza o dedo do usuário e captura imagens 3D do mesmo para uma análise posterior com o banco de dados (GALHARDO, 2011).

2.5.3.4.2 Geometria das Mãos

Método em que faz o reconhecimento das características das mãos do usuário, através da análise de uma imagem 3D das mesmas. São avaliados o comprimento, a largura dos dedos, área da mão e, tomando como base que nenhuma pessoa possui a geometria da

mão similar à de outra, as imagens são analisadas por *scanners* e apontam o responsável pelo palmo. O usuário não pode portar anéis durante o processo de reconhecimento (SILVA; FILHO, 2011).

2.5.3.4.3 Leitura da Retina ou Íris

Sistema biométrico de alto custo e praticamente isento de erros, a leitura de retina consiste em uma análise dos vasos sanguíneo do globo ocular do usuário para emitir um parecer. O mapeamento da íris funciona de forma parecida, porém como o próprio nome já diz, o foco é analisar a vizinhança da pupila para chegar a uma conclusão. Esses equipamentos para manter o alto grau de precisão, necessitam ser constantemente higienizados, pois qualquer cisco ou poeira pode vir a impossibilitar o seu diagnóstico (SILVA; FILHO, 2011).

2.5.3.4.4 Identificação da Face

Essa técnica, de acordo com Galhardo (2011) faz uma leitura dos pontos delimitadores da face para identificação de tamanhos, proporções, formas e distâncias para conseguir êxito no reconhecimento da imagem do rosto do usuário, mesmo que este tenha alterado o cabelo, sobrancelhas, barba e bigode. Essa tecnologia possui como fraqueza a análise de irmãos gêmeos idênticos, associando na maioria das vezes a mesma pessoa para identificações diferentes.

2.5.3.4.5 Reconhecimento de Voz

Essa técnica consiste em capturar uma palavra ou uma pequena frase e na sequência, auxiliado por um conversor analógico-digital, digitalizar a fala que se quer reconhecer para obter o domínio espectral, separando a frase original em pequenas sílabas, fazendo uso da análise de Fourier para isso. O *software* na sequencia compara com seu banco de dados e informa o usuário, porém, apesar da tecnologia embutida nessa técnica de biometria, ela pode ser facilmente burlada, por exemplo, com o uso de gravadores (SILVA; FILHO, 2011).

2.5.3.4.6 Reconhecimento de Caligrafia

Essa técnica consiste na análise da assinatura do usuário, identificando a forma como a pessoa escreve e na sequencia reconhecendo o autor. Porém esse método pode ser facilmente burlado e em consequência disto surgiram variações que não analisam apenas a forma da assinatura, mas sim o tempo que se leva para fazê-la, a aceleração e velocidade da escrita, a pressão exercida na superfície, a angulação, o número de vezes em que se levanta a caneta, entre outros, que tornam esse processo de biometria bastante seguro e confiável. Após toda essa análise, o *software* indica o autor da assinatura e permite ou não o seu acesso ao ambiente (GALHARDO, 2011).

2.5.3.5 RFID

É uma tecnologia que utiliza a frequência de rádio para capturar dados, sendo utilizada para rastrear, identificar e gerenciar documentos, produtos e até pessoas, sem a necessidade de contato físico ou visual. Isso é possível pelo fato do RFID (*Radio Frequency Identification*) ser composto por uma antena, um transceptor responsável pela leitura e transpasse dos dados e uma etiqueta de RF (*Radio Frequency*) que irá conter as informações. Essa tecnologia tem se mostrado muito eficaz para proteção de ativos, por não haver a necessidade de um contato com o mesmo, sendo excelente para rastreá-los, podendo ser usado em servidores, mídias de *backups* físicas e outros materiais, com o objetivo de garantir a segurança dos mesmos. Em contrapartida desses benefícios, o RFID apresenta como empecilhos o alto preço para implantar o sistema, já que é necessário o uso de outros equipamentos com a tecnologia, o que eleva em muito o investimento e a curta vida da bateria presente nas etiquetas de RF, que demanda uma reposição em pouco tempo, ocasionando em transtornos ao invés de comodidade (GALHARDO, 2011).

2.6 Auditoria de Segurança de Sistemas

Após a implantação de proteção ao acesso físico e lógico nos sistemas é de suma importância a auditoria de segurança, pois é ela que vai averiguar se as informações presentes atendem aos requisitos de segurança da informação, que são confiabilidade, disponibilidade e integridade e também se os controles internos foram implementados corretamente. Essa etapa do projeto tem como objetivo fazer avaliações e possíveis recomendações nos sistemas de informações da empresa, comprovando por exemplo a efetividade da rede e de seus periféricos, afim de garantir uma segurança física e logica da corporação (GARCIA, 2004).

A auditoria de segurança de sistemas consiste nas etapas de planejamento, na qual é feito um reconhecimento do ambiente e são determinados quais serão os pontos de controle e o critério de análise de risco que será utilizado. A etapa seguinte feita pelos profissionais especializados é a auditoria propriamente dita. Na sequência é feita uma documentação do trabalho realizado e exposto a conclusão do serviço feito, diagnosticando o estado em que se encontram os pontos de controles e suas fraquezas, caso possuam. Por fim, caso o sistema apresente deficiências, o que é natural em uma primeira implantação, é realizado o acompanhamento dos pontos com debilidades, verifica-se se o problema foi resolvido, identifica-se medidas cautelosas para que a falha não volte a ocorrer e gera-se um certificado dos pontos de controle auditados. A auditoria de segurança de sistemas implica um gasto para as empresas contratantes, porém isto pode ser encarado como um investimento perante a qualidade de serviço e maior nível de segurança que estará em vigor na empresa após esta ser auditada (GARCIA, 2004).

3 Trabalhos Relacionados

Há algum tempo que a segurança dos ativos de informação deixou de ser luxo e passou a ser necessidade, possuindo até verbas destinadas em algumas instituições que prezam excessivamente pela segurança dos seus dados. Vários trabalhos que possuem como tema principal a segurança da informação foram desenvolvidos nos últimos anos. Usando o Portal de Periódicos CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) e a ferramenta Google Acadêmico, foram encontradas algumas pesquisas que possuem valia para o presente trabalho, na qual destacamos as seguintes:

O trabalho “Política de integração de segurança e ética na Internet: Perspectivas de uma melhor proteção para as informações” de Silva e Silva (2014) faz um estudo sobre perspectivas em relação à melhora da proteção para as informações, citando quais motivos que levam uma rede a ser atacada, algumas formas de ataques utilizadas pelos invasores e alguns antídotos em relação a isso, mencionando algumas ferramentas de defesa com o objetivo de evitar ataques.

O trabalho “Segurança em redes de computadores uma visão sobre o processo de Pentest” de Cardoso, Menezes e Rocha (2015) destina-se aos testes de vulnerabilidade, falando da importância dos mesmos para identificar falhas na rede antes que um invasor se adiante para essa possibilidade e obtenha sucesso em seu ataque. O trabalho cita também algumas ferramentas disponíveis no mercado, usadas neste tipo de teste, os tipos de ataques que ajudam a dimensionar o nível de segurança empregado na rede em questão.

O trabalho “Information Security: A Case Study. Completion of Course Work. Degree in Computing” de Saraiva (2012) faz uma análise dos perigos existentes causados pelos ataques *hackers*, mostrando as vulnerabilidades que podem ser exploradas e ressaltando a importância que a segurança da informação possui atualmente, principalmente para ambientes corporativos que guardam grandes quantidades de dados para o funcionamento habitual.

4 Materiais e Métodos

Este trabalho propõe um procedimento de segurança a fim de diminuir os riscos aos quais uma rede de computadores está exposta. Partindo desse princípio apresentaremos o MASC (Método Alternativo de Segurança Corporativa), método este que consiste em alguns passos descritos a seguir, escolhidos de acordo com a pesquisa relacionada e as necessidades presentes nas corporações.

4.1 Proteção no Acesso Físico ao Servidor

Como já dito anteriormente, a proteção física do servidor é de extrema importância para se ter um ambiente seguro, e parte desse processo passa pelas pessoas que tem acesso direto ao servidor. Partindo do pressuposto que quanto menos pessoas tenham acesso ao mesmo mais seguro ficará o sistema, o MASC define algumas diretivas:

4.1.1 Estrutura da Sala

O espaço que vai alocar o servidor deve ter capacidade física para acomodar os cabos *ethernet*, os fios e os equipamentos, com folga também para os funcionários que necessitarem acessar a sala para desempenharem suas funções, podendo ser profissionais da empresa ou responsáveis pela manutenção e limpeza do ambiente.

A alocação das maquinas e equipamentos deve ser feita com *racks*, estrutura essa geralmente de ferro ou aço e que são próprias para essa função. Em relação ao chão da sala, emborracha-lo é de grande valia, pois torna o ambiente anti escorregadio, diminuindo a chance de uma queda e também a energia estática do local, já que a borracha é considerada um ótimo isolante.

Outro ponto vital é em relação a temperatura do ambiente, já que devido a transmissão de energia, corrente e por ser um ambiente fechado, acarreta em um aumento da mesma, podendo aquecer os equipamentos e danifica-los. Manter o a ambiente a uma temperatura de 21º com a ajuda de um ar refrigerado é o ideal. Para alimentar todos os aparatos eletroeletrônicos do local, é indispensável *nobreak* para em casos de emergência onde falte energia elétrica

Tabela 1 – Estrutura da Sala

ITEM	**VALOR DEFINIDO**
Máquinas e equipamentos	Sala fechada ou *racks*
Piso	Emborrachado
Temperatura	=>15º e <= 21º
Proteção elétrica	*Nobreak*

4.1.2 Acesso a Sala do Servidor

O acesso a sala do servidor deve ser restrito ao menor número possível de pessoas, evitando um fluxo intenso de indivíduos e, seguindo a premissa que, quanto menos pessoas adentrarem o local, mais seguro estará o servidor. A liberação de acesso ao ambiente deve ser dada apenas as pessoas qualificadas e que tenham necessidade de uso do servidor, seja para checar dados e informações, cadastrar novos usuários ou manutenção. A equipe responsável pela limpeza do local deve passar por um treinamento especifico para que possam perpetrar suas funções sem colocar em risco o funcionamento dos servidores.

As salas sempre devem estar trancadas, mesmo quando houver pessoas em seu interior. Também é preferível uma tranca biométrica, o que aumentaria segurança e eliminaria a possibilidade de cópias da chave e furto da mesma, além de facilitar o registro de acesso. Este tipo de barreira necessita de um alto custo de investimento e não são todas as empresas que podem arcar com isso. A tradicional porta com tranca a chave não oferece a mesma proteção, mas também não pode ser descartada. Implementando uma política de segurança na qual a chave fique em local seguro e o usuário que desejar fazer uso da mesma faça um registro informando nome, data, hora, cargo, motivo e uma rubrica, já é suficiente para ter um controle.

Em relação aos servidores, apenas pessoas capacitadas devem ter poder de opera-los. O MASC informa um máximo de 3 usuários com poder de administrador do sistema, sendo que 2 dos 3 administradores devem ser pessoas físicas e o terceiro administrador pode ser apenas uma conta sem vínculo com quaisquer pessoas, utilizada apenas em eventuais emergências, nas quais nenhum dos outros 2 responsáveis possam executar a função.

Tabela 2 – Acesso a Sala do Servidor

ITEM	**VALOR DEFINIDO**
Acesso a sala de equipamentos	Somente pessoas autorizadas
Pessoas autorizadas	Somente previamente cadastradas
Cadastramento de pessoas autorizadas	Após treinamento
Trancas	Biométrica e/ou a chave
Operação do servidor	Pessoas autorizadas e previamente capacitadas. Quantidade restrita
Conta administrador	Máximo 3 contas, ficando uma de reserva

4.2 Domínio, Árvore e Floresta

Para o gerenciamento dos servidores, o MASC utiliza o sistema desenvolvido pela Microsoft e destinado aos servidores, *Windows Server*. Este sistema operacional possui ferramentas e configurações distintas daquelas encontradas nas versões domésticas, que possibilitam restringir e/ou liberar acessos a recursos, além de um controle completo sobre os usuários do sistema, o que torna mais apropriado para uso em uma rede corporativa.

Uma das ferramentas do *Windows Server* é o *Active Directory*, que é o serviço líder de

gerenciamento de diretórios, graças a sua segurança, seu desempenho e sua disponibilidade. Este *software* possui estruturas que compreendem grande importância para este trabalho, que são as seguintes (MICROSOFT, 2008):

- **Domínio:** Talvez seja a estrutura mais importante relacionada ao *Active Directory*, pois possui como principais funções a limitação administrativa para um objeto, restringindo o que faz parte da rede e o que não faz, impedindo uma migração de lados, sendo também um gerenciador de contas e recursos do *Active Directory*, essencial para exercer esse controle (MICROSOFT, 2008).
- **Árvore:** A árvore surge da necessidade de criação de um novo domínio, que pode ser considerado filho ou raiz do primeiro. Após a criação do mesmo, tendo assim um domínio pai com seus filhos, denomina-se como árvore de domínio, pois poderão dividir o mesmo sufixo DNS (*Domain Name System*), *schema*, relação de confiança, porém em distribuições hierárquicas (MICROSOFT, 2008).
- **Floresta:** Floresta é uma interligação de várias árvores que dividem o mesmo *schema* e configurações partilhadas, representado por um único *Global Catalog*, conectados pelas arvores que fazem parte do conjunto que possuem relação de confiança transitivas. O primeiro domínio de uma floresta é chamado de *Root Domain* e a floresta receberá o nome deste. A floresta poderá também ser formada por apenas um domínio ou estar subdividida em várias árvores (MICROSOFT, 2008).

Tabela 3 – Domínio, Árvore e Floresta

ITEM	**VALOR DEFINIDO**
Active Directory	Para 1 servidor, nova árvore e nova floresta. Para 2 ou mais servidores, associar o segundo em diante como membros de uma floresta existente

4.3 Funções e Responsabilidades dos Usúarios

Em qualquer área profissional os funcionários precisam ter certas funções e assumir responsabilidades afim de exercer sua tarefa sem colocar em risco sua segurança e a da própria empresa. Partindo disso, o MASC deixa claro aos usuários do sistema algumas normas para que possam exercer suas funções sem comprometer o patrimônio físico e virtual da corporação.

O usuário cliente tem como função desempenhar seu trabalho da melhor forma possível, pensando nas consequências de suas ações consigo próprio e para a empresa, sempre colocando a segurança de forma prioritária. O mesmo também é responsável por seu ambiente virtual de trabalho, sendo proibida a instalação de quaisquer *softwares* senão aqueles já presentes na máquina. Caso o mesmo precise de um novo programa deve solicitar ao administrador da rede e o mesmo fará uma análise o pedido e responderá diante da necessidade.

O MASC também alerta para o perigo de usar o computador para carregar *smartphones* e *tablets* através de cabos USB (*Universal Serial Bus*), podendo haver troca de dados que possam vir a comprometer o ambiente virtual, proibindo a conexão de cabos USB nos servidores, permitindo apenas nas outras máquinas.

O administrador além das incumbências e responsabilidades já citadas para o usuário comum, também deve ser idôneo para a sua função, tendo uma atenção ainda maior com o seu *login* e senha de acesso do que os usuários clientes, devido a responsabilidade e poder que seu acesso possui. Lembrando que todos os usuários, tanto cliente quanto administrador, terão senhas individuais.

Tabela 4 – Funções e Responsabilidades dos Usuários

ITEM	**VALOR DEFINIDO**
Usuário administrador	Senha reservada para uso em situação de emergência. Guardar em local de acesso controlado
Usuários com poder de administrador	Somente 1 usuário. Responsabilidade do administrador da rede (até 2 pessoas capacitadas para administração de servidores)
Instalação de softwares e serviços	Usuário com poder de administrador
Conectar cabos USB no servidor	Não permitido. As transfêrencias de arquivos somente por estação cliente e devidamente protegidas por *softwares* antivírus

4.4 Proteção e Uso da Senha do Administrador e Administrador com Privilégio

O administrador deve ter uma atenção redobrada em relação a sua senha, pois o seu acesso ao sistema possibilita várias inserções, modificações, exclusões que, se feito por pessoas não capacitadas ou má intencionadas, pode culminar em um desastre para a corporação.

No MASC cada administrador deve portar apenas a sua senha, não tendo acesso um administrador a senha do outro. Também haverá criação de um usuário com poderes administrativos privilegiados do domínio, que ficará inerte, sendo utilizado apenas para realizações de *backups*, instalação, remoção e atualizações de *softwares*, inserção e exclusão de administradores. A senha desse administrador reserva ficará a cargo de um profissional do setor de TI da corporação, seção esta que elegerá apenas um profissional apto e responsável para execução dos serviços supracitados.

Os profissionais do setor de TI serão compelidos a ter um controle dos dados cadastrais dos clientes, podendo ser feito este controle com a ajuda de *softwares* específicos, planilhas digitais ou em último caso em anotações manuscritas, para que se possa gerar novas senhas, caso as pessoas percam ou esqueçam a sua e também para que possa ativar ou desativar o *login* dos usuários.

Tabela 5 – Uso da Senha do Administrador

ITEM	**VALOR DEFINIDO**
Alterar senhas	Usuário com poder de administrador

4.4.1 Procedimentos Para Uso Controlado da Senha Administrativa

As senhas administrativas devem ser usadas com o intuito de acessar funções do sistema operacional que não são permitidas aos usuários comuns, com a justificativa que um cliente sem ciência de suas ações pode comprometer a segurança da rede, infectando-a ou abrindo brechas no sistema para possíveis ataques e/ou invasões.

As pessoas que possuem a senha administrativa serão beneficiadas em função dos seus cargos e funções dentro da corporação. Entendendo que determinadas tarefas carecem de compartilhamento de arquivos entre setores, modificações em pastas e documentos ou uso de *softwares* exclusivos, o portador da senha deve usar a mesma apenas em prol dos seus afazeres, não sendo permitido em hipótese alguma qualquer tipo de engenharia social, correndo o risco de ter sua conta administrativa suspensa ou cancelada.

4.4.2 Padrão de Criptografia

Imagine um invasor que consigo invadir uma sala passando por diversas barreiras de segurança, tanto física quanto lógica e, por fim, consiga ter acesso ao disco rígido da empresa, onde estão os dados e informações da corporação. Ao tentar acessá-lo o invasor se depara com uma criptografia de 256 *bits*, que combinada com uma senha que misture letras maiúsculas, minúsculas, números e caracteres especiais, levaria milhões de ano para ser quebrada através de algoritmos de força bruta, em caso de sucesso.

Esse é o propósito da criptografia, fazer com que uma informação esteja clara e disponível apenas a membros autorizados e, quando vista por agentes externos, seja apenas um emaranhado de lista desordenada, impossibilitando uma compreensão.

Aproveitando-se dessa técnica de segurança, o MASC utiliza o modelo de criptografia AES 256 (*Advanced Encryption Standard*), modelo este de chave simétrica. Devido ao seu alto grau de segurança e complexidade para pessoas não autorizadas descriptografar tal técnica, MASC faz uso da mesma nas senhas de todos os usuários da corporação, além de empregar o AES 256 em suas mídias físicas, aumentando assim o grau de segurança das senhas e das informações contidas em seus HDs (*Hard Disk*).

Tabela 6 – Criptografia

ITEM	**VALOR DEFINIDO**
Criptografia	AES 256 - Gerenciador de Servidor, Ferramentas, Usuários e computadores do *Active Directory*, Usuários, Conta, Criptografia 256 *bits* Kerberos

4.5 Definição de Políticas Para Cadastro de Usuários

As políticas para cadastro de usuários são de extrema importância, pois pode ser considerada a primeira triagem que a corporação realiza, autorizando ou não as pessoas terem acesso ao sistema e o nível dessa permissão, se será um usuário cliente ou administrador.

O MASC possui como norma para a criação do *login* do usuário o uso do registro do funcionário, pois esse número é único e associado a apenas uma pessoa, o que já resolveria a questão de conflitos de *login*. Também é interessante o uso pois permite uma busca mais rápida e direta no sistema para modificar permissões ou adicionar restrições, caso isso venha a ocorrer.

Em relação a senha do usuário o MASC tem como diretriz um tamanho mínimo de 8 e máximo de 25 caracteres, sendo obrigatório o uso de letras maiúsculas e minúsculas, números e caracteres especiais, já que isso torna a senha mais complexa e consequentemente mais segura. O código de acesso terá que ser atualizado a cada 2 meses, sem a opção de manter a mesma senha ou usar uma outra que já tenha sido utilizada nas ultimas 5 vezes. Por fim, como mais uma ferramenta de proteção ao sistema, cada usuário poderá errar no máximo 3 vezes sua senha, sendo que a partir da 4ª tentativa seu acesso estará bloqueado e o mesmo deverá procurar um administrador para o desbloqueio da conta.

Tabela 7 – Política para Cadastro de Usuários

ITEM	**VALOR DEFINIDO**
Login	Número de registro do funcionário
Senha	Entre 8 e 25 caracteres. Habilitar requisitos de complexidade: Senha contendo letras maiúsculas, minúsculas, números e caracteres especiais
Tempo de senha	Expira em 2 meses. Histórico das últimas 5 senhas não permitido
Tentativas para *logar* no sistema	Máximo de 3 tentativas sem bloquear a senha
Desbloqueio de senha	Somente com a intervenção do administrador

4.6 Definição de Políticas de Grupos de Usuários

As políticas de grupos de usuários são recursos incorporados ao sistema operacional que permitem gerenciar computadores e/ou usuários específicos, afim de definir diretrizes a serem seguidas que possam facilitar a integração dos membros do grupo e principalmente melhorar a eficácia dos mesmos em suas funções. O MASC evidencia que é preciso ter políticas rígidas que não gerem impasses aos membros e assim a taxa de infrações tenda a não existir.

Os usuários cliente de todos os grupos, independente do setor, em consequência das normas em suas políticas, não terão permissão para:

- **Instalação de Programas:** Uma vez que se não for o programa original e licenciado pode acarretar problemas a empresa, tanto no aspecto de segurança quanto em relação a propriedade intelectual.
- **Instalação de *Updates*:** A atualização sem a verificação dos requisitos do sistema pode impossibilitar o uso do *software*, gerando contratempos a empresa.
- **Remoção de Programas:** Pode ser um programa não utilizado por um usuário, mas crucial para outro cliente, por isso a impossibilidade de remoção de *software*.
- **Alteração das Configurações de Rede:** A alteração errada da configuração já existente pode gerar transtornos a corporação e enfraquecer a segurança da mesma.
- **Desativar o Serviço de Impressão:** Pode ser necessário em determinada ocasião, então é importante que esteja ativo.
- **Ocultar Ícones de Aplicação:** É importante todos os programas estarem à vista dos usuários.
- **Bloquear a Barra de Tarefas:** Determinados usuários sabem apenas acessar pastas ou programas a partir dela, por isso fica proibido o bloqueio da mesma.
- **Acessar o *Prompt* de Comando e o Executar:** São comandos que possuem um grande poder no sistema, por isso a opção por bloqueá-los aos usuários cliente.

Essas são as principais normas da política de grupos que o MASC possui, porém nada impede que as empresas incluam novas regras que se adequem mais ao seu perfil, porém as normas supracitadas deverão ser mantidas para a preservação da segurança da informação corporativa.

Tabela 8 – Política de Grupos de Usuários

ITEM	**VALOR DEFINIDO**
Políticas de grupos de usuários	Somente permitido aos administradores

4.7 *Active Directory*

O MASC confia toda a proteção de acesso a diretórios, pastas e arquivos ao *Active Directory*, o serviço de gerenciamento presente no *Windows Server*. É o serviço mais usado para esse propósito por grandes, médias e pequenas corporações e devido ao seu grau elevado de segurança, disponibilidade e confiabilidade também será o serviço de diretório escolhido para gerenciar as redes que utilizarem os métodos presentes no MASC. O *Active Directory* pode ser dividido em três categorias, sendo elas:

- **Recursos Físicos:** Aqui se encontram todos os equipamentos disponíveis na rede, tais como impressoras, computadores, servidores, estações de trabalho, entre outros.

- **Serviços Disponíveis:** Nesta categoria se enquadram os serviços de *email*, de impressão, transferência de arquivos, entre outros.
- **Usuários:** Está relacionada à conta dos usuários, restringindo os acessos a recursos que cada um terá.

Assim sendo, quando o usuário *logar* no sistema, independentemente de ser o cliente ou administrador, o *Active Directory* irá fazer a detecção e permitir ou limitar o acesso a pastas, arquivos, diretórios entre outros, fazendo para isso uma ACL.

Por essas características e por ele ser o gerenciador do sistema, o *Active Directory* é o responsável pela segurança e acesso nos sistemas de grande importância para a corporação, como nos diretórios de executáveis e no diretório de dados da empresa, onde ficam as informações não só dos usuários, como informações de projetos da empresa e projetos já concluídos tal como o planejamento futuro da corporação.

Como já mencionado, também é função do *Active Directory* a proteção às pastas de cada usuário, onde ficam registradas as informações pessoais dos mesmos, tal como endereço, telefone, filiação, número de documentos entre outras informações que não devem sem compartilhadas, apenas para ciência da empresa. Além das pastas dos usuários, as pastas de grupos de usuários também são de responsabilidades do *Active Directory*, impedindo que clientes fora do grupo tenham acesso a informações de setores diferentes dos quais atuam ou até mesmo potenciais invasores.

O MASC faz uso, para controle das pastas pessoais e de grupos dos usuários, de uma das boas práticas da Microsoft, que são diretrizes consideradas ideias para a configuração de um servidor, denominada AGDLP (*Acount, Global, Domain Local, Permission*). Ela recomenda que para permitir um serviço ou acesso a arquivos deve-se ter grupos aninhados no qual aconselha que novas contas devem ser adicionadas a um grupo global, que seja membro de um domínio local e possua as permissões necessárias, facilitando assim a organização e o controle das permissões.

Tabela 9 – *Active Directory*

ITEM	**VALOR DEFINIDO**
Proteção de acesso a diretórios, pastas e arquivos	*Active Directory* somente usuário com poder de administrador

4.8 Políticas de *Backup*

O *backup* periódico é essencial para manter o acesso aos dados da empresa caso haja o sumiço virtual dessas informações ou a perda física das máquinas que as contem, tal como roubo ou *hardware* queimado. E para esses *backups* o MASC tem algumas políticas afim de otimiza-los e a empresa não perca as informações da corporação, de projetos, informações dos usuários ou quaisquer outros dados que possuam valia para a mesma.

O MASC na política de *backup* decreta que seja feito um *backup full* uma vez por semana, gravando todos os dados por completo em uma mídia, que seria mantida por 5 ciclos e após isso seria guardada em um local seguro para manter o histórico dos dados. O método deste projeto também enfatiza para que a mídia com o *backup* completo não seja guardado no mesmo local físico aonde ocorre o *backup* em tempo real do servidor, para que em caso de uma catástrofe no lugar todos os *backups* sejam destruídos. Replicar os dados na nuvem também, através de um serviço com pagamento mensal, é de suma importância, ajudando a prevenir em situações como essa de ficar sem nenhuma informação da corporação.

As senhas, tanto dos usuários comuns, quanto dos administradores, são armazenadas em um banco de dados e no MASC é necessário um *backup* incremental diário das mesmas, já que as senhas podem ser alteradas a qualquer hora do dia, onde as mídia teria 7 ciclos, sendo guardada e não regravada após isso, para que os dados da corporação sejam mantidos.

Ao fim de cada mês será feito um *backup* completo em uma mídia que terá 12 ciclos e, no fim de cada ano, um *backup full* em uma mídia que não será regravável, servindo de histórico para a corporação.

Tabela 10 – *Backups*

ITEM	**VALOR DEFINIDO**
Backups	Histórico - *Backup* Completo uma vez ao ano (mídia não regravável). Mensal - *Backup* completo (mídia mantida por 12 ciclos). Semanal - *Backup* completo (mídia mantida por 5 ciclos). Diário - *Backup* incremental (mídia mantida por 7 ciclos).
Mídias físicas de *backup*	Não guardar no mesmo local físico dos servidores
Dados na nuvem	Utilizar um serviço confiável para replicar os dados

4.8.1 Plano de Contingência

Um plano de contingência consiste em estratégias para uma situação de emergência, com o intuito de diminuir os estragos em caso de um evento não planejado. E o MASC tem um plano de contingência especifico para as mídias físicas de *backup*, no qual consiste em replicar seus dados e informações para outros discos.

A princípio o MASC determina a implementação do método RAID (*Redundant Array of Independent Disks*), que é um mecanismo que tem o objetivo de melhorar a segurança, confiabilidade e o desempenho dos discos rígidos existentes nos computadores, fazendo para isso o uso de outros HDs para replicar as informações. Os discos rígidos atualmente já possuem uma placa controladora neles, o que é necessário para o uso do método, porém se o mesmo não tiver é possível a aquisição da placa separadamente.

A configuração depende do modelo e geração dos servidores, mas consiste basicamente nos seguintes passos:

- Acessar o setup e habilitar o RAID pela placa controladora;
- Selecionar os discos que serão utilizados pelo RAID e configurar suas *arrays*;
- Instalar o sistema operacional;
- Instalar os *drivers* da controladora;
- Ativar e habilitar o RAID pela BIOS (*Basic Input/Output System*) e selecionar a controladora.

Existem vários tipos diferentes de RAIDs, e os mais utilizados são o RAID 0, RAID 1, RAID 0 + 1, RAID 5 e RAID 10, porém no MASC é utilizado o RAID 5 devido ao seu desempenho de leitura ser bastante eficaz, quando comparado com os outros, ter a tolerância de permitir que um disco falhe e seu custo não ser tão elevado quanto o RAID 10. Para a implementação do RAID 5 são necessários ao menos 3 discos rígidos, sendo que um destes será utilizado para paridade, mas não sempre o mesmo, o que permite caso um HD falhe continue a troca de dados entre eles, em uma menor velocidade para compensar o que não está em funcionamento.

Tabela 11 – Plano de Contingência

ITEM	**VALOR DEFINIDO**
Plano de contingência	Implantar a técnica de replicação RAID 5

4.9 Políticas Para Evitar Invasões

As invasões são as que mais colocam em risco a segurança da corporação, merecendo diretivas especiais para seu combate, assegurando a proteção das informações da instituição em questão. Muitas vezes o risco é ocasionado por falta de informação ou inocência do empregado, facilitando a obtenção da informação necessária por parte do atacante para a invasão do sistema, técnica conhecida como engenharia social. O MASC tem políticas para o tratamento dessa manipulação psicológica e algumas outras com o intuito de coibir invasões.

4.9.1 Treinamento

Todos os funcionários da empresa devem passar por um treinamento inicialmente, ministrado por um profissional de TI, informando a importância de suas funções para a corporação como um todo, seus deveres e suas responsabilidades. Nesse treinamento deve ser enfatizado a importância e o poder que a senha de cada um possui e o quanto ela deve ser resguardada e não disponibilizada para quaisquer pessoas a não ser o dono da mesma.

Também será salientada as normas que impedem *download* de programas executáveis e os danos que os mesmos podem causar caso estejam infectados com vírus ou algum *malware*, o acesso a determinados sites, conexão de periféricos e celulares ao computador entre outros. Será informado no treinamento também a função e importância da equipe de TI e os serviços que os mesmos podem prestar.

Tabela 12 – Treinamento

ITEM	**VALOR DEFINIDO**
Treinamento	Ministrado por um profissional de TI

4.9.2 *Firewall* e DMZ

Outra proteção imprescindível para a segurança da informação é o uso de *firewall*, para monitorar o tráfego na rede, tanto de entrada quanto de saída. Além do controle do tráfego, um *firewall* tem mais dois objetivos como principais que é ser imune a penetrações e ser o caminho único de entrada e saída dos dados de uma rede (PETRY, 2013). Existem duas vertentes de *firewalls*, que são o *firewall hardware*, que são dispositivos físicos conectados a computadores e o *firewall software* que são programas instalados diretamente no computador.

O MASC, prezando sempre pela segurança, determina a instalação e configuração de ambos, pelo fato do *firewall* de *software* proteger apenas a máquina no qual foi instalado e o *firewall* de *hardware* possuir a capacidade de proteção de vários computadores ao mesmo tempo, possibilitando a proteção de toda a rede específica, porém necessitando de uma configuração mais complexa.

Aproveitando-se que a rede contará ao menos com dois *firewalls*, o MASC impõe a criação de uma DMZ, aumentando assim o nível de segurança da rede do sistema. Ao ter uma DMZ ativa no sistema, a mesma será responsável pelas portas FTP (*File Transfer Protocol*) e HTTP (*HyperText Transfer Protocol*) do servidor, protocolos responsáveis pela comunicação entre computadores na Internet. O HTTP funciona mandando requisições ao servidor do site que está tentando o acesso, permitindo uma comunicação e uma navegação pelos sites, já o FTP é utilizado para o carregamento de arquivos e ficheiros e enviar informações para a nuvem. Ter o controle do tráfego de informações dessas portas do servidor aumenta consideravelmente a segurança da rede, pois o gerenciador da mesma terá ciência dos dados transferidos entre as redes interna e externa.

Tabela 13 – *Firewall* e DMZ

ITEM	**VALOR DEFINIDO**
Firewall	Deve-se ter um *firewall hardware* e um *firewall software* configurados
DMZ	A DMZ será utilizada sempre que houver servidores de acesso externo

4.9.3 *Softwares* de Proteção

Os *softwares* de proteção são imprescindíveis para a segurança do sistema, pois englobam uma categoria responsável pelo combate aos *malwares*, códigos maliciosos que possuem como objetivo a contaminação do sistema alvo, colocando em risco as informações contidas no ambiente de trabalho.

No MASC a instalação de um antivírus é necessário para aumentar o grau de proteção do sistema. Estes programas possuem assinaturas que são trechos de arquivos, ao executar

o antivírus, este compara o trecho do programa com o seu banco de dados de *malware*, caso encontre segmentos iguais, o arquivo é detectado como malicioso. Após feita essa identificação, é possível excluir o arquivo ou mantê-lo em quarentena, onde é possível a recuperação do arquivo. Atualmente os antivírus possuem integrado ferramentas que não combatem apenas vírus, mas também *spywares*, *trojans*, entre outros *malwares*, sendo assim uma ferramenta completa no combate a esses códigos maliciosos.

É necessário manter sempre o antivírus atualizado, pois a cada atualização há uma lista maior de *malwares* em sua assinatura, diminuindo a chance de um código malicioso desconhecido se aproprie de arquivos, dados ou informações. O MASC exige não só do antivírus, mas que todos os programas instalados estejam sempre atualizados, o que ocasiona menor vulnerabilidade do sistema, porém faz um adendo para que as máquinas cliente sejam atualizadas automaticamente e os servidores sejam atualizados manualmente após uma análise do que será alterado, pois novas atualizações podem conter incompatibilidade de *hardware* e/ou *softwares*, o que poderia prejudicar ou impossibilitar o funcionamento do mesmo.

Tabela 14 – *Softwares* de Proteção

ITEM	**VALOR DEFINIDO**
Combate a *malware*	Instalar e configurar um antivírus nos servidores cliente e administrador
Updates	Atualizações automáticas para cliente e manual para servidores

4.10 Servidor Controlador de Domínio

Para gerir um ambiente cliente/servidor é necessário que se tenha um servidor controlador de domínio, aquele que será responsável por monitorar o espaço alocado para a rede do sistema. Este servidor tem como função gerenciar o banco de dados dos usuários, para que quando este *logar* no domínio, os aplicativos, impressoras, funções e recursos do sistema estejam disponíveis para esses clientes após a verificação de suas permissões. No *Windows* NT (*New Technology*) um domínio combina algumas das vantagens de um grupo de trabalho e um diretório.

Um outro servidor também muito importante para a corporação é o servidor DNS, que é a máquina responsável por distribuir IP para toda a rede de computadores a ele conectados. Este servidor é encarregado pela comunicação com a Internet, traduzindo para endereços IP os *links* nos quais digitamos no navegador.

Por serem servidores imprescindíveis para a instituição, o MASC ordena para que sejam maquinas potentes e atualizadas, utilizadas somente para esse fim, em exclusivo para o controle de domínio e outro único para DNS, tendo que estar ambos em locais seguros, climatizados e com acesso restrito apenas aos responsáveis por gerir esses servidores.

Tabela 15 – Servidores

ITEM	**VALOR DEFINIDO**
Servidores	Máquinas potentes e atualizadas

4.11 Recursos Para Auditoria do Sistema

A auditoria do sistema é uma parte importante do processo de segurança pois faz uma análise completa do sistema, verificando a rede de acesso à Internet, os computadores, os servidores e os recursos do sistema, informando se estão alinhados com as normas de segurança vigente ou se há alguma falha que coloque em risco a segurança do ambiente. Para que a auditoria de segurança seja realizada, alguns recursos são importantes para a sua ocorrência e auxiliem para que se chegue em uma conclusão, dentre esses recursos o principal é o *log* do sistema.

4.11.1 Controle de *Log* do Sistema

Os *logs* são arquivos gerados pelo sistema com o intuito de informar a ocorrência de um evento, podendo este ser relacionado a ferramentas, segurança ou sobre o próprio sistema.

Em relação ao registro de acesso do sistema operacional dos servidores, o *Windows Server* possui uma ferramenta chamada UAL (*User Access Logging*) que apresenta essa função, facilitando e criando um controle de quem utilizou o sistema, a hora e o que acessou no mesmo. O UAL já vem habilitado por padrão e no MASC o mesmo não pode ser desabilitado em hipóteses alguma, pois ele que irá auxiliar os administradores dos servidores em relação ao *log* do sistema e também a quantificar as solicitações dos clientes e relatar o uso nas pastas de trabalho.

Tabela 16 – *Log* do Sistema

ITEM	**VALOR DEFINIDO**
Log do sistema	UAL, Gerenciar, Registro de acesso

5 Desenvolvimento

Afim de constatar a utilidade do MASC, foi simulado um ambiente próximo ao que consta no método, que será detalhado neste capítulo. O objetivo foi verificar o nível de segurança do servidor e quais as fragilidades que o mesmo apresentava de acordo com os testes. Para efeito de comparação, foi usado um servidor com as configurações padrões já presentes no *Windows Server* e feita uma bateria de testes, para verificar a eficiência do MASC.

5.1 Configuração do Ambiente Padrão

Para caracterizar o ambiente padrão, foi utilizado um desktop com as seguintes configurações:

- Processador: Intel Core^{TM} i3 2ª geração;
- *Chipset*: Intel Q65 *Express*;
- Memória: 16 GB Ram;
- Opções Gráficas: Intel HD *Graphics* 2000 integrada;
- Disco Rígido: 3,5"SATA de 6 Gbit/s, 7.200 RPM de 500 GB;
- Sistema Operacional: *Windows Server* 2012 R2.

Nesta máquina foi feita a instalação padrão do *Windows Server* 2012 R2.

5.2 Configuração do Ambiente MASC

Para caracterizar o ambiente MASC, foi utilizado um desktop com as seguintes configurações:

- Processador: Intel Core^{TM} i3 2ª geração;
- *Chipset*: Intel Q65 *Express*;
- Memória: 16 GB Ram;
- Opções Gráficas: Intel HD *Graphics* 2000 integrada;
- Disco Rígido: 3,5"SATA de 6 Gbit/s, 7.200 RPM de 500 GB;
- Sistema Operacional: *Windows Server* 2012 R2.

Nesta máquina, foi feita a configuração seguindo o método MASC, com a instalação e configuração do antivírus *Kaspersky Total Security*.

Uma proteção que não foi implementada neste ambiente MASC foi a instalação e a configuração de um *firewall hardware*, devido à falta de verba, porém não há dúvidas dos benefícios em relação à segurança que o mesmo pode agregar ao ambiente.

5.3 Configuração da Máquina Cliente

Para simular um usuário comum acessando o sistema, foi configurada uma estação cliente com uma máquina com as seguintes configurações:

- Processador: Intel Core^{TM} i3 2ª geração;
- *Chipset*: Intel Q65 *Express*;
- Memória: 16 GB Ram;
- Opções Gráficas: Intel HD *Graphics* 2000 integrada;
- Disco Rígido: 3,5"SATA de 6 Gbit/s, 7.200 RPM de 500 GB;
- Sistema Operacional: *Windows* 10 *Pro*.

Foi utilizada a configuração padrão do *Windows* 10 quando conectado ao domínio do ambiente padrão. Ao fazer o teste no ambiente MASC, foi instalado e configurado o antivírus *Kaspersky Total Security*, como manda o método.

5.4 Bateria de Testes

Para verificar a eficiência do método MASC, o mesmo foi submetido a vários testes com o objetivo de compara-lo com a configuração padrão do *Windows Server* 2012 R2 e verificar se há ganho ou não em segurança, quando se faz uso desse método. Os testes foram escolhidos por serem situações que podem acontecer diariamente nas corporações. Há vários outros testes que poderiam ser feitos, porém devido ao prazo do projeto, estes foram os escolhidos.

A escala de mensuração utilizada para comparar ambos os métodos será denominada nível e indicará o grau quantitativo de dificuldades impostas ao atacante para atingir seu objetivo, onde cada obstáculo físico e/ou logico representará o acréscimo de uma unidade a escala. Sendo assim, quanto maior o valor final do nível, mais seguro teoricamente estará o ambiente.

Há de se ressaltar que os testes foram executados em máquinas físicas distintas, porém com as configurações anteriormente citadas e presentes no mesmo ambiente físico, dentro de uma sala com o ar refrigerado e que possui porta com tranca, na instituição de ensino Pitágoras unidade de Ipatinga.

5.4.1 Acesso Físico a Sala do Servidor

O teste consiste em adentrar a corporação, passar por todas as barreiras físicas presentes e obter acesso presencial ao servidor.

Ambiente Padrão

A instituição na qual o teste foi realizado possui importantes barreiras que auxiliam na proteção ao acesso físico a sala do servidor. Na entrada do prédio há uma porta de vidro, seguida de um balcão com pessoas responsáveis pela identificação, o que já proporciona 2 dificuldades ao invasor. Para acessar o ambiente no qual se encontra o servidor há mais uma porta com fechadura biométrica e por fim uma porta com tranca, somando mais 2 níveis de dificuldades ao invasor.

Nível: 4

MASC

Ambos os servidores estavam alocados no mesmo ambiente físico, o que gera um resultado similar para os métodos. O objetivo deste teste foi mostrar que a instituição onde os mesmos foram realizados, possui importantes valores em relação a segurança física e a importância disso para assegurar que pessoas não autorizadas tenham acesso presencial ao servidor, o que pode acarretar possibilidade de invasão ou até danos físicos ao mesmo.

Nível: 4

5.4.2 Backups

O teste consiste em verificar as formas de *backups* nos ambientes em questão, analisando a cobertura e a garantia de recuperação dos dados caso necessário. Por não possuir um ambiente de produção pleno, onde há um grande fluxo de dados e usuários, o teste se limitará a parte teórica e não a prática.

Ambiente Padrão

No ambiente padrão, a ferramenta de recurso do *Windows Server* 2012 para realização de *backups* não vem mais nativamente no sistema desde a versão anterior, o *Windows Server* 2008. Sendo assim ela deixou de der uma função do sistema e passou a ser um recurso.

Após ativada, a ferramenta permite agendar *backups* completos de todas as partições, de volumes específicos e/ou de pastas e arquivos separados, o que lhe garante 3 dificuldades em nossa escala de mensuração.

Nível: 3

MASC

No ambiente MASC os *backups* já são implementados desde o início o que já se torna uma vantagem para o método. O MASC garante um *backup full* para a sua inicialização e um outro a cada semana, ocorrendo nesse meio tempo o *backup* incremental, abrangendo partições completas, volumes específicos e quaisquer pastas, o que lhe garante 4 dificuldades em nossa escala de mensuração.

Por conter diretivas claras sobre a política de *backup*, é observado que pode ser recuperado quaisquer arquivos criados em um período de 24 horas.

Nível: 4

5.4.3 Acesso a Pastas Particulares e de Grupos

O teste consiste em tentar acessar a pasta de um outro usuário sem estar *logado* na conta do mesmo e a de um grupo no qual a pessoa não faz parte.

Ambiente Padrão

No ambiente padrão, ao realizar o primeiro *login* na máquina, é criada uma pasta particular para o usuário e, quando um outro usuário tenta acessá-la, se depara com uma mensagem dizendo que a ação não é permitida, o que ocasiona uma dificuldade a quem não possui o acesso.

Em relação a pasta compartilhada por grupos, por padrão o *Windows Server* 2012 permite acesso a todos os usuários, o que possibilita a um usuário não pertencente ao grupo, tenha acesso a mesma.

Nível: 1

MASC

O método MASC faz uso da boa prática AGDLP da *Microsoft* que recomenda que ao criar um usuário, seja especificada uma pasta base ao mesmo, que será mapeada para o cliente assim que ele fizer *login* no sistema, onde o mesmo poderá guardar seus arquivos pessoais e outros usuários não terão acesso a este diretório, o que garante uma segurança para o usuário e uma dificuldade para quem tentar acessar.

Em relação a pasta compartilhada por grupos, o MASC possui diretivas rígidas nas quais não permite acesso, leitura, gravação ou quaisquer outras ações a quem não pertencer ao grupo, emitindo a mensagem de acesso não permitido caso um usuário que não seja membro tente acessar a pasta, resguardando as informações contidas na mesma e ocasionando uma dificuldade ao invasor.

Nível: 2

5.4.4 Contaminação por Vírus

O teste consiste em conectar um *pen drive* infectado com vírus na máquina, tentar executar o arquivo na estação cliente e observar se há a propagação do vírus.

Ambiente Padrão

No ambiente padrão não houve empecilhos para conectar o *pen drive* e executar o arquivo, contaminando assim a estação cliente. Porém o usuário comum não possui permissão de acesso e nem de escrita no servidor, o que pode ser considerada uma dificuldade, fazendo com que apenas a estação do mesmo fique contaminada.

Nível: 1

MASC

No ambiente MASC, ao conectar o *pen drive* a porta USB da máquina, o antivírus faz uma varredura nos arquivos presentes no dispositivo portátil a procura de vírus e/ou *malwares* e, só permite o uso na máquina do mesmo se nenhuma detecção de arquivo suspeito for identificada. Após conectar e ter sido feita a varredura, o antivírus acusou um arquivo suspeito e não permitiu a execução do mesmo, acarretando uma dificuldade em propagar vírus na máquina e mantendo a estação cliente sem infecção.

No MASC, o usuário comum também não possui permissão de acesso e nem escrita ao servidor, o que ocasiona maior segurança e uma dificuldade a mais para propagação de vírus e/ou *malwares*. A não permissão para escrita no servidor é a melhor estratégia de defesa, pois vírus são criados constantemente, o que impossibilita os antivírus de serem completamente eficientes no combate a esses *malwares*.

Nível: 2

5.4.5 Exclusão de Arquivos do Sistema Operacional

O teste consiste em tentar excluir um arquivo qualquer do sistema operacional diretamente pela opção excluir ou remover um *software* pelo painel de controle.

Ambiente Padrão

No ambiente padrão o usuário possui a liberdade para a exclusão de um arquivo qualquer ou desinstalar um programa, não enfrentando resistência alguma por parte do sistema para concluir as ações. O usuário consegue excluir um arquivo ou programa diretamente pela opção excluir ou se preferir, consegue entrar no painel de controle do sistema operacional e executar e remoção ou desinstalação do *software*.

Nível: 0

MASC

No ambiente MASC, o usuário não possui permissão para excluir um arquivo diretamente, pois ao tentar fazer tal procedimento, o sistema solicita uma conta e um *login* de um administrador do sistema para concluir a ação, gerando assim uma dificuldade ao usuário, pois sem isso não é possível a exclusão.

Se o usuário optar por desinstalar um programa diretamente pelo painel de controle também não obterá sucesso, pois o acesso ao mesmo e as configurações da máquina não são liberadas para o usuário, deparando-se com uma mensagem que a operação foi cancelada devido as restrições existentes, o que ocasiona mais uma dificuldade ao usuário.

Nível: 2

5.4.6 Tentativa Para Descoberta de Senha do Usuário Administrador

O teste consiste em tentar descobrir a senha dos usuários, através de tentativas e erros.

Ambiente Padrão

No ambiente padrão as tentativas para tentar descobrir a senha dos usuários são ilimitadas o que confere uma fraqueza na segurança, pois apesar das senhas obedeceram aos requisitos de complexidade e gerar uma dificuldade aos atacantes, uma ferramenta que faça uso da força bruta, ou seja, inserção de exaustivas combinações de senhas, apresenta um risco considerável, pois este *software* pode conseguir quebrar as senhas e obter acesso ao sistema.

Nível: 1

MASC

No ambiente MASC as senhas dos usuários possuem um número máximo de 3 tentativas incorretas antes de serem bloqueadas, o que gera uma dificuldade aos atacantes, pois terão poucas tentativas para adivinhar a senha. Essa diretiva é importante pois limitando o número de *logon* praticamente acaba com a efetividade das ferramentas que utilizam força bruta para quebrar a senha, que são as mais utilizadas atualmente.

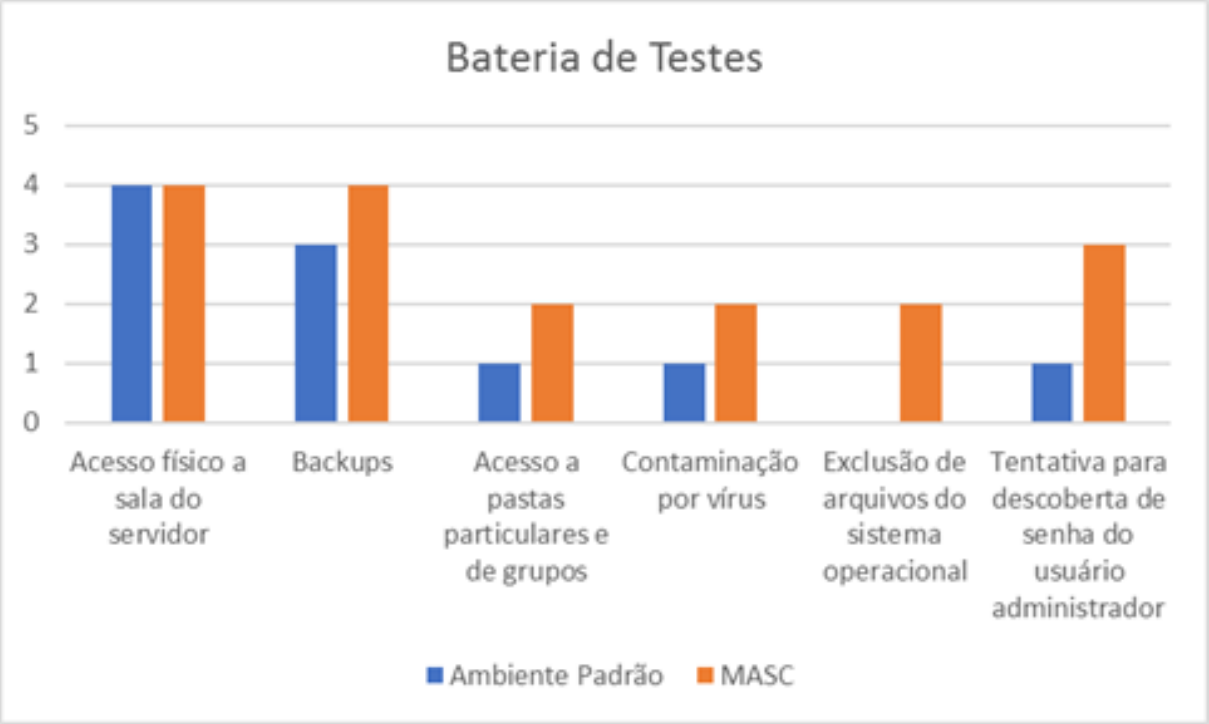
Nesse método também as senhas satisfazem os requisitos de complexidade do sistema, além de não permitir as últimas 5 senhas utilizadas pelo usuário, culminando em mais 2 dificuldades para que as mesmas sejam descobertas.

Nível: 3

5.5 Resultado dos Testes

O gráfico a seguir ilustra o resultado da bateria de testes realizados entre um ambiente com a configuração padrão e um outro caracterizado de acordo com o método MASC.

Figura 1 – Bateria de Testes



6 Conclusão

Tendo como base a segurança da informação, foi criado um método no qual fosse preservado os pilares desse conceito e consequentemente aumentasse o grau de segurança do sistema em que fosse aplicado. Para isso foi levantada as principais causas que ameaçam um sistema e também suas antíteses, as que qualificam a proteção do sistema para que, com um conhecimento mais amplo do assunto, fosse alcançado o objetivo proposto, um método que qualifique a confiança no sistema ao qual o mesmo seja aplicado.

Tendo essa gnose, defrontou-se um desafio: a criação de um método que tivesse as qualidades necessárias para atingir a meta do trabalho, e assim foi gerado o MASC. Porém era necessário colocá-lo em pratica para ter uma comprovação positiva ou negativa de sua capacidade e, novamente surgiu um desafio: se familiarizar com um ambiente servidor de um sistema operacional.

Após configurar o MASC em um ambiente cliente/servidor, foi elaborada uma bateria de testes para compara-lo com a configuração padrão do *Windows Server* e os resultados obtidos demonstraram que o MASC é sim eficaz e pode representar uma importante segurança para os ativos da informação.

6.1 Contribuições do Trabalho

O presente trabalho apresentou o MASC, método este no qual foi possível obter um ganho de segurança relacionado a um ambiente cliente/servidor quando aplicado em um sistema operacional *Windows Server*.

6.2 Trabalhos Futuros

Como foi demonstrado ao longo do trabalho, a segurança digital nunca deve ser deixada de lado e deve ser constantemente atualizada, afim de evitar que novos códigos maliciosos ou ações de engenharia social consigam burlar a defesa de um sistema. Como oportunidades de pesquisas referentes ao presente trabalho, as seguintes indicações são relevantes:

- Aplicar o método MASC em ambientes cliente/servidor *Linux* e comparar os resultados;
- Aplicar o método MASC na versão mais atualizada do sistema operacional *Windows* e comparar os resultados;
- Aplicar o método MASC em um ambiente no qual haja a implementação dos mecanismos de *firewall* para o acesso externo da rede;
- Aplicar o método MASC e realizar uma bateria de testes mais exaustiva, coletando os resultados e inferindo sobre os mesmos;

- Aplicar o método MASC e realizar os testes em um ambiente de produção plena.

Referências

ABNT. *NBR ISO / IEC 17799: 2005 Tecnologia da Informação – Código de prática para a gestão da segurança da informação*. [S.l.], 2005. Citado na página 17.

ABNT. *NBR ISO / IEC 27002: 2013 Tecnologia da Informação – Código de prática para a gestão da segurança da informação*. [S.l.], 2013. Citado na página 18.

ARAUJO, E. E. de. *A Vulnerabilidade Humana na Segurança da Informação*. Uberlândia - MG: [s.n.], 2005. Disponível em: <http://docplayer.com.br/514163-A-vulnerabilidade-humana-na-seguranca-da-informacao.html>. Citado na página 18.

BEAL, A. *Segurança da Informação, Princípios e melhores Práticas para Proteção dos Ativos de Informação nas Organizações*. São Paulo - SP: Atlas S.A., 2005. Citado na página 21.

BORBA, J. *Backup de dados*. Pelotas - RS: [s.n.], 2014. Citado nas páginas 22 e 23.

CARDOSO, L. M.; MENEZES, P. M.; ROCHA, F. G. Segurança em redes de computadores uma visão sobre o processo de pentest. Interfaces Científicas – Exatas e Tecnológicas, Aracaju - SE, v. 1, n. 2, p. 85–96, 2015. Citado na página 29.

DIAS, C. *Segurança e auditória da tecnologia da informação*. Rio de Janeiro - RJ: Axcel Books, 2000. Citado na página 15.

DIOGENES, Y.; MAUSER, D. *Certificação Security - da Prática Para o Exame Syo – 301*. 2. ed. Rio de Janeiro - RJ: NOVATERRA, 2013. Citado nas páginas 17, 19 e 21.

DUMONT, C. *Segurança Computacional – Segurança em Servidores Linux em Camadas*. Lavras - MG: [s.n.], 2006. Disponível em: <http://www.ginux.ufla.br/files/mono-CarlosDumont.pdf>. Citado na página 18.

FILHO, C. F. *História da Computação: O Caminho do Pensamento e da Tecnologia*. 1. ed. Porto Alegre - RS: EDIPUCRS, 2007. Citado na página 14.

FONTES, E. *Segurança da Informação: O Usuário faz a Diferença*. 1. ed. São Paulo - SP: Saraiva, 2006. Citado nas páginas 15 e 18.

FOROUZAN, B. *Comunicação de Dados e Redes de Computadores*. 3. ed. Porto Alegre - RS: Bookman, 2006. Citado nas páginas 15 e 17.

GALHARDO, A. T. *Sistemas Eletrônicos de Controle de Acesso*. Campinas - SP: [s.n.], 2011. Disponível em: <http://lyceumonline.usf.edu.br/salavirtual/documentos/2141.pdf>. Citado nas páginas 24, 25, 26, 27 e 28.

GARCIA, C. E. Planejamento da auditoria de saúde e segurança no trabalho – ohsas 18001. 2004. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiDyPGQw9fUAhWHMz4KHY0YD40QFggnMAA&url=http%3A%2F%2Fwww.simpep.feb.unesp.br%2Fanais%2Fanais_11%2Fcopiar.php%3Farquivo%3D188-Garcia_Planejamento%2520da%2520auditoria.pdf&usg=AFQjCNG18nFpnJvKLI8y1vbdat9smW8Quw>. Citado na página 28.

MICROSOFT. *Florestas, Árvores e Domínios*. 2008. Acesso online em 05 de agosto de 2016. Disponível em: <https://blogs.technet.microsoft.com/brzad/2008/12/11/conceitos-florestas-rvore-e-domnios/>. Citado na página 32.

PETRY, A. C. *Desenvolvimento de Firewall com Hardware de Baixo Desempenho e Fácil Configuração em Nível de Usuário*. Santa Maria - RS: [s.n.], 2013. Disponível em: <http://www.redes.ufsm.br/docs/tccs/Anderson_Petry.pdf>. Citado na página 40.

SARAIVA, F. M. *Information Security: A Case Study. Completion of Course Work. Degree in Computing*. Patos - PB: [s.n.], 2012. Disponível em: <http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/3882/1/PDF%20-%20Fernanda%20Monteiro%20Saraiva.pdf>. Citado nas páginas 19, 20, 21, 22 e 29.

SEGURANçA, C. e. *Os 10 Modelos de Câmeras de Segurança do Mercado*. 2017. Acesso online em 30 de março de 2017. Disponível em: <http://blog.cameraeseguranca.com.br/modelos-de-cameras-de-seguranca/>. Citado na página 24.

SILVA, I. B. A. da; SILVA, M. G. A. da. Política de integração de segurança e ética na internet: Perspectivas de uma melhor proteção para as informações. Trilha Digital, São Paulo - SP, v. 2, n. 1, p. 126–138, 2014. Citado na página 29.

SILVA, M. S. da; FILHO, V. S. Biometria através da impressão digital. Cadernos UniFOA, v. 6, n. 5, p. 19–28, 2011. Citado na página 27.

SILVA, S. R. F. da. *Proposta de Modelo de Controle de Acesso Lógico por Servidores Públicos aos Recursos Computacionais da Administração Pública*. Brasília - DF: [s.n.], 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/sergio_roberto.pdf>. Citado na página 22.

APÊNDICE A – Método MASC

ITEM	VALOR DEFINIDO
Máquinas e equipamentos	Sala fechada ou *racks*
Piso	Emborrachado
Temperatura	=>15º e <= 21º
Proteção elétrica	*Nobreak*
Acesso a sala de equipamentos	Somente pessoas autorizadas
Pessoas autorizadas	Somente previamente cadastradas
Cadastramento de pessoas autorizadas	Após treinamento
Controle de acesso	Registro em livro de controle
Trancas	Biométrica e/ou a chave
Operação do servidor	Pessoas previamente autorizadas e capacitadas. Quantidade restrita
Conta administrador	Máximo 3 contas, ficando uma de reserva
Active Directory	Para 1 servidor, nova árvore e nova floresta. Para 2 ou mais servidores, associar o segundo em diante como membros de uma floresta existente
Usuário administrador	Senha reservada para uso em situação de emergência. Guardar em local de acesso controlado
Usuário com poder de administrador	Somente 1 usuário. Responsabilidade do administrador da rede (até 2 pessoas capacitadas para administração de servidores)
Instalação de *softwares* e serviços	Usuário com poder de administrador
Conectar cabos USB no servidor	Não permitido. As transferências de arquivos somente por estação cliente e devidamente protegidas por *softwares* antivírus
Alterar senhas	Usuário com poder de administrador

Criptografia	AES 256 - Gerenciador do Servidor, Ferramentas, Usuários e computadores do *Active Directory*, Usuários, Conta, Criptografia 256 *bits* Kerberos
Login	Número de registro do funcionário
Senha	Entre 8 e 25 caracteres. Habilitar requisitos de complexidade: Senha contendo letras maiúsculas e minúsculas, números e caracteres especiais
Tempo de senha	Expira em 2 meses. Histórico das últimas 5 senhas não permitido
Tentativas para logar no sistema	Máximo de 3 vezes sem bloquear a senha
Desbloqueio de senha	Somente com intervenção do administrador
Políticas de grupos de usuários	Somente permitido aos administradores
Proteção de acesso a diretórios, pastas e arquivos	*Active Directory* somente usuário com poder de administrador
Backups	Histórico - *Backup* Completo uma vez ao ano (mídia não regravável). Mensal - *Backup* completo (mídia mantida por 12 ciclos). Semanal - *Backup* completo (mídia mantida por 5 ciclos). Diário - *Backup* incremental (mídia mantida por 7 ciclos).
Mídias físicas de *backup*	Não guardar no mesmo local físico dos servidores
Dados na nuvem	Utilizar um serviço confiável para replicar os dados
Plano de contingência	Implantar a técnica de replicação RAID 5
Treinamento de novos usuários	Ministrado por um profissional de TI
Firewall	Deve-se ter um *firewall hardware* e um *firewall software* configurados
DMZ	A DMZ será utilizada sempre que houver servidores de acesso externo

Combate a *malwares*	Instalar e configurar um antivírus nos servidores administrador e cliente
Updates	Atualizações automáticas para cliente e manual para servidores
Servidores	Máquinas potentes e atualizadas
Log do sistema	UAL, Gerenciar, Registro de acesso

Fonte: Autor