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

CRISTIANE MOREIRA CANDIDO

FERRAMENTAS DE AUDITORIA EM SEGURANÇA DA INFORMAÇÃO

Com ênfase no uso da ferramenta MBSA

Americana, SP
2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

CRISTIANE MOREIRA CANDIDO

FERRAMENTAS DE AUDITORIA EM SEGURANÇA DA INFORMAÇÃO

Com ênfase no uso da ferramenta MBSA

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Faculdade de Tecnologia de Americana.

Orientador: Professor Especialista Edson Roberto Gaseta

Americana, SP.

2016

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

C223a CANDIDO, Cristiane Moreira
Auditoria em sistemas de informação: com ênfase no uso da ferramenta MBSA. / Cristiane Moreira Candido. – Americana: 2016.
80f..

Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Edson Roberto Gaseta

1. Auditoria em sistemas de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.3

CRISTIANE MOREIRA CANDIDO

FERRAMENTAS DE AUDITORIA EM SEGURANÇA DA INFORMAÇÃO

Com ênfase no uso da ferramenta MBSA

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

Americana, 09 de dezembro de 2016.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Professor Especialista
Faculdade de Tecnologia de Americana

Leandro Halle Naim (Membro)
Professor - Mestre
Faculdade de Tecnologia de Americana

Pedro Domingos Antoniolli (Membro)
Professor - Doutor
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Primeiramente a Deus, por todas as bênçãos concedidas durante o período do curso.

Ao meu orientador Edson Roberto Gaseta, que além da orientação, demonstrou dedicação dispensada ao desenvolvimento deste trabalho, somando meu interesse na continuação dos estudos relacionada à área em questão.

À professora Maria Cristina Aranda e todos os professores da FATEC – Americana, pela contribuição em minha formação.

À Secretaria de Graduação da FATEC - Americana, pelo apoio e esclarecimento de todas as dúvidas existentes.

Ao meu noivo, Jonatha Lucas Carvalho Oliveira e minha mãe, Paula Aparecida Moreira Candido, por todas as demonstrações de atenção e incentivo durante todo o período do curso.

Aos amigos e amigas de graduação, pela convivência, amizade, reuniões e debates durante todo o curso.

DEDICATÓRIA

A toda minha família, que sempre me incentivou em todos os momentos, seja em minha vida pessoal ou profissional, mas principalmente em minha busca na obtenção do título de graduação do curso de Segurança da Informação.

RESUMO

A tecnologia da informação é extremamente importante para as organizações que desejam alcançar a inovação em seu negócio de atuação, porém não se trata apenas disso: manter os sistemas computacionais em segurança é tão importante quanto à criatividade em suas atividades. A informação da empresa se tornou o bem mais valioso. Invasores buscam de todas as maneiras possíveis descriptografar dados, invadir pastas e roubar arquivos. Os pilares da segurança da informação tornaram-se objetivos a serem alcançados por qualquer empresa, para trazer confiabilidade e disponibilidade de seus sistemas, e integridade de dados e informações. Uma forma de prever as vulnerabilidades dos sistemas das empresas, alertando-as de riscos, é através da auditoria. Este trabalho busca demonstrar de maneira teórica e prática, a importância da segurança da informação. Em um primeiro momento, será abordado neste trabalho um referencial teórico que além de conceitos básicos da área de segurança da informação e parâmetros que envolvem a auditoria, especifica ferramentas utilizadas para minimizar os riscos de segurança para proposições de melhorias posteriores. Será abordada uma ferramenta, na qual será detalhada sua instalação e funcionalidades, que foi utilizada para execução de varreduras no ambiente computacional de um hospital da região metropolitana de Campinas, verificando sua viabilidade de uso em um processo de auditoria, de modo que foram mitigadas grande parte das vulnerabilidades encontradas.

Palavras-chave: Ferramentas; auditoria; segurança da informação; vulnerabilidades; varredura.

Formatado: Inglês (EUA)

ABSTRACT

Information technology is extremely important for organizations that want to achieve innovation in their business, but it's not just about that: keeping computer systems safe is just as important as creativity in their business. Company information has become the most valuable asset. Invaders search in every possible way to decrypt data, invade folders, and steal files. The pillars of information security have become goals to be achieved by any company, to bring reliability and availability of their systems, and integrity of data and information. One way to predict the vulnerabilities of corporate systems by alerting them to risks is through auditing. This paper seeks to demonstrate in a theoretical and practical way, the importance of information security. Firstly, a theoretical framework will be approached in this work, which, in addition to the basic concepts of the information security area and parameters that involve auditing, specifies tools used to minimize security risks for subsequent improvement propositions. It will be approached a tool, which will be detailed its installation and functionalities, which was used to perform scans in the computational environment of a hospital in the metropolitan region of Campinas, verifying its feasibility of use in an audit process, so that were mitigated large Part of the vulnerabilities found.

Keywords: *Tools; audit; information security; vulnerabilities, scanning.*

LISTA DE FIGURAS

Figura 1 – Pilares da segurança da informação 16
Figura 2 - Percentual de uso dos sistemas operacionais 23
Figura 3 - Módulo ferramenta Pentana 28
Figura 4 - Relatórios da ferramenta Magique Galileo 29
Figura 5 - Tela inicial ferramenta ACL 30
Figura 6 - Processo de varredura com o Superscan 31
Figura 7 - Tela inicial da ferramenta MBSA 32
Figura 8 - Topologia do ambiente 35
Figura 9 - Página de download do MBSA 38
Figura 10 - Plataformas disponíveis para download 39
Figura 11 – Início do processo de instalação 39
Figura 12 - Processo de instalação do MBSA 40
Figura 13 - Contrato de licença 40
Figura 14 - Diretório de destino 41
Figura 15 - Progressão da instalação 41
Figura 16 - Término de instalação 42
Figura 17 - Acesso ao arquivo readme.html 42
Figura 18 - Arquivo readme.html 43
Figura 19 - Verificação da versão instalada 44
Figura 20 - Funcionalidades do MBSA 44
Figura 21 - Janela de varredura de um computador 45
Figura 22 - Janela de varredura de múltiplos computadores 47
Figura 23 - Histórico de varreduras já realizadas 48
Figura 24 - Varredura do notebook de suporte de TI 49
Figura 25 - Janela de download de atualizações 49
Figura 26 - Relatório da varredura no notebook de suporte técnico 50
Figura 27 - Desktop do setor Faturamento 51
Figura 28 – Desktop do setor Contabilidade 52
Figura 29 – Desktop de acesso remoto do setor de TI 52
Figura 30 - Desktop de backup do servidor do setor de TI 52
Figura 31 - Desktop de suporte técnico do setor de TI 53

Figura 32 - Desktop do setor Financeiro 53
Figura 33 - Vulnerabilidades administrativas notebook de suporte 54
Figura 34 - Firewall do Windows notebook de suporte.....55
Figura 35 - Informações adicionais notebook de suporte.....55
Figura 36 - Opções aprovadas notebook de suporte 56
Figura 37 - Atualizações Microsoft Office desktop faturamento 57
Figura 38 - Vulnerabilidades administrativas desktop faturamento 57
Figura 39 - Informações adicionais desktop faturamento.....58
Figura 40 - Vulnerabilidades administrativas desktop contabilidade 58
Figura 41 - Informações adicionais desktop contabilidade.....59
Figura 42 - Vulnerabilidades administrativas terminal remoto.....60
Figura 43 - Recomendação Microsoft terminal remoto.....60
Figura 44 - Informações adicionais terminal remoto.....61
Figura 45 - IE Zones terminal remoto.....61
Figura 46 - Vulnerabilidades administrativas desktop servidor.....62
Figura 47 - Informações adicionais desktop servidor 64
Figura 48 - Atualizações de segurança desktop de suporte.....65
Figura 49 - Vulnerabilidades administrativas desktop de suporte 66
Figura 50 - Informações adicionais desktop suporte.....66
Figura 51 - Atualização de segurança desktop financeiro.....67
Figura 52 - Atualizações de ferramentas desktop financeiro.....67
Figura 53 - Vulnerabilidades administrativas desktop financeiro.....68
Figura 54 - Informações adicionais desktop financeiro 69
Figura 55 - Gráfico de análise de contas e senhas 70
Figura 56 - Grau de classificação das atualizações 73
Figura 57 - Comparação do status do firewall.....74
Figura 58 - Comparativo de antivírus 75

LISTA DE QUADROS

Quadro 1 - Diferenças básicas entre auditoria interna e externa 20
Quadro 2 - Setores informatizados no ambiente 34
Quadro 3 - Descrição dos computadores da Contabilidade 36
Quadro 4 - Descrição dos computadores da Tecnologia da Informação.....36
Quadro 5 - Requisitos de senha segura 76

LISTA DE ABREVIATURAS E SIGLAS

ACL	Audit Command Language
BACEN	Banco Central do Brasil
FATEC	Faculdade de Tecnologia
HD	Hard Disk
IE	Internet Explorer
IP	Internet Protocol
ISO	International Organization for Standardization
MBSA	Microsoft Baseline Security Analyzer
NTFS	New Technology File System
OPME	Órteses, Próteses e Materiais Especiais
PABX	Private Automatic Branch Exchange
PS	Pronto Socorro
RH	Recursos Humanos
SAC	Serviço de Atendimento ao Cidadão
SAME	Serviço de Arquivo Médico e Estatística
SI	Segurança da Informação
TI	Tecnologia da Informação
TMED	Tecnologia Médica
UTI	Unidade de Tratamento Intensivo
WSUS	Windows Server Update Service

SUMÁRIO

1 INTRODUÇÃO 13

2 SEGURANÇA DA INFORMAÇÃO 15

2.1 A SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES 17

3 CONCEITOS GERAIS DE AUDITORIA 19

3.1 SURGIMENTO 19

3.2 NATUREZA DA AUDITORIA 20

3.3 AUDITORIA EM SEGURANÇA DA INFORMAÇÃO 21

3.3.1 Técnicas de auditoria em sistemas 24

4 FERRAMENTAS DE AUDITORIA EM SEGURANÇA DA INFORMAÇÃO 26

4.1 AMEAÇA E VULNERABILIDADE EM SEGURANÇA DA INFORMAÇÃO 26

4.2 EXEMPLOS DE FERRAMENTAS QUE AUXILIAM A AUDITORIA 27

4.2.1 Pentana 27

4.2.2 Magique Galileo 28

4.2.3 Audit Command Language (ACL) 29

4.2.4 Superscan 30

4.2.5 Microsoft Baseline Security Analyzer (MBSA) 31

5 ETAPAS DA AUDITORIA 33

5.1 PLANEJAMENTO 33

5.2 EXECUÇÃO 37

5.2.1 Instalando o MBSA 38

5.2.2 Configurando o MBSA 42

5.2.3 Executando o MBSA no ambiente....48
5.3 DIAGNÓSTICO....53
5.4 PLANO DE AÇÃO....69
5.4.1 Correções realizadas no sistema....69
5.4.2 Recomendações de segurança da informação....74
6 CONSIDERAÇÕES FINAIS....77
REFERÊNCIAS....ERRO! INDICADOR NÃO DEFINIDO.

Excluído: 79

1 INTRODUÇÃO

A TI (Tecnologia da Informação) está em constante crescimento, e presente no cotidiano das pessoas ao redor do mundo. É praticamente inviável para uma organização manter seus negócios e operações sem o uso informatizado de suas informações. Recursos computadorizados permitem não apenas manter processos no formato digital, como também agilidade destes, melhores condições para o armazenamento de informações, facilidade na manipulação de dados, comodidade na transferência de arquivos, entre tantos outros benefícios.

O centro de qualquer negócio bem estruturado e de sucesso reside além do processamento e armazenamento, à interpretação para utilização de suas informações, porém, o que muitos estudos apontam é que as empresas não estão preparadas para garantir a proteção de seus dados, que são, na maioria das vezes, o patrimônio mais importante que uma empresa possui.

As organizações tem sido alvo de *hackers* e estes invasores procuram invadir seus sistemas, procurando por informações valiosas para ter conhecimento, roubando estas, prejudicando as empresas, seja na divulgação, rompimento, troca ou até mesmo prejuízo financeiro na busca pela recuperação de informação.

O presente trabalho busca analisar um ambiente de TI de um hospital localizado na região metropolitana de Campinas. Através da ferramenta MBSA (*Microsoft Baseline Security Analyzer*), será possível analisar os recursos mais importantes deste ambiente, identificando falhas e vulnerabilidades, na busca de melhorias, garantindo maior segurança da informação em seus recursos, sejam virtuais ou não, melhorando a aplicabilidade de seu negócio e agilidade em suas operações.

O método científico de pesquisa utilizado foi o de pesquisa bibliográfica, com base em varreduras utilizadas em um ambiente real.

O **objetivo geral** consiste em analisar os princípios dos sistemas de informação nas empresas, de modo a compreender a função da auditoria com o uso de ferramentas específicas, que auxiliam o auditor a garantir aos gestores e acionistas da organização a confiabilidade dos investimentos, aperfeiçoando a segurança da rede, combatendo fraudes e problemas técnicos e operacionais, apontando tais deficiências e sugerindo medidas de correção e prevenção.

Entre os **objetivos específicos**, destacam-se:

- Realizar um levantamento bibliográfico sobre a auditoria em sistemas e sua relação com a segurança da informação das empresas;
- Realizar testes nos recursos computacionais da empresa;
- Documentar e analisar os problemas relacionados à segurança da informação, para análise posterior;
- Explorar o funcionamento da ferramenta MBSA, para realizar tais investigações, verificando benefícios da mesma em prol de alcançar tais objetivos.

O trabalho foi estruturado em seis capítulos, onde o **primeiro** é referente a esta introdução sobre o assunto que será abordado durante toda a pesquisa realizada.

O **segundo capítulo** descreve conceitos básicos relacionados à segurança da informação, seus pilares, requisitos principais e a classificação da informação. Também aborda a segurança da informação dentro das organizações

O **terceiro capítulo** traz os conceitos básicos de auditoria, abordando inicialmente um breve histórico, classes de identificação, classificação da mesma, focando posteriormente no tipo de auditoria que será abordado em todo este trabalho, que diz respeito à auditoria de tecnologia da informação voltada à segurança da informação, que pode ser atingida por meio de diferentes técnicas.

O **quarto capítulo** aborda a importância das ferramentas que podem ser utilizadas na auditoria de sistemas em segurança da informação, com uma simples descrição das exemplificações, seguidas pela ferramenta que terá maior foco durante todo o estudo realizado.

O **quinto capítulo** diz respeito ao estudo de caso, e as etapas da auditoria, onde no planejamento, são contidas informações sobre todo o ambiente abordado, descrição dos recursos computacionais; execução, onde as varreduras foram realizadas por meio da ferramenta; diagnóstico, que descrevem os principais fragmentos dos relatórios obtidos por meio da varredura; plano de ação, que propõe soluções para mitigar as vulnerabilidades, por meio do auxílio da ferramenta e outras recomendações. O **sexto capítulo** diz respeito às considerações finais diante os resultados deste trabalho e estudo.

2 SEGURANÇA DA INFORMAÇÃO

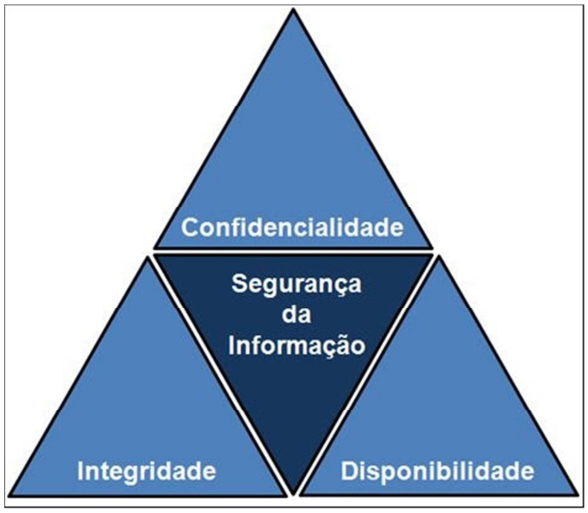
A Segurança da informação, de modo geral, pode ser definida como o resguardo da confidencialidade, integridade e disponibilidade, e em “como a sua proteção contra ameaças visa minorar os riscos e assegurar a continuidade do negócio, ampliando as oportunidades” (ARAÚJO, 2015, p.5).

Cabral (2015) complementa que ela “cobre todo o processo das informações, sejam elas físicas ou eletrônicas, independentemente do envolvimento de pessoas e tecnologia ou relações internas, externas ou clientes para sua geração”.

Dessa forma, sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas. É necessário proteger a informação, e Fontes (2006), ainda ressalta que é necessário garantir:

- Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão;
- Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida;
- Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia;
- Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como os princípios éticos seguidos pela organização e desejados pela sociedade;
- Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;
- Não repúdio de auditoria: o usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua auditoria.

Figura 1 – Pilares da segurança da informação



Fonte: Universidade Federal do Rio de Janeiro (2012) [1]

A classificação da informação é o processo de estabelecer o grau de importância das informações mediante seu impacto no negócio, ou seja, quanto mais estratégica e decisiva para a manutenção ou sucesso da organização, maior será sua importância. A classificação deve ser realizada a todo instante, em qualquer meio de armazenamento.

Ferreira e Araújo (2008, p. 77), explicam: “existem regras que devem ser consideradas durante a classificação e a principal delas é a determinação de proprietários para todas as informações, sendo este o responsável por auxiliar na escolha do meio de proteção”. Nos casos onde houver um conjunto de informações armazenadas em um mesmo local, e elas possuírem diferentes níveis, deve-se adotar o critério de classificar todo o local com o mais alto nível de classificação.

As informações armazenadas em qualquer local devem estar de acordo com os critérios de classificação e devem possuir uma identificação que facilite o reconhecimento do seu grau de sigilo (FERREIRA; ARAÚJO, 2008, p. 78). Para iniciar o processo de classificação, é necessário conhecer o negócio da organização,

[1] Disponível em: <http://www.gta.ufrj.br/grad/12_1/seg_smartgrid/possiveisataques.html>. Acesso em: 09 ago. 2016.

compreender os processos e atividades realizadas e, a partir desse momento, iniciar as respectivas classificações.

Segundo Ferreira e Araújo (2008) é de extrema importância estabelecer no início do processo algumas definições:

a) Classificação: atividade pela qual se atribuirá o grau de sigilo às informações, seja em meios magnéticos, impressos, etc.;

b) Proprietário: profissional de uma determinada área responsável pelos ativos de informação da organização;

c) Custodiante: profissional responsável por assegurar que as informações estão de acordo com o estabelecido pelo proprietário da informação;

d) Criptografia: codificação que permite proteger documentos contra acessos e/ou alterações indevidas;

e) Perfil de acesso: definição dos direitos de acesso às informações, transações, em meios magnéticos ou impressos de acordo com a necessidade de uso de cada usuário.

2.1 A segurança da informação nas organizações

Nas organizações, todos devem ser orientados em relação à proteção das informações, ações a serem realizadas e normas a serem cumpridas.

O elo mais frágil da corrente de segurança é alvo de ações fraudulentas. A preocupação do infrator é a não existência (ou destruição) da trilha de auditoria, que diz respeito a uma trilha de ações realizadas no sistema, permitindo que seja possível a identificação de quem causou determinado problema de segurança (FONTES, 2006).

Os arquivos de *log* (registros dos eventos de um sistema de informação) são fundamentais para consultas sobre fatos que aconteceram. Mas as informações gravadas devem ser efetivas, corretas e íntegras. De pouco adianta ter registrado no arquivo de auditoria as identificações de um usuário que acessou determinada

informação, se uma mesma identificação for utilizada por várias pessoas de um mesmo departamento (FONTES, 2006, p. 18).

A informação, independente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. Sem informação, a organização não realiza seu negócio. A informação utilizada pela organização é um bem valioso e precisa ser protegida e gerenciada.

Fontes (2006, p. 18) ressalta: “Para que a proteção da informação seja eficaz no dia a dia da organização, os conceitos e os regulamentos de segurança devem ser compreendidos e seguidos por todos os usuários”.

3 CONCEITOS GERAIS DE AUDITORIA

Este capítulo apresenta o referencial teórico sobre auditoria, desde o seu surgimento, diferentes classificações e sua ligação com a segurança da informação.

3.1 Surgimento

Segundo Chiquito (2005, p. 1), o "termo auditor vem do latim, com o sentido de aquele que ouve, ou ouvinte, sendo este adotado com o tempo para representar aquele que opina sobre algo comprovado ser ou não verdade". Admitiu-se que o surgimento da auditoria foi relatado inicialmente na Idade Média, com exames sistemáticos de contas públicas, por volta de 1314 na Inglaterra, ganhando força na Revolução Industrial, com a finalidade de controlar os registros contábeis e financeiros, prevendo a taxação do imposto de renda e resultados apurados em balanço, passíveis de erros. Sua evolução foi marcada pelo desenvolvimento econômico, impulsionado pelas grandes empresas, formadas por capitais de muitas pessoas, necessitando de um controle adequado para a proteção de seus patrimônios (APARECIDA, 2010).

No Brasil, o desenvolvimento da auditoria foi marcado pelas filiais e subsidiárias de firmas estrangeiras, financiamento de empresas brasileiras através de entidades internacionais, criação das normas de auditoria promulgadas pelo BACEN (Banco Central do Brasil) e também da criação da Comissão de Valores Mobiliários e da Lei de Sociedades Anônimas (CREPALDI, 2006).

Em 1950, ocorreram mudanças drásticas nos ambientes de negócios, onde grupos de companhias, conglomerados e organizações multinacionais começaram a ter uma expansão e complexidade de suas atividades com grande velocidade. Toda coleta de dados e sistemas de controle internos passaram a necessitar de padrões computacionais mais complexos, aumentando assim as técnicas e as ferramentas de avaliação de sistemas, e principalmente a preocupação com a segurança da informação (IMONIANA, 2011).

3.2 Natureza da auditoria

Com o crescimento da área, a procura e necessidade das organizações por processos de auditoria, também aumentou, sendo necessária a contratação seja interna ou externa, de profissionais da área. Dessa forma, surgiram alguns conceitos e classes de identificação, oferecendo uma ampla visão deste processo:

- **Órgão fiscalizador**

De maneira geral, a auditoria interna e a auditoria externa possuem trabalhos praticamente idênticos, pois ambos utilizam técnicas de auditorias parecidas, voltadas ao controle interno, em busca de investigar e detectar possíveis pontos fracos nas organizações, que mais tarde serão mitigados em forma de sugestões e mudanças baseadas em determinados processos (APARECIDA, 2010).

Porém, existem algumas diferenças básicas, citadas no quadro abaixo:

Quadro 1 - Diferenças básicas entre auditoria interna e externa

Auditoria Interna	Auditoria Externa
Realizado por órgão interno	Realizado por instituição externa
A revisão das atividades é contínua	A revisão é periódica, geralmente semestral ou anual
Preocupa-se em reduzir as probabilidades de erros, fraudes e políticas ineficazes	Procura emitir um parecer sobre a gestão de recursos, situação financeira e legalidade
Presta contas diretamente à direção	Deve ser independente da entidade fiscalizada

Fonte: Adaptado de Chiquito (2005)

Vale ressaltar que, o trabalho conjunto da auditoria interna com a auditoria externa é conhecido por auditoria articulada.

Perez Junior *et al.* (2011) especificam alguns tipos de auditoria:

- **Auditoria contábil:** verifica os registros e procedimentos realizados na empresa junto à área contábil, avaliando o cumprimento dos Princípios Fundamentais da Contabilidade;

- **Auditoria operacional:** investiga o desempenho das responsabilidades administrativas da empresa, seja a organização como um todo ou através da divisão entre setores;
- **Auditoria da qualidade:** voltado à alta gerência. Analisada em prol dos produtos destinados aos clientes e o fornecimento de matérias-primas;
- **Auditoria ambiental:** considerada a classificação mais recente. Investiga os possíveis impactos das empresas no meio ambiente;
- **Auditoria de programas de governo:** análise da execução de programas e projetos governamentais;
- **Auditoria administrativa:** engloba o plano da organização, seus procedimentos, diretrizes e documentos de suporte à tomada de decisão;
- **Auditoria financeira:** envolve a análise de contas, finanças, orçamentos, e se estão de acordo com os termos legais e regulatórios;
- **Auditoria de legalidade:** verifica a conformidade com a legislação em vigor das atividades e operações da organização;
- **Auditoria da Tecnologia da Informação:** totalmente operacional, existindo análise dos sistemas de informática e computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e deficiências. A auditoria em segurança da informação será o foco no presente trabalho, e será especificada no próximo tópico.

3.3 Auditoria em segurança da informação

Em um mundo onde a informação se torna cada vez mais valiosa para as empresas, existem pessoas com más intenções que procuram na mesma intensidade invadir os sistemas, prejudicando a confidencialidade, integridade e disponibilidade desta. Os sistemas computacionais estão sempre vulneráveis, devido à exposição contra vírus, erros, fraudes, invasões de rede. Informações podem ser adulteradas e perdidas, podendo até mesmo ser vendidas para os concorrentes diretos da empresa.

A preocupação com a segurança da informação deve ser de todos os colaboradores da organização, e não apenas de um grupo de pessoas (LYRA, 2008). Devemos nos atentar que, todos esses casos citados podem ser advindos de

funcionários da própria empresa, sejam terceirados, diretos, ex-funcionários em busca de vingança, etc.

Assim sendo, Cabral (2015, p. 174) define que a missão da auditoria é o "gerenciamento de risco operacional envolvido e a adequação das tecnologias e sistemas de informação [...] que envolvem o processamento de informações críticas para a tomada de decisão". Através de registros, é possível analisar uma trilha de ações que foram realizadas no sistema, de forma que seja possível identificar quem realizou algo e o que realizou.

Os auditores são os profissionais responsáveis por analisar toda esta complexidade, examinando as informações de forma cuidadosa, sendo especializados em estabelecer soluções para o combate das falhas existentes nos ambientes organizacionais, também prevendo o que pode vir além do que foi planejado e estabelecido.

A auditoria em segurança da informação procura certificar-se que as informações estão protegidas contra fraudes (acesso lógico: recursos computacionais, *softwares*, aplicativos, programas fontes), acesso indevido a Banco de Dados (senhas armazenadas), procura a segurança e monitoramento da Rede, além da proteção física, das instalações, equipamentos, preparação para situações de emergência (inundações, incêndios).

Realizar a escolha de uma ferramenta de auditoria para ser utilizada em um determinado ambiente é uma tarefa muito complicada e específica para cada tipo de organização. É preciso fazer o levantamento de alguns detalhes, quanto ao tipo da ferramenta, preço, atualizações, licenças e treinamentos, o que varia dependendo do foco de sua utilização.

Segundo Gusmão (2014, p. 1):

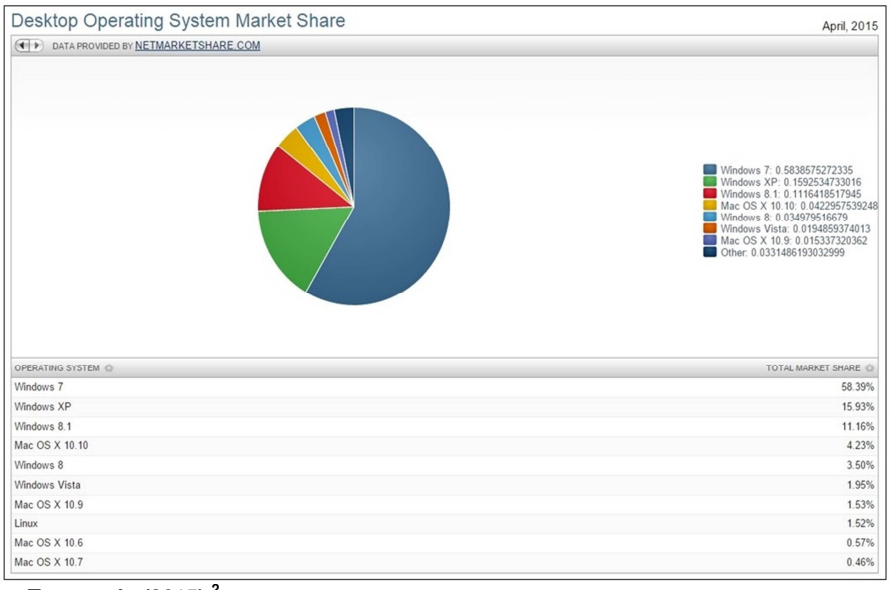
> "Existem disponíveis no mercado de ferramentas voltadas aos ambientes operacionais *Windows*, Linux e Mac OS. [...] Um estudo realizado pela *Assespro* Nacional em parceria com a Associação das Empresas de TI da América Latina, Caribe, Portugal e Espanha (ALETI), o sistema operacional mais utilizado nas empresas ainda é o sistema da *Microsoft* ®. A pesquisa envolveu 849 empresas. O *Windows* está presente em 78% das empresas seguidas pelo Linux que é adotado em 41% das empresas entrevistadas. O sistema da Apple é utilizado apenas por 10% das empresas, e os sistemas operacionais móveis contam com 28% da participação das companhias de TI. Vale ressaltar que há empresas que utilizam vários sistemas operacionais, e por isso a soma das porcentagens ultrapassa os 100%".

Uma pesquisa mais específica em relação à versão dos sistemas operacionais, realizada em 2015 pela *Net Market Share*, aponta que o *Windows* 7 detêm, 39% do mercado de Sistemas Operacionais para computadores, sendo seguido do *Windows* XP com 15,93% e do *Windows* 8.1 com 11,16%. Na sequência, surgem o Mac OS X 10.10 com 4,23%, o *Windows* 8 com 3,50% e o *Windows* Vista com 1,95%. Do total de usuários de PCs no planeta, apenas 1,50% adotam o Linux (DAQUINO, 2015).

Em 2016, com a chegada do *Windows* 10, é provável que tais dados sejam alterados. Além disto, o Linux vem ganhando cada dia mais conhecimento por parte de usuários, que divulgam o conceito de código aberto em fóruns que participam, compartilhando informações entre grupos que fazem parte.

Logo, por possuir uma *interface* mais agradável aos usuários, de fácil entendimento, além do oferecimento de suporte e serviços, os sistemas da *Microsoft*® mantem o maior índice no mercado de sistemas operacionais, conforme demonstrado no gráfico a seguir:

Figura 2 - Percentual de uso dos sistemas operacionais



OPERATING SYSTEM	TOTAL MARKET SHARE
Windows 7	58.39%
Windows XP	15.93%
Windows 8.1	11.16%
Mac OS X 10.10	4.23%
Windows 8	3.50%
Windows Vista	1.95%
Mac OS X 10.9	1.53%
Linux	1.52%
Mac OS X 10.6	0.57%
Mac OS X 10.7	0.46%

Fonte: Tecmundo (2015) [2]

[2] Disponível em: <http://www.tecmundo.com.br/windows-7/79298-windows-7-continua-sendo-sistema-operacional-usado-mundo.htm/>. Acesso em: 22 jun. 2016.

3.3.1 Técnicas de auditoria em sistemas

A auditoria de TI engloba os controles que influenciam a segurança de informação e o correto funcionamento dos sistemas.

A auditoria da segurança de informação determina a postura da organização diante da segurança, analisando a política de segurança e aspectos que envolvem o acesso lógico, acesso físico, planos de contingência e continuidade de serviços. Além disso, é possível especificá-los em:

- **Auditoria de controles organizacionais e operacionais**

Os controles organizacionais e operacionais são os controles administrativos instalados nos processos de fluxo das transações econômicas e financeiras dos sistemas de informações, auxiliando-os na consecução dos objetivos dos negócios.

Para isto, devem ser criadas políticas organizacionais, que envolvam responsabilidades, descrições de cargos, treinamento do pessoal, onde as informações devem ser claras e objetivas (IMONIANA, 2011).

- **Auditoria de controles de *hardware***

Busca garantir se os equipamentos são capazes de restringir acessos internamente dentro da organização, preocupando-se com a proteção de terminais, unidade central de processamento, servidores, etc.

Além disso, preocupa-se também se há equipamentos que restrinjam acessos físicos de pessoas alheias ao ambiente de processamento, devido às informações e as permissões de quem pode ou não acessá-las (IMONIANA, 2011, p. 104).

- **Auditoria de Controles de Acesso**

Pensando no acesso físico, relacionamos diretamente controle sobre o acesso físico ao *hardware*, e no acesso lógico controles sobre o acesso aos

recursos do sistema, incluindo a possibilidade de acesso a dados ou a processamento de programas e transações.

- **Auditoria de controles de suporte técnico**

Seu objetivo é de constatar se os recursos de alta tecnologia da empresa estão sendo utilizados adequadamente. Ou seja, confirmar se os referidos recursos desenvolvidos e implementados estão contribuindo para o aumento de valor agregado ou ajudando a destruir o valor da empresa.

4 FERRAMENTAS DE AUDITORIA EM SEGURANÇA DA INFORMAÇÃO

O uso de *softwares* e utilitários para auxiliar a auditoria pode ser utilizado em conjunto para facilitar em todo processo investigativo. Para tanto, antes de serem exemplificadas, faz-se necessário compreender os conceitos de ameaça e vulnerabilidade.

4.1 Ameaça e vulnerabilidade em segurança da informação

Os ativos da informação podem possuir vulnerabilidades. Tanto a ameaça como a vulnerabilidade, podem ser medidas e quantificadas dando a exata noção da probabilidade e da chance de uma falha de segurança acontecer e de seu impacto, ou seja, das consequências sob o negócio da organização.

Prado e Souza (2015) compreendem as ameaças como “causas potenciais de um incidente não desejado, podendo resultar em danos a um sistema ou organização”. Em contrapartida, a “vulnerabilidade é uma falha ou brecha, que pode ser explorada por ameaças”, complementam.

A proteção da informação deve ser definida por meio dos pilares da segurança da informação (confidencialidade, integridade e disponibilidade). A perda da confidencialidade, por exemplo, causa dano à imagem da organização e a parada de suas atividades e processos (PRADO; SOUZA, 2015).

Sendo assim, é possível entender que controle é todo e qualquer mecanismo utilizado para diminuir as fraquezas de um ativo da informação. A função da auditoria de sistemas é promover adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informação da empresa, bem como avaliar a utilização dos recursos humanos, materiais e tecnológicos envolvidos no processamento dos mesmos (SCHIMIDIT, 2006 *apud* LYRA, 2008).

A auditoria de sistemas deve atuar em todos os sistemas da organização, seja no nível operacional, tático ou estratégico. As ferramentas de auditoria são

poderosos aliados para a extração, seleção de dados e transações a serem validadas, auxiliando na evidenciação de discrepâncias e desvios.

4.2 Exemplos de ferramentas que auxiliam a auditoria

Muitas ferramentas podem ser utilizadas para realizar varreduras para auxiliar uma auditoria, como, verificação de portas abertas no sistema, examinar arquivos de *logs* no sistema, levantamento de vulnerabilidades existentes, e tantos outros fins específicos.

Essas ferramentas podem ser classificadas em generalistas, de utilidade geral ou especializadas. Segundo o Congresso de Segurança da Informação ([s.d]), "as ferramentas do tipo generalista possuem como características principais a análise e simulação de diversas funções". É possível utilizar softwares que processam vários arquivos ao mesmo tempo, independente de seu formato ou tamanho.

As ferramentas de utilidade geral podem ser classificadas com *softwares* utilitários, próprios para a execução de funções muito comuns de processamento. Por fim, as ferramentas especializadas são softwares desenvolvidos para executarem atividades em certos momentos específicos.

Podem ser desenvolvidos pelo auditor, por terceiros, contratados pelo auditor ou por especialistas da empresa que está sendo "auditada". Nos próximos sub tópicos, serão descritas as principais ferramentas que auxiliam o processo de auditoria. A escolha de uma ferramenta faz parte da etapa de planejamento neste processo, que será descrito no próximo capítulo, haja vista que, o estudo de caso foi baseado em uma destas opções executada em um determinado ambiente computacional.

4.2.1 Pentana

Esta ferramenta foi desenvolvida em 1992, no Reino Unido. Oferece quadros de monitoramento e avaliações de qualidade e desempenho da auditoria. Entre suas principais funcionalidades, permite (SEPIA SOLUTIONS, 2015):

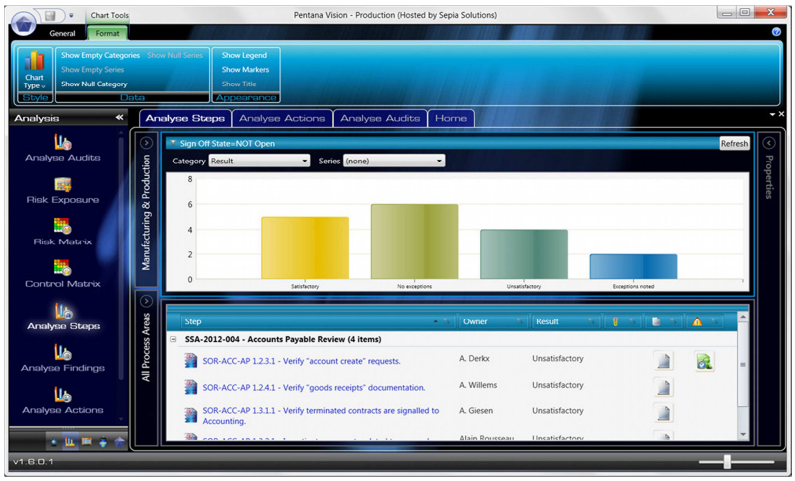
- Realizar trabalho de auditoria específico: o usuário aplica filtros e seleciona áreas voltadas a sua necessidade, agrupando determinados

dados em um mesmo grupo, permitindo uma descrição detalhada para emissão de relatórios;

- Trabalhar no modo *off-line*: quando não é possível conectar-se a rede, conta com a funcionalidade *check-out*, para que o auditor possa continuar a analisar seus testes e pontos de revisão mesmo que esteja *off-line*.
- Análise de relatórios: módulo que permite a análise dos resultados e fornece recomendações.

Como é possível visualizar na figura abaixo, é possível utilizar uma parte de um gráfico gerado para chegar ao elemento desejado. Esta função utiliza como base os passos da auditoria, seus resultados, ano e status.

Figura 3 - Módulo ferramenta Pentana



Fonte: Sepia Solutions (2015) [3]

4.2.2 Magique Galileo

O Magique Galileo é uma ferramenta de gestão de auditoria baseada no gerenciamento de risco, que pode ser adaptado às necessidades específicas de

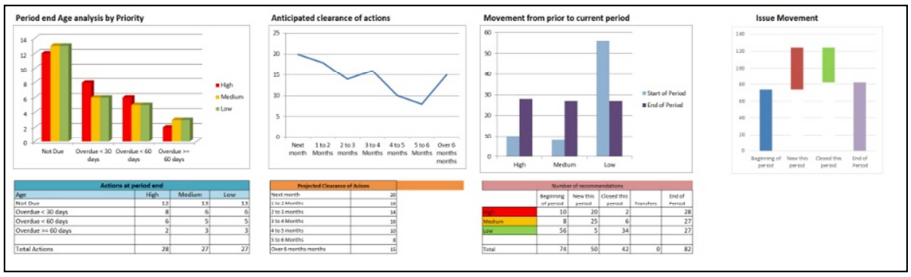
[3] Disponível em: <https://www.sepiasolutions.net/Software/Pentana_for_Auditors.html>. Acesso em: 02 set. 2016.

uma auditoria interna para suas investigações, fornecendo modelos de risco para planejamento estratégico. (MAGIQUE GALILEO, 2016).

Uma diferenciação em seus relatórios, é que estes geram datas planejadas, permitindo a conclusão exata de cada estágio da auditoria. Além disso, o gerenciamento da equipe de auditoria pode ser monitorado, definindo um período de atividades para cada membro, controlado por gráficos.

Há o acompanhamento do progresso das atividades prevendo atrasos e problemas. Para exportar os relatórios, é possível realizar a interação com as ferramentas do *Microsoft Office*.

Figura 4 - Relatórios da ferramenta Magique Galileo



Fonte: Magique Galileo (2015) [4]

O sistema produz estatísticas de apuramento e desempenho com *benchmarking* e tendências. Os relatórios abrangem movimentos em números, análise de idade e futuras desagregações de apuramento, entre outros.

A segurança abrangente é fornecida para permitir a resposta *on-line* e o rastreamento por proprietários de ações (MAGIQUE GALILEO, 2016).

4.2.3 Audit Command Language (ACL)

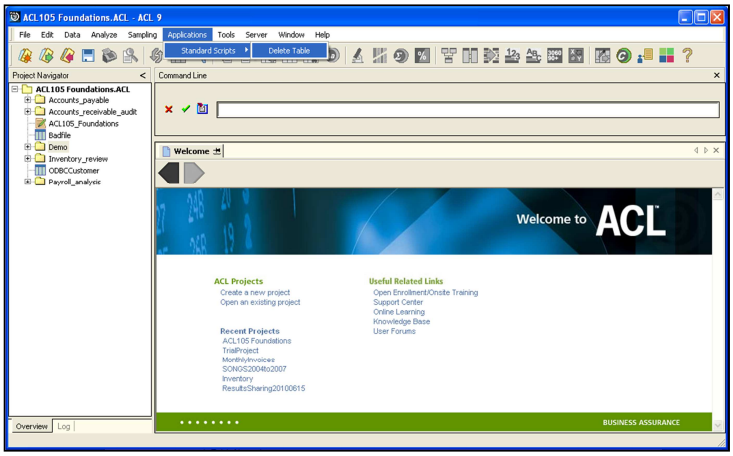
[4] Disponível em: < http://www.magiquegalileo.com/hsl/hslwebsite.nsf>. Acesso em: 02 set. 2016.

O *Audit Command Language* é uma ferramenta canadense criada em 1987, para auxiliar nos processos de auditoria. Deve-se adquirir sua licença por meio de uma empresa credenciada. É voltada para análise de dados existentes no sistema.

Os arquivos que são lidos pelo ACL podem estar em diferentes formatos, como tabelas criadas no *Microsoft Excel* e *Microsoft Access*, onde as informações são extraídas independentemente do tamanho do arquivo.

Segundo Sousa e Barbosa ([s.d]), é uma ferramenta que depende muito do conhecimento do usuário, o que "exige um forte conhecimento dos dados disponíveis [...], projetando-os em expressões à serem utilizadas".

Figura 5 - Tela inicial ferramenta ACL



Fonte: ACL (2013) [5]

4.2.4 Superscan

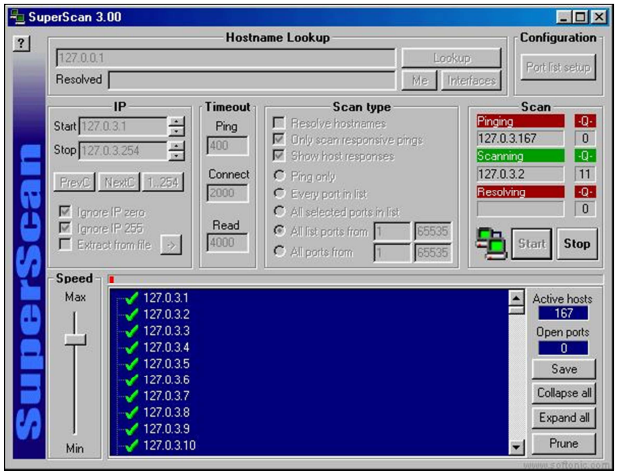
O Superscan é uma ferramenta de varredura de portas do *Windows*, fator que deve ser tratado em um processo de auditoria. Entre algumas de suas funções, destacam-se (MCAFEE, 2012):

- Alta velocidade de digitalização;
- Geração de relatórios;

[5] Disponível em: <http://www.acl.com/>. Acesso em: 02 set. 2016.

- Resolução de nome de *host*;
- Suporte para endereços de rede;
- Identificação de portas de origem e de saída;
- Integração com ferramentas e comandos, como *ping* e *whois.*

Figura 6 - Processo de varredura com o Superscan



Fonte: Superscan (2013) [6]

É possível realizar o download gratuito da versão mais atual da ferramenta diretamente no site da *McAfee*.

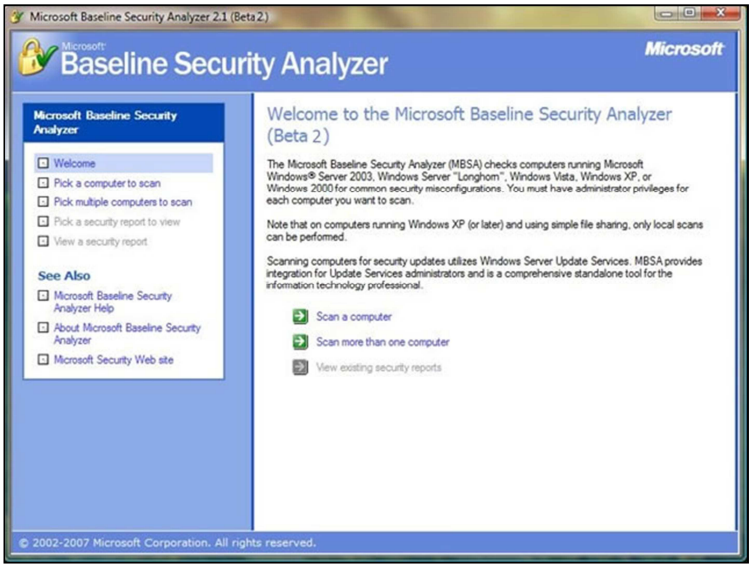
4.2.5 *Microsoft Baseline Security Analyzer* (MBSA)

Segundo Soares (2014), o MBSA foi lançado em 2004, criada para profissionais de TI, que ajuda empresas de pequeno e médio porte a determinar o estado da segurança de seus sistemas de acordo com as recomendações de segurança da *Microsoft* ® e oferece diretrizes de atualizações específicas. Manter essa segurança é de grande importância para manter os processos em andamento e garantir a viabilidade da auditoria.

[6] Disponível em: <http://superscan.softonic.com.br/>. Acesso em: 03 set. 2016.

O processo de gerenciamento de segurança pode ser aprimorado utilizando o MBSA para detectar erros comuns de configuração relacionados à segurança. Um ponto forte desta ferramenta é a sua gratuidade e o fácil processo de instalação (SOARES, 2014).

Figura 7 - Tela inicial da ferramenta MBSA



Fonte: *Microsoft* ® (2014) [7]

[7] Disponível em: < https://technet.microsoft.com/pt-br/library/cc668448.aspx />. Acesso em: 03 set. 2016.

5 ETAPAS DA AUDITORIA

A auditoria de sistemas preocupa-se, sobretudo, com os processos e operações envolvendo as áreas mais críticas de uma empresa: se estão em conformidade com os objetivos e políticas, quais vulnerabilidades podem impactar diretamente o negócio da organização, de forma a analisar minimamente os sistemas, para que seja possível mitigar riscos e fraudes.

Logo, a auditoria de sistemas possui etapas que a partir de um planejamento, que detalha quais as ferramentas serão utilizadas, qual o escopo em questão, permite a execução de testes, verificando vulnerabilidades relacionados a segurança da informação, permitindo uma análise estratégica para correção, prevenção ou tomada de decisão para que ocorra a diminuição destes problemas.

5.1 Planejamento

O planejamento dos testes de auditoria que foram realizados neste estudo de caso é uma etapa muito delicada. Em primeiro lugar, é necessário conhecer o ambiente a ser investigado, procurando entender o funcionamento tanto de sua rede e configurações, como das atividades que são realizadas. Assim, torna-se possível definir um escopo, torna-se possível a escolha da ferramenta mais adequada.

O ambiente em estudo é um hospital particular, localizado na região metropolitana de Campinas, escolhido pela conveniência de estagiar neste local e conhecer o ambiente, que conta atualmente com um quadro de aproximadamente 600 funcionários. Possui uma estrutura com mais de 130 leitos para atendimentos e exames, além de sete salas cirúrgicas, realizando por mês, uma média de 1.000 procedimentos.

Diante deste cenário considerado complexo e minucioso, onde deve existir exatidão dos dados e agilidade em seus processos, uma gestão da tecnologia da informação bem planejada nos hospitais vem se tornando como uma exigência para que estes possam manter-se competitivos no mercado.

O quadro a seguir descreve a relação dos nove departamentos do ambiente em questão que são informatizados e controlados pela equipe de tecnologia da informação. Estes departamentos estão divididos em um total de 31 setores.

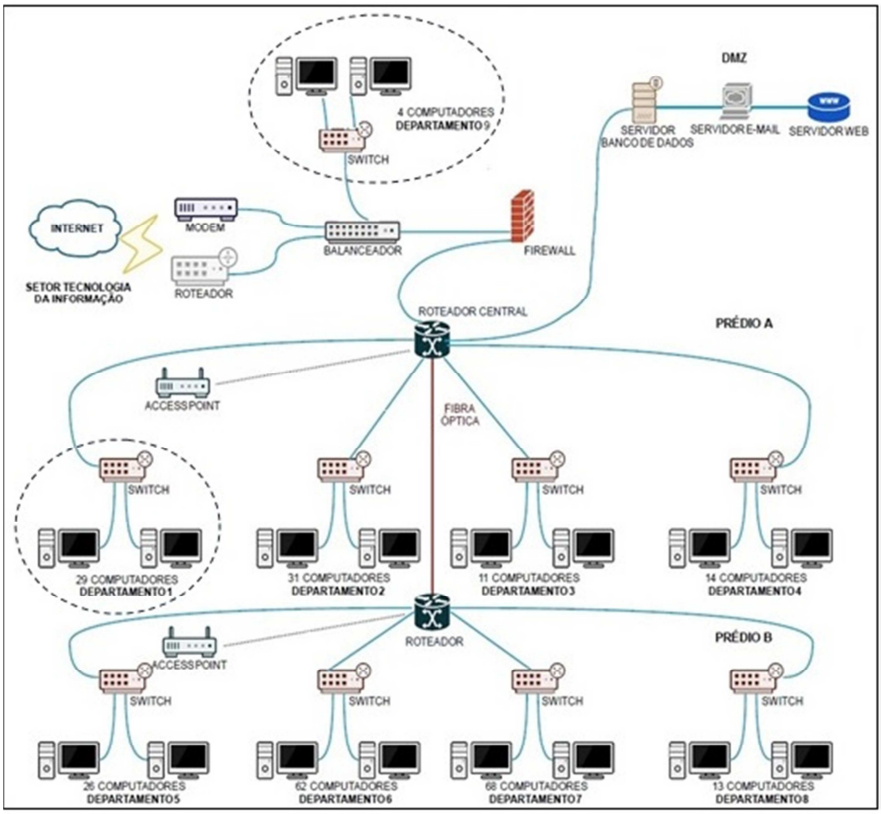
Quadro 2 - Setores informatizados no ambiente

Departamentos	Setores
Departamento 1	• Diretoria; • Financeiro; • Faturamento; • Contabilidade.
Departamento 2	• Compras; • Contas médicas; • Revisão de Contas; • PABX/SAC.
Departamento 3	• Recursos Humanos; • Serviço Social.
Departamento 4	• SESMT; • SAME.
Departamento 5	• Recepção Pronto Socorro (PS); • Recepção Internação; • Consultório de Atendimento.
Departamento 6	• Centro Cirúrgico; • Hemodinâmica; • OPME; • Radiologia/Ultrassonografia; • Central de cópias.
Departamento 7	• Alas (A, B, C); • UTI (adulto, pediátrica, neonatal); • Unidade Coronariana.
Departamento 8	• Farmácia; • Central de materiais esterilizados; • Almoxarifado.
Departamento 9	• Tecnologia da Informação.

Fonte: Autoria própria (2016)

A figura 8 exemplifica a topologia do ambiente informatizado da empresa em estudo:

Figura 8 - Topologia do ambiente



Fonte: Autoria Própria (2016)

O escopo para realização do estudo de caso baseia-se nas duas áreas circuladas da topologia:

- **Departamento 1,** onde após análise do ambiente, verificou-se que neste estão concentrados três dos setores mais críticos do hospital, que devem manter-se sempre em funcionamento para bom andamento dos processos legais e jurídicos.

  O setor de contabilidade, trabalha paralelo ao setor financeiro à respeito de normas e diretrizes a serem seguidas, sejam nos pagamentos de impostos, funcionários, fornecedores de materiais e medicamentos, do ramo alimentício e de higiene, e devoluções à pacientes, para que a emissão/cancelamento de notas fiscais e relatórios de contas médicas possam ser realizadas pelo

setor faturamento, que deverão ser registradas no sistema contábil, sob autorização e supervisão da diretoria.

A descrição das máquinas onde as varreduras foram realizadas deste departamento pode ser visualizada no quadro abaixo:

Quadro 3 - Descrição dos computadores da Contabilidade

Setor	Endereço de rede	Configurações
Contabilidade	192.168.5.115	Desktop Dell com processador Intel® Core 2 Duo Sistema Operacional *Windows* 7 - 32 bits Memória RAM: 4 GB Disco Rígido (HD): 500 GB
Faturamento	192.168.5.11	
Financeiro	192.168.5.98	

Fonte: Autoria própria (2016)

- **Departamento 9**, onde as varreduras foram realizadas em 4 máquinas do setor de tecnologia da informação, como demonstra o quadro. A equipe de TI é uma empresa terceirizada, com especialização na área de saúde e experiência há mais de 20 anos neste tipo de negócio.

Quadro 4 - Descrição dos computadores da Tecnologia da Informação

Descrição do computador	Endereço de rede	Configurações
- Suporte Técnico: Notebook de suporte utilizado para testes da funcionalidade de pontos de rede e hardware das máquinas dos usuários do hospital.	192.168.5.9	Notebook Dell com processador Intel® Core 2 Duo Sistema Operacional *Windows* 7 - 32 bits Memória RAM: 6 GB Disco Rígido (HD): 500 GB
- Suporte Técnico: Máquina de suporte utilizada na resolução de problemas relacionados ao sistema de gerenciamento do hospital.	192.168.5.16	Desktop Dell com processador Intel® Core 2 Duo Sistema Operacional *Windows* 8 - 64 bits Memória RAM: 6 GB Disco Rígido (HD): 500 GB

Descrição do computador	Endereço de rede	Configurações
- Acesso Remoto: Máquina que disponibiliza acesso remoto a computadores de outras unidades da mesma rede hospitalar.	192.168.5.81	Desktop Dell Intel® Celeron® Dual Core Sistema Operacional *Windows* Server 2003 Memória RAM: 8 GB Disco Rígido (HD): 500 GB
- Backup Servidor: Onde são armazenadas as cópias de restaurações do banco de dados e de sistemas internos, como o de catraca de acesso.	192.168.5.215	Desktop Dell com processador Intel® Core 2 Duo Sistema Operacional *Windows* 7 - 32 bits Memória RAM: 4 GB Disco Rígido (HD): 500 GB

Fonte: Autoria própria (2016)

Vale ressaltar que a máscara de rede 255.255.255.0 e o *gateway* 192.168.5.1 são padrões nos computadores de todas as máquinas em estudo.

Baseando-se no sistema operacional mais utilizado no ambiente em estudo, foi utilizada a ferramenta MBSA, que é específica gratuita da *Microsoft* ® para realizar este processo de identificação de vulnerabilidades para viabilizar uma auditoria.

Dessa forma, torna-se possível especializar-se nesta ferramenta, analisando quais tipos de dados ela permite coletar, onde é possível ter uma percepção da viabilidade de sua utilização.

A disponibilidade, que é um ponto crucial para manter o ambiente em funcionamento, é uma questão abordada pelo MBSA. Os sistemas estão vulneráveis a falhas e ataques, como vírus, *hackers*, entre outros. Silva ([s.d]) complementa que esta ferramenta realiza varreduras que reportam falhas como “senhas, acesso anônimo, *auto-logon*, compartilhamentos e gera um relatório com essas vulnerabilidades descrevendo-as com *status* e *links* para *downloads* das correções necessárias além do que pode ser feito para solucionar tais problemas”.

5.2 Execução

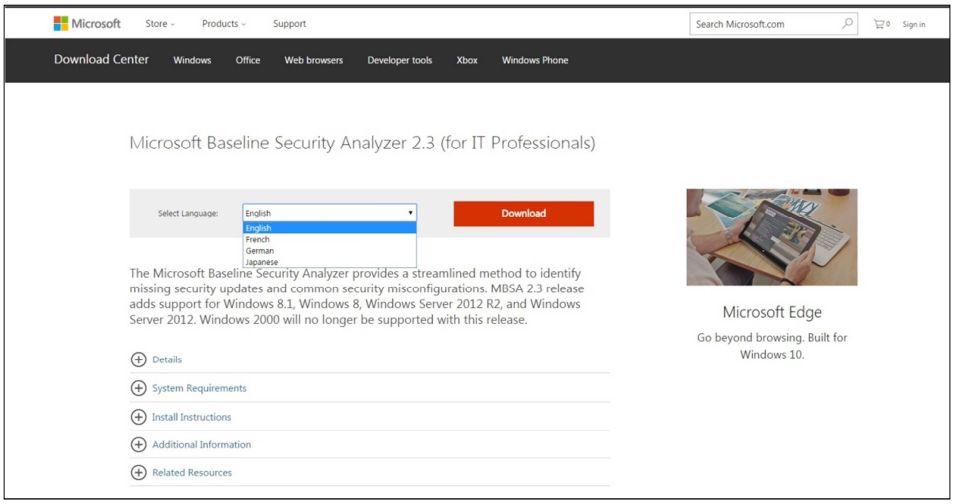
A etapa de execução está dividida em três seções:

- O passo-a-passo da instalação da ferramenta escolhida;
- A configuração da ferramenta para entendimento de suas funcionalidades;
- A execução da ferramenta no ambiente em estudo.

5.2.1 Instalando o MBSA

a) O MBSA está disponível gratuitamente para download no site oficial da *Microsoft* ®, através do link: <https://www.microsoft.com/enus/download/details.aspx?id=7558>, nos idiomas: Inglês, Francês, Alemão e Japonês.

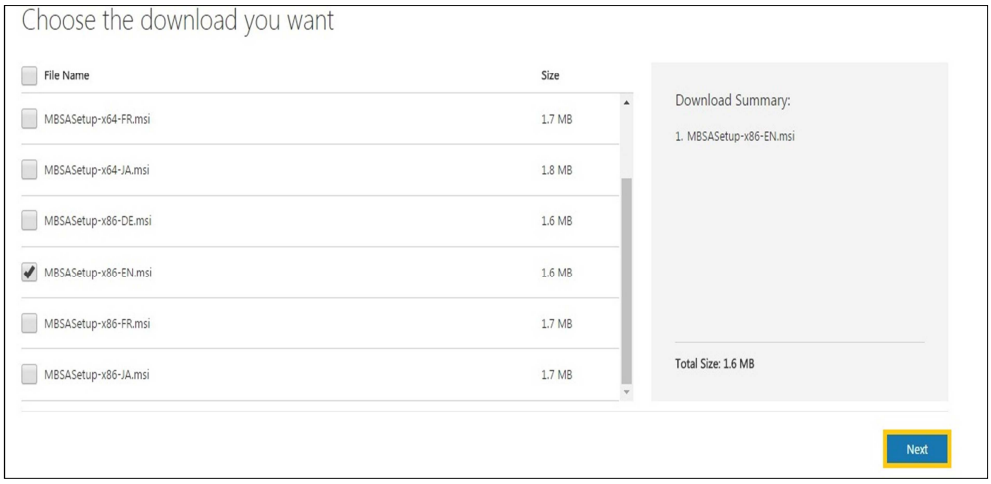
Figura 9 - Página de download do MBSA



Fonte: Autoria própria (2016)

b) Além da escolha do idioma, é necessário também fazer a escolha da plataforma mais adequada ao ambiente em que será utilizado: 32 bits (x86) ou 64 bits (x64), para que o processo de *download* possa ser iniciado.

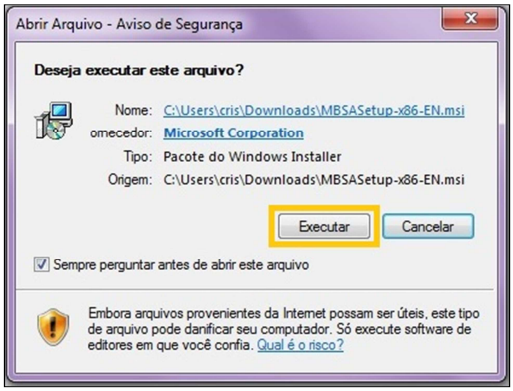
Figura 10 - Plataformas disponíveis para download



Fonte: Autoria própria (2016)

c) Após o *download* ser concluído, basta identificar o arquivo MBSASetup-x(*plataforma escolhida*)-(*idioma escolhido*).msi, criado na pasta padrão e executá-lo para seguir as instruções.

Figura 11 – Início do processo de instalação



Fonte: Autoria própria (2016)

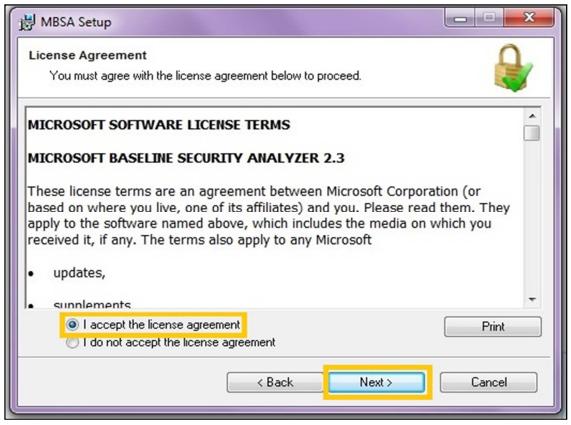
d) Na janela "*Welcome to the Microsoft Baseline Security Analyzer*", basta clicar em *Next* para continuar:

Figura 12 - Processo de instalação do MBSA

Fonte: Autoria própria (2016)

e) É possível imprimir o contrato de licença em "*Print*", para leitura do deste, antes do aceite do contrato de licença. Só é possível seguir com a instalação após aceitar os termos presentes no contrato.

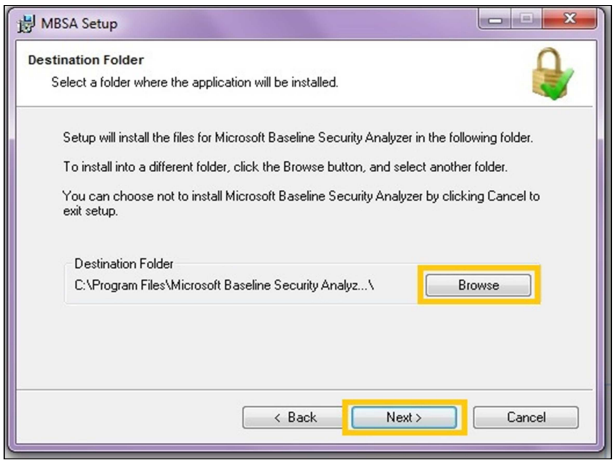
Figura 13 - Contrato de licença



Fonte: Autoria própria (2016)

f) Na escolha do diretório de destino, é possível optar por mantê-lo na pasta padrão ou alterá-lo, clicando em "*Browse*". Após a escolha, basta prosseguir clicando em "*Next*".

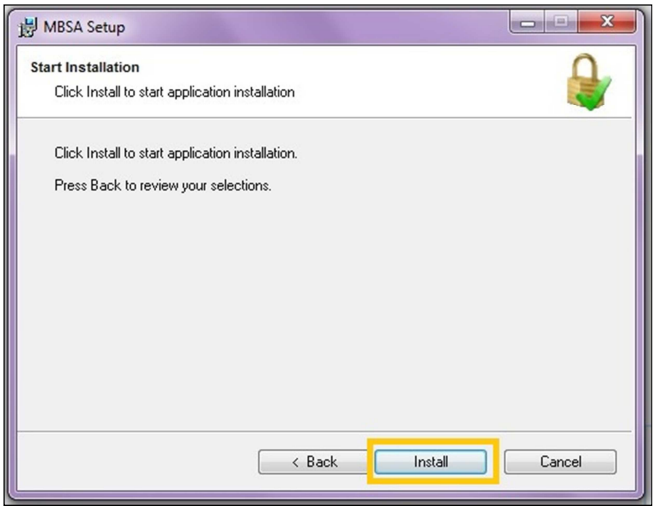
Figura 14 - Diretório de destino



Fonte: Autoria própria (2016)

g) Por fim, basta clicar em "*Back*" caso seja necessário alterar algum dos itens selecionados nos passos anteriores ou em "*Install*" para prosseguir a instalação:

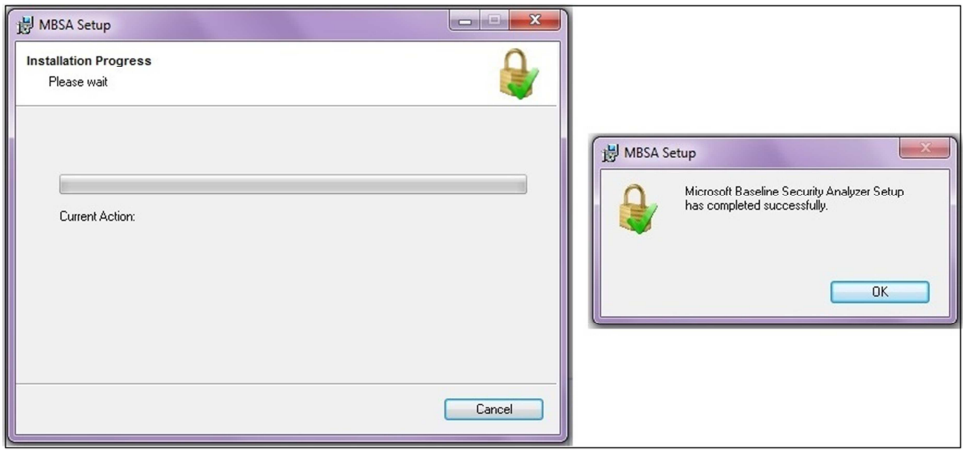
Figura 15 - Progressão da instalação



Fonte: Autoria própria (2016)

h) Uma vez que o progresso de instalação é completamente carregado, é exibido um *pop-up* confirmando que a instalação foi realizada com sucesso.

Figura 16 - Término de instalação



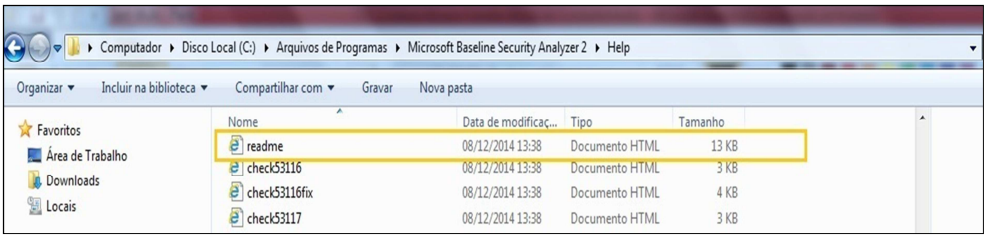
Fonte: Autoria própria (2016)

5.2.2 Configurando o MBSA

No disco local do computador, é criada a pasta *"Microsoft Baseline Security Analyzer* 2", após a finalização da instalação da ferramenta. Nela, estão contidos todos os dados a respeito do programa.

A pasta *Help*, contém o arquivo .html *readme*, que fornece informações que devem ser lidas antes de sua utilização para melhor entendimento sobre informações de compatibilidade e suporte.

Figura 17 - Acesso ao arquivo readme.html



Fonte: Autoria própria (2016)

Entre as principais informações contidas neste arquivo, estão descritas as "Características Adicionais" comparadas a versão anterior, como o modo *off-line* da

interface, facilidade na atualização da versão e compartilhamento dos relatórios gerados.

Outra informação diz respeito que, o MBSA verifica atualizações de segurança em todos os produtos suportados pelo *Microsoft Update*, como:

- *Windows XP*, *Windows Server* 2003, *Windows Vista*, *Windows Server* 2008, *Windows* 7, *Windows Server* 2008 R2, *Windows* 8, *Windows Server* 2012, *Windows* 8.1, *Windows Server* 2012 R2 - incluindo 64-bit (x64 e ia64);
- *Microsoft Windows XP Embedded* (limitado a digitalização remota e limitado a digitalização local, através da opção de linha de comando / *xml out*);
- Todos os componentes do *Windows* (como o *Windows Media Player*, *Outlook Express* / *Windows Mail*);
- *.Net Framework* 1.0 e posterior;
- *SQL Server* 2000 com *Service Pack* 3 e versões posteriores.

Figura 18 - Arquivo readme.html

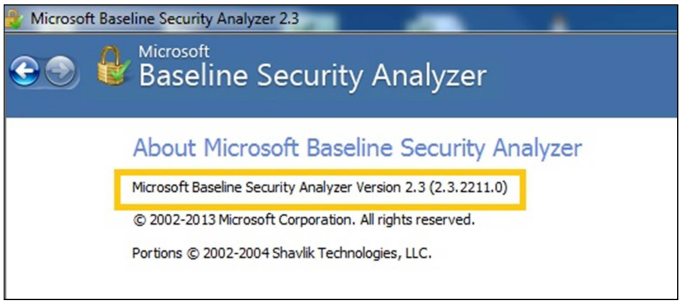
Fonte: Autoria própria (2016)

Após a instalação ser sido realizada, o acesso do MBSA pode acontecer pelo ícone criado na área de trabalho ou acessando o menu de *programas e arquivos* do

Windows. A recomendação da *Microsoft* ® é que seja executada a versão 2.3 do MBSA, por ser a mais recente, lançada em janeiro de 2015.

Para isto, basta verificar a seção "*About Microsoft Baseline Security Analyzer*", no campo superior esquerdo da tela inicial, que disponibiliza essa informação:

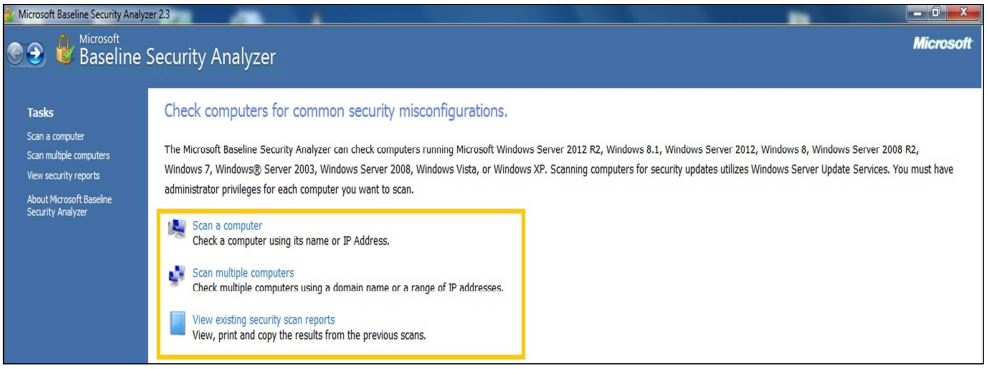
Figura 19 - Verificação da versão instalada



Fonte: Autoria própria (2016)

Na página inicial da ferramenta, como é demonstrado na figura abaixo, existem 3 funções principais:

Figura 20 - Funcionalidades do MBSA



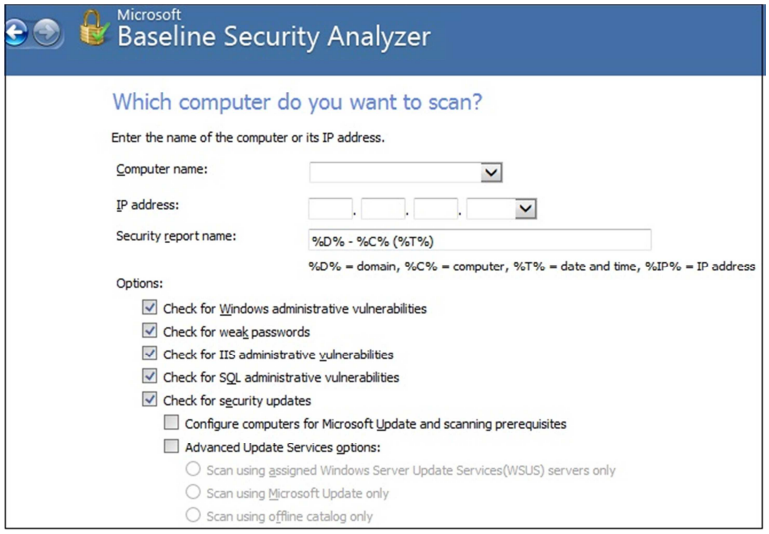
Fonte: Autoria própria (2016)

Onde:

1) *Scan a computer*: Onde as vulnerabilidades são verificadas por uma varredura em apenas um computador, seja através do seu nome ou endereço

de IP (Internet Protocol). Por padrão, o computador onde o MBSA está sendo executado será o mesmo a receber a varredura, porém é possível alterar para o que desejar.

Figura 21 - Janela de varredura de um computador



Fonte: Autoria própria (2016)

Após a escolha do computador, a ferramenta oferece opções que podem ser ativadas ou não, do que a varredura irá buscar:

- ***Check for Windows administrative vulnerabilities*** **(Verificar vulnerabilidades administrativas do Windows)**: Esta opção irá verificar o tipo do sistema de arquivos e quais deles estão sendo compartilhados. Permite a identificação de quais usuários têm permissão de “Administrador” da máquina, e por fim, o status da conta “Convidado” do computador.

- ***Check for weak passwords (*****Verificar a existência de senhas fracas):** Esta opção busca, sobretudo, senhas consideradas fracas ou a existência de senhas no computador. O tempo desta verificação varia de acordo com a quantidade de contas de usuários.

- ***Check for Internet Information Services (IIS) administrative vulnerabilities*** **(Verificar vulnerabilidades administrativas do IIS)** – Esta opção preocupa-se com segurança relacionada ao IIS, sejam aplicativos ou diretórios virtuais do computador. Por ser voltada a servidores, a ferramenta informa se o bloqueio do IIS foi executado no computador, à fim de facilitar na configuração e proteção destes.

- ***Check for SQL administrative vulnerabilities*** **(Verifica vulnerabilidades administrativas do SQL):** Busca vulnerabilidades do *SQL Server* e *Microsoft Data Engine* (MSDE), como por exemplo, o modo de autenticação e as associações de conta de serviço.

- ***Check for security updates/ missing updates*** (**Verificar se há atualizações de segurança/ atualizações em falta):** Realiza a busca de atualizações e *service packs* tanto para clientes gerenciados pelo *Microsoft Update* como por aqueles gerenciados pelo *Windows Server Update Service* (WSUS). O MBSA baseia-se em um catálogo *off-line* atualizado frequentemente pela *Microsoft* ® que é utilizado para verificar as atualizações de segurança.

    - ***Configure computers for Microsoft Update and scanning prerequisites*** **(computadores configurados para atualização e digitalização pré-requisitos da Microsoft):** Esta opção vem desativada. Se por optar por selecioná-la, o MBSA irá instalar ou atualizar de forma automática o agente do *Windows Update* (WUA) para uma varredura de atualização de segurança bem sucedida. Ao manter essa opção não selecionada, o processo de varredura não irá alterar a configuração do computador, mas em alguns casos, o computador não será verificado até que o agente do *Windows Update* esteja atualizado.

    - ***Advanced Update Services options:***

        - ***Scan using assigned Windows Update Services servers only*** **(Digitalizar utilizando apenas os servidores Windows Update Services atribuídos):** Ao selecionar esta opção, os

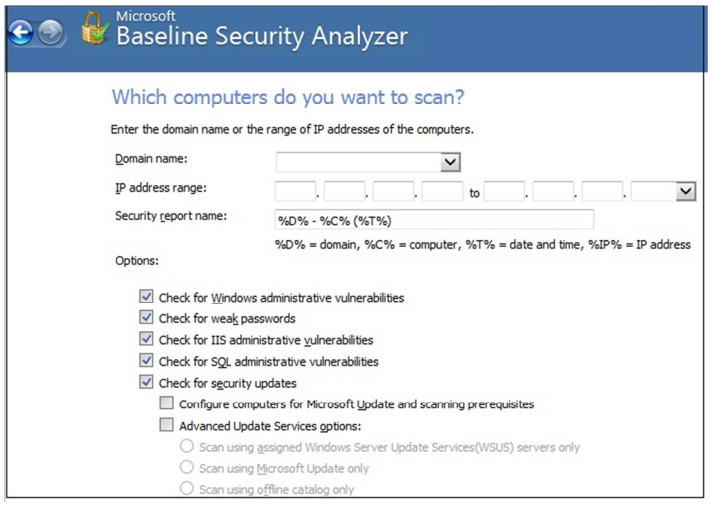
clientes não relacionados à um servidor WSUS receberão uma mensagem de erro informando que não pôde ser verificado. Dessa maneira, apenas os computadores gerenciados e atribuídos pelo WSUS serão incluídos.

- ***Scan using Microsoft Update only* (Digitalizar utilizando apenas Microsoft Update):** Ao selecionar esta opção, serão avaliadas as atualizações mediante ao *Microsoft Update* ou catálogo *off-line*. Serão ignoradas computadores atribuídos à um servidor WSUS.

- ***Scan using offline catalog only* (Digitalizar utilizando apenas catálogo *off-line*):** Serão descartadas as opções anteriores, levando em conta somente o catálogo *off-line*, quando este por sua vez, estiver disponível.

2) *Scan multiple computers:* Permite a varredura em múltiplos computadores em uma rede local, por um nome de domínio ou range de endereços IP. Também possui algumas opções que podem ser escolhidas antes iniciar a varredura. Estas opções são as mesmas detalhadas na função anterior.

Figura 22 - Janela de varredura de múltiplos computadores

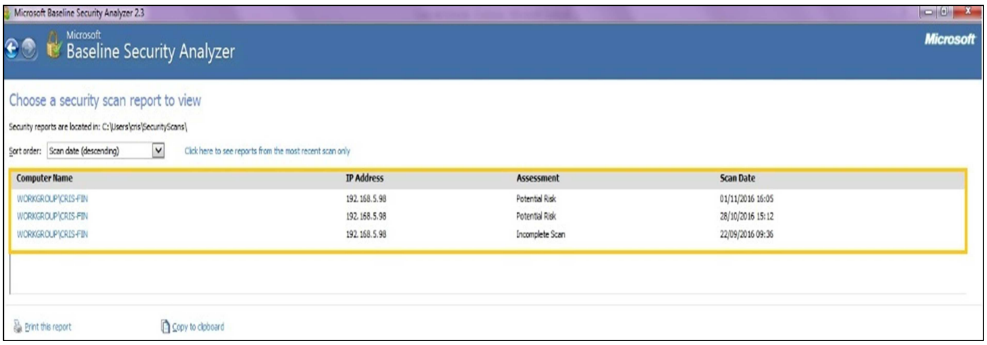


Fonte: Autoria própria (2016)

3) *View existing security scan reports:* Onde permite a visualização, impressão e cópia do histórico de varreduras já realizadas na máquina em que a ferramenta está sendo executada. É composto pelo nome e IP do computador em que a varredura foi realizada, o tipo de avaliação, além da data e hora de execução.

Destacando que, caso nenhuma varredura tenha sido realizada, não se torna possível realizar esta visualização.

Figura 23 - Histórico de varreduras já realizadas



Fonte: Autoria própria (2016)

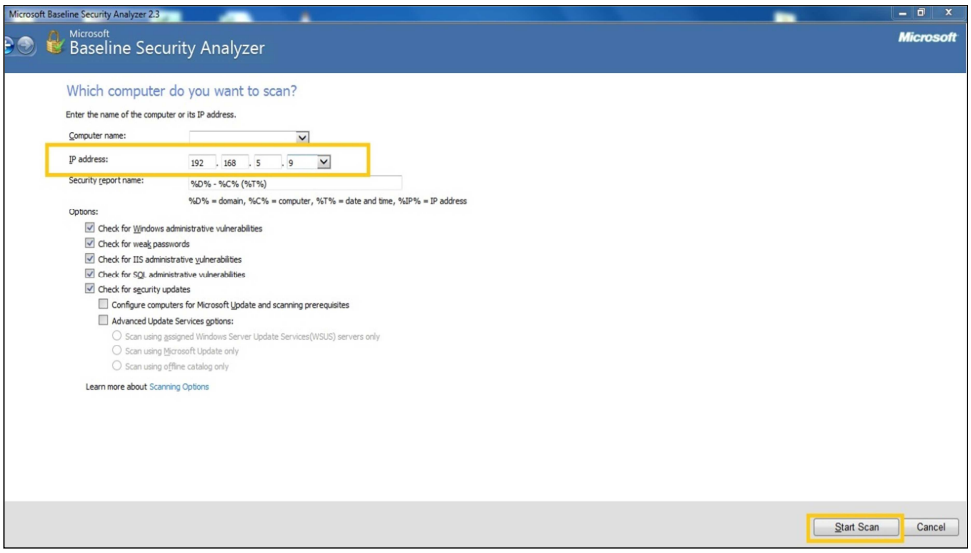
5.2.3 Executando o MBSA no ambiente

Após a instalação da ferramenta e suas respectivas configurações terem sido realizadas, já se torna possível realizar a varredura no ambiente.

A primeira máquina em que foi executada a varredura foi o *notebook* de suporte utilizado pela equipe de TI. Neste caso, a primeira opção de varredura foi escolhida (apenas um computador).

O campo IP pode ser preenchido, mas por default da ferramenta, ela executará na máquina em que está sendo utilizada. Como a figura 24 demonstra, basta clicar em *"Start Scan*":

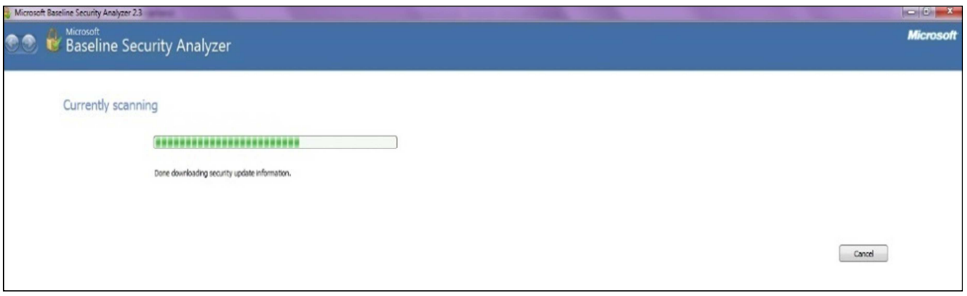
Figura 24 - Varredura do notebook de suporte de TI



Fonte: Autoria própria (2016)

Será realizado o *download* das informações de atualizações:

Figura 25 - Janela de download de atualizações

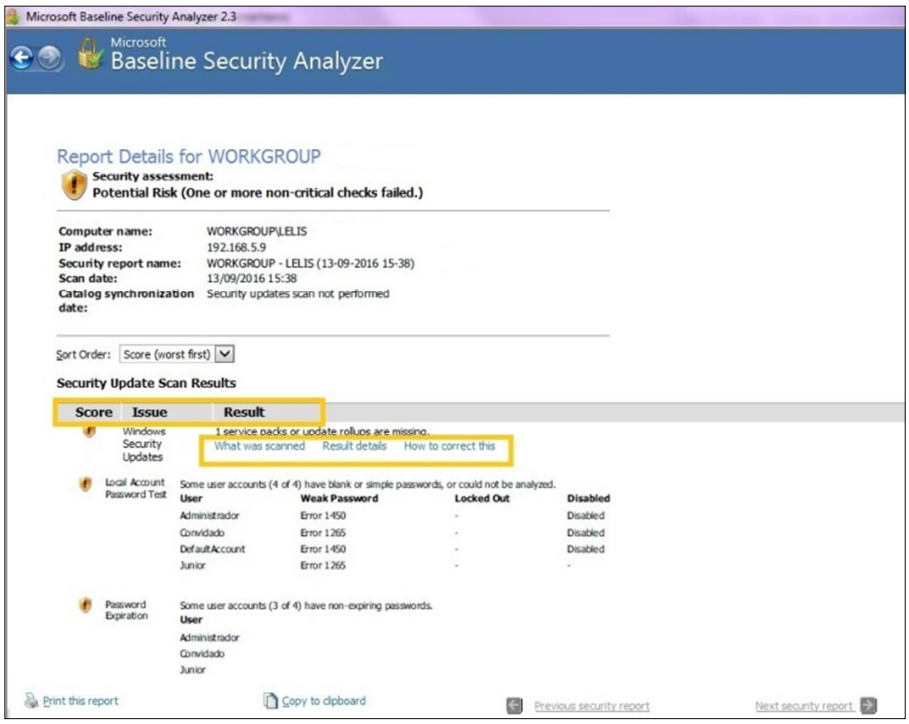


Fonte: Autoria própria (2016)

Após o término da varredura, será carregada a janela conforme figura 26. Ela contém o relatório completo do que foi coletado na máquina em questão. Todos os relatórios executados no MBSA são armazenados na pasta *Security Scans* do perfil do usuário.

Arquivos de relatório são nomeados com a extensão de arquivo .MBSA, que poderão ser visualizados no *Windows Explorer.*

Figura 26 - Relatório da varredura no notebook de suporte técnico



Fonte: Autoria própria (2016)

Os itens destacados na imagem são de identificação para o relatório:

- ***Score:*** diferencia os status das varreduras por meio de ícones;
- ***Issue:*** apresenta o assunto que foi verificado;
- ***Result:*** fornece o que foi encontrado por meio da varredura. Neste item, são demonstradas outras três seções:

    - ***What was scanned:*** descreve a varredura por completo;
    - ***Result details:*** detalha o resultado da varredura;

- ***How to correct this:*** apresenta sugestões e orientações de como corrigir o problema encontrado na varredura.

Algumas varreduras retornam esta última opção no lugar de simplesmente gerar um risco ou potencial de falha, indicado por um ícone azul. Geralmente, incluem as atualizações incompletas e configurações do *firewall* do *Windows*.

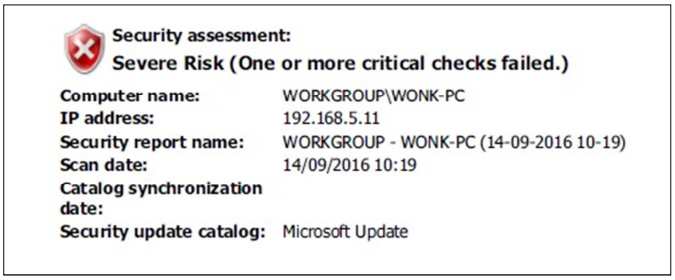
Em *"Print this report"* é possível imprimir ou salvar o relatório para análise posterior, enquanto em *"Copy to clipboard"* é possível copiar o arquivo para transferi-lo para o formato de arquivo aceito pelas ferramentas do *Microsoft Office.*

No cabeçalho do relatório, constam tais informações:

- Nome do computador;
- Endereço de IP;
- Nome do relatório de segurança;
- Data da digitalização;
- Data de sincronização do catálogo;
- Catálogo de atualizações de segurança.

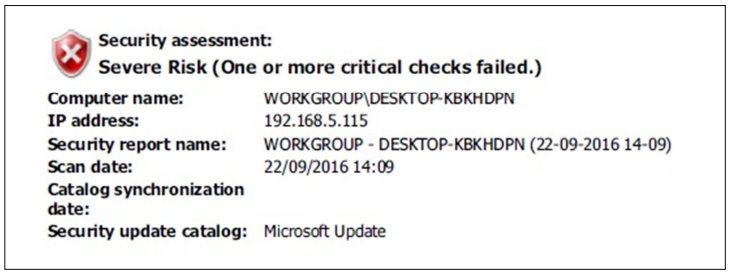
Os demais relatórios deste estudo de caso, conforme demonstrados pelos cabeçalhos abaixo, foram realizados na seguinte ordem cronológica:

Figura 27 - Desktop do setor Faturamento



Fonte: Autoria própria (2016)

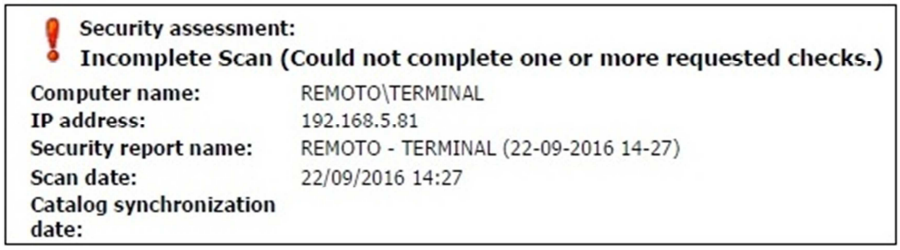
Figura 28 – Desktop do setor Contabilidade



Fonte: Autoria própria (2016)

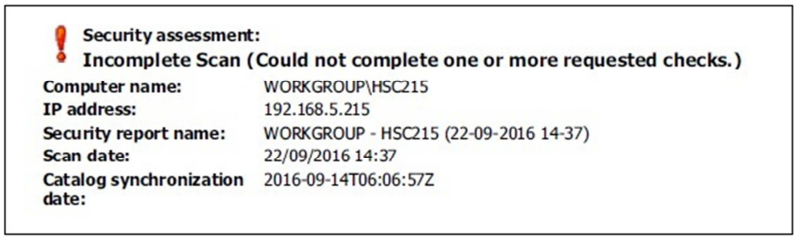
Os dois relatórios abaixo, como demonstram os cabeçalhos das figuras 29 e 30, tiveram varredura incompleta, pois devido a um problema com conexão à internet, não realizaram acesso a todas as atualizações disponíveis do *Microsoft Update.*

Figura 29 – Desktop de acesso remoto do setor de TI



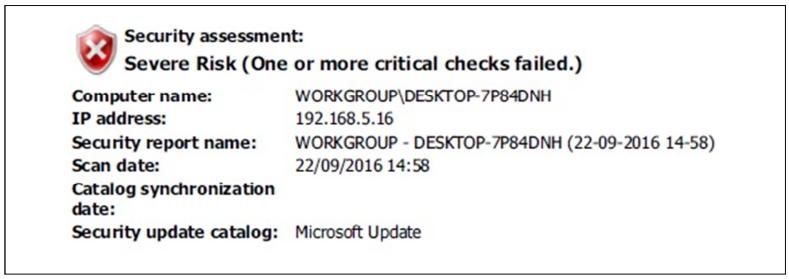
Fonte: Autoria própria (2016)

Figura 30 - Desktop de backup do servidor do setor de TI



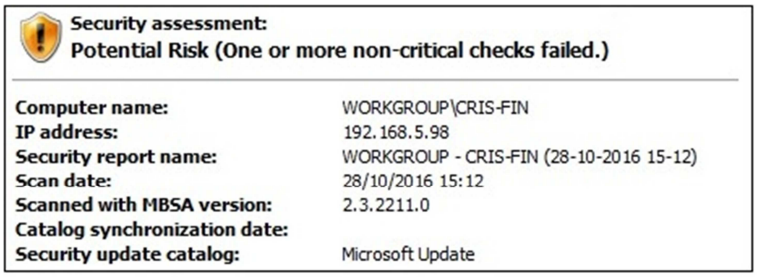
Fonte: Autoria própria (2016)

Figura 31 - Desktop de suporte técnico do setor de TI



Fonte: Autoria própria (2016)

Figura 32 - Desktop do setor Financeiro



Fonte: Autoria própria (2016)

Todos os relatórios seguem esta mesma estrutura, diferenciando-os apenas pelos resultados, devido às atualizações e configurações serem divergentes em cada máquina. Com o conjunto dos relatórios, é possível realizar comparações, na busca de identificar e corrigir as vulnerabilidades presentes em seus sistemas.

5.3 Diagnóstico

Foram retirados os principais fragmentos dos relatórios, em ordem cronológica de execução, visando melhor aproveitamento e visualização dos resultados:

- **Notebook suporte de TI**

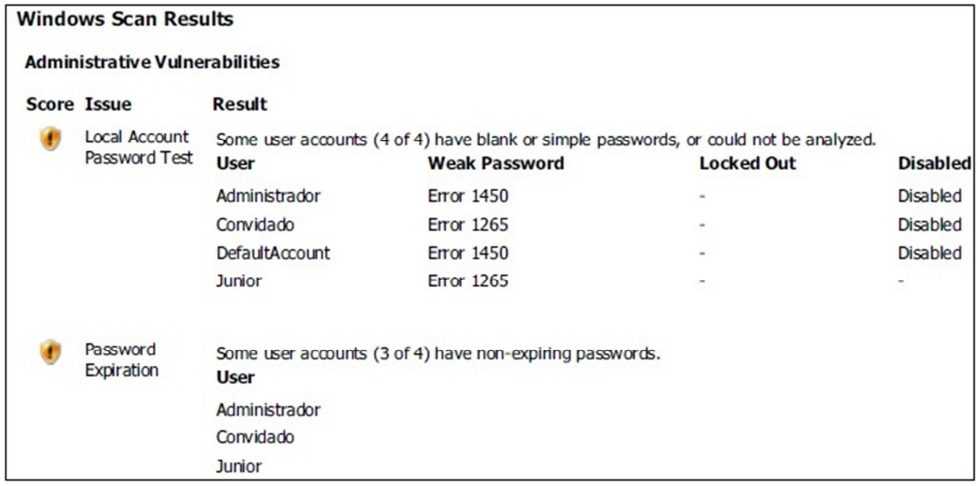
O primeiro trecho relevante do relatório do *notebook* de suporte de TI diz respeito às vulnerabilidades administrativas relacionadas a senhas.

Nos testes de senha em conta local, foram encontrados 4 usuários, que possuem senhas simples, em branco, ou que não puderam ser analisadas:

- Administrador;
- Convidado;
- DefaultAccount;
- Junior.

O erro 1265 diz respeito a danos que podem ser causados no arquivo de sistemas do *Windows*, enquanto o erro 1450 é relacionado à exposição a vírus e malware. Além disso, três dessas contas possuem senhas que nunca expiram.

Figura 33 - Vulnerabilidades administrativas notebook de suporte



Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (4 of 4) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Administrador	Error 1450	-	Disabled
Convidado	Error 1265	-	Disabled
DefaultAccount	Error 1450	-	Disabled
Junior	Error 1265	-	-

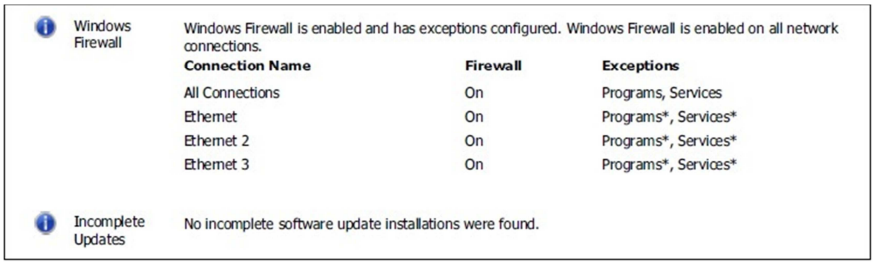
Score	Issue	Result
	Password Expiration	Some user accounts (3 of 4) have non-expiring passwords.

User
Administrador
Convidado
Junior

Fonte: Autoria própria (2016)

O *firewall* do *Windows* está habilitado para todas as conexões de rede, com exceções configuradas a alguns programas e serviços:

Figura 34 - Firewall do Windows notebook de suporte



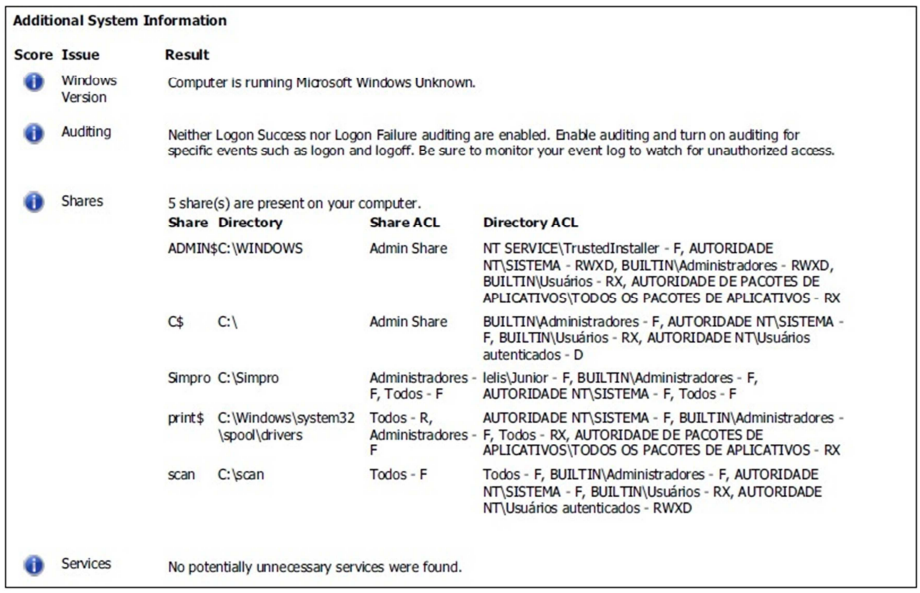
Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.		
	Connection Name	**Firewall**	**Exceptions**
	All Connections	On	Programs, Services
	Ethernet	On	Programs*, Services*
	Ethernet 2	On	Programs*, Services*
	Ethernet 3	On	Programs*, Services*
Incomplete Updates	No incomplete software update installations were found.		

Fonte: Autoria própria (2016)

Em informações adicionais do sistema, foram encontrados problemas como:

- A versão do *Windows* não foi identificada;
- Em dois dos compartilhamentos de diretório (administradores do *Windows* e da área de digitalização do setor), os usuários possuem permissão total de leitura, escrita, execução e deleção (RWXD – *Read, Write, Execute, Delete*).

Figura 35 - Informações adicionais notebook de suporte



Additional System Information

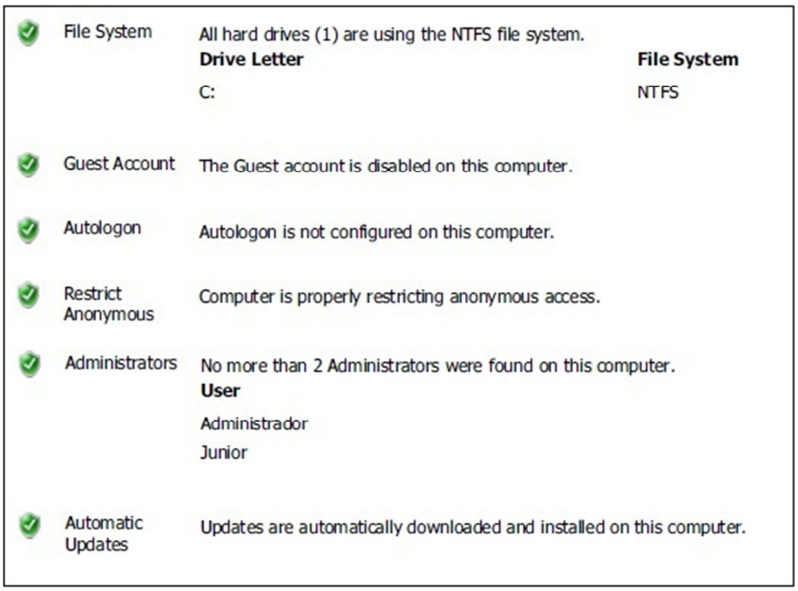
Score	Issue	Result			
	Windows Version	Computer is running Microsoft Windows Unknown.			
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.			
	Shares	5 share(s) are present on your computer.			
		Share	**Directory**	**Share ACL**	**Directory ACL**
		ADMIN$	C:\WINDOWS	Admin Share	NT SERVICE\TrustedInstaller - F, AUTORIDADE NT\SISTEMA - RWXD, BUILTIN\Administradores - RWXD, BUILTIN\Usuários - RX, AUTORIDADE DE PACOTES DE APLICATIVOS\TODOS OS PACOTES DE APLICATIVOS - RX
		C$	C:\	Admin Share	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - D
		Simpro	C:\Simpro	Administradores - F, Todos - F	Ielis\Junior - F, BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, Todos - F
		print$	C:\Windows\system32\spool\drivers	Todos - R, Administradores - F	AUTORIDADE NT\SISTEMA - F, BUILTIN\Administradores - F, Todos - RX, AUTORIDADE DE PACOTES DE APLICATIVOS\TODOS OS PACOTES DE APLICATIVOS - RX
		scan	C:\scan	Todos - F	Todos - F, BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - RWXD
	Services	No potentially unnecessary services were found.			

Fonte: Autoria própria (2016)

Entre as opções marcadas como classificadas, constam que:

- O disco rígido está utilizando o sistema de arquivo NTFS (*New Technology File System*);
- A conta de usuário “Convidado” está desativada;
- O autologon não está configurado;
- O computador restringe corretamente o acesso anônimo;
- Como segue a recomendação da *Microsoft* ®, não foram encontrados mais de dois usuários administradores na máquina, sendo estes: “Administrador” e “Junior”;
- As atualizações são baixadas e instaladas automaticamente;

Figura 36 - Opções aprovadas notebook de suporte



Fonte: Autoria própria (2016)

- ***Desktop* Faturamento**

O fragmento demonstrado a seguir, retirado do relatório obtido do desktop do setor faturamento, é relacionado a problemas de atualizações de segurança do *Microsoft Office*. Durante a varredura, seis atualizações foram perdidas, incluindo também *Microsoft Office Outlook, PowerPoint* e *Excel*.

Figura 37 - Atualizações Microsoft Office *desktop* faturamento

Security Updates

Score	Issue	Result
	Office Security Updates	6 security updates are missing.

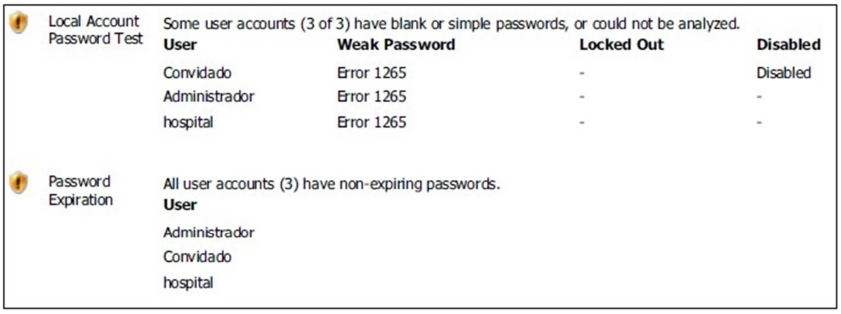
Security Updates

Score	ID	Description	Maximum Severity
Missing	MS16-107	Security Update for Microsoft Office 2010 (KB2553432) 32-Bit Edition	Critical
Missing	MS16-107	Security Update for Microsoft Office 2010 (KB3118309) 32-Bit Edition	Critical
Missing	MS16-107	Security Update for Microsoft Outlook 2010 (KB3118313) 32-Bit Edition	Important
Missing	MS16-107	Security Update for Microsoft PowerPoint 2010 (KB3115467) 32-Bit Edition	Important
Missing	MS16-107	Security Update for Microsoft Excel 2010 (KB3118316) 32-Bit Edition	Important
Missing	MS16-107	Security Update for Microsoft Office 2007 suites (KB3118300)	Critical

Fonte: Autoria própria (2016)

O resultado da varredura relacionado a vulnerabilidades administrativas demonstrou que os três usuários existentes na máquina (Convidado, Administrador e Hospital), possuem vulnerabilidades em suas senhas e, além disso, estas nunca expiram.

Figura 38 - Vulnerabilidades administrativas *desktop* faturamento



Local Account Password Test — Some user accounts (3 of 3) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Convidado	Error 1265	-	Disabled
Administrador	Error 1265	-	-
hospital	Error 1265	-	-

Password Expiration — All user accounts (3) have non-expiring passwords.

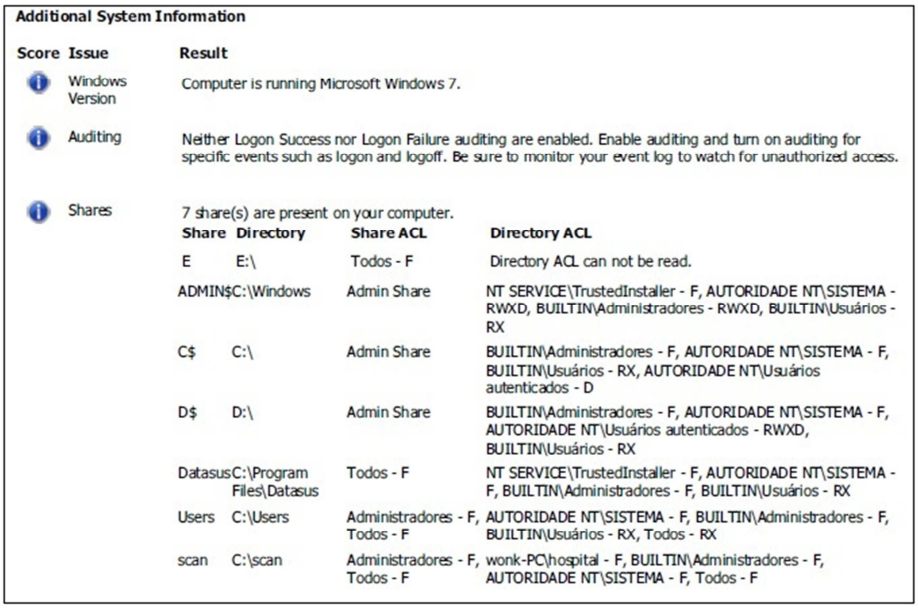
User
Administrador
Convidado
hospital

Fonte: Autoria própria (2016)

O MBSA identificou o *Microsoft Windows* 7 como o sistema operacional instalado.

Na área de compartilhamento de arquivos no diretório D:\, onde estão contidas todas as notas fiscais de venda e serviços emitidas tanto pelo hospital como tomador ou prestador, nos últimos 12 meses, os usuários que se autenticarem irão possuir permissão total de leitura, escrita, execução e deleção (RWXD – *Read, Write, Execute, Delete).*

Figura 39 - Informações adicionais *desktop* faturamento



Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 7.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	7 share(s) are present on your computer.

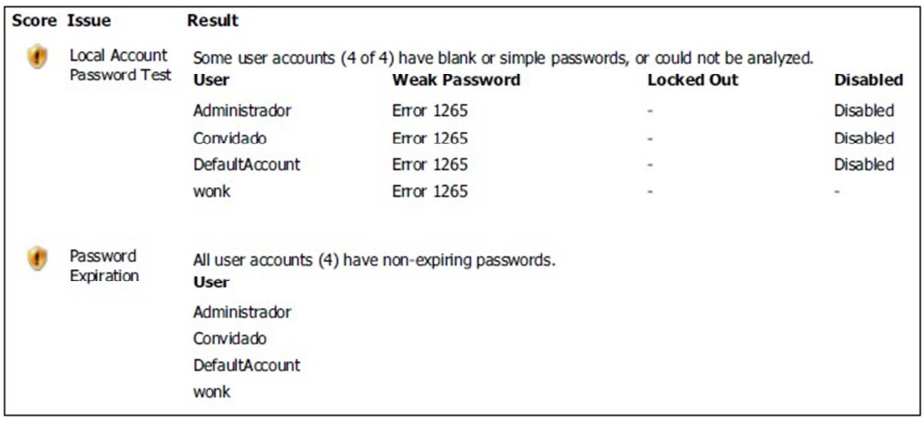
Share	Directory	Share ACL	Directory ACL
E	E:\	Todos - F	Directory ACL can not be read.
ADMIN$	C:\Windows	Admin Share	NT SERVICE\TrustedInstaller - F, AUTORIDADE NT\SISTEMA - RWXD, BUILTIN\Administradores - RWXD, BUILTIN\Usuários - RX
C$	C:\	Admin Share	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - D
D$	D:\	Admin Share	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, AUTORIDADE NT\Usuários autenticados - RWXD, BUILTIN\Usuários - RX
Datasus	C:\Program Files\Datasus	Todos - F	NT SERVICE\TrustedInstaller - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Administradores - F, BUILTIN\Usuários - RX
Users	C:\Users	Administradores - F, Todos - F	AUTORIDADE NT\SISTEMA - F, BUILTIN\Administradores - F, BUILTIN\Usuários - RX, Todos - RX
scan	C:\scan	Administradores - F, Todos - F	wonk-PC\hospital - F, BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, Todos - F

Fonte: Autoria própria (2016)

- ***Desktop* Contabilidade**

Através do relatório do desktop da contabilidade, foi possível coletar que os quatro usuários existentes não possuem senhas ou estas estão em branco, porém somente o usuário “Wonk” está ativo neste computador.

Figura 40 - Vulnerabilidades administrativas desktop contabilidade



Score	Issue	Result
	Local Account Password Test	Some user accounts (4 of 4) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Administrador	Error 1265	-	Disabled
Convidado	Error 1265	-	Disabled
DefaultAccount	Error 1265	-	Disabled
wonk	Error 1265	-	-

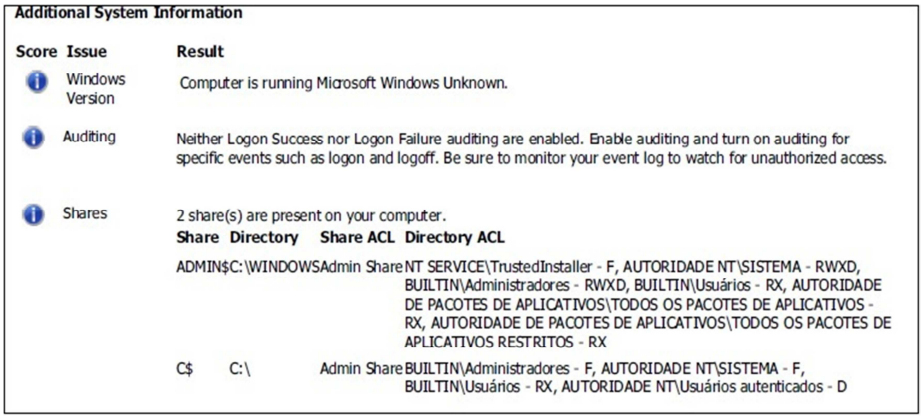
Score	Issue	Result
	Password Expiration	All user accounts (4) have non-expiring passwords.

User
Administrador
Convidado
DefaultAccount
wonk

Fonte: Autoria própria (2016)

Nos diretórios de compartilhamento, todos os usuários estão com acesso e permissão total.

Figura 41 - Informações adicionais desktop contabilidade



Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows Unknown.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	2 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\WINDOWS	Admin Share	NT SERVICE\TrustedInstaller - F, AUTORIDADE NT\SISTEMA - RWXD, BUILTIN\Administradores - RWXD, BUILTIN\Usuários - RX, AUTORIDADE DE PACOTES DE APLICATIVOS\TODOS OS PACOTES DE APLICATIVOS - RX, AUTORIDADE DE PACOTES DE APLICATIVOS\TODOS OS PACOTES DE APLICATIVOS RESTRITOS - RX
C$	C:\	Admin Share	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - D

Fonte: Autoria própria (2016)

- **Terminal remoto**

Durante a varredura na máquina que oferece acesso remoto a computadores de outras unidades da mesma rede hospitalar, foram identificados 20 usuários.

Os principais serviços utilizados via este tipo de acesso são:

- Os fornecidos pela máquina da farmácia, para realização de entrada e saída de insumos e medicamentos em seu estoque;
- Da máquina de suporte, para manutenção do banco de dados, visto que o sistema de gerenciamento hospitalar não é o mesmo em todas as unidades.

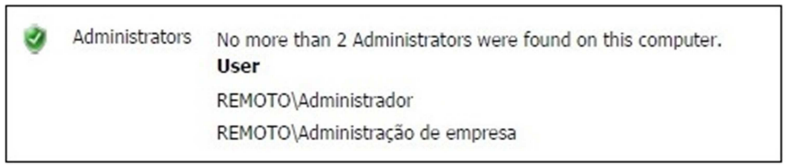
Deste total, 17 usuários possuem a vulnerabilidade de segurança da informação em que senhas estão configuradas para nunca expirar.

Figura 42 - Vulnerabilidades administrativas terminal remoto

Fonte: Autoria própria (2016)

Apesar disso, não existem mais que 2 administradores nesta máquina.

Figura 43 - Recomendação Microsoft terminal remoto



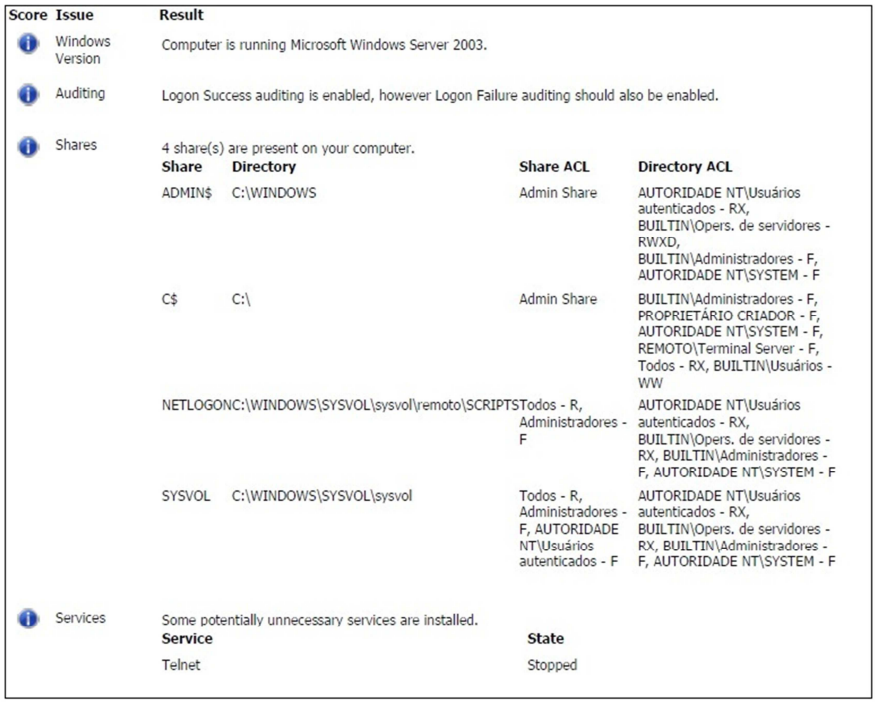
Fonte: Autoria própria (2016)

A ferramenta identificou o *Microsoft Windows Server* 2003 como o sistema operacional instalado.

No diretório de compartilhamento NETLOGON, os usuários possuem permissão de leitura e execução dos scripts para realizar o acesso remoto.

O serviço *Telnet,* apesar de estar no status “parado”, está instalado de maneira desnecessária no computador.

Figura 44 - Informações adicionais terminal remoto

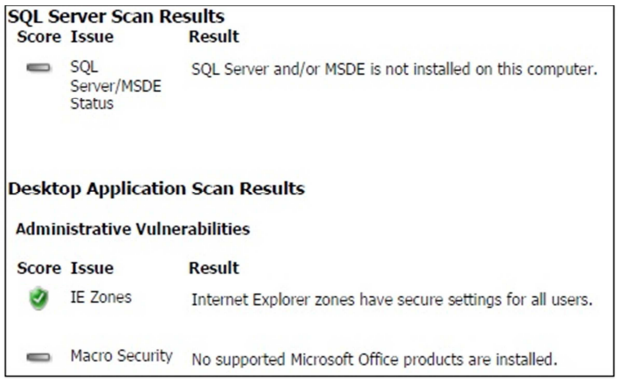


Score	Issue	Result			
	Windows Version	Computer is running Microsoft Windows Server 2003.			
	Auditing	Logon Success auditing is enabled, however Logon Failure auditing should also be enabled.			
	Shares	4 share(s) are present on your computer.			
		Share	**Directory**	**Share ACL**	**Directory ACL**
		ADMIN$	C:\WINDOWS	Admin Share	AUTORIDADE NT\Usuários autenticados - RX, BUILTIN\Opers. de servidores - RWXD, BUILTIN\Administradores - F, AUTORIDADE NT\SYSTEM - F
		C$	C:\	Admin Share	BUILTIN\Administradores - F, PROPRIETÁRIO CRIADOR - F, AUTORIDADE NT\SYSTEM - F, REMOTO\Terminal Server - F, Todos - RX, BUILTIN\Usuários - WW
		NETLOGON	C:\WINDOWS\SYSVOL\sysvol\remoto\SCRIPTS	Todos - R, Administradores - F	AUTORIDADE NT\Usuários autenticados - RX, BUILTIN\Opers. de servidores - RX, BUILTIN\Administradores - F, AUTORIDADE NT\SYSTEM - F
		SYSVOL	C:\WINDOWS\SYSVOL\sysvol	Todos - R, Administradores - F, AUTORIDADE NT\Usuários autenticados - F	AUTORIDADE NT\Usuários autenticados - RX, BUILTIN\Opers. de servidores - RX, BUILTIN\Administradores - F, AUTORIDADE NT\SYSTEM - F
	Services	Some potentially unnecessary services are installed.			
		Service		**State**	
		Telnet		Stopped	

Fonte: Autoria própria (2016)

Por fim, as zonas de segurança e as configurações do IE (Internet Explorer) têm definições seguras para todos os usuários, fornecendo maior controle de *cookies* e registros.

Figura 45 - IE Zones terminal remoto



SQL Server Scan Results

Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones have secure settings for all users.
	Macro Security	No supported Microsoft Office products are installed.

Fonte: Autoria própria (2016)

- **Máquina *Backup***

Na varredura da máquina de backup do servidor, onde são armazenadas as cópias de restaurações do banco de dados e de sistemas internos, foram coletadas as seguintes informações:

- Os usuários “Administrador” e “Convidado” possuem senha fraca, enquanto o usuário “Serv” não possui senha;
- A conta de convidado não está desativada neste computador;
- As senhas de usuário nunca expiram;
- A funcionalidade de atualização automática está desativada;
- O *firewall* do *Windows* está desativado;
- Foi identificado o sistema de arquivos NTFS;
- O autologon não está configurado.

Figura 46 - Vulnerabilidades administrativas desktop servidor

Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (2 of 3) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Administrador	Weak	-	Disabled
Convidado	Weak	-	-
Serv	-	-	-

	Guest Account	The Guest account is not disabled on this computer.
	Password Expiration	All user accounts (3) have non-expiring passwords.

User
Administrador
Convidado
Serv

	Automatic Updates	The Automatic Updates feature is disabled on this computer.
	Windows Firewall	Windows Firewall is disabled and has exceptions configured.

Connection Name	Firewall	Exceptions
All Connections	Off	Ports, Programs, Services
Conexão local	Off*	Ports*, Programs*, Services*

	Incomplete Updates	No incomplete software update installations were found.
	File System	All hard drives (1) are using the NTFS file system.

Drive Letter	File System
C:	NTFS

	Autologon	Autologon is not configured on this computer.

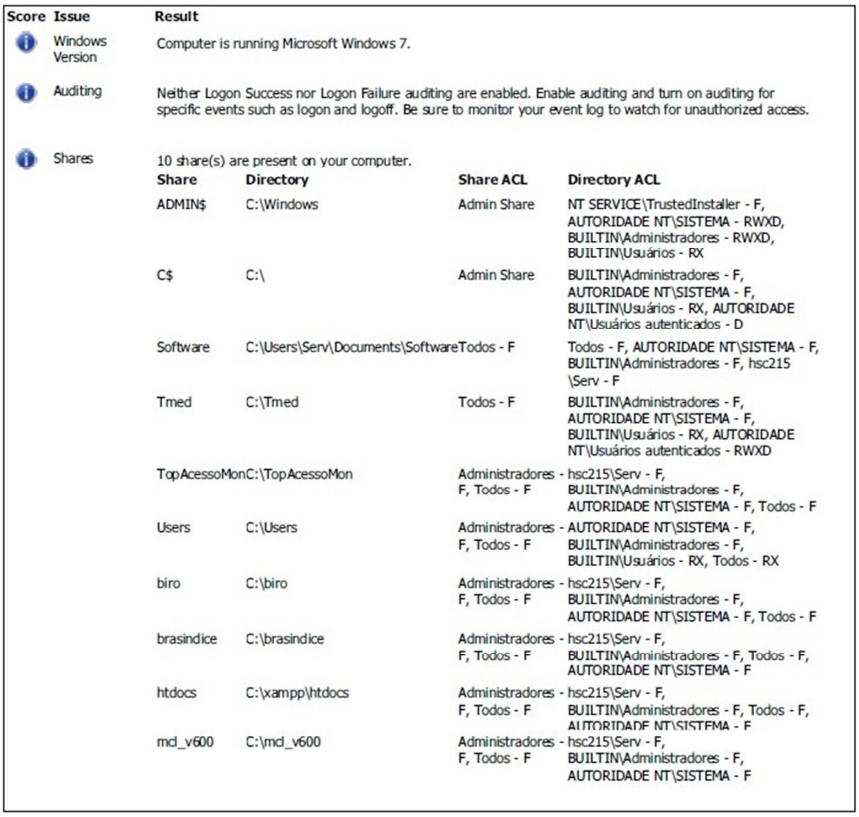
Fonte: Autoria própria (2016)

Foi identificada a versão *Microsoft Windows* 7 como sistema operacional no computador.

Por obter função da disponibilização de serviços a outras máquinas, foram identificados 10 compartilhamentos de diretórios:

1) **C:\Windows:**
   Compartilhamento de arquivos do Windows;
2) **C:\:**
   Compartilhamento da pasta raiz;
3) **C:\Users\Serv\Documents\SoftwareTODOS – F:**
   Compartilhamento de softwares que possuem instalação autorizada à todos os setores;
4) **C:\Tmed:**
   Permite acesso ao módulo de Tecnologia Médica;
5) **C:\TopAcessoMon:**
   Acesso ao sistema de monitoramento;
6) **C:\Users:**
   Compartilhamento da pasta Usuários;
7) **C:\biro:**
   Acesso ao sistema utilizado pelo setor de RH;
8) **C:\brasindice:**
   Acesso ao sistema utilizado pelos setores de farmácia e almoxarifado relacionamento a descrição de medicamentos e sua especificação, como preços e impostos;
9) **C:\xampp\htdocs:**
   Acesso e gerenciamento do banco de dados;
10) **C:\mcl_v600:**
    Diretório relacionado a licenças HTML.

Figura 47 - Informações adicionais *desktop* servidor



Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 7.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	10 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\Windows	Admin Share	NT SERVICE\TrustedInstaller - F, AUTORIDADE NT\SISTEMA - RWXD, BUILTIN\Administradores - RWXD, BUILTIN\Usuários - RX
C$	C:\	Admin Share	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - D
Software	C:\Users\Serv\Documents\Software	Todos - F	Todos - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Administradores - F, hsc215 \Serv - F
Tmed	C:\Tmed	Todos - F	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - RWXD
TopAcessoMon	C:\TopAcessoMon	Administradores - F, Todos - F	hsc215\Serv - F, BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, Todos - F
Users	C:\Users	Administradores - F, Todos - F	AUTORIDADE NT\SISTEMA - F, BUILTIN\Administradores - F, BUILTIN\Usuários - RX, Todos - RX
biro	C:\biro	Administradores - F, Todos - F	hsc215\Serv - F, BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, Todos - F
brasindice	C:\brasindice	Administradores - F, Todos - F	hsc215\Serv - F, BUILTIN\Administradores - F, Todos - F, AUTORIDADE NT\SISTEMA - F
htdocs	C:\xampp\htdocs	Administradores - F, Todos - F	hsc215\Serv - F, BUILTIN\Administradores - F, Todos - F, AUTORIDADE NT\SISTEMA - F
mcl_v600	C:\mcl_v600	Administradores - F, Todos - F	hsc215\Serv - F, BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F

Fonte: Autoria própria (2016)

- ***Desktop* de suporte**

No *desktop* de suporte técnico, utilizado sobretudo, para resolução de problemas no sistema de gerenciamento hospitalar, houve um bom agradável após a varredura, pois nenhuma atualização de segurança foi perdida, sendo possível assim, analisar a importância de cada uma por meio de seu grau de criticidade.

Figura 48 - Atualizações de segurança *desktop* de suporte

Security Updates

Score	Issue	Result			
	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing.			
		Current Update Compliance			
		Score	ID	Description	Maximum Severity
		Installed	MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Important
	Office Security Updates	No security updates are missing.			
		Current Update Compliance			
		Score	ID	Description	Maximum Severity
		Installed	MS15-081	Security Update for Microsoft Office 2013 (KB3039798) 64-Bit Edition	Critical
		Installed	MS16-107	Security Update for Microsoft Office 2013 (KB3118268) 64-Bit Edition	Critical
		Installed	MS16-107	Security Update for Microsoft Outlook 2013 (KB3118280) 64-Bit Edition	Important
		Installed	MS16-099	Security Update for Microsoft OneNote 2013 (KB3115256) 64-Bit Edition	Important
		Installed	MS16-107	Security Update for Microsoft Excel 2013 (KB3118284) 64-Bit Edition	Important
		Installed	MS15-013	Security Update for Microsoft Office 2013 (KB2910941) 64-Bit Edition	Important
		Installed	MS15-116	Security Update for Microsoft Publisher 2013 (KB3085561) 64-Bit Edition	Important
		Installed	MS16-099	Security Update for Microsoft Office 2013 (KB3114340) 64-Bit Edition	Important
		Installed	2850036	Service Pack 1 for Microsoft Office 2013 (KB2850036) 64-Bit Edition	
		Installed	MS15-081	Security Update for Microsoft Office 2013 (KB3054816) 64-Bit Edition	Important
		Installed	MS16-107	Security Update for Microsoft PowerPoint 2013 (KB3115487) 64-Bit Edition	Important
	SQL Server Security Updates	No security updates are missing.			
		Current Update Compliance			
		Score	ID	Description	Maximum Severity
		Installed	MS06-061	MSXML 6.0 RTM Security Update (925673)	Critical

Fonte: Autoria própria (2016)

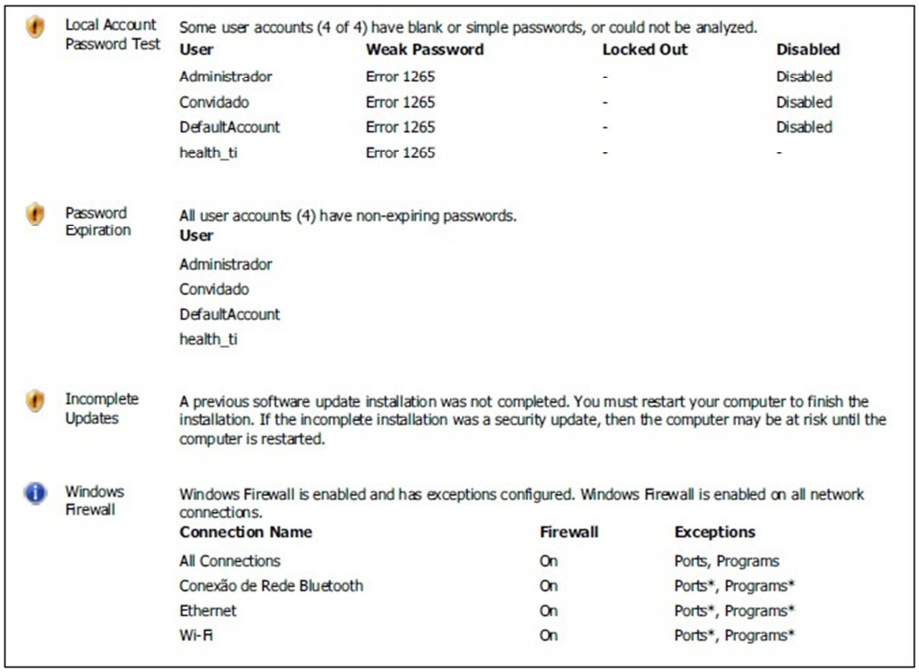
Nos testes de senha em conta local, foram encontrados 4 usuários, que possuem senhas simples, em branco, ou que não puderam ser analisadas:

- Administrador;
- Convidado;
- DefaultAccount;
- Health_ti.

O último usuário é o único ativo no computador, que diz respeito ao analista de suporte da equipe de TI. Além disso, todas as contas possuem senhas que nunca expiram.

O *firewall* do *Windows* encontra-se ativo para todas as conexões, sejam de rede Bluetooth, Cabeada ou sem fio.

Figura 49 - Vulnerabilidades administrativas desktop de suporte



Local Account Password Test

Some user accounts (4 of 4) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Administrador	Error 1265	-	Disabled
Convidado	Error 1265	-	Disabled
DefaultAccount	Error 1265	-	Disabled
health_ti	Error 1265	-	-

Password Expiration

All user accounts (4) have non-expiring passwords.

User
Administrador
Convidado
DefaultAccount
health_ti

Incomplete Updates

A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted.

Windows Firewall

Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.

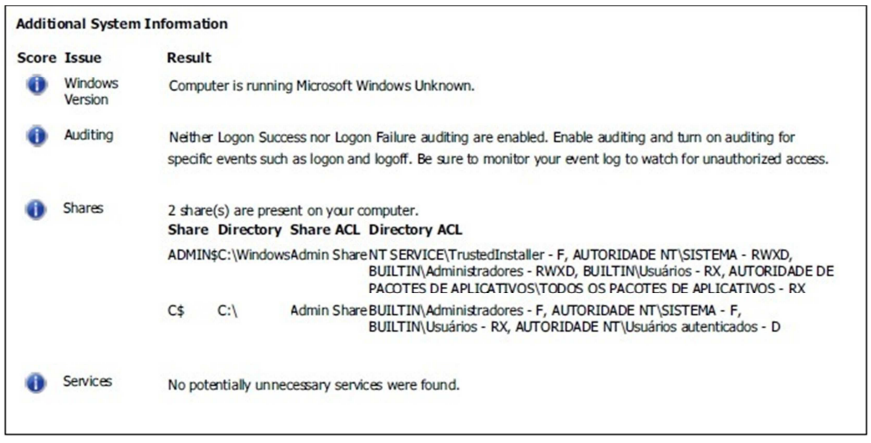
Connection Name	Firewall	Exceptions
All Connections	On	Ports, Programs
Conexão de Rede Bluetooth	On	Ports*, Programs*
Ethernet	On	Ports*, Programs*
Wi-Fi	On	Ports*, Programs*

Fonte: Autoria própria (2016)

O fragmento demonstrado na figura 50 nos dá a informação que não foi possível identificar a versão do *Windows*.

Nos diretórios de compartilhamento, todos os usuários estão com acesso e permissão total.

Figura 50 - Informações adicionais desktop suporte



Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows Unknown.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	2 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\Windows	Admin Share	NT SERVICE\TrustedInstaller - F, AUTORIDADE NT\SISTEMA - RWXD, BUILTIN\Administradores - RWXD, BUILTIN\Usuários - RX, AUTORIDADE DE PACOTES DE APLICATIVOS\TODOS OS PACOTES DE APLICATIVOS - RX
C$	C:\	Admin Share	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - D

	Services	No potentially unnecessary services were found.

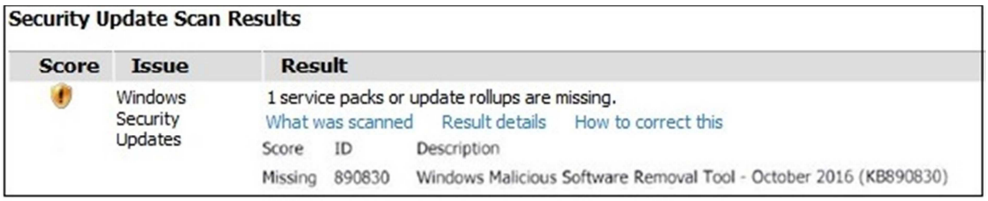
Fonte: Autoria própria (2016)

- ***Desktop* Financeiro**

A última varredura foi realizada em 28 de outubro, em um dos computadores do setor financeiro.

Uma atualização de segurança, identificada pela ID 890830, relacionada a ferramenta de remoção de *software* mal-intencionado do *Windows*, não foi encontrada.

Figura 51 - Atualização de segurança desktop financeiro



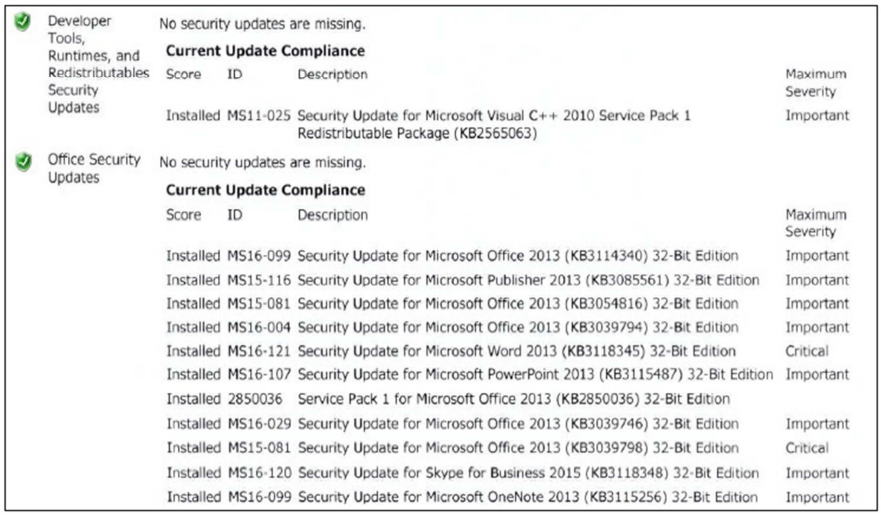
Security Update Scan Results

Score	Issue	Result
	Windows Security Updates	1 service packs or update rollups are missing. What was scanned Result details How to correct this Score ID Description Missing 890830 Windows Malicious Software Removal Tool - October 2016 (KB890830)

Fonte: Autoria própria (2016)

As atualizações de ferramentas específicas da *Microsoft* ®, como *Microsoft Visual C ++,* também foram realizadas com *status* de aprovação, sendo classificadas mediante seu grau de gravidade máxima.

Figura 52 - Atualizações de ferramentas desktop financeiro



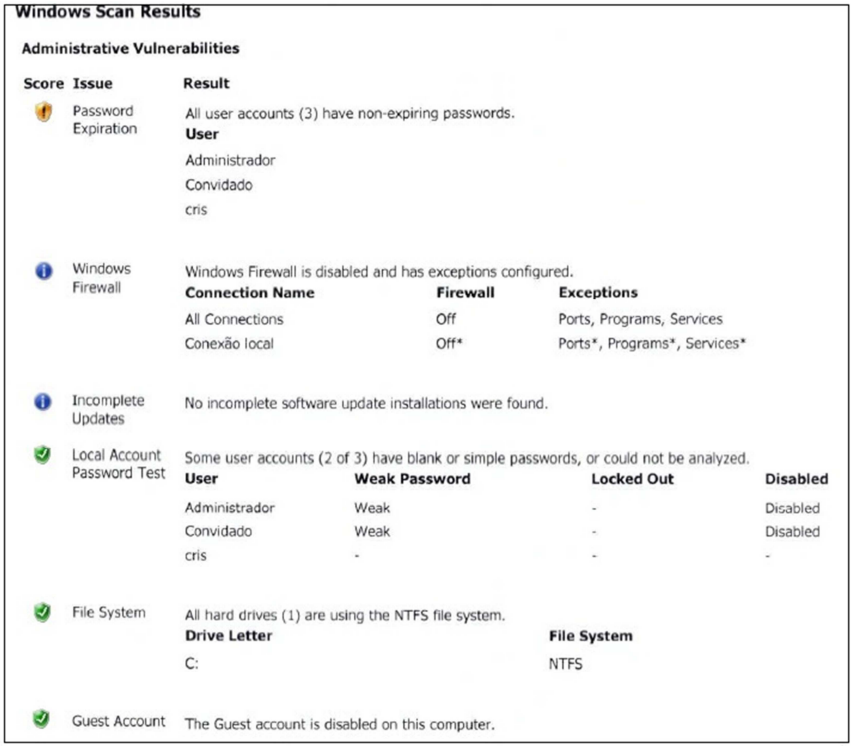
Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing.			
	Current Update Compliance			
	Score	ID	Description	Maximum Severity
	Installed	MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Important
Office Security Updates	No security updates are missing.			
	Current Update Compliance			
	Score	ID	Description	Maximum Severity
	Installed	MS16-099	Security Update for Microsoft Office 2013 (KB3114340) 32-Bit Edition	Important
	Installed	MS15-116	Security Update for Microsoft Publisher 2013 (KB3085561) 32-Bit Edition	Important
	Installed	MS15-081	Security Update for Microsoft Office 2013 (KB3054816) 32-Bit Edition	Important
	Installed	MS16-004	Security Update for Microsoft Office 2013 (KB3039794) 32-Bit Edition	Important
	Installed	MS16-121	Security Update for Microsoft Word 2013 (KB3118345) 32-Bit Edition	Critical
	Installed	MS16-107	Security Update for Microsoft PowerPoint 2013 (KB3115487) 32-Bit Edition	Important
	Installed	2850036	Service Pack 1 for Microsoft Office 2013 (KB2850036) 32-Bit Edition	
	Installed	MS16-029	Security Update for Microsoft Office 2013 (KB3039746) 32-Bit Edition	Important
	Installed	MS15-081	Security Update for Microsoft Office 2013 (KB3039798) 32-Bit Edition	Critical
	Installed	MS16-120	Security Update for Skype for Business 2015 (KB3118348) 32-Bit Edition	Important
	Installed	MS16-099	Security Update for Microsoft OneNote 2013 (KB3115256) 32-Bit Edition	Important

Fonte: Autoria própria (2016)

A seção de vulnerabilidades administrativas gerou os seguintes resultados:

- As senhas dos três usuários existentes na máquina estão configuradas para nunca expirar;
- O *firewall* do *Windows* está desativado;
- Dois usuários possuem senhas em branco;
- Foi identificado o sistema de arquivos NTFS;
- A conta de convidado está desativada.

Figura 53 - Vulnerabilidades administrativas desktop financeiro



Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Password Expiration	All user accounts (3) have non-expiring passwords. **User** Administrador Convidado cris
	Windows Firewall	Windows Firewall is disabled and has exceptions configured. **Connection Name** / **Firewall** / **Exceptions** All Connections / Off / Ports, Programs, Services Conexão local / Off* / Ports*, Programs*, Services*
	Incomplete Updates	No incomplete software update installations were found.
	Local Account Password Test	Some user accounts (2 of 3) have blank or simple passwords, or could not be analyzed. **User** / **Weak Password** / **Locked Out** / **Disabled** Administrador / Weak / - / Disabled Convidado / Weak / - / Disabled cris / - / - / -
	File System	All hard drives (1) are using the NTFS file system. **Drive Letter** / **File System** C: / NTFS
	Guest Account	The Guest account is disabled on this computer.

Fonte: Autoria própria (2016)

Foram identificados a versão do sistema operacional e os diretórios compartilhados:

Figura 54 - Informações adicionais *desktop* financeiro

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 7.
	Shares	3 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\Windows	Admin Share	NT SERVICE\TrustedInstaller - F, AUTORIDADE NT\SISTEMA - RWXD, BUILTIN\Administradores - RWXD, BUILTIN\Usuários - RX
C$	C:\	Admin Share	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - D
scan	C:\scan	Todos - F	BUILTIN\Administradores - F, AUTORIDADE NT\SISTEMA - F, BUILTIN\Usuários - RX, AUTORIDADE NT\Usuários autenticados - RWXD

Fonte: Autoria própria (2016)

5.4 Plano de ação

A última etapa realizada neste estudo de caso diz respeito ao plano de ação que foi realizado no ambiente após a varredura e diagnóstico dos relatórios gerados. Este plano está dividido em duas seções:

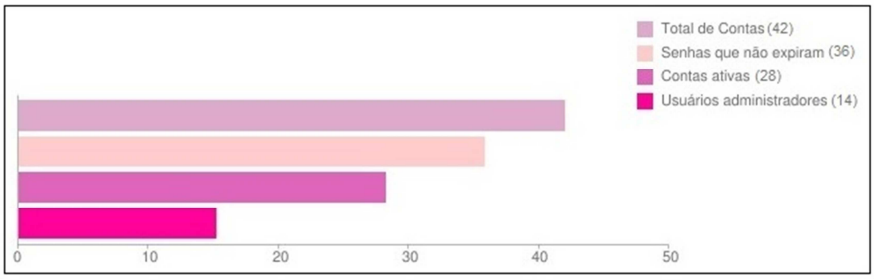
a) Correções realizadas no sistema seguindo recomendações da ferramenta MBSA;
b) Recomendações de segurança da informação.

5.4.1 Correções realizadas no sistema

O plano de ação serve como uma proposição de melhoria as vulnerabilidades encontradas. Ao comparar os resultados coletados, é possível perceber o que possuem de semelhanças e diferenças, realizando correções a fim de garantir a segurança dos sistemas em questão.

Em relação aos itens coletados sobre contas de usuários, por exemplo, é possível comparar todas as máquinas deste estudo nos 4 aspectos descritos no gráfico da página seguinte:

Figura 55 - Gráfico de análise de contas e senhas



Fonte: Autoria própria (2016)

No total, foram coletadas 42 contas de usuário, sendo que apenas 28 deles estão ativos. A primeira recomendação da ferramenta, é que sempre que um novo usuário for criado, uma boa prática é que este altere a senha padrão no primeiro login.

Nesta análise, 36 contas possuem a vulnerabilidade que estão configuradas para não expirar. Com a finalidade de garantir a segurança no aspecto de acesso aos sistemas, o MBSA traz a recomendação que estas contas devem ser revistas, alterando esta configuração através dos seguintes passos:

1. Abrir o Painel de Controle;
2. Clicar duas vezes em Ferramentas Administrativas e, em seguida, clicar duas vezes em Gerenciamento do Computador;
3. Clicar duas vezes na pasta Utilizadores e Grupos Locais e, em seguida, clique na pasta Utilizadores;
4. No painel direito, clicar duas vezes na conta que será alterada;
5. Na caixa de diálogo Propriedades, desmarque a caixa de seleção Senha nunca expira.

A última informação demonstrada pelo gráfico da figura 55, diz respeito que dos usuários ativos, 14 possuem permissão de administradores do sistema, sendo que, assim como recomenda a *Microsoft* ®, cada máquina não possui mais que dois administradores.

Nos testes de senha de conta local, 20 contas de usuários possuem senha em branco ou senhas consideradas fracas, que é uma das principais causas de

violação de segurança. Senhas comuns são datas de aniversário, animais de estimação, nome de algum familiar próximo ou até mesmo do time de futebol.

A ferramenta não consegue analisar essas informações, pois é muito específico por ser único e pessoal de cada usuário. Entretanto, a ferramenta consegue filtrar senhas fracas por meio de:

- Senhas em branco;
- A senha é igual ao nome do computador;
- A senha é composta pela palavra “senha”;
- A senha é composta pela palavra “admin” ou “administrador”.

É preciso adotar uma política de senha forte, pois apesar de simples, é uma forma muito eficaz de garantir a segurança dos sistemas. Para alterar as configurações de diretiva de senha, a ferramenta indica adotar a seguinte solução:

1. Abrir o Painel de Controle.

2. Clicar duas vezes em Ferramentas administrativas e, em seguida, clicar duas vezes em Diretiva de segurança local.

3. Clicar duas vezes na pasta Diretivas de Conta e, em seguida, selecione a pasta Diretiva de Senha.

4. Clicar duas vezes na política que pretende alterar e, em seguida, especificar a nova definição de política.

Outra vulnerabilidade comum entre as máquinas encontrada na varredura, diz respeito aos diretórios compartilhados. Os sistemas operacionais *Microsoft* ® permitem que os usuários compartilhem arquivos uns com os outros. Porém, se um compartilhamento não estiver protegido, usuários não autorizados poderão acessar as informações no compartilhamento.

Como solução, a ferramenta indica a lista de compartilhamentos deve ser analisada, para remoção de ações que não são necessárias. Para os compartilhamentos necessários no sistema, as permissões de compartilhamento devem ser revisadas para garantir que o acesso é limitado a usuários autorizados e não compartilhado com todos. A primeira ação antes de definir as permissões serão atribuídas a cada usuário, diz respeito a desativar o compartilhamento entre as máquinas da seguinte forma:

1. Abrir o Painel de Controle;

2. Clicar duas vezes em Ferramentas Administrativas e, em seguida, clicar duas vezes em Gerenciamento do Computador;

3. Clicar com o botão direito do mouse no compartilhamento para desativar o compartilhamento ou alterar as permissões de compartilhamento.

Após as permissões terem sido configuradas, o próximo passo diz respeito ao processo de auditoria do *Windows*. A auditoria é um passo vital na detecção de intrusões do sistema ou atividade maliciosa em seus sistemas e rede. O Visualizador de Eventos do *Windows* não registra entradas de eventos no log de segurança, a menos que seja ativado.

Para habilitar a auditoria em um computador com sistema operacional *Windows*, é necessário seguir os seguintes passos:

1. Abrir o Painel de Controle;

2. Realizar um duplo clique em Ferramentas administrativas e, em seguida, clicar em Política de segurança local;

3. Nas definições de segurança local, clicar em Políticas locais, em Política de auditoria e, em seguida, clicar nos eventos que pretende auditar. O MBSA recomenda que sejam auditados os seguintes eventos:

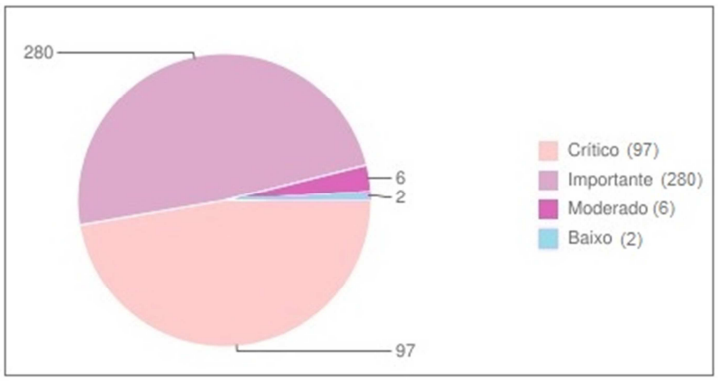
- Eventos de logon de auditoria de contas (Sucesso, Falha);
- Gerenciamento de contas de auditoria (Sucesso, Falha);
- Auditar o acesso ao serviço de diretório (Falha);
- Eventos de logon de auditoria (Sucesso, Falha);
- Auditoria de acesso a objetos (Falha);
- Alteração da política de auditoria (Sucesso, Falha);
- Eventos do sistema de auditoria (Sucesso, Falha).

Para visualizar os registos de eventos, clique em Iniciar, Programas, Ferramentas administrativas e, em seguida, em Visualizador de eventos. Com a auditoria ativada, é possível monitorar, por exemplo, tentativas *logon* com êxito ou falha. Além disso, determinados arquivos e diretórios podem ser auditados em sistemas de arquivos NTFS para modificações ou exclusões.

Os itens de atualização de segurança levantados durante a varredura são pontos cruciais no processo de mitigar os riscos que cercam o ambiente.

Após a análise do resultado das varreduras realizadas nas 7 máquinas, referentes às atualizações de segurança do *Windows*, foi coletado um total de 385 itens e pacotes divididos entre os seguintes níveis*: Critical, Important, Moderate* e *Low.* O gráfico a seguir exemplifica esta análise:

Figura 56 - Grau de classificação das atualizações



Fonte: Autoria própria (2016)

Para garantir que as atualizações de segurança mais recentes sejam aplicadas, é preciso instalar os *service packs* e atualizações individuais mais recentes.

O relatório de verificação do MBSA identifica quais atualizações de segurança estão em falta no computador. Os usuários podem clicar no link no relatório de segurança para exibir o boletim de segurança da *Microsoft* ® ou a página de *download*, que inclui o local de instalação para a atualização de segurança.

O *Firewall* do *Windows* é um *software* que fornece proteção para computadores, controlando quais informações são comunicadas do computador para e da Internet ou de outros computadores em uma rede.

Durante as varreduras, foram identificadas um total de 21 conexões de rede. Porém, nem todas estão com o *firewall* habilitados.

Como demonstra a figura 57, o número de conexões que mantém o *firewall* ativo mantém praticamente a mesma proporção daquelas que o mantém desativado.

Figura 57 - Comparação do status do *firewall*

Fonte: Autoria própria (2016)

Por questões de segurança, é necessário ativar o *firewall* do *Windows* em todas as conexões de rede, seguindo as instruções definidas pelo MBSA:

Autenticado como usuário administrador, é necessário:

1. Abrir o Painel de Controle;
2. Clicar no ícone do *Firewall* do *Windows*;
3. Escolher a opção “Ative ou desative o *Firewall* do *Windows*” e selecionar Ativado (recomendado).

Por fim, é necessário remover os serviços potencialmente desnecessários que estão instalados nos computadores, mesmo que estejam com o status “pausado”, como foi visto no relatório obtido na varredura do *desktop* de acesso remoto.

Manter este tipo de serviço como o *Telnet*, pode chamar a atenção de hackers, que se mal-intencionados, poderão realizar uma invasão no sistema, quebrando os pilares da segurança da informação.

5.4.2 Recomendações de segurança da informação

Como já foi visto até este ponto de todo o estudo, as principais vulnerabilidades do ambiente abordado estão relacionadas a senhas de usuários e a

permissão destes na rede. Outra preocupação é relacionada à falta de mecanismos de proteção contra vírus.

Com a realização das correções de configurações do sistema, seguindo orientações da própria ferramenta MBSA como foi descrito no tópico anterior deste capítulo, foi possível sanar grande parte das vulnerabilidades encontradas. A definição das permissões de usuário, por exemplo, viabilizaram a auditoria que não era realizada por falta de dados inconsistentes.

A primeira recomendação que a equipe de TI deve seguir, diz respeito à escolha de um antivírus padrão em todas as máquinas do hospital. Existem diversos mecanismos disponíveis no mercado, sejam estes pagos ou gratuitos. A escolha deve ser baseada no desempenho, na usabilidade e na proteção desejada.

O quadro a seguir descreve um comparativo realizado pela AV TEST em junho de 2015:

Figura 58 - Comparativo de antivírus

Fonte: AV TEST (2015) [8]

[8] Disponível em: <https://www.av-test.org/en/antivirus/home-windows/windows-8/june-2015/>. Acesso em: 27 out. 2016.

Independente da escolha é necessário à certificação de que todas as máquinas tenham um antivírus instalado e configurado, para proteção no acesso à internet e no recebimento de arquivos, visto que grande parte é carregada nos diretórios de compartilhamento.

Além disso, é necessária a conscientização dos usuários em relação ao acesso e transferência de dados, que deve ocorrer somente baseado em fontes confiáveis. O acesso a sites indesejáveis deve ser bloqueado e deve haver uma política de segurança descrevendo como deve ocorrer o compartilhamento de arquivos via mídia removível.

Por fim, uma última recomendação que pode ser declarada diz respeito à criação de senhas seguras, seguindo o que é indicado pela ISO 27001/ISO 27002. Os usuários devem entender esta importância, não criando senhas com uma única sequência de caracteres, data de nascimento, nome de login, entre outras informações conhecidas. Manter a mesma senha em contas diferentes também é uma opção a ser considerada, assim como mantê-las diferentes de senhas já utilizadas.

Podem ser descritos alguns requisitos:

Quadro 5 - Requisitos de senha segura

Requisito	Exemplo
Letras maiúsculas	A-Z
Letras minúsculas	a-z
Números	0-9
Caracteres especiais	! % @ # $
Quantidade de caracteres: Superior à 8	E1exX&&Mmpp!0

Fonte: Autoria própria (2016)

6 CONSIDERAÇÕES FINAIS

Antigamente, a auditoria era realizada por profissionais que não possuíam tecnologias de auxílio, ou computadores de qualidade suficiente para o processamento de dados. Mas, a auditoria evoluiu, com presença não somente na área contábil, como também em sistemas de informação, seja de pequenas, médias ou grandes empresas.

O avanço da tecnologia em um determinado negócio não significa necessariamente que este está protegido contra as ameaças relacionadas à segurança da informação. No ambiente de TI do hospital em que foi baseado este estudo de caso, os problemas que podem ser observados à grosso modo seguem uma dessas três vertentes:

- Praticantes da engenharia social buscam, através de suas práticas, acesso a informações sigilosas, sejam relacionados a valores financeiros, recursos humanos, dados pessoais de funcionários, pacientes e médicos;

- Como algumas máquinas não possuem um mecanismo como um antivírus, a transmissão de vírus se torna incontrolável, seja via e-mail, seja no compartilhamento de dados via unidade removível;

- A outra preocupação ocorre internamente. O sistema de gestão hospitalar é o mesmo em todos os departamentos, onde os usuários acessam o módulo referente ao seu setor. Por mais que o sistema permita o acesso do funcionário apenas a sua área exclusiva, os computadores não possuem registros íntegros daquilo que está sendo realizado, pois algumas máquinas encontram-se sem nenhuma proteção relacionada à senha de acesso.

A segurança da informação se tornou o ponto mais importante a ser discutido, pois com a perda de um dado restrito, a empresa perde confiabilidade e valor diante de seus clientes e investidores. Logo, assim como foi visto no referencial teórico, a auditoria se torna crucial para prever riscos e, se possível, detectar todas as causas do problema, permitindo melhores práticas de segurança, por meio medidas seguras como políticas, mecanismos como antivírus, configurações de *firewall* e conscientização de usuários.

Por meio do estudo de caso, foi possível verificar que toda a teoria sobre o assunto pode ser vista na prática. A ferramenta MBSA foi de grande valia para execução das varreduras do ambiente. Como pontos positivos, vale ressaltar que apesar de ser uma ferramenta gratuita, ela é muito completa no que se diz respeito à identificação de vulnerabilidades em sistemas. Após uma varredura ter sido realizada em um computador, os relatórios que são gerados ficam armazenados em um histórico para que possam ser realizadas análises e comparações entre os mesmos. As informações coletadas são classificadas por meio de seu grau de criticidade. Além disso, ela descreve como mitigar tais vulnerabilidades, com o intuito de manter o ambiente mais seguro.

Entre alguns dos poucos pontos negativos, esta ferramenta é exclusiva para sistemas da *Microsoft* ®, não sendo possível executá-la em outros sistemas operacionais. Outra questão diz respeito que, em redes que não são configuradas com o conceito de domínio, como no caso do ambiente deste estudo, as varreduras precisam ser realizadas máquina a máquina.

Durante a coleta de informações, foi possível perceber que muito se discute sobre a semelhança do funcionamento do MBSA se comparado ao *Microsoft Update*. É importante esclarecer que, o *Microsoft Update* indica as atualizações de segurança em um único computador, indicando quais precisam ser instaladas, somente se a máquina estiver conectada à internet. Enquanto isso, o MBSA permite a avalição de vários computadores, até mesmo remotamente, sem precisar necessariamente do acesso ao site do *Microsoft Update*, além da forma detalhada como são descritas as vulnerabilidades identificadas.

Como continuidade a este trabalho, por meio de todas as informações que foram levantadas, a ferramenta será executada em todo o ambiente e em máquinas que não foram analisadas neste estudo, procurando identificar e corrigir todas as vulnerabilidades existentes. Após essa etapa ser concluída, serão realizadas novas varreduras a cada 3 meses, para verificar o status de todos os computadores.

Enfim, fica claro a importância do estudo nesta área, devido a todos os custos existentes ao realizar toda a infraestrutura de uma empresa, com equipamentos de última geração e instalações de qualidade excelente, porém a atenção deve ser voltada também a informação contida em tal estrutura, e as melhores formas de protegê-la.

REFERÊNCIAS

APARECIDA, Franciele. **Origem da auditoria**. Disponível em: < http://www.webartigos.com/artigos/origem-da-auditoria/37327/>. Acesso em: 08 ago. 2016.

ARAÚJO, Victor Melo de. **Segurança da Informação:** Uma abordagem holística com foco na implantação de um SGSI. 2015. 37 f. Monografia (Especialização) - Curso de Redes e Telecomunicações, Universidade Salvador Laureate, Salvador, 2015.

CABRAL, Carlos. **Trilhas em segurança da informação:** Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2015. 256 p.

CHIQUITO, Antônio Ricardo. **Princípios da auditoria**. Disponível em: < http://www.contabeis.com.br/artigos/63/principios-da-auditoria-contabil-externa/>. Acesso em: 08 ago. 2016.

CREPALDI, Sílvio Aparecido. **Origem, evolução e desenvolvimento da auditoria.** Disponível em: <http://www.classecontabil.com.br/artigos/origem-evolucao-e-desenvolvimento-da-auditoria>. Acesso em: 15 mai. 2016.

DAQUINO, Fernando. **Windows 7 continua sendo o sistema operacional mais utilizado no mundo.** Disponível em: < http://www.tecmundo.com.br/windows-7/79298-windows-7-continua-sendo-sistema-operacional-usado-mundo.htm>. Acesso em: 30 mar. 2016.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação:** guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Ciência Moderna Ltda., 2008. 259 p.

FONTES, Edison. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006. 172 p.

GUSMÃO, Gustavo. **Linux é usado em 41% das empresas brasileiras de TI.** Disponível em: <http://exame.abril.com.br/tecnologia/noticias/linux-e-usado-em-41-das-empresas-brasileiras-de-ti-aponta-pesquisa> Acesso em: 30 mar. 2016.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação.** 2. ed. São Paulo: Atlas, 2011. 208 p.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação.** 1. ed. Rio de Janeiro: Ciência Moderna, 2008. 253 p.

Magique Galileo. Disponível em: <http://www.magiquegalileo.com/hsl/hslwebsite.nsf> Acesso em: 02 set. 2016.

Mcafee. **Free tools.** Disponível em: <www.mcafee.com/br/downloads/free-tools>. Acesso em: 19 fev. 2016.

PEREZ JUNIOR, José Hernandez *et al.* **Auditoria das demonstrações contábeis.** 2. ed. Rio de Janeiro: Fgv Management, 2011. 184 p.

Portal Educação. **Origem e evolução da auditoria.** Disponível em: http://www.portaleducacao.com.br/educacao/artigos/24024/origem-e-evolucao-da%20auditoria#ixzz4A3bSou9v> Acesso em: 10 mai. 2016.

PRADO, Edmir; SOUZA, Cesar Alexandre de. **Fundamentos de Sistemas de Informação.** São Paulo: Elsevier, 2015. 312 p.

SEPIA Solutions. Disponível em: < https://www.sepiasolutions.net/Software/Pentana_for_Auditors.html>. Acesso em: 02 set. 2016.

SOARES, Gildo. **A ferramenta MBSA.** Disponível em: <https://technet.microsoft.com/pt-br/library/cc668448.aspx> Acesso em: 10 abr. 2016.

SOUSA, Rafael Alexandre Alves de; BARBOSA, Luis Filipe de Faria Pereira Wiltgen. **Utilização do software ACL para redução do índice de perdas comerciais em concessionárias de energia elétrica.** Vale do Paraíba, [s.d]. Disponível em: <http://www.inicepg.univap.br/cd/INIC_2008/anais/arquivosINIC/INIC0497_02_A.pdf >. Acesso em: 05 set. 2016. 5p.