UNIVERSIDADE DE CAXIAS DO SUL

ALEX GILMAR BOENO DE LIMA

FERRAMENTAS DE GESTÃO PARA A SEGURANÇA DA INFORMAÇÃO

CAXIAS DO SUL

2017

ALEX GILMAR BOENO DE LIMA

FERRAMENTAS DE GESTÃO PARA A SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.
Orientadora Prof. Maria de Fátima Webber do Prado Lima

CAXIAS DO SUL

2017

ALEX GILMAR BOENO DE LIMA

FERRAMENTAS DE GESTÃO
PARA A SEGURANÇA DA INFORMAÇÃO

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

Aprovado em: __/__/__.

Banca Examinadora

_____

Prof. Maria de Fátima Webber do Prado Lima

Universidade de Caxias do Sul

_____

Prof. Iraci Cristina da Silveira De Carli

Universidade de Caxias do Sul

_____

Prof. Giovanni Ely Rocco

Universidade de Caxias do Sul

Dedico este trabalho a minha namorada Mariana e aos meus pais Gilmar e Salete cujo o apoio e o incentivo foram fundamentais para que fosse possível completar mais essa jornada.

AGRADECIMENTOS

Agradeço em primeiro lugar aos meus pais Gilmar e Salete por acreditarem em mim e sempre estarem presentes me apoiando.

Agradeço a minha namorada Mariana pela dedicação, paciência e o apoio cujo foi essencial durante toda a trajetória.

Agradeço também a Profa. Dra. Maria de Fátima Webber do Prado Lima pelo suporte e dedicação durante esta etapa, e aos demais professores.

Agradeço ainda aos colegas, amigos e demais pessoas que, de alguma forma, contribuíram para a concretização deste objetivo.

RESUMO

Este trabalho tem como objetivo analisar e avaliar softwares de Sistemas de Gestão da Segurança da Informação com o intuito de identificar o software com mais aderência a norma ABNT NBR ISO/IEC 27001. Para embasar esta avaliação, foram estudados alguns conceitos de Segurança da Informação, Sistemas de Gestão da Segurança da Informação, as principais normas da área de Segurança da Informação (ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27003 e ABNT NBR ISO/IEC 27004) e as normas que regem padrão para avaliação da qualidade de softwares (ABNT NBR ISO/IEC 25020 e ABNT NBR ISO/IEC 25030). A partir dos estudos foram definidos os critérios, métricas e casos de testes para a avaliação dos softwares, de acordo com as funcionalidades fundamentais definidas pela norma ABNT NBR ISO/IEC 27001. Os softwares selecionados para a avaliação foram o OSSIM e o EBIOS. De acordo com os critérios utilizados, o software que atingiu a melhor avaliação foi o OSSIM.

Palavras-chave: Sistemas de Segurança da Informação, Softwares, Avaliação.

ABSTRACT

This study has the objective of analyzing and evaluating software of Information Security Management Systems in order to identify the software with more adherence to the ABNT NBR ISO / IEC 27001 standard. To support this evaluation, it has been studied some concepts of Information Security, Information Security Management Systems, the main standards in the area of Information Security (ABNT NBR ISO / IEC 27001, ABNT NBR ISO / IEC 27003 and ABNT NBR ISO / IEC 27004) and standards that govern standard for the evaluation of the Quality of software (ABNT NBR ISO / IEC 25020 and ABNT NBR ISO / IEC 25030). From the study, the criteria, metrics and tests cases for software evaluation were defined, according to the fundamental functionalities defined by ABNT NBR ISO / IEC 27001. The software selected for evaluation was OSSIM and EBIOS. According to the criteria used, the software that achieved the best evaluation was OSSIM.

Keywords: Information Security Systems, Softwares, Evaluation.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ISO	Organização Internacional de Normalização
IEC	Comissão Eletrotécnica Internacional
NBR	Norma Brasileira
SGSI	Sistemas de Gerenciamento da Segurança da Informação
TCC	Trabalho de Conclusão de Curso
UCS	Universidade de Caxias do Sul

SUMÁRIO

1 INTRODUÇÃO

A Segurança da Informação refere-se à proteção existente das informações e se aplica tanto a informações corporativas quanto às pessoas. Pode-se entender informação como sendo um conjunto de dados armazenados e que organizados possuem um significado (MCGEE e PRUSAK, 1994). As informações representam a inteligência e um ativo intangível que proporciona vantagens competitivas às organizações (SÊMOLA, 2003). A aplicação e o uso produtivo da informação caracterizam o conhecimento (BOISOT, 1998). Segundo a norma ABNT NBR ISO/IEC 27002:2005 a definição de Segurança da Informação é *"Segurança da informação é a proteção de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio"*.

A segurança da informação atua em três princípios básicos que sempre devem ser respeitados ou a segurança correrá riscos. Estes princípios são (CAMPOS, 2007):

a) Confidencialidade: não permitir o acesso indevido às informações, mantendo-as em sigilo;
b) Integridade: é essencial que a informação não seja modificada indevidamente;
c) Disponibilidade: as informações devem sempre estar disponíveis quando forem necessárias, mas somente às pessoas autorizadas.

O uso da Segurança da Informação nas organizações geralmente têm a finalidade de diminuir o nível de exposição aos riscos em todos os ambientes para que a empresa possa estender a segurança aos seus produtos e serviços, resultando em uma satisfação maior por parte dos clientes. Outro ponto relevante da Segurança da Informação é a importância dos benefícios da Segurança nos Negócios. Por exemplo podemos citar: redução da probabilidade de fraudes, redução de riscos contra vazamento de informações sigilosas e/ou confidenciais, manuseio correto de informações confidenciais e diminuição de erros devido a treinamento e mudança de comportamento.

O crescente avanço da tecnologia fez com que as informações se tornassem um dos principais patrimônios e diferenciais para qualquer organização. Sabendo do valor das informações, é de extrema importância que as mesmas sejam mantidas de forma segura e confiável, como qualquer outro ativo da empresa (ABNT, 2005).

Segundo a EY Brasil (2013) os dados da 16ª Pesquisa Anual Global sobre Segurança, feita com mais de 1.000 executivos de 64 países, apontam que dos participantes 83% acreditam que a sua área de segurança é ineficiente, desta pesquisa também 31% acredita que os incidentes relacionados à segurança aumentaram no mínimo 5% no ano de 2013 dentro de suas organizações.

No ano de 2016 o Brasil foi o país que mais sofreu ataques cibernéticos as organizações da América Latina e o 9º país no mundo (KASPERSKY BRASIL, 2016). Os principais perigos que ameaçam a Segurança da Informação de uma empresa são a falta de conscientização, conhecimento e crença por parte dos funcionários e liderança além da falta dos planos de ação a pragas virtuais, como Vírus, Cavalo de Tróia, Phishing, Malware, Spyware, Adware, Ransomware e Extortionware. A figura 1 representa o crescimento dos ataques cibernéticos em 2016 no Brasil em comparação com o resto do mundo e dividido em setores.

Figura 1: Gráfico com percentual de crescimento de ataques cibernéticos

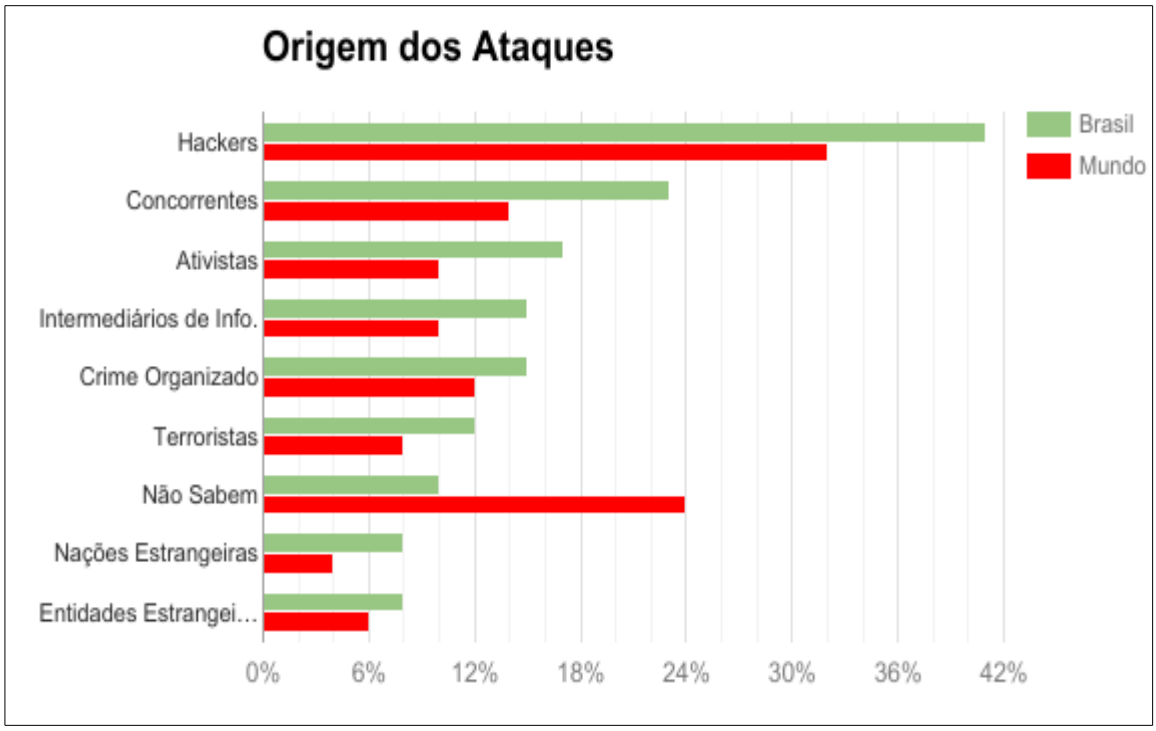
Fonte: PWC Brasil (2016)

As empresas necessitam revisar as suas estratégias de segurança. Conforme Computer World (2017) quatro em cada dez alertas críticos de segurança não são

devidamente investigados, deste número 28% são realmente alertas legítimos e menos da metade destes são devidamente corrigidos, estes dados foram retirados da edição de 2017 do Relatório Anual de Cibersegurança da Cisco. Mais de um terço dos entrevistados relataram que passaram por falhas de segurança no ano passado, que resultaram em perdas de clientes, receitas e/ou oportunidades. “As empresas estão investindo de forma errada em segurança”, afirma Ghassan Dreibi, gerente de desenvolvimento de negócios de Segurança da Cisco para a América Latina.

A figura 2 apresenta a provável origem dos ataques a organizações brasileiras conforme levantamento feito pela Trend Micro (2014) que é uma empresa especializada em segurança online.

Figura 2: Gráfico sobre a origem dos ataques



Fonte: Trend Micro (2014)

Para que a segurança da informação seja implantada, é necessário que se definam e implementem controles que sejam continuamente monitorados e analisados, buscando o seu aperfeiçoamento (MORAES, 2003 apud VIANEZ, SEGOBIA e CAMARGO, 2008). Com base nesses dados fica evidente que as organizações precisam estar bem preparadas para estes tipos de situações e estar sempre à frente dos crimes cibernéticos, para isso existem os Sistemas de Gestão

da Segurança da Informação (SGSI) que possuem como base um programa estruturado para a implantação de procedimentos, diretrizes, políticas, orientações e normas para a proteção do conhecimento e da marca da organização.

A ISO 27001 descreve basicamente como desenvolver um SGSI podendo considerar este como uma abordagem sistemática para a proteção e gestão das informações dessa organização. Os tipos de controles para segurança da informação que serão implementados nas organizações geralmente são decididos com embasamento nos resultados da avaliação dos riscos e nos requisitos previamente solicitados. Estes controles devem ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde e quando necessário, para que os objetivos da organização sejam atendidos (MORAES, 2003 apud VIANEZ, SEGOBIA e CAMARGO, 2008).

A identificação mais apropriada de quais controles necessitam ser implementados requer um planejamento cuidadoso e bem detalhado. Para obter sucesso na implantação de um SGSI nas organizações o processo precisa do apoio de todos os colaboradores da organização, desde a participação da alta direção, acionistas, fornecedores e terceiros. Dessa forma, podemos afirmar que o SGSI não é um assunto apenas do setor de Tecnologia da Informação (TI).

Três pontos importantes de se levar em conta para implantação de um SGSI e que são considerados como pré-requisitos da segurança da informação: avaliar os riscos para a segurança da empresa, avaliar os estatutos, a regulamentação, os contratos e a legislação vigentes e por último levar em conta os conglomerados particulares de objetivos, princípios e requisitos de negócio da organização em específico.

Ao tratarmos os controles fica evidenciado como uma questão particular de cada organização para definir os seus critérios e níveis de aceitação e tratamento dos riscos. Também é interessante deixar claro que as organizações enfrentam legislações e regulamentações diferentes conforme o seu segmento, dessa forma varia e depende totalmente de cada organização a maneira como ela interage e seleciona os seus controles para a proteção de seus ativos. Segundo Defenda (2012) quando a governança da segurança da informação é desenvolvida apropriadamente, retorna à organização os resultados dos alinhamentos estratégicos, gestão de riscos, gestão de recursos, gestão de desempenho e entrega de valor.

Atualmente o mercado nos apresenta diversas opções de softwares de alto escalão para o gerenciamento da segurança da informação entre os mais conhecidos podemos citar ferramentas bem populares no mercado como OSSIM (Open Source Security Information Management) que é um software de código aberto. Outros exemplos de sucesso são a IBM Security Radar, a HP Arcsight, a LogRhythm, a Security Onion, a ELK Stack e a Logalyze.

1.1 Problema de Pesquisa

Vivemos hoje em um ecossistema que gera muita exposição aos crimes cibernéticos, consequentemente as organizações precisam encontrar a forma correta de se proteger e gerenciar a segurança das informações e para isso existem diversas ferramentas de gerenciamento disponíveis no mercado.

Contudo, diante das possibilidades oferecidas e disponíveis a decisão de escolher qual é a ferramenta ideal para a sua organização deve ser tomada com todo cuidado. Deve se ter ciência que essa escolha possivelmente acarretará inúmeras consequências que não poderão ser previstas.

Os processos de TI precisarão ser fortalecidos, pois a implantação de um projeto dessa magnitude necessita de diversos levantamentos e algumas conformidades exigidas pelo negócio. Possivelmente se imagina que poderá ocorrer diminuição de custos, em virtude de alguns processos serem reforçados com as melhores práticas do mercado da segurança da informação. Entre tantas outras consequências que essa implantação pode gerar se faz necessário escolher a ferramenta certa com consciência.

Questão de pesquisa: Qual(is) a ferramenta(s) de código livre, dentre as selecionadas, possui(em) aderência quanto a norma ABNT NBR 27001?

1.2 Objetivo

A proposta de solução deste trabalho é analisar softwares desenvolvidos em código livre a fim de verificar quais softwares realizam o gerenciamento do SGSI de acordo com a norma ABNT/NBR 27001.

1.2.1 Objetivos Específicos

Os objetivos específicos a serem abordados no trabalho são:

a) Aprofundar os conhecimentos sobre SGSI;
b) Definir critérios de avaliação de softwares de SGSI de acordo com a norma ABNT/NBR 27001;
c) Testar e avaliar softwares que gerenciem SGSI.

1.3 Metodologia

A metodologia utilizada neste trabalho consiste em um estudo teórico, abrangente e exploratório da literatura disponível sobre o tema a ser estudado. Essa metodologia permite que a análise do tema e o desenvolvimento de um conhecimento teórico sobre o assunto permita um maior entendimento sobre as variáveis do problema proposto e na construção dos resultados esperados.

No decorrer do desenvolvimento serão utilizadas as normas ABNT/NBR 27000 e derivadas visando manter o padrão estabelecido nas normas relacionadas à SGSI. Para análise dos softwares a serem testados foram utilizadas as normas ABNT NBR ISO/IEC 25020 e 25030 normas que auxilia na implementação de um Sistema de Gerenciamento de Serviço de Tecnologia da Informação (SGSTI).

A partir disso e os estudos realizados sob a literatura fica possível então concretizar os objetivos propostos sobre a pesquisa e chegar a algumas soluções e considerações sobre o problema. Desta forma, os processos metodológicos estão divididas em etapas da seguinte forma:

a) 1ª Etapa: Levantamento e seleção do material bibliográfico a ser utilizado;
b) 2ª Etapa: Definir quais softwares SGSI desenvolvidos em código aberto a serem estudados e testados;
c) 3ª Etapa: Através da metodologia de análise das normas ABNT NBR ISO/IEC 25020 e 25030 efetuar testes nos softwares;
d) 4ª Etapa: Análise das ferramentas visando identificar qual a opção mais completa de software SGSI utilizando a metodologia encontrada na norma ABNT NBR ISO/IEC 27001.

1.4 Estrutura do Trabalho

O capítulo 2 descreve as principais normas relacionadas a Segurança da Informação (ABNT/NBR 27001, 27003, 27004) e as normas referentes a avaliação de software (ABNT/NBR 25020 e 25030).

O capítulo 3 é composto pela proposta de solução do trabalho, aonde ocorre a definição dos softwares que foram utilizados no projeto e são apresentados os critérios, métricas e casos de testes que foram utilizados na avaliação dos softwares selecionados.

O capítulo 4 apresenta as avaliações e os testes efetuados nos softwares OSSIM e EBIOS conforme as definições de critérios, métricas e casos de testes definidos no capítulo 3.

No capítulo 5 são avaliados os resultados apresentados pelos testes efetuados nos softwares no capítulo 4, com os resultados dos testes dos softwares também é feita a avaliação dos resultados para definir o software mais aderente as definições da norma ABNT NBR ISO 27001.

Por fim, o capítulo 6 faz uma conclusão do estudo realizado, indicando se algum software está de acordo com o objetivo proposto pelo trabalho.

2 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Segundo Moura (2007) um SGSI é planejado para se certificar de que a seleção de controles de segurança sejam proporcionais e adequados para proteger os ativos de informação e gerar confiança às partes interessadas. Um SGSI visa trazer parâmetros de resposta para alguns métodos que implementam, operam, monitoram, revisam, mantém e melhoram o sistema de gestão da segurança da informação. Pode-se definir um SGSI como uma junta multidisciplinar que possui como seus principais objetivos estabelecer as políticas de segurança, ampliar o conhecimento envolvido e também definir os seus responsáveis e as medidas a serem tomadas (ABNT ISO 27001, 2013).

Conforme (VERHEIJEN, 2008) o sistema de gestão de segurança da informação é uma decisão estratégica para uma organização, visando preparar para estabelecer e implementar requisitos que mantenham e melhorem continuamente o sistema de segurança da informação. Cada organização possui características específicas que devem ser levadas em consideração na implantação de um SGSI. De acordo com Moura (2007) a fase de modelagem das especificações deve incluir os requisitos de controle de segurança personalizados para que seja possível adaptar as características e exigências de cada organização.

A preocupação com a segurança da informação dos sistemas computacionais não é de hoje. O procedimento da definição de padrões e regras de segurança iniciou na década de 60 (Guerra Fria), atingindo o seu ponto alto com a publicação, no ano de 2000, da norma Internacional de Segurança da Informação ISO/IEC-17799.

Os objetivos das normas de segurança como um todo são oferecer orientações para a gestão da segurança da informação para aqueles que são os responsáveis pela introdução, implementação ou manutenção da segurança nas organizações. Elas também funcionam de forma oferecer um embasamento comum para o desenvolvimento de normas e de práticas voltadas à segurança organizacional e também estabelecer a confiança nas relações entre as organizações.

Um SGSI é um sistema de gestão apto de se obter certificação. Ela ocorre a partir das evidências, práticas e documentos, do aglomerado de controles implantados os quais devem ser continuamente exercidos e adequadamente registrados:

> A certificação configura uma forma de organização empresarial de se colocar as coisas nos seus devidos lugares de maneira sistêmica; ajuda as companhias a entender o que se passa internamente e, de certa forma, orienta no tratamento dos processos e ações que devem ser executados para que não conformidades não ocorram novamente (TSO, I., 2012).
>
> .

Dessa forma fica evidente que as normas e as certificações hoje são práticas de competitividade entre as organizações e quem as segue e acompanha leva vantagens sobre os concorrentes. Na área da segurança existem diversas normas e certificações. Dentre elas estão as normas da família ISO 27000 que é formada por uma série de 15 normas que abordam padrões de sistemas de gerenciamento e segurança. As próximas seções apresentam algumas destas normas como a ISO 27001, ISO 27003 e a ISO 27004.

2.1 ABNT NBR ISO/IEC 27001

A ISO 27001 (ABNT ISO 27001, 2013), uma das normas da família ISO 27000, representa um padrão de utilização quando se fala em gerenciamento e gestão de segurança da informação. A norma pode ser aplicada em organizações de qualquer porte ou tipo e sua aplicação caracteriza uma organização como confiável, disponibilizando assim maior segurança para os seus clientes.

A norma ISO 27001 provê e apresenta requisitos para que uma organização possa estruturar seu SGSI. A norma funciona como guia para implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI. Ela incorpora um processo de escalonamento de risco e valorização de ativos, orientando quanto à análise e identificação de riscos e a implantação de controle para minimizá-los. A norma permite que as organizações no mundo todo possam se certificar de suas práticas de gestão de segurança da informação (MANOEL, 2014, p.90).

Publicada pela International Standardization Organization (ISO) em 2006, a versão mais utilizada é a versão de 2013, que também vem sendo melhorada ao

decorrer do tempo, auxiliando as organizações a conter riscos causados por possíveis vulnerabilidades (ISO 27001, 2013).

Na implantação de um SGSI apoiado na ISO 27001 a norma dá suporte para que a organização possa utilizar as melhores técnicas para monitoramento e controles, envolvendo recursos tecnológicos e humanos.

Para que isso ocorra é necessário o devido treinamento para todos os colaboradores da organização, gerando assim conscientização por parte dos colaboradores, os treinamentos devem ser todos registrados. Esse processo auxilia na avaliação das normas que estão sendo postas em práticas pelos colaboradores, identificando e avaliando vulnerabilidades, riscos e ameaças que possam ocorrer e os seus níveis de impacto na organização.

Esta norma inclui requisitos para a avaliação e tratamento de riscos da segurança da informação voltadas para as necessidades da organização (ABNT ISO 27001, 2013). Com a alta direção compromissada e o treinamento eficaz dos colaboradores, é possível se reduzir o número de ameaças que exploram eventuais vulnerabilidades. Na Tabela 1 se apresentam requisitos existentes na norma ISO 27001.

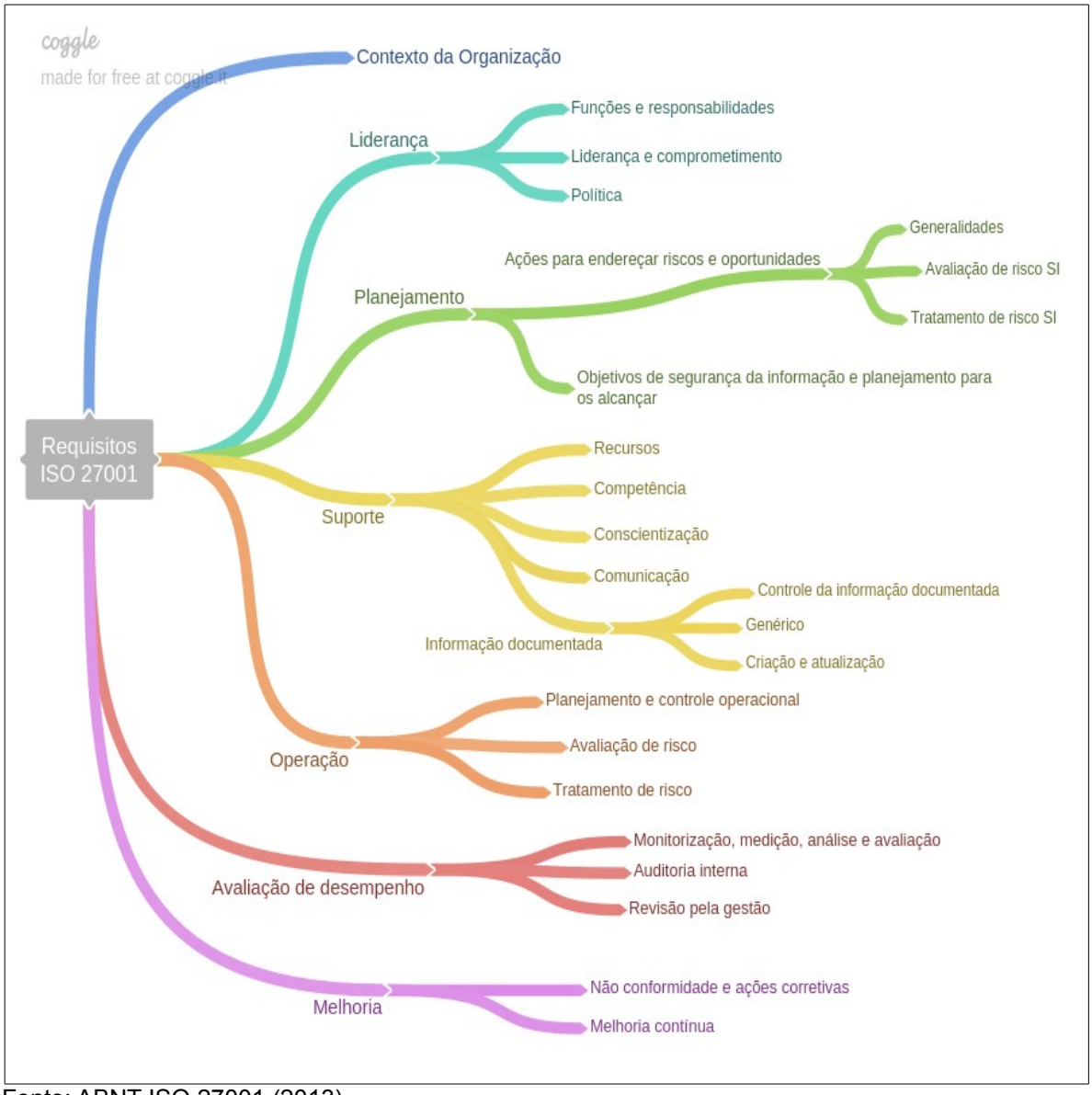
Tabela 1: Requisitos da Norma ISO 27001

Nº	**Requisito**	**Descrição**
1	Escopo	Abrangência da Norma
2	Referência Normativa	Normas e padrões relacionados à norma 27001
3	Termos e Definições	Termos e definições relacionadas à segurança da informação
4	SGSI	Referente à criação, implementação, monitoramento e melhoria do SGSI, também trata de documentação e registros de informações
5	Responsabilidade da Direção	Definição de responsabilidades, treinamento e provisão de recursos do SGSI
6	Auditorias Internas	Auditorias internas realizadas por pessoal treinado e comprometido com o SGSI
7	Análise Crítica do SGSI	Análise realizada pelo corpo diretivo da organização das ações efetuadas pelo SGSI
8	Melhoria do SGSI	Trata das ações corretivas e preventivas efetuadas pelo SGSI

Fonte: ABNT ISO 27001 (2013)

A ISO 27001 em sua constituição possui a determinação de regras e condições para a sua utilização. Para melhor visualizar, a Figura 3 apresenta um diagrama exibindo alguns requisitos da norma.

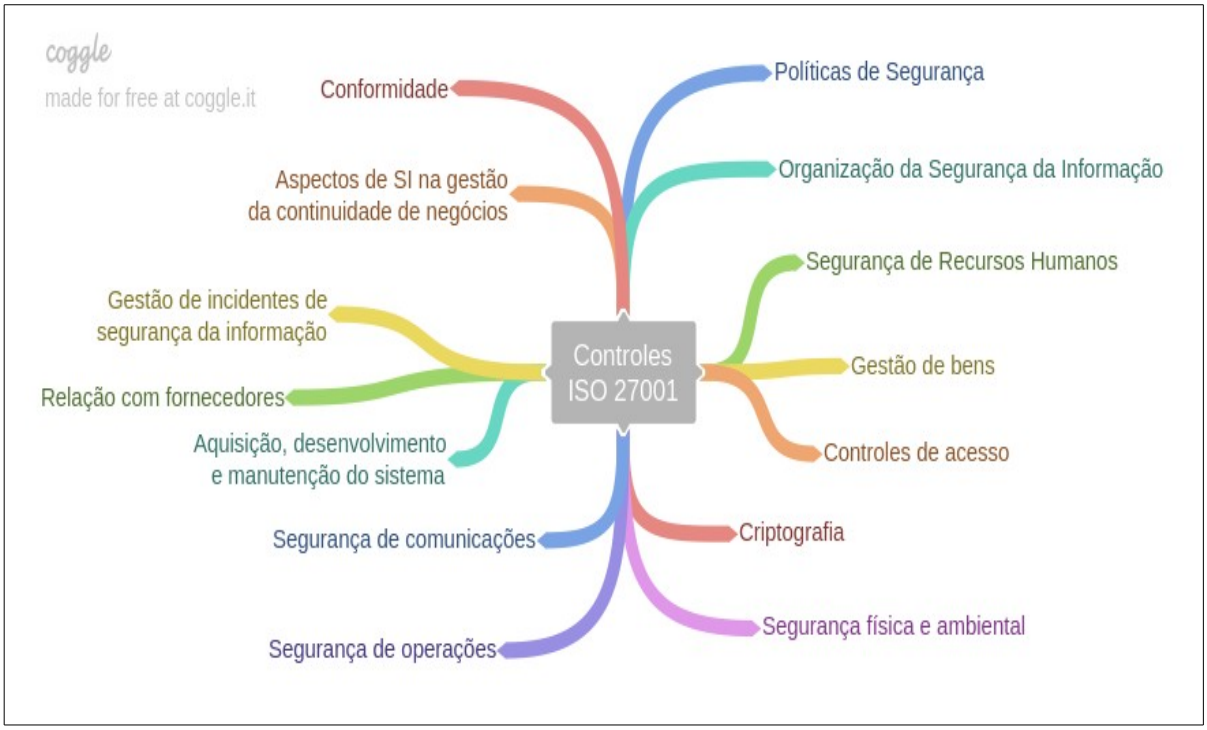
Figura 3: Requisitos da ISO 27001



Fonte: ABNT ISO 27001 (2013)

A norma também tem um componente, denominado de ANEXO A, que é composta pelo conjunto de controles que as organizações devem utilizar conforme sua necessidade (Figura 4). Os controles definidos no Anexo também são mais detalhados na norma ISO 27002.

Figura 4: Controles da ISO 27001



Fonte: ABNT ISO 27001 (2013)

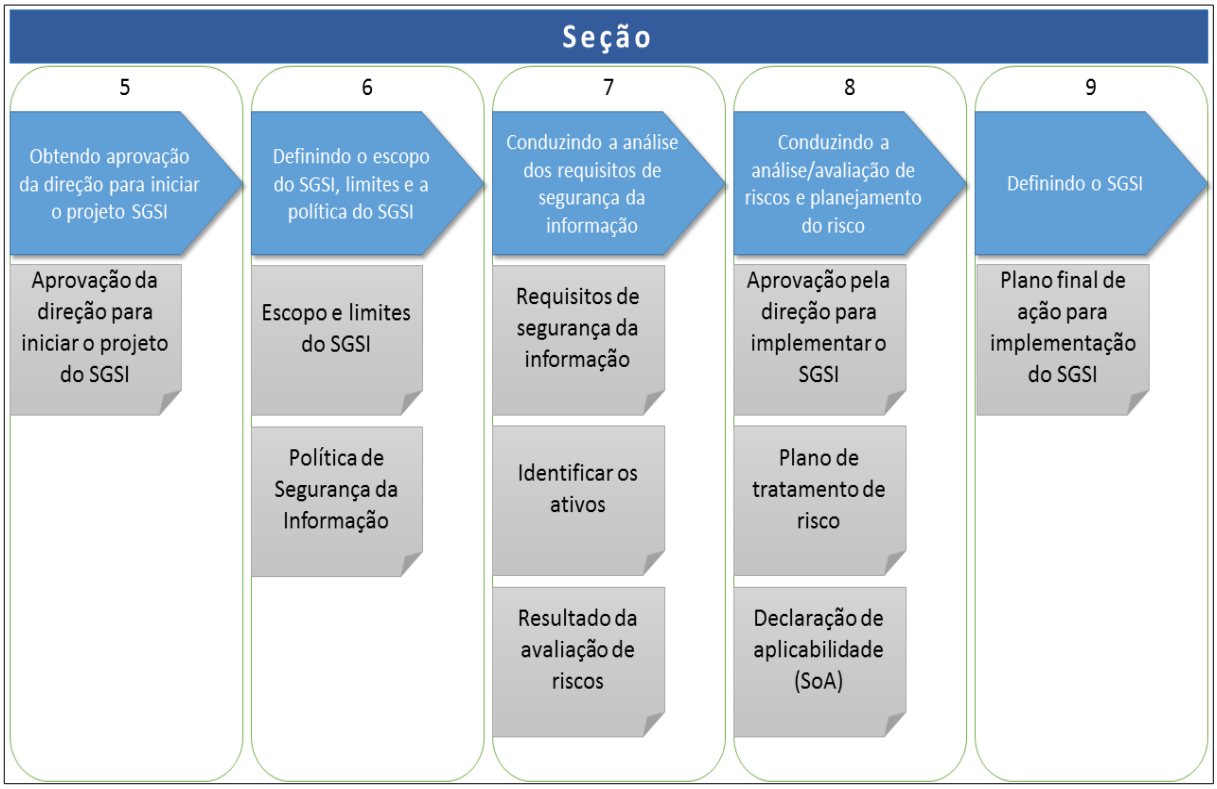
Toda organização que trata informações em seus dispositivos e as transmite para fora da própria organização deve trabalhar com o SGSI, de acordo com as normas da ISO 27001 (ALMEIDA, 2013).

2.2 ABNT NBR ISO/IEC 27003

O processo descrito na ISO 27003 foi idealizado para proporcionar apoio à implantação da ISO 27001, tendo em vista deixar a organização preparada para a implantação do SGSI. De modo a definir a estrutura organizacional de projeto e conquistando a aprovação da direção, definindo as atividades críticas para o projeto e como atender aos requisitos da ISO 27001.

A ISO 27003 (ABNT ISO/IEC 27003:2011) apresenta orientações para a implantação de um SGSI. Ela é construída com base em planejamento, elaboração e definição de um projeto de implantação de um SGSI, projeto este que é dividido em 5 fases, sendo que cada fase é separada por uma seção da norma (Figura 5).

Figura 5: Seções da ISO 27003



Fonte: ABNT ISO 27003 (2011)

Com a utilização da ISO 27003, a organização se torna capaz de desenvolver um processo para a gestão da segurança da informação, garantindo às partes interessadas que os riscos aos ativos de informação da organização são monitorados e mantidos dentro dos limites de segurança aceitáveis.

A norma não atende atividades operacionais e do SGSI, todavia aborda conceitos sobre como desenvolver essas atividades. Estes conceitos resultam no plano final de implantação do projeto do SGSI.

A norma pode ser aplicada em organizações de qualquer porte ou tipo, incluindo agências governamentais, organizações sem fins lucrativos e empresas comerciais. Os riscos e as complexidades são únicos de cada organização e os seus requisitos direcionam à implantação do SGSI.

A norma traz ainda no Anexo A a descrição da lista de verificação; no Anexo B os papéis e responsabilidades pela Segurança da Informação; no Anexo C as informações sobre auditoria interna; no Anexo D a estrutura das políticas; e no Anexo E o monitoramento e medição.

2.3 ABNT NBR ISO/IEC 27004

A norma ABNT NBR ISO 27004:2010 foi publicada em 2010. Ela sugere padrões para desenvolvimento de métricas e medidas de desempenho como forma de avaliar os SGSI. A norma fornece orientação e ajuda para as organizações, para que elas melhorem a eficácia e a eficiência dos seus SGSI, gerando dessa forma indicadores e formas para medir a eficácia e eficiência (MANOEL, 2014, p.92).

Esta norma é um guia para auxiliar quem deseja implementar um SGSI nas organizações. Se atribui esta implementação a componentes existentes na ISO 27001 assim como gestão de risco, politicas, controles, processos e procedimentos.

A norma permite que as organizações avaliem a eficiência dos seus controles sob a sua segurança da informação, e que avaliem a eficiência da implementação de um SGSI, para verificar métricas que indicam se os requisitos de segurança estão sendo corretamente aplicados, auxilia na melhoria do desempenho da segurança ao que se trata de riscos de negócios e fornece dados para a gestão visando auxiliar a tomada de decisão. Alguns dos objetivos das normas são:

a) Avaliar a eficácia dos controles;
b) Avaliar a eficácia do SGSI;
c) Verificar se os requisitos da SI foram atendidos;
d) Melhorias nos controles implantados;
e) Melhorias na análise de riscos;
f) Auxiliar a tomada de decisões gerenciais;
g) SGSI sob uma perspectiva de negócios;
h) Facilitar decisão de investimento em SI.

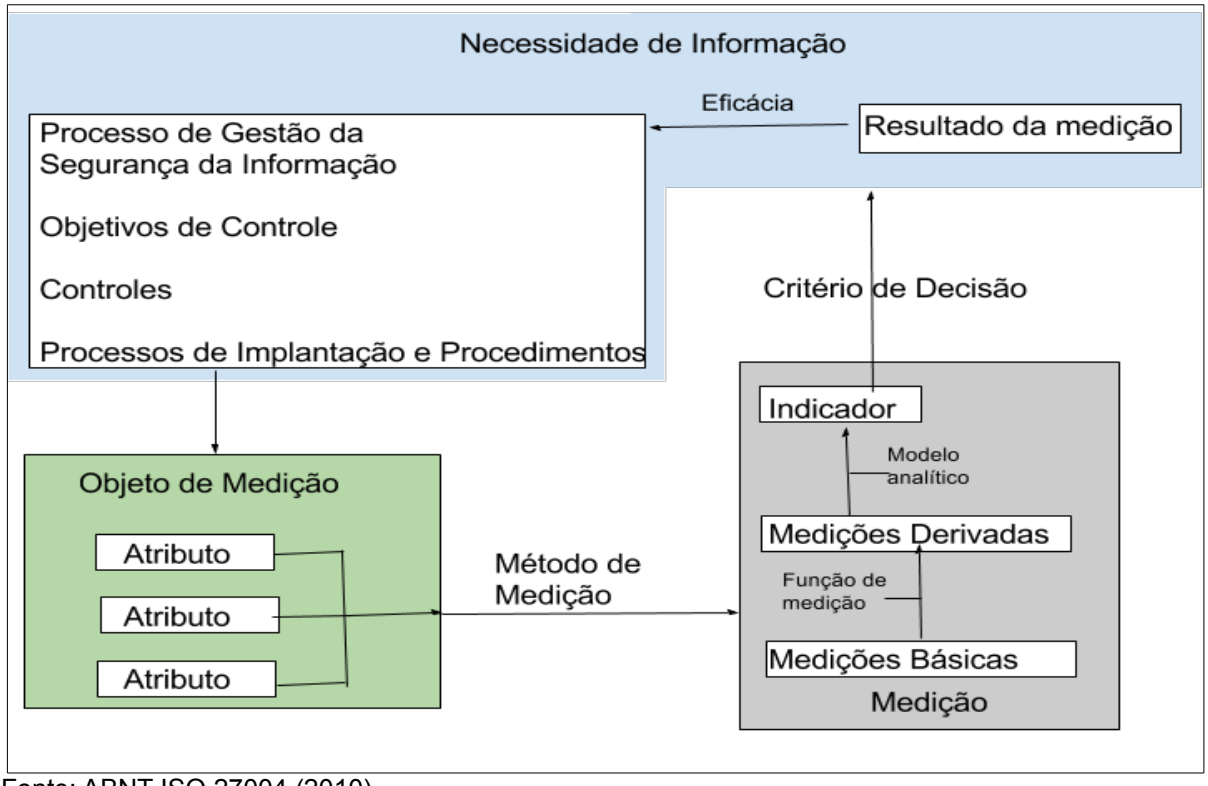
A norma apresenta como implementar um Programa de Medição da Segurança da Informação (PMSI) que é um sistema de medição que possibilita uma visão adequada dos investimentos em segurança da informação, servindo de apoio para a tomada de decisão da alta administração. Um PMSI leva em conta a complexidade do SGSI, os seus papéis, responsabilidades e medidas implementadas além de considerar também os processos de negócios. Para ser considerado efetivo um PMSI deve incluir os seguintes processos:

a) Desenvolvimento de medidas e medições;
b) Operação da medição;
c) Relato do resultado da análise de dados e medições;
d) Avaliação e melhoria do PMSI.

Dentre os benefícios da implantação do PMSI está a demonstração de conformidade da organização com requisitos legais, apoio a identificação de questões relativas à segurança da informação, também colabora em satisfazer as necessidades da administração quanto a definição das medições para atividades e é usado como entrada para o processo de gestão de risco em segurança da informação, para auditorias internas do SGSI e análise críticas dos resultados.

A norma cita os requisitos mínimos para um modelo de medição como definir o propósito da medição, os objetivos de controles, o objeto de medição e o processo para coleta e análise dos dados, a Figura 6 apresenta um modelo de medição conforme a norma 27004.

Figura 6: Modelo de medição da ISO 27004



Fonte: ABNT ISO 27004 (2010)

Objeto de medição é a caracterização de um item através da medição dos seus atributos. Ele está diretamente ligado a necessidade de informação e pode ser um produto, serviço ou um processo. O método de medição é uma sequência de operações usada na quantificação de um atributo dentro de uma escala. Medida básica é a medida definida e pode ser divida em escalas. A medida derivada se trata da função realizada para combinar medidas básicas. Indicador é a medida do atributo conforme as necessidades de informação definidas. Os critérios de decisão são as margens, alvos ou os padrões usados para determinar a necessidade ou não de uma tomada de ação. E por fim o resultado da medição se trata dos indicadores e suas interpretações que atendam uma necessidade de informação.

A norma 27004 também foi projetada com a ideia de ser flexível e para isso cita o modelo cíclico PDCA (Figura 7). Dentre essas, a etapa de planejamento (Plan) define políticas, processos, objetivos, metas e procedimentos importantes para a gestão de risco e desenvolve os processos de segurança da informação para assim atrair resultados consistentes com os objetivos organizacionais. A etapa de fazer (Do), que possui como objetivo a implementação dos processos, procedimentos e políticas definidos na etapa de planejamento. Assim na etapa de checagem (Check) é feito um balanço de ações corretivas. E na etapa de agir (Act) seja garantido que existam ações preventivas e de melhorias baseadas nas implicações resultantes do processo de auditoria interna para que assim haja contínua melhoria do processo de gestão do SGSI (CAMPONAR, 2004).

Figura 7: Modelo PDCA

Fonte: ABNT ISO 27004 (2010)

2.4 ABNT NBR ISO/IEC 25020

A norma ABNT NBR ISO/IEC 25020 faz parte da série de normas 25000 SQuaRE, que tem por objetivo normatizar áreas como a engenharia de software, requisitos de qualidade e avaliação do produto de software, a série 25000 (Figura 8) contém um conjunto de normas distribuídas nas seguintes divisões:

a) Divisão da Gestão da Qualidade (ISO / IEC 2500n);
b) Divisão de Modelo de Qualidade (ISO / IEC 2501n);
c) Divisão de Medição de Qualidade (ISO / IEC 2502n);
d) Divisão de Requisitos de Qualidade (ISO / IEC 2503n);
e) Divisão de Avaliação da Qualidade (ISO / IEC 2504n).

Figura 8: Organização da série 25000 SQuaRE

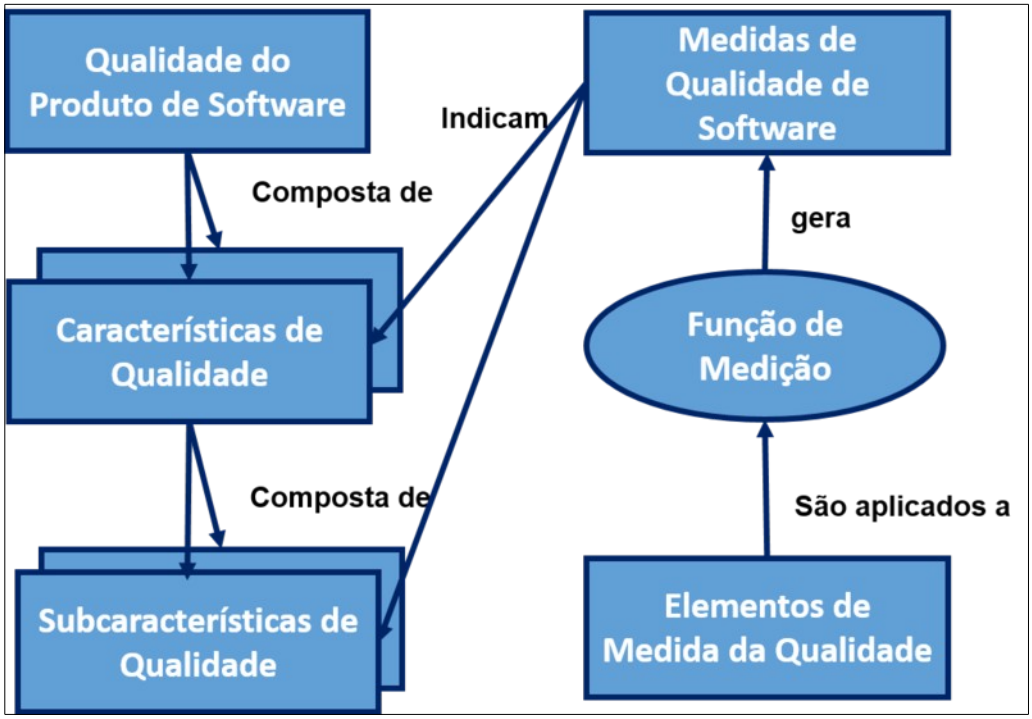
Fonte: ABNT ISO 25020 (2009)

O desenvolvimento da série 25000 SQuaRE de padrões internacionais é interessante para as organizações que são unificadas e logicamente organizadas pois ela abrange três processos complementares: especificação, medição e avaliação de requisitos. As normas da série 25000 SQuaRE tem como objetivo auxiliar aqueles que desenvolvem e também aqueles que compram produtos de software com a especificação e avaliação dos requisitos de qualidade do produto. Ela estabelece critérios de especificação dos requisitos de qualidade dos produtos de software e a sua avaliação. Incluindo um modelo de qualidade para alinhar as definições de qualidade do cliente com as características do produto de software.

Dentre os principais benefícios das normas 25000 SQuaRE incluem a orientação sobre medição e avaliação da qualidade dos produtos de software, a orientação para a especificação dos requisitos de qualidade dos produtos de software, e a harmonização com a norma ISO/IEC 15939 sob a forma de modelo de referência de medição de qualidade.

A norma ISO 25010 fornece um modelo e defini termos para as características de qualidade do produto de software e estas características são decompostas em subcaracterísticas. A norma ISO 25020, divisão de medição de qualidade, fornece informações e orientações sobre como medir as características e subcaracterísticas de um modelo de qualidade. Esta norma fornece uma referência modelo e guia para a medição das características de qualidade definidas na ISO 25010. Os padrões associados e os relatórios técnicos da divisão de medição de qualidade descrevem medidas de qualidade ao longo do ciclo de vida do produto (Figura 9).

Figura 9: Modelo para a medição de qualidade de produto de software



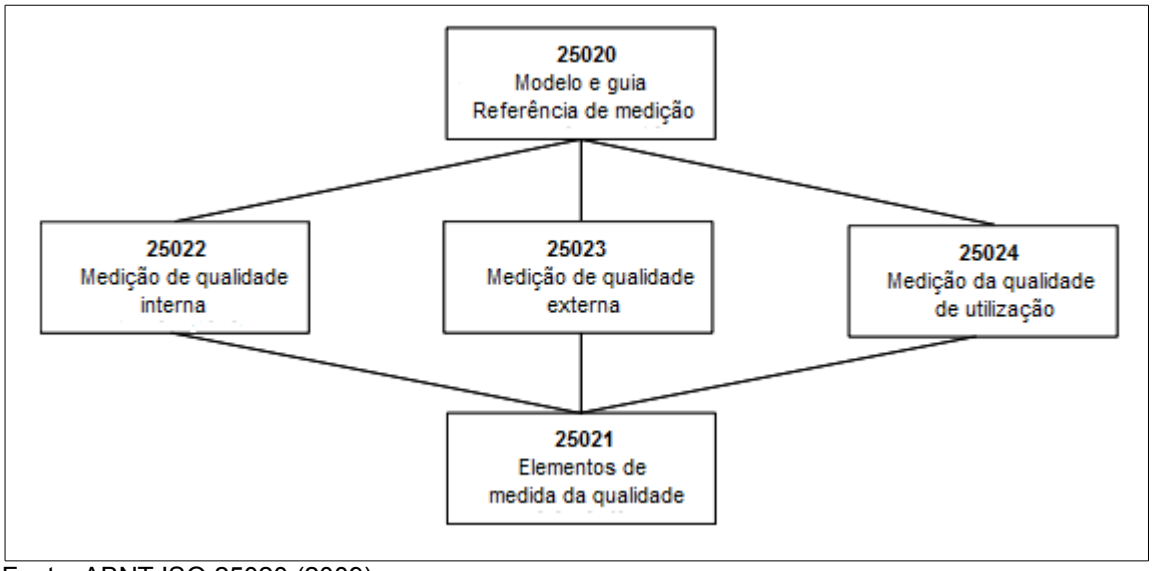
Fonte: ABNT ISO 25020 (2009)

A ISO 25020 também possui subdivisões (Figura 10), como por exemplo a ISO 25021 que nos oferece elementos de medida de qualidade que podem ser usados para construir medidas de qualidade de software. Os elementos de medida

de qualidade podem medir uma representação estática do software, o comportamento ou os efeitos do software quando ele é usado.

ISO 25022, ISO 25023 e ISO 25024 descrevem medidas para as características do modelo de qualidade. Medidas internas caracterizam a qualidade do produto de software com base em representações estáticas do software, medidas externas caracterizam a qualidade do produto de software com base no comportamento do sistema baseado em computador, incluindo o software, e medidas de qualidade em uso caracterizam a qualidade do produto de software com base nos efeitos do uso do software.

Figura 10: Estrutura da divisão de Medição da Qualidade



Fonte: ABNT ISO 25020 (2009)

Desenvolvedores, avaliadores, gerentes de qualidade, clientes, fornecedores e outros usuários de software podem selecionar medidas e relatórios técnicos para a medição de características de qualidade de interesse. Na prática, isto pode ser no que diz respeito à definição de requisitos, avaliação de produtos de software, gestão da qualidade e outros fins.

2.5 ABNT NBR ISO/IEC 25030

Assim como a ISO 25020 a norma ABNT NBR ISO/IEC 25030 faz parte da série de normas 25000 SquaRE. Ela contém uma série de normas distribuídas nas seguintes divisões:

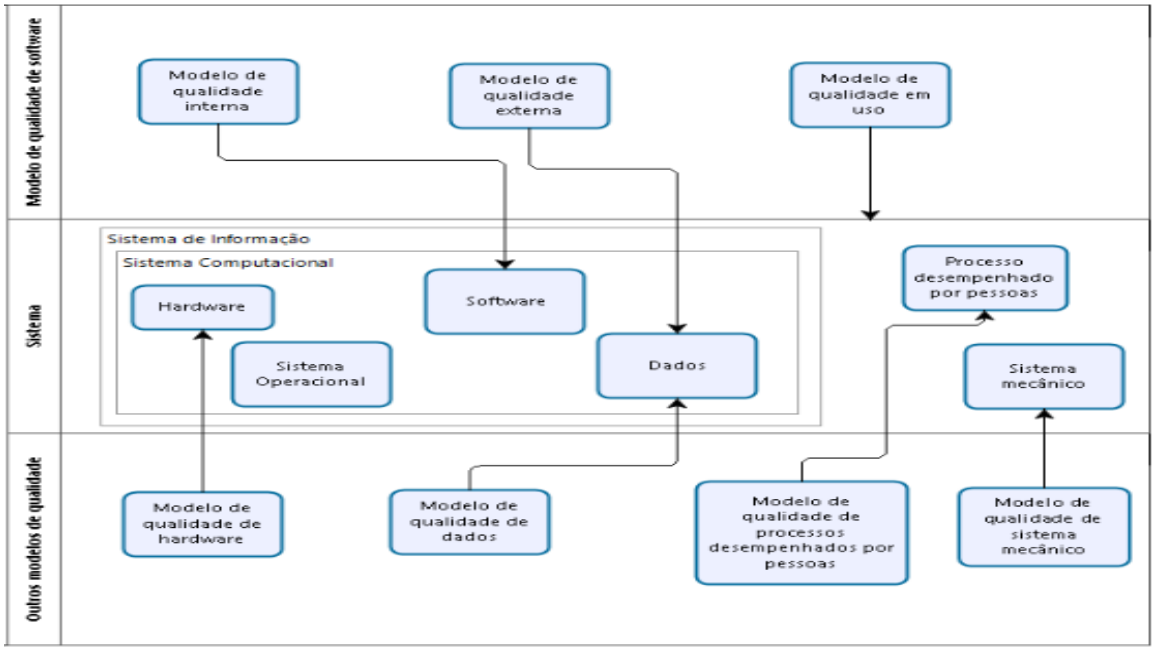
a) Divisão da Gestão da Qualidade (ISO / IEC 2500n);
b) Divisão de Modelo de Qualidade (ISO / IEC 2501n);
c) Divisão de Medição de Qualidade (ISO / IEC 2502n);
d) Divisão de Requisitos de Qualidade (ISO / IEC 2503n);
e) Divisão de Avaliação da Qualidade (ISO / IEC 2504n).

Os requisitos de qualidade de um software devem ser devidamente identificados como parte dos requisitos para um produto de software. A norma ISO/IEC 25030 visa o estudo dos requisitos de qualidade de software, mas ela também tem uma concepção de sistema.

Os requisitos de qualidade de software também possuem uma relação com os requisitos funcionais e eles podem resultar em novos requisitos funcionais. Os requisitos de qualidade do software podem ser categorizados usando um modelo de qualidade. O modelo de qualidade (Figura 11) define 3 diferentes concepções de qualidade:

a) Qualidade do software em uso;
b) Qualidade externa de software;
c) Qualidade interna do software.

Figura 11: Modelo de Sistema e Qualidade



Fonte: ABNT ISO 25030 (2008)

A qualidade de um sistema é dependente da qualidade dos seus elementos e as suas interações. A qualidade do software é a capacidade do produto de software em satisfazer necessidades do sistema. O modelo de qualidade do produto de software encontrado na ISO/IEC 25010 define 6 características de qualidade que são funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade.

A ISO/IEC 25030 impõe uma característica de qualidade a mais, a Qualidade em Uso, que mensura a capacidade do software em permitir que usuários atinjam suas metas com produtividade, eficácia, satisfação e segurança.

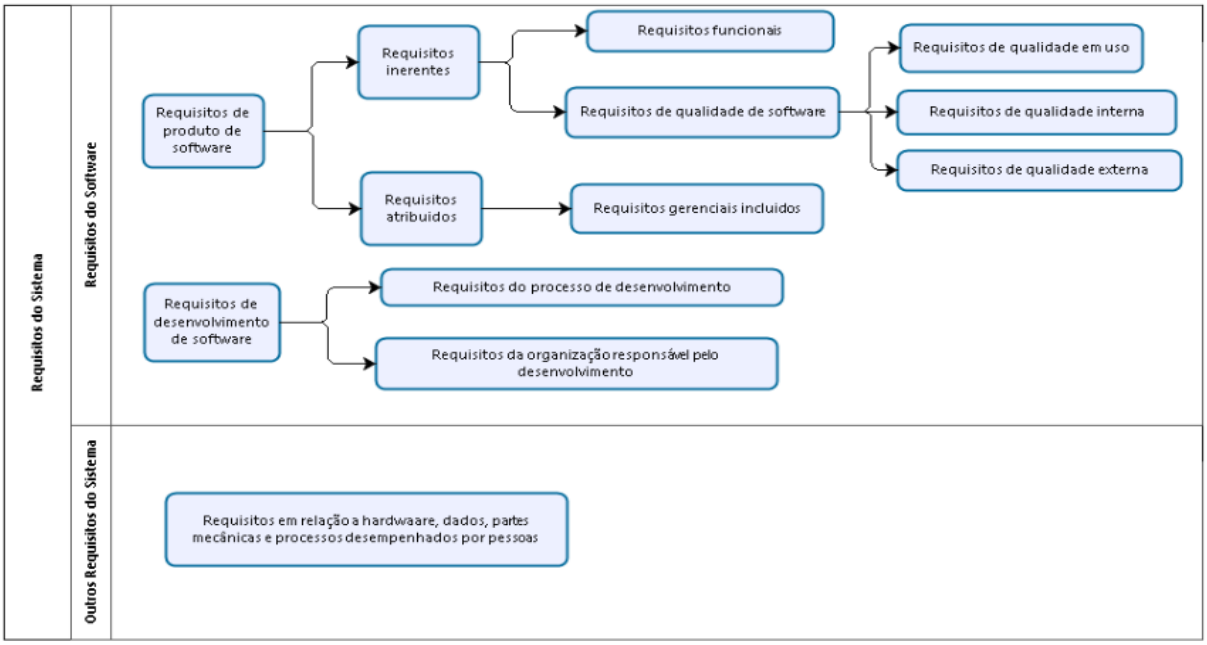
As características de qualidade de um software possuem subcaracterísticas e a norma leva em conta as subcaracterísticas definidas pelo usuário. Em um modelo de medição de qualidade de software os atributos do software podem ser mensurados quantitativa ou qualitativamente.

Os atributos de qualidade de um software são mensurados pela aplicação de um método de medição. Um método de medição é uma sucessão de operações lógicas utilizadas na quantificação de um atributo em relação a uma escala, o resultado desse método de medição é a medida básica.

As características e subcaracterísticas de qualidade de software também podem ser quantificadas por meio da aplicação de funções de medição, que são algoritmos utilizados para combinar elementos de medida de qualidade dos softwares. A aplicação de uma função de medição resulta na medida de qualidade de software, e mais de uma delas podem ser utilizadas para mensurar uma característica ou uma subcaracterística de qualidade.

Os requisitos de qualidade dos produtos de software (Figura 12) são necessários para especificação, planejamento, desenvolvimento e avaliação do software. Algumas recomendações de requisitos de qualidade de produto de software que a norma ISO/IEC 25030 indica são os requisitos especificados e os não especificados pelo cliente, os requisitos legais e regulatórios relacionados com o produto desenvolvido, e outros requisitos necessários determinados pela organização.

Figura 12: Classificação de requisitos do sistema



Fonte: ABNT ISO 25030 (2008)

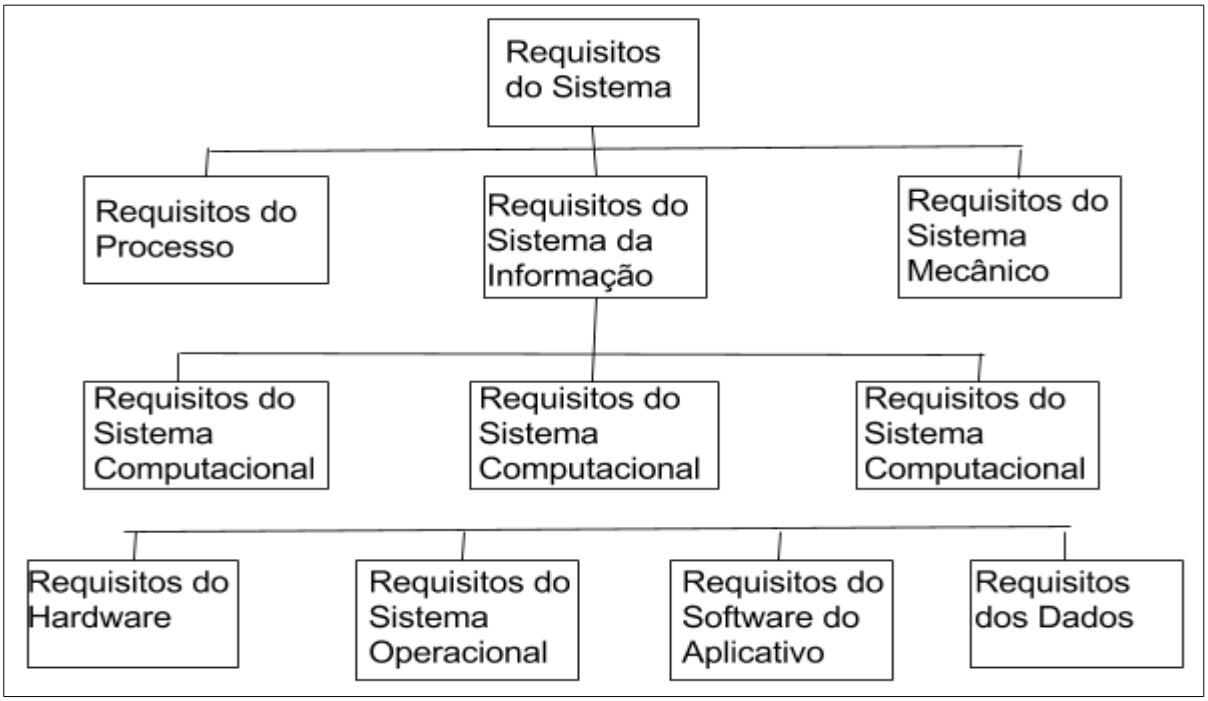
A norma ISO/IEC 25030 tem por padrão que esses requisitos de qualidade podem ser usados no processo de elicitação de requisitos de qualidade para um produto de software que venha a ser desenvolvido ou como um processo de entrada para avaliação de um software.

Se os requisitos de qualidade do software não forem claramente definidos, podem ser vistos, interpretados, implementados e avaliados de forma diferente por pessoas diferentes. Isto pode resultar em software que é inconsistente com as expectativas dos usuários e assim se tornando um software de má qualidade, deixando usuários, clientes e desenvolvedores insatisfeitos, e ocorrendo perda de tempo e custo para retrabalho de software.

Todos os requisitos de qualidade de software levantados pelas partes interessadas devem ser considerados, quando possível e necessário o desenvolvimento de cenários e interações com os usuários do sistema devem ser utilizados para identificar os requisitos de qualidade.

Com a execução de um processo para análise é possível fazer com que estes requisitos ganhem uma visão técnica, para que dessa forma esses requisitos possam ser utilizados para produzir o sistema desejado. Essa visão técnica dos requisitos é conhecida como requisitos do sistema. Os requisitos do sistema são verificáveis e devem indicar quais as características que o sistema deve ter para que possa atender os requisitos definidos pelas partes interessadas (Figura 13).

Figura 13: Hierarquia dos requisitos do sistema e do software



Fonte: ABNT ISO 25030 (2008)

Os requisitos de qualidade do software devem estar sempre relacionados com as características ou subcaracterísticas de qualidade conforme determinado no modelo de qualidade aplicado. Os requisitos de qualidade de software tem de ser estabelecidos quanto a medidas de qualidade de software e o valor esperado.

As medidas de qualidade de software utilizadas e os critérios utilizados para a seleção destas medidas precisam ser documentadas de acordo a ISO/IEC 25020, e também é preciso registrar para quais funções do software o requisito de qualidade é aplicável. Ao estabelecer um valor esperado de um requisito de qualidade de software, a tolerância aceitável também deve ser documentada.

Os limites funcionais e as limitações de implementação do software precisam ser documentados, a documentação deve apontar os limites estruturais do software em níveis altos na estrutura do sistema com relação as funções que serão implementadas como parte do software.

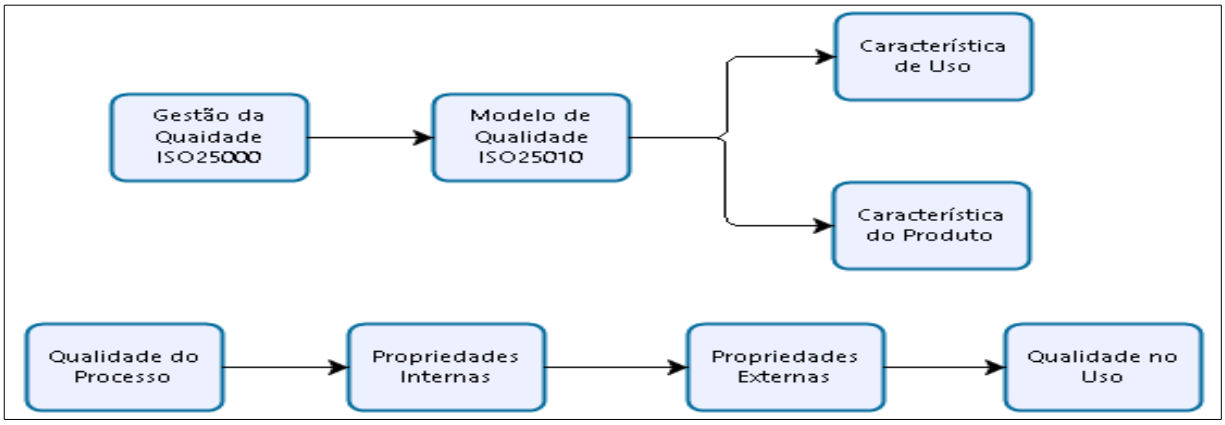
2.5.1 Critérios

Na área de medidas de qualidade do produto de software os padrões são derivados das normas ISO/IEC 9126 e 14598, os atributos dos softwares podem ser

avaliados por medição direta, indireta ou medição de suas consequências, tudo depende dos critérios que serão utilizados na avaliação do produto de software e na forma que forem exploradas as definições e o detalhamento da aplicação de medidas práticas de qualidade interna, externa e de uso.

Segundo a norma ABNT 25030 (2008) o recomendado para a correta avaliação de qualidade de um produto de software, é necessário que seja definido um modelo de qualidade (Figura 14) e que este modelo de qualidade seja utilizado nas definições dos critérios de avaliação dos softwares e na definição das metas de qualidade para os produtos de software final e intermediários.

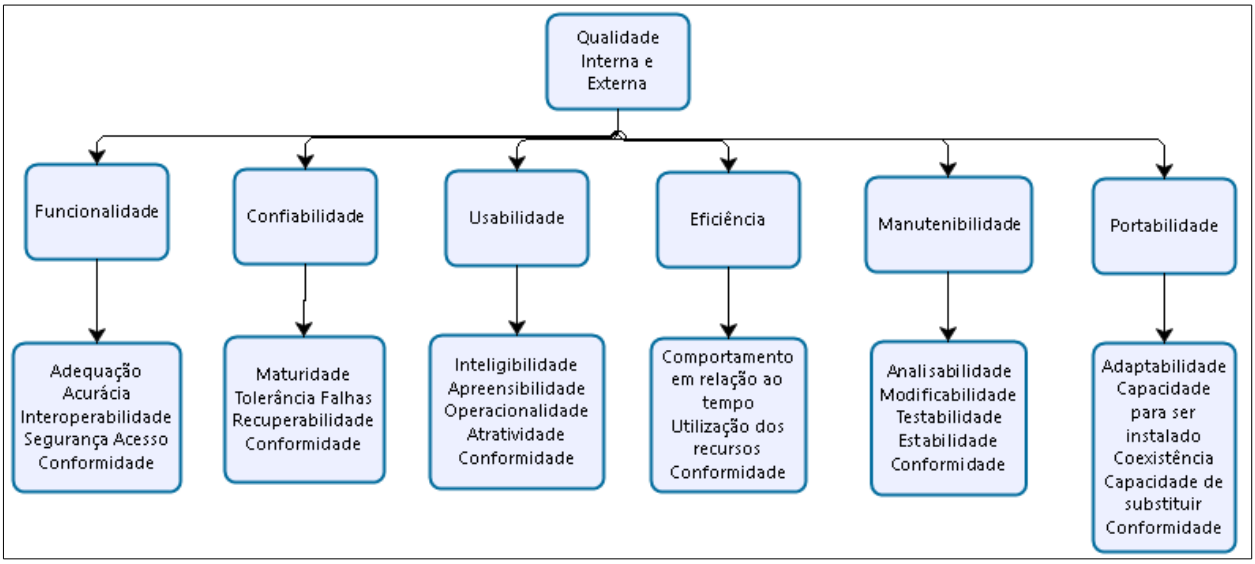
Figura 14: Modelo de qualidade



Fonte: ABNT ISO 25010 (2011)

Conforme abordado na norma ISO/IEC 25010 (2011) existe uma divisão de modelo de qualidade do produto de software definido em seis características de qualidade. A norma apresenta as características e subcaracterísticas de qualidade interna e externa (Figura 15).

Figura 15: Características e Subcaracterísticas do Modelo de Qualidade



Fonte: ABNT ISO 25010 (2011)

a) Funcionalidade: Capacidade do software em disponibilizar funções que satisfaçam as necessidades quando utilizado em condições específicas:
   - Adequação: se o software faz o que ele deveria fazer;
   - Acurácia: se o software faz o que ele promete corretamente;
   - Interoperabilidade: se o software interage com os outros sistemas;
   - Segurança de Acesso: se o software não permite acesso não autorizado a dados e programas;
   - Conformidade: se o software esta de acordo com as normas e leis.

b) Confiabilidade: Capacidade do software de manter um bom nível de desempenho quando utilizado em condições específicas:
   - Maturidade: apresenta a frequência que o software apresenta falhas;
   - Tolerância a Falhas: com que flexibilidade o software reage as falhas;
   - Recuperabilidade: se o software consegue recuperar os dados em caso de falhas;
   - Conformidade: se o software está de acordo com os padrões e normas de confiabilidade.

c) Usabilidade: Capacidade do software em ser entendido, assimilado, utilizado e atraente ao ponto de vista do usuário:

- Inteligibilidade: se é fácil de entender o conceito e a aplicação do software;
- Apreensibilidade: se é fácil de aprender a utilizar o software;
- Operacionalidade: se é fácil de operacionalizar e controlar o software;
- Atratividade: se o software é atrativo aos usuários;
- Conformidade: se o software está de acordo com os padrões e normas de usabilidade.

d) Eficiência: Capacidade do software de manter o desempenho adequado em condições explícitas:
   - Comportamento em relação ao tempo: se o software tem um bom tempo de resposta e velocidade de execução;
   - Utilização dos recursos: se o software utiliza muitos recursos;
   - Conformidade: se o software está de acordo com os padrões e normas de eficiência.

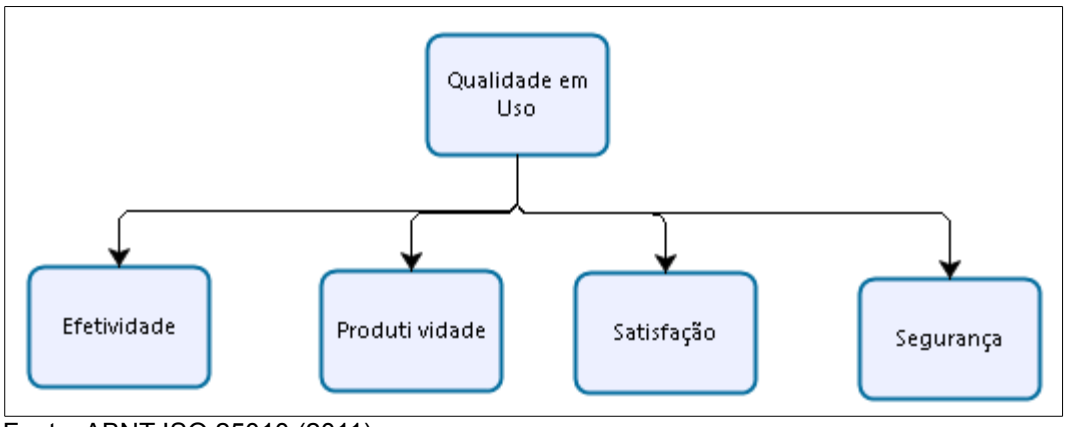
e) Manutenibilidade: Capacidade do software em ser alterado. As alterações podem ser melhorias, correções ou adaptações do software:
   - Analisabilidade: se é fácil de detectar as falhas do software;
   - Modificabilidade: se é fácil modificar e adaptar o software;
   - Testabilidade: se é fácil testar as mudanças feitas no software;
   - Estabilidade: se há riscos ao fazer alterações no software;
   - Conformidade: se o software está de acordo com os padrões e normas de manutenibilidade.

f) Portabilidade: Capacidade do software em ser migrado de ambiente:
   - Adaptabilidade: se é possível adaptar o software a outros ambientes;
   - Capacidade para ser instalado: se é fácil de instalar o software em outros ambientes;
   - Coexistência: se pode coexistir com outros produtos independentes;
   - Capacidade de Substituir: se é fácil substituir o software por outro;
   - Conformidade: se software está de acordo com padrões de portabilidade.

A ISO/IEC 25030 também apresenta e indica o uso da característica de Qualidade em Uso, que mensura a capacidade do software em permitir que usuários atinjam suas metas com produtividade, efetividade, satisfação e segurança (Figura 16):

a) Efetividade é a capacidade que o software tem para fazer com que o usuário consiga atingir os seus objetivos de negócio de forma correta e completa.
b) Produtividade é a capacidade do software em permitir que o usuário consiga utilizar a quantidade necessária de recursos com eficácia para que ele possa atingir um objetivo em específico.
c) Satisfação é a capacidade do software de satisfazer o seu usuário enquanto ele o utiliza.
d) Segurança é a capacidade do software de apresentar níveis aceitáveis de riscos para o cliente.

Figura 16: Características de Qualidade em Uso



Fonte: ABNT ISO 25010 (2011)

Sabendo que é necessário alocar recursos para a avaliação dos softwares, muitas vezes medir todas as subcaracterísticas internas e externas de todas as partes de um software de grande porte não é possível. Da mesma maneira, não é prático medir a qualidade em uso para todos os cenários de uso.

Dessa forma, dependendo dos objetivos de negócios e da natureza do produto e dos processos utilizados nas avaliações as definições dos critérios a serem utilizados podem definir por onde o seguimento do projeto vai andar. Com

base nas características e subcaracterísticas citadas neste capítulo será possível definir os critérios de avaliação dos softwares que serão testados.

2.5.2 Métricas

As características de qualidade de um software não permitem mensurar diretamente as suas características e subcaracterísticas, dessa forma se faz necessário determinar métricas que se relacionam com as características do software. Todos os atributos, tanto interno quanto externo, do software que interajam com o ambiente e se relacionem com alguma característica do software pode vir a se tornar uma métrica.

Métricas internas são os indicadores para avaliar um software. Elas são as medições de um software considerando as suas próprias características internas, ou seja, sem a execução dos programas.

Métricas externas são os indicadores para avaliar um software. Elas são as medições de um software considerando o comportamento do seu sistema ou dos seus resultados no ambiente.

As métricas de qualidade em uso são os indicadores utilizados para avaliar um software. Elas são as medições de um software considerando a qualidade do software em cenários e tarefas do dia a dia dos usuários.

As definições de bases para as escolhas das métricas dependem das metas selecionadas de negócios para o produto em questão e também das necessidades de quem avalia o produto. Necessidades estas que geralmente são especificadas por critérios de medidas.

Para que comparações entre produtos de software sejam feitas com êxito, é necessário que sejam selecionadas métricas rigorosas para avaliar estes softwares. Os processos para mensurar as características e subcaracterísticas de qualidade do software devem possuir uma precisão suficiente para que possam ser estabelecidos critérios e comparações entre os softwares. É preciso também que seja considerada uma tolerância a possíveis falhas de medição.

Na relação dos resultados das métricas definidas para que ocorram as comparações entre softwares, o relatório deve explanar se as métricas utilizadas são objetivas, empíricas e utilizem uma escala válida e, ainda, sejam reprodutíveis.

Para que sejam consideradas objetivas, as métricas devem possuir um procedimento para demarcar o número ou categoria ao atributo do produto. Para que sejam consideradas empíricas, os dados devem ser alcançados por observação ou através de um questionário. Para utilizarem uma escala válida, os dados devem se basear em itens de valor igual ou com um valor conhecido. Para que sejam consideradas reprodutíveis, os processos de medição de software devem gerar resultados nas mesmas medidas, mesmo que sendo geradas por pessoas e ocasiões diferentes fazendo as mesmas medições do software.

É importante que as métricas possuam algumas correlações. Como quando, por exemplo, é necessário que uma medida interna de um atributo de software específico possa correlacionar-se com alguma medida externa. Também é importante que as medições resultem valores que se aproximem com as expectativas dos usuários.

2.6 Considerações Finais do Capítulo

As normas citadas neste capítulo procuram proporcionar opções de melhorias e padronização quanto a qualidade dos requisitos de qualidade de um software SGSI. Elas disponibilizam requisitos e recomendações para requisitos de qualidade e orientações para os processos utilizados durante a definição e análise dos requisitos de qualidade.

As normas serão utilizadas visando estabelecer um padrão para critérios e métricas para auxiliar na avaliação dos softwares que serão utilizados no decorrer do trabalho.

3 PROPOSTA DE SOLUÇÃO

A proposta de solução deste trabalho consiste em analisar softwares, desenvolvidos em código livre, a fim de verificar quais destes softwares realizam o gerenciamento do SGSI de acordo com a norma ABNT/NBR 27001, que rege um padrão para o gerenciamento e gestão da segurança da informação nas organizações.

Para chegar ao resultado esperado serão definidas duas ferramentas de softwares de gerenciamento de segurança da informação para serem avaliadas, os critérios e métricas para avaliar estes softwares serão definidos com base nas normas ABNT/NBR 25020 e 25030 visando seguir um padrão de avaliação de softwares.

3.1 Ferramentas SGSI de Código Aberto

Conforme Hermanowski (2015) existe um bom número de ferramentas SGSI proprietárias e de código livre disponíveis. Entre as ferramentas proprietárias pode-se citar, como por exemplo a IBM Security Radar, a HP Arcsight e a LogRhythm. Também existem as ferramentas não comerciais, que são as ferramentas de código aberto, entre elas pode-se citar a Security Onion, a Ebios, a ELK Stack, o Prelude-OSS, a Logalyze e a OSSIM (Tabela 2). Os softwares citados foram selecionados após uma pesquisa que envolveu consultas a materiais disponíveis na internet, principalmente revistas digitais e artigos como Open Source Security Information And Event Management System (2014), Tryfonas e Askoxylakis (2015), Antolik (2013), Hermanowski (2015) e Upguard (2017).

Considerando os prós e os contras, que foram definidos com base em dados retirados dos sítios dos desenvolvedores dos softwares disponíveis e citados, a decisão foi selecionar dois software para dar seguimento com os testes: OSSIM e Ebios. Apenas essas ferramentas foram selecionadas para avaliação por serem os softwares que possuem as funcionalidades mais próximas ao estabelecido na norma ABNT NBR 27001.

Tabela 2: Prós e Contras dos Softwares SGSI

Nome do Software	Prós	Contras
OSSIM	Código livre; Administrar rede; Detecção de intrusão; Prevenção; Interface gráfica amigável.	Desenvolvido para suportar infraestruturas pequenas.
Security Onion	Código livre; Administrar rede; Detecção de intrusão; Prevenção.	Sem camada de integração de ferramentas.
Logalyze	Código livre; Monitoramento e gerenciamento de log; Atua em tempo real.	Trata apenas log e não possui atualização desde 2013.
Ebios	Código livre; Gerenciamento de riscos, ameaças e vulnerabilidades; Tratamento de problemas na identificação dos riscos.	Desenvolvido para suportar infraestruturas pequenas.
ELK Stack	Código livre; Análise, registro e visualização de dados.	Exige a implementação de mecanismos de alimentação de dados.
Prelude-OSS	Código livre; Análises estáticas; Correlações e alertas.	Não possui documentação, gerenciamento de recursos e scanner de vulnerabilidades.

Fonte: HERMANOWSKI (2015)

A ferramenta Open Source Security Information Management (OSSIM) é um sistema de gerenciamento de eventos e informações de segurança de fonte aberta, integrando uma seleção de ferramentas livres e abertas projetadas para suportar administradores de rede em segurança de computadores, detecção de intrusão e prevenção. É considerado como uma camada acima da segurança comum com ferramentas que unificam sua gestão em uma única e consistente interface amigável.

OSSIM executa funções de um SGSI usando outros componentes de segurança de software de fonte aberta bem conhecidos. A interface fornece ferramentas de análise gráfica para informações coletadas dos componentes de software de código aberto subjacentes, muitos dos quais são apenas ferramentas de

linha de comando, e permite o gerenciamento centralizado de suas opções de configuração.

OSSIM é desenvolvido como iniciativa da empresa AlienVault, cujo principal objetivo é a integração das ferramentas subjacentes e o desenvolvimento da correlação destas ferramentas (ALIENVAULT, 2017).

O Clube Ebios criou a Divisão Central de Segurança de Sistemas de Informação na França. A ferramenta é suportada por uma organização chamada Clube Ebios. Esta ferramenta é de código aberto e de utilização gratuita. Funciona com o princípio do método 5 fases do Clube Ebios. Todo o trabalho e os resultados permitem ao usuário capturar os documentos resultantes. A ferramenta está disponível em 4 idiomas e inglês, francês, espanhol e alemão. É usado por países da União Européia como França, Bélgica, Luxemburgo e outros. Fora da União Européia, é usado em países como Tunísia e Quebec.

Hoje, esta ferramenta é usada em cerca de 1.000 entidades principalmente do setor privado. A Ebios é atribuída a organizações governamentais e supranacionais, tanto comerciais como não comerciais. O Ebios é um aplicativo independente que tem como base a linguagem de programação Java que funciona com o tipo de documentos XML. Portanto, não importa, qual plataforma o usuário usa os serviços Ebios. A ferramenta também suporta a edição de riscos, ameaças e vulnerabilidades. Além disso, oferece tratamento de problemas na identificação de riscos (CLUBEBIOS, 2017).

Dentre os softwares que não foram selecionados para dar seguimento com os testes, o Security Onion que é uma ferramenta de distribuição Linux, contendo um conjunto de ferramentas de segurança semelhante ao OSSIM, mas sem qualquer camada de integração. Cada ferramenta é usada separadamente. Ela está sendo bastante usada como uma distribuição de análise de segurança de rede (LLC, 2017).

Logalyze é um software de código aberto de monitoramento e gerenciamento de log. É capaz de executar correlação em tempo real e gerar relatórios sobre conformidades. Não houve nenhuma atualização no projeto desde 2013 (ZURIEL, 2017).

A ELK Stack é uma solução geral para uma pesquisa mais aprofundada, análise de dados, registro e visualização de dados centralizados. Esta não é certamente uma solução das mais utilizadas pois ela exige a implementação de

mecanismos de alimentação e análise de dados o que a deixa atrás ao compará-la com outras ferramentas SGSI (ELASTICSEARCH, 2017).

Prelude-OSS é uma versão de código aberto do Prelude comercial. Ele armazena eventos por padrão em formato Intrusion Detection Message Exchange Format (IDMEF). Ele pode realizar análises estáticas, correlações e alertas. Infelizmente não tem documentação integrada, nenhum gerenciamento de recursos e nenhum scanner de vulnerabilidades. A solução não é amplamente adotada (PREWIKKA, 2017).

3.2 Critérios Para Avaliação Dos Softwares

Conforme colocado na seção 2.5.1 o modelo de qualidade do produto de software por padrão é dividido em seis características de qualidade interna e externa, que são subdividas em subcaracterísticas (Figura 15).

Com base no entendimento do modelo de qualidade selecionado, na definição dos softwares a serem avaliados e no que é mais relevante para o desenvolvimento do trabalho conforme a norma ABNT/NBR 27001 foram selecionados alguns critérios para a avaliação dos softwares (Tabela 3).

A característica funcionalidade foi selecionada pois é importante que o sistema cumpra aquilo que ele propunha com êxito, por isso serão utilizadas algumas subcaracterísticas de funcionalidade como adequação, acurácia e conformidade.

A característica confiabilidade foi selecionada pois é importante saber se o software possui a capacidade de manter um bom nível de desempenho quando utilizado em condições específicas e por isso serão utilizadas algumas subcaracterísticas de confiabilidade como maturidade e tolerância a falhas.

A característica usabilidade foi selecionada pois é importante que o sistema seja atrativo perante o usuário para que ele possa sentir confiança ao utilizar o sistema e por isso serão utilizadas algumas subcaracterísticas de usabilidade como operacionalidade e atratividade.

A característica eficiência foi selecionada pois é importante entender se o software tem a capacidade de manter o desempenho adequado em condições

explícitas e por isso serão utilizadas algumas subcaracterísticas de eficiência como comportamento em relação ao tempo e utilização de recursos.

A característica portabilidade foi selecionada pois é importante entender se o sistema é hábil para ser utilizado em outros ambientes e plataformas e por isso serão utilizadas algumas subcaracterísticas de portabilidade como adaptabilidade e coexistência.

A outra característica de qualidade, que não será utilizada, é Manutenibilidade pois o objetivo do trabalho não é alterar ou incluir novas funcionalidades no software e sim testar as suas funcionalidades já impostas.

Quanto as características de qualidade em uso, serão utilizados todos os critérios de efetividade e produtividade, pois elas funcionam como indicadores para avaliar o software. Elas são as medições de um software considerando a qualidade do software em cenários e tarefas do dia a dia dos usuários, e convém com os testes que serão aplicados nos softwares. As características selecionas foram a efetividade e a produtividade.

Efetividade foi selecionada pois ela é capaz de mensurar se o software permiti que o usuário consiga atingir os seus objetivos de negócio de forma correta e completa.

Produtividade foi selecionada pois ela é importante para mensurar se o software permiti que o usuário consiga utilizar a quantidade necessária de recursos com eficácia para que ele possa atingir um objetivo em específico.

As demais características do modelo de qualidade em uso não serão considerados, a característica de Segurança por se tratar de somente testes internos feitos no software ele não corre riscos de ataques externos, dessa forma impossibilitando de mensurar as métricas dessa característica. A outra característica que não será utilizada é Satisfação pois, a forma de avaliação dessa característica seria através de questionários na população que realizou os testes e somente seria válido se outras pessoas testassem os sistemas.

Tabela 3: Critérios para Avaliação

Área	Critérios	Considerado	Descartado
Características de Qualidade Interna e Externa			
Funcionalidade	Adequação	X	
	Acurácia	X	
	Interoperabilidade		X
	Segurança de Acesso		X
	Conformidade	X	
Confiabilidade	Maturidade	X	
	Tolerância a Falhas	X	
	Recuperabilidade		X
	Conformidade		X
Usabilidade	Inteligibilidade		X
	Apreensibilidade		X
	Operacionalidade	X	
	Atratividade	X	
	Conformidade		X
Eficiência	Comportamento em Relação ao Tempo	X	
	Utilização dos Recursos	X	
	Conformidade		X
Manutenibilidade			X
Portabilidade	Adaptabilidade	X	
	Capacidade Para Ser Instalado		X
	Coexistência	X	
	Capacidade de Substituir		X
	Conformidade		X
Características de Qualidade em Uso			
Efetividade		X	
Produtividade		X	
Satisfação			X
Segurança			X

Fonte: ABNT ISO 25010 (2011)

Um fator importante na avaliação dos softwares é o momento de definição dos critérios de avaliação, dada essa definição, o próximo passo é definir as métricas de avaliação dos softwares, para que seja possível mensurar esses critérios que foram definidos e assim chegar ao resultado desejado.

3.3 Métricas Para Avaliação Dos Softwares

Após a definição dos critérios a serem utilizados para a avaliação dos softwares foram definidas as métricas para mensurar esses critérios, as métricas selecionadas vão ser divididas entre os critérios.

Em alguns casos a escala vai ser dividida em três categorias que são alto, médio e baixo, em outros casos que não exijam maior complexidade a escala vai ser dividida em duas categorias que são satisfatório ou insatisfatório. Basta apenas que as categorias sejam especificadas de forma antecipada para que a avaliação dos softwares ocorra de forma correta.

As métricas internas são as medições de um software considerando as suas próprias características internas, ou seja, sem a execução dos programas. Com base nesse conceito fica evidente que avaliar os softwares, do ponto de vista do usuário, através da utilização de métricas internas se torna inviável, dessa forma elas não serão utilizadas.

As métricas externas são as medições de um software considerando o comportamento do seu sistema ou dos seus resultados no ambiente. Com base nisso foram definidas a utilização de algumas métricas externas (Tabela 4) para o seguimento do trabalho.

As métricas de qualidade em uso são as medições de um software considerando a qualidade do software em cenários e tarefas do dia a dia dos usuários. Com base nisso foram definidas a utilização de algumas métricas de qualidade em uso (Tabela 5) para o desenvolvimento desse trabalho.

A escolha dessas métricas se deu com base nas metas selecionadas de negócios para o produto em questão e também das necessidades de quem avalia o produto, dessa forma as métricas foram selecionadas com base na relevância que elas tem quanto as qualificações exigidas pela norma ABNT/NBR 27001 quanto ao gerenciamento e a gestão da segurança perante uma organização.

E também definição das métricas se deram também com base no objetivo do trabalho, para que comparações entre os produtos de software seja boa é necessário que sejam selecionadas métricas rigorosas para avaliar estes softwares. Os processos para mensurar as características e subcaracterísticas de qualidade do software devem possuir uma precisão suficiente para que possam ser estabelecidos critérios e comparações entre os softwares.

Tabela 4: Métricas de Qualidade Externa de Avaliação

Característica	Subcaracterística	Métrica	Propósito da métrica	Método de aplicação	Medida e Fórmula	Interpretação	Tipo de escala	Tipo de medida
Funcionalidade	Adequação	Adequação Funcional	Quão adequadas são as funções avaliadas?	Número de funções que são adequadas para executar as tarefas especificadas em comparação com o número de funções avaliadas.	X = 1-A / B A = Número de funções nas quais os problemas são detectados na avaliação B = Número de funções avaliadas	0 <= X <= 1 Quanto mais perto de 1, mais adequado.	Absoluta	Quantitativa
Funcionalidade	Acurácia	Precisão	Com que frequência os usuários finais encontram resultados com precisão inadequada?	Registre o número de resultados com precisão inadequada. Através dos relatórios emitidos pelas ferramentas e pelas consultas realizadas.	X = A / T A = Número de resultados encontrados pelos usuários com um nível de precisão diferente do requerido T = tempo de operação	0 <= X O mais próximo de 0 é o melhor.	Relação	Quantitativa Tempo
Funcionalidade	Conformidade	Conformidade de funcionalidade	Quão compatível é a funcionalidade do produto com os regulamentos, padrões e convenções aplicáveis?	Contar o número de itens que exigem conformidade que foram atendidos e comparar com o número de itens que exigem conformidade na especificação. Teste os casos de teste de acordo com os itens de conformidade. Realize testes funcionais. Contar o número de itens de conformidade que foram satisfeitos.	X = 1 - A / B A = Número de itens de conformidade de funcionalidade especificados que não foram implementados durante o teste B = Número total de itens de conformidade de funcionalidade especificados	0 <= X <= 1 O mais próximo de 1,0 é o melhor.	Absoluto	Quantitativa

Usabilidade	Operacionalidade	Consistência operacional em uso	Quão consistente é o componente da interface do usuário?	Observe o comportamento do usuário e peça a opinião.	Y = N / UOT N = Número de operações que o usuário encontrou inaceitavelmente inconsistente com a expectativa do usuário UOT = tempo de operação do usuário	0 <= Y O menor e mais próximo de 0,0 é o melhor.	Relação	Tempo
Usabilidade	Atratividade	Capacidade de personalização da interface	Qual proporção de elementos de interface pode ser personalizada em aparência para a satisfação do usuário?	Conduzir o teste e observar o comportamento.	X = A / B A = Número de elementos de interface personalizados na aparência para a satisfação do usuário B = Número de elementos de interface que o usuário deseja personalizar	0 <= X <= 1 O mais próximo de 1,0 é o melhor.	Absoluto	Quantitativo
Portabilidade	Adaptabilidade	Adaptabilidade ambiental do hardware (Adaptabilidade a dispositivos de hardware e instalações de rede)	O usuário ou mantenedor pode facilmente adaptar o software ao ambiente? O sistema de software é capaz de se adaptar ao ambiente de operação?	Observe o comportamento do usuário ou do mantenedor quando o usuário está tentando adaptar o software ao ambiente de operação.	X = 1 - A / B A = Número de funções operacionais das quais as tarefas não foram concluídas ou não foram suficientes para atender a níveis adequados durante o teste operacional combinado com hardware ambiental B = Número total de funções que foram testadas	0 <= X <= 1 Quanto maior é o melhor.	Absoluto	Quantitativo

Portabilidade	Coexistência	Coexistência disponível	Com que frequência o usuário encontra restrições ou falhas inesperadas ao operar em simultâneo com outro software?	Use o software avaliado em simultâneo com outros softwares que o usuário geralmente usa.	X = A / T A = Número de restrições ou falhas inesperadas que o usuário enfrenta ao operar em simultâneo com outro software T = tempo de operação simultânea de outros softwares	0 <= X O mais próximo de 0 é o melhor.	Relação	Quantitativo Tempo

Fonte: ABNT ISO 25010 (2011)

Tabela 5: Métricas de Qualidade Em Uso para Avaliação

Característica	**Métrica**	**Propósito da métrica**	**Método de aplicação**	**Medida e Fórmula**	**Interpretação**	**Tipo de escala**	**Tipo de medida**
Efetividade	Frequência de Erro	Qual é a frequência de erros?	Teste com o Usuário	X = A / T A = número de erros tomados pelo usuário T = tempo ou número de tarefas	0 <= X Quanto mais próximo de 0, melhor.	Absoluta	Quantitativo
Produtividade	Tempo da Tarefa	Quanto tempo demora para completar uma tarefa?	Teste com o Usuário	X = Ta / Tb Ta = tempo ocioso do usuário Tb = tempo da tarefa	X >= 0 Quanto menor, melhor.	Intervalo	Tempo

Fonte: ABNT ISO 25010 (2011)

Dentre as métricas citadas na Tabela 3 está a subcaracterística de Adequação, aonde são mensuradas as funcionalidades das ferramentas. Para medir é necessário primeiro definir quais serão as funcionalidades mensuradas. De acordo com conceitos de funcionalidades encontrados na norma ABNT NBR ISO/IEC 27001 (Figura4) foram definidas as seguintes funcionalidades para a avaliação dos softwares:

a) Análise de risco: É preciso que o software permita estabelecer os critérios de aceitação dos riscos e a definição de como esses riscos serão mensurados. Também que ele permita avaliar as possíveis consequências dos riscos identificados e a probabilidade de que ocorram e seus níveis. Medida: satisfatória ou insatisfatória;

b) Cadastramentos sobre tarefas: Funcionalidade aonde ocorrem os cadastramentos dos papéis e responsabilidades e amarrações das tarefas. Medida: satisfatória ou insatisfatória;

c) Cadastramentos de controles: Funcionalidade aonde ocorrem os cadastramentos dos controles de segurança existentes e a serem implementados. Medida: satisfatória ou insatisfatória;

d) Cadastramentos funcionais: Funcionalidade aonde ocorrem os cadastramentos dos ativos, ameaças, vulnerabilidades, consequências e planos de ação. Medida: satisfatória ou insatisfatória;

e) Correlação do evento: Correlacionar os eventos de segurança ocorridos para identificar alguma relação entre os mesmos. Medida: alta, média e baixa;

f) Armazenamento dos eventos: Armazenar os eventos de segurança ocorridos e permitir acesso ao histórico de armazenamento. Medida: satisfatória ou insatisfatória;

g) Acompanhamentos: Funcionalidades aonde ocorrem os acompanhamentos das implantações das medidas de segurança e a implantação do SGSI. Medida: satisfatória ou insatisfatória;

h) Documentação: Possibilidade de anexar documentos como termos, documentos assinados pela direção. Medida: satisfatória ou insatisfatória.

As métricas correspondentes a característica de Funcionalidade Adequação serão consideradas com um peso maior que as demais características, pois ela mensura as funcionalidades do software, que para o caso em questão é de grande relevância. Dessa forma a divisão dos pesos de medidas são 40% para a subcaracterística de Adequação e os outros 60% divididos pelas demais subcaracterísticas.

3.4 Casos de Testes

Definidos os softwares que serão avaliados, os critérios e as métricas para a avaliação destes softwares é necessário a definir os casos de testes que servirão como base para padronizar os testes e avaliações sob os softwares.

Os casos de testes (Tabela 5 a Tabela 17) tem como base as métricas e funcionalidades citadas no capítulo 3, que foram definidas com base nos modelos de qualidades revisados e com a norma ISO 27001.

Os critérios utilizados para a definição dos casos de testes foram encontrar nos requisitos e controles da ISO 27001 casos que pudessem ser utilizados para mensurar as características dos softwares e que também abrangessem mais de uma métrica.

A relação de cada caso de teste com os critérios e métricas, previamente selecionados para a utilização, se encontram no corpo de cada caso, mais especificamente na linha Resumo das tabelas, onde é descrito quais métricas atendem cada caso de teste.

Tabela 6: Caso de Teste 1

Caso de Teste	Parametrização do Sistema
Resumo	Testar se o software permite parametrizar o sistema de acordo com os critérios definidos, a abordagem, os níveis de impacto e o cálculo do risco. Atende as métricas de: Adequação, Atratividade, Adaptabilidade e Frequência de Erro.
Pré-condições	Software parametrizável.
Ação	Configurar o sistema de acordo com os critérios definidos. Configurar se a abordagem é quantitativa ou qualitativa. Configurar os níveis de impacto (baixo, médio ou alto). Configurar a forma de cálculo do risco.
Resultados Esperados	Sistema parametrizado.

Tabela 7: Caso de Teste 2

Caso de Teste	Análise e Avaliação de Risco
Resumo	Testar se o software consegue detectar os riscos existentes na rede, medir a probabilidade dos riscos de acontecer e apresentar os níveis dos riscos (Alto, Médio ou Baixo). Atende as métricas de: Adequação, Coexistência, Frequência de Erro e Tempo da Tarefa.
Pré-condições	Detecção de risco.
Ação	Avaliar consequências dos riscos. Avaliar a probabilidade dos riscos acontecerem. Mensurar os níveis dos riscos.
Resultados Esperados	Relatório apresentando as consequências dos riscos, a probabilidade de que ocorram e seus níveis.

Tabela 8: Caso de Teste 3

Caso de Teste	Aceitação de Riscos
Resumo	Testar se o software permite cadastrar os critérios de aceitação de riscos e definir como mensurá-los. Atende as métricas de: Adequação, Acurácia, Operacionalidade, Frequência de Erro e Tempo da Tarefa.
Pré-condições	Riscos identificados.
Ação	Cadastrar os critérios de aceitação. Cadastrar como mensurar os riscos.
Resultados Esperados	Software configurado com os critérios de aceitação e como medir os riscos.

Tabela 9: Caso de Teste 4

Caso de Teste	Tratamento de Riscos
Resumo	Testar se o software consegue determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos. Atende as métricas de: Adequação, Acurácia, Frequência Erro e Tempo da Tarefa.
Pré-condições	Cadastro dos critérios de aceitação de riscos.
Ação	Software detecta risco e define se está dentro dos critérios aceitáveis ou executa o tratamento do risco.
Resultados Esperados	Software tratar o risco ou software aceita o risco.

Tabela 10: Caso de Teste 5

Caso de Teste	Cadastros
Resumo	Testar se o software permite o cadastramento sobre as tarefas, de controles e funcionais. Esse cadastros podem servir para as próximas avaliações (PDCA – contínuo). Atende as métricas de: Adequação, Acurácia, Conformidade, Operacionalidade, Atratividade, Frequência de Erro e Tempo da Tarefa.
Pré-condições	Caso de teste 1.
Ação	Cadastro de papéis, responsabilidades e amarrações de tarefas. Cadastro de controles de segurança, ativos, ameaças, vulnerabilidades, consequências e planos de ação.
Resultados Esperados	Cadastros efetuados com sucesso.

Tabela 11: Caso de Teste 6

Caso de Teste	Correlacionar Eventos de Segurança
Resumo	Testar se o software correlaciona os eventos de segurança ocorridos para identificar alguma relação entre os mesmos. Atende as métricas de: Adequação, Acurácia, Operacionalidade, Coexistência, Frequência de Erro e Tempo da Tarefa.
Pré-condições	Eventos de segurança. Padrões de eventos.
Ação	Correlacionar os eventos de segurança.
Resultados Esperados	Relação de eventos de segurança semelhantes.

Tabela 12: Caso de Teste 7

Caso de Teste	Armazenamento dos Eventos de Segurança
Resumo	Testar se o software permite armazenar os eventos de segurança ocorridos e dá acesso ao armazenamento. Atende as métricas de: Adequação, Adaptabilidade, Atratividade, Operacionalidade, Frequência de Erro e Tempo da Tarefa.
Pré-condições	Eventos de segurança. Configurar armazenamento.
Ação	Armazenar os eventos de segurança.
Resultados Esperados	Relação de eventos de segurança armazenados.

Tabela 13: Caso de Teste 8

Caso de Teste	Métricas e Relatórios
Resumo	Testar se o software permite a configuração das métricas de desempenho e gerar relatórios de segurança. Atende as métricas de: Adequação, Acurácia, Operacionalidade, Atratividade, Adaptabilidade, Frequência Erro e Tempo Tarefa.
Pré-condições	Riscos a serem mensurados.
Ação	Mensurar os riscos. Gerar relatórios com os dados mensurados.
Resultados Esperados	Relatório de segurança mensurando os riscos.

Tabela 14: Caso de Teste 9

Caso de Teste	Análise de Desempenho
Resumo	Testar se o software permite mensurar e monitorar as funcionalidades, através da aplicação de indicadores que possibilitem a análise da eficiência do software. Atende as métricas de: Adequação, Acurácia, Conformidade, Operacionalidade, Adaptabilidade, Coexistência, Frequência de Erro e Tempo da Tarefa.
Pré-condições	Funcionalidades do software documentadas. Indicadores de eficiência das funcionalidades.
Ação	Mensurar/monitorar a eficiência das funcionalidades.
Resultados Esperados	Relatórios de eficiência das funcionalidades do software.

Tabela 15: Caso de Teste 10

Caso de Teste	Adaptabilidade
Resumo	Testar se o software roda em diversos Sistemas Operacionais. Atende as métricas de: Adaptabilidade, Coexistência, Frequência de Erro.
Pré-condições	Software instalado.
Ação	Executar software em diversos Sistemas Operacionais
Resultados Esperados	Software instalado em diversos Sistemas Operacionais.

Tabela 16: Caso de Teste 11

Caso de Teste	Coexistência
Resumo	Testar se o software roda sem apresentar restrições ou falhas ao operar em simultâneo com outro software. Atende as métricas de: Coexistência, Frequência de Erro.
Pré-condições	Softwares instalados.
Ação	Executar software em simultâneo com outros softwares.
Resultados Esperados	Software não apresenta restrições ou falhas ao executar simultaneamente com outro software.

Tabela 17: Caso de Teste 12

Caso de Teste	Documentação
Resumo	Testar se o software permite anexar documentos e termos. Atende as métricas de: Adequação e Conformidade.
Pré-condições	Documentação.
Ação	Anexar documentação ao software.
Resultados Esperados	Documentação anexada ao software.

Tabela 18: Caso de Teste 13

Caso de Teste	Conformidade
Resumo	Testar se o software é compatível com os regulamentos, padrões e convenções aplicáveis ao produto. Atende as métricas de: Adequação e Conformidade.
Pré-condições	Software classificado como produto.
Ação	Verificar compatibilidade do software com conformidade.
Resultados Esperados	Software dentro da conformidade.

Os casos de testes tem como principal função servir como a apoio para avaliar as ferramentas que foram selecionadas para a avaliação, através das métricas pré definidas, dessa forma é possível garantir que as avaliações das ferramentas ocorram de forma justa e igual pois todas as ferramentas são testadas da mesma maneira, assim se torna mais adequado para avaliar qual a software mais apropriado para o caso em questão.

3.5 Considerações Finais do Capítulo

O capítulo apresenta a proposta de solução do trabalho, quanto a analisar softwares, desenvolvidos em código livre, a fim de verificar quais destes softwares realizam o gerenciamento do SGSI de acordo com a norma ABNT/NBR 27001. Neste capítulo também são conhecidas as ferramentas de software SGSI que serão avaliadas, foram estudadas diversas ferramentas e somente 2 foram selecionadas para dar seguimento a OSSIM e o EBIOS.

Após a definição das ferramentas que serão trabalhadas foram selecionados os critérios e métricas para a avaliação dos softwares, os critérios funcionam como a base para a avaliação pois é na definição dos critérios aonde se defini o que realmente será avaliado em cada ferramenta. As métricas são o seguimento pois com a definição das métricas é possível definir a forma como melhor mensurar os critérios que foram selecionados.

A definição dos casos de teste é necessário também, pois os casos de teste vão reger um padrão de testes para avaliar os softwares, eles funcionam como o caminho para chegar ao resultado esperado, que é a definição da ferramenta de software SGSI mais adequado com a norma ABNT NBR ISO/IEC 27001.

4 TESTE E AVALIAÇÃO DAS FERRAMENTAS OSSIM E EBIOS

De acordo com o que foi definido na proposta de solução (seção 3.1), os softwares selecionados para verificar a aderência a norma ABNT NBR 27001 foram o OSSIM e o Ebios. Os testes realizados nas duas ferramentas seguiram os casos de testes definidos na seção 3.2.

Para realizar os testes nos softwares é importante utilizar os mesmos dados, dessa forma garantindo a padronização dos testes. Os testes foram realizados utilizando o caso de estudo realizado na disciplina de Segurança da Informação sobre o caso da empresa MERCUR S/A (ANTINARELLI, 2013). O caso de estudo consta no Anexo A.

4.1 OSSIM

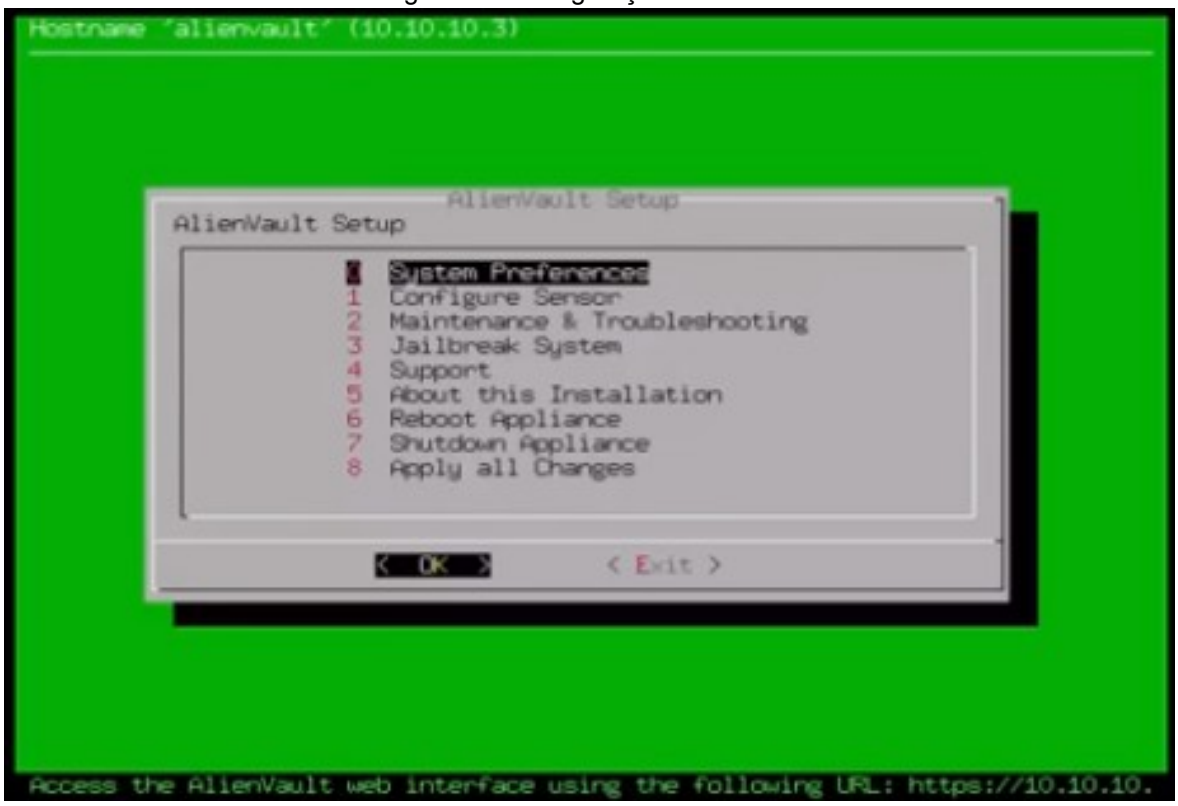
OSSIM é um software de gerenciamento de segurança da informação de código aberto da empresa AlienVault. Ele é distribuído como uma imagem ISO instalável projetada para ser implantada em um host físico ou virtual como o sistema operacional principal do host. O OSSIM é construído usando a distribuição Debian GNU / Linux como seu sistema operacional subjacente.

É uma versão disponível gratuitamente da ferramenta comercial da empresa, o SIEM. O OSSIM foi desenvolvido por engenheiros da segurança, devido a falta de ferramentas de código aberto. A AlienVault considera que o desenvolvimento do OSSIM é uma porta de entrada para que as organizações entendam a importância da segurança da informação.

O processo de instalação do software é simples. Ele funciona como um sistema operacional sem interface. Foi utilizada uma máquina virtual para a instalação. A única exigência durante a instalação é que seja alocado no mínimo 2GB de memória RAM, para que o sistema consiga trabalhar de forma que ele apresente o seu melhor desempenho.

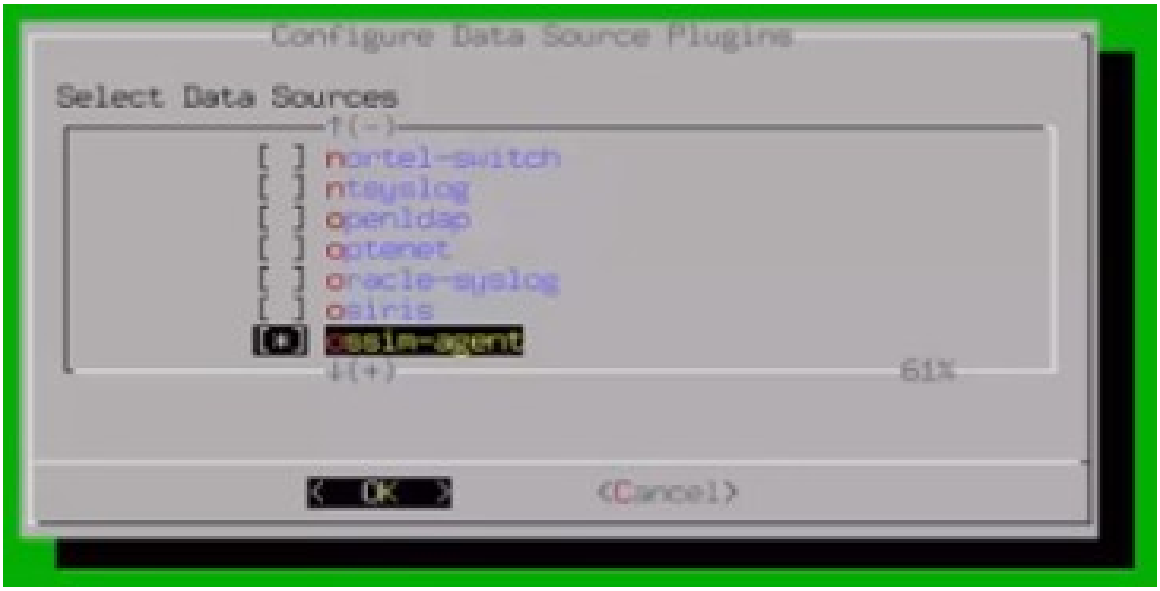
Após a instalação é possível configurar o sistema, ainda dentro da máquina virtual. Nesse momento é possível definir as preferências do sistema, configurações de rede, configuração dos sensores, atualizar o OSSIM, entre outras configurações (Figura 17).

Figura 17: Configuração do OSSIM



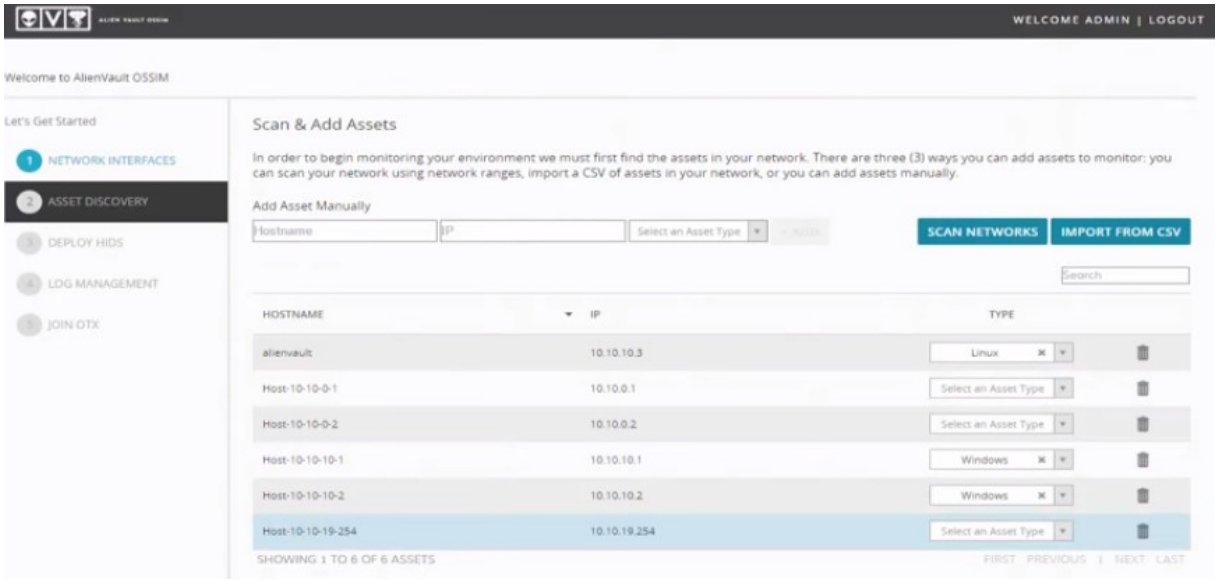
Dentro da parametrização dos sensores, sensores é a denominação para um conjunto de softwares disponíveis no OSSIM que auxiliam o gerenciamento da segurança, é possível configurar quais sensores serão utilizados (Figura 18). Foram selecionados alguns sensores para teste como o OSSIM Agent, Nessus e Snort.

Figura 18: Configuração dos Sensores



Feitas as pré-configurações do sistema, a interface é acessível via web. No primeiro acesso é necessário cadastrar um usuário administrador, para que o usuário possa realizar as outras configurações do sistema. Nesse passo foi possível realizar o cadastro dos ativos da rede a serem monitorados (Figura 19).

Figura 19: Cadastros de Ativos



Durante a configuração do sistema também é possível vincular o sistema ao OTX (*Open Threat Exchange*), uma comunidade de inteligência da segurança aonde a AlienVault reúne dados de ameaças e invasões de todo o mundo de forma aberta para que seja possível compartilhar informações.

Terminadas as configurações solicitadas pelo sistema, finalmente é possível acessar a sua interface principal. A interface é formada por um menu repleto de opções para administrar e configurar a segurança da organização. O ponto negativo é que a interface utiliza a língua inglesa sem possibilidade de alterar o idioma para a língua portuguesa.

A interface inicial do software é a apresentação do painel de controle do sistema, onde são apresentados diversos gráficos que mostram as ações e eventos que estão ocorrendo na rede, em tempo real (Figura 20).

Figura 20: Painel de Controle

Em um SGSI, uma das primeiras atividades que devem ser realizadas é o cadastro dos ativos. O OSSIM permite o cadastramento (Figura 21) e a edição (Figura 19) dos ativos assim como o cadastramento dos ativos em grupos distintos para facilitar o gerenciamento (Figura 22).

Figura 21: Manutenção de Ativos

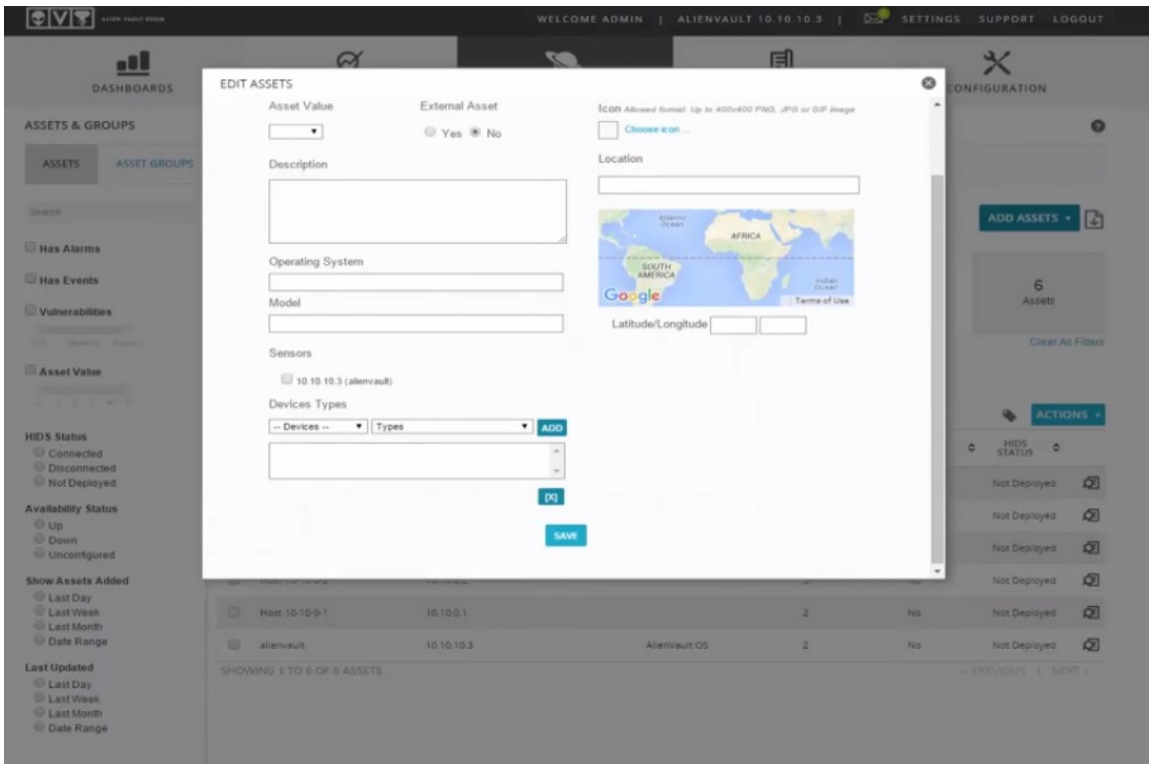
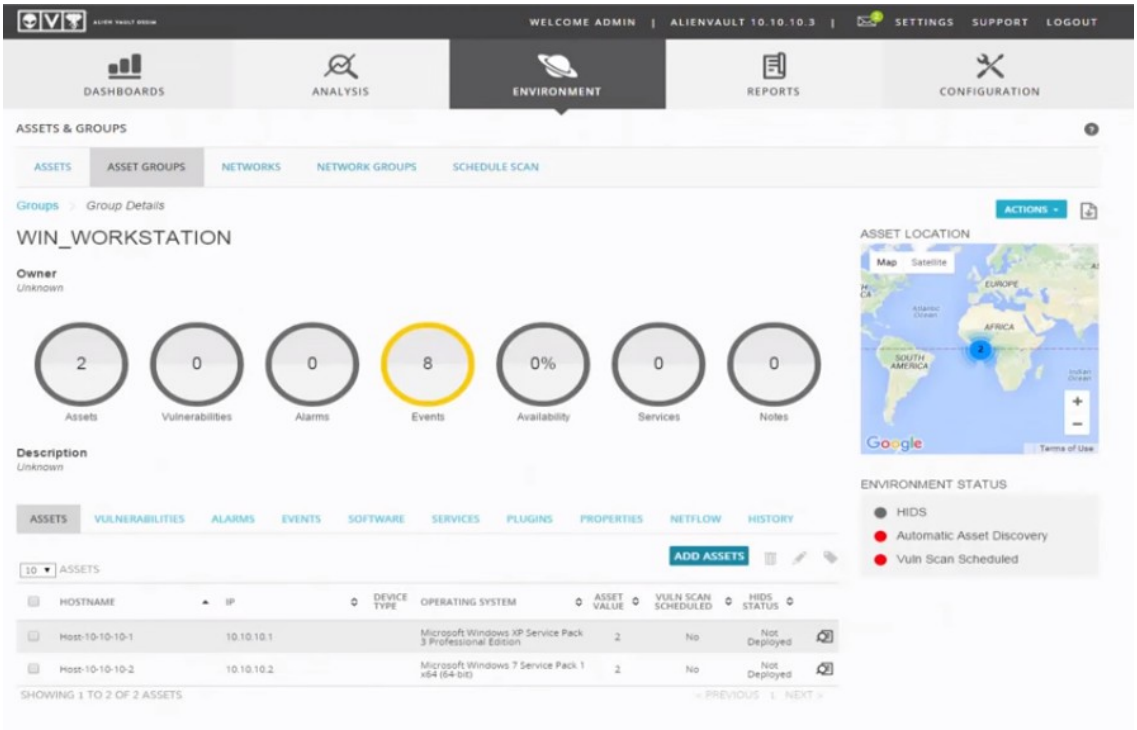
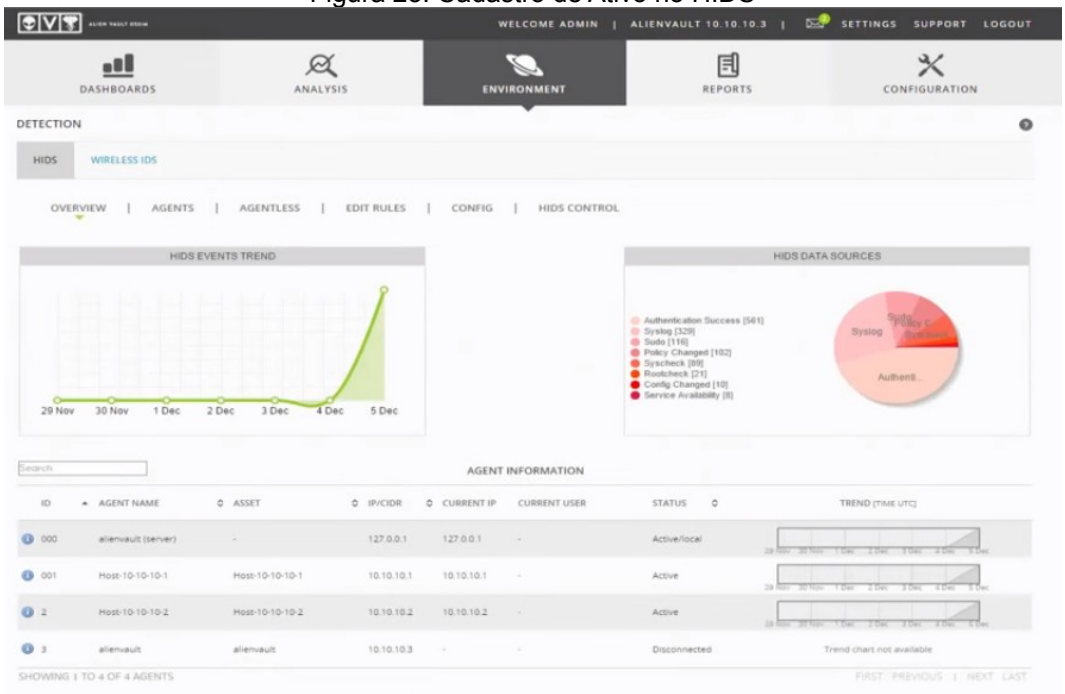


Figura 22: Cadastro de Grupos de Ativos



No menu Ambiente, opção Detecção é possível vincular um ativo a um agente do sistema de detecção de intrusão baseado no host (HIDS). Essa vinculação permite o monitoramento do ativo através das ações do agente pelas visualizações do ativo (Figura 23).

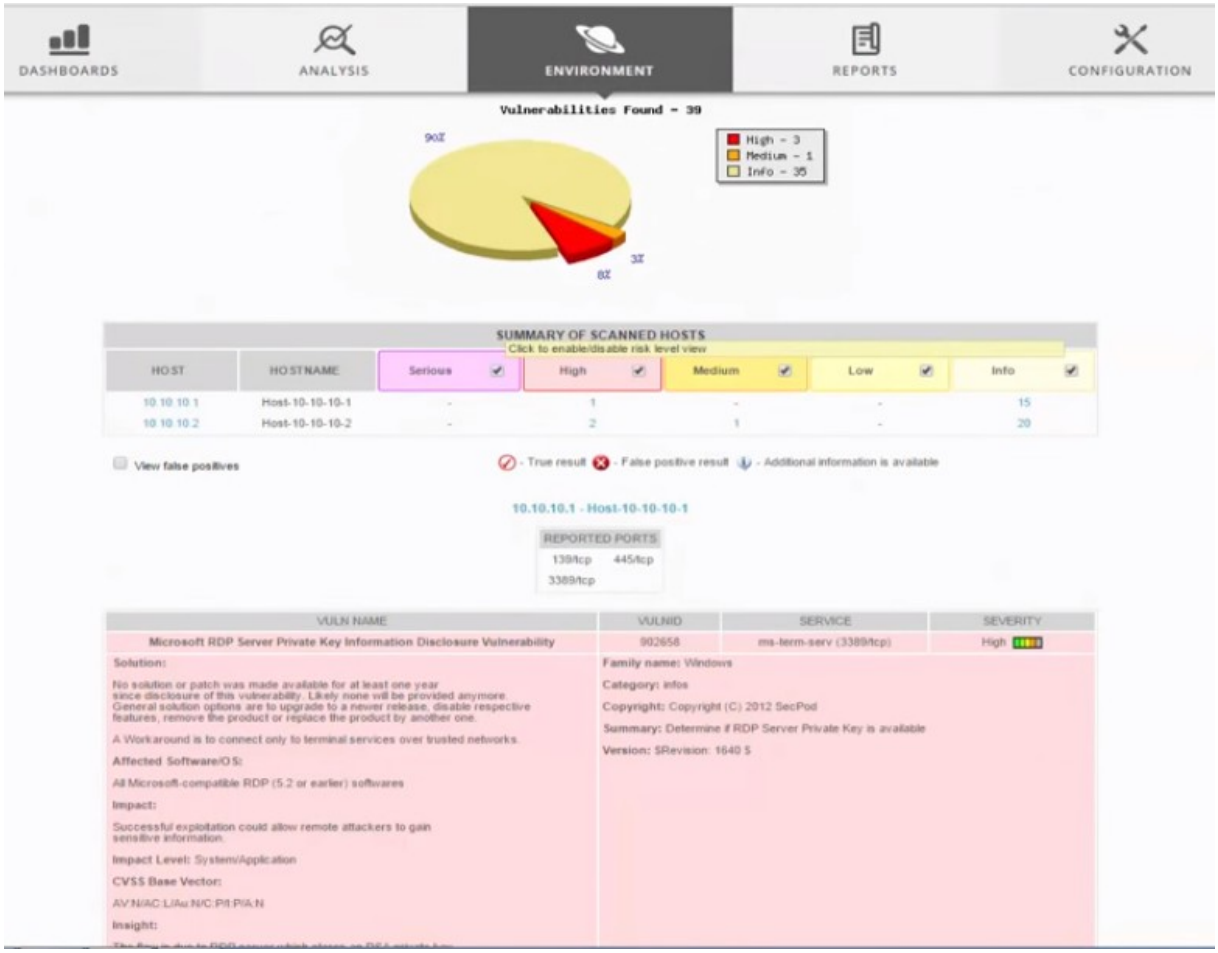
Figura 23: Cadastro de Ativo no HIDS



O menu Ambiente permite ainda a parametrização das regras de aceitação de riscos do sistema. Nele é possível visualizar e editar as regras existentes e também criar regras novas. É possível visualizar o código fonte dessas regras e editar o seu grau de periculosidade, aceitação e a abordagem do risco perante determinada rede.

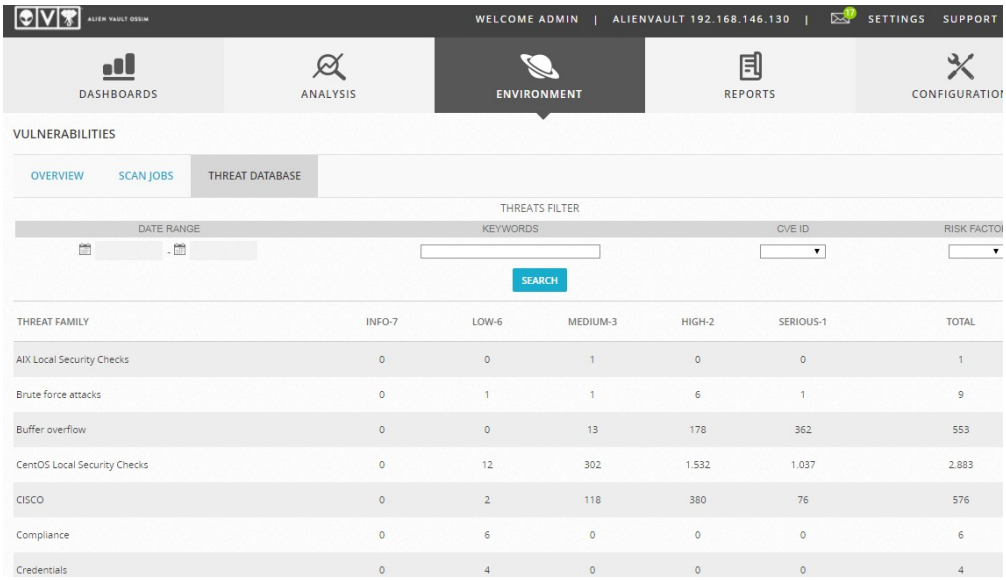
No menu Ambiente, opção Vulnerabilidades podem ser configurados os trabalhos de escaneamento da rede. Através desse menu é possível agendar o escaneamento da rede, de um grupo ou de um ativo. Após o escaneamento é possível verificar os resultados. O sistema apresenta um gráfico de pizza onde ele aponta a quantidade de eventos detectados e também qual a gravidade destes eventos (alta, média ou baixa). Abaixo do gráfico de pizza o sistema lista os eventos encontrados apontando o possível causador do evento e como solucionar, além de outras informações como a gravidade do evento, o local onde ele se encontra e seu número de registro no sistema. A Figura 24 ilustra esse relatório apresentado pelo sistema.

Figura 24: Eventos de Vulnerabilidade



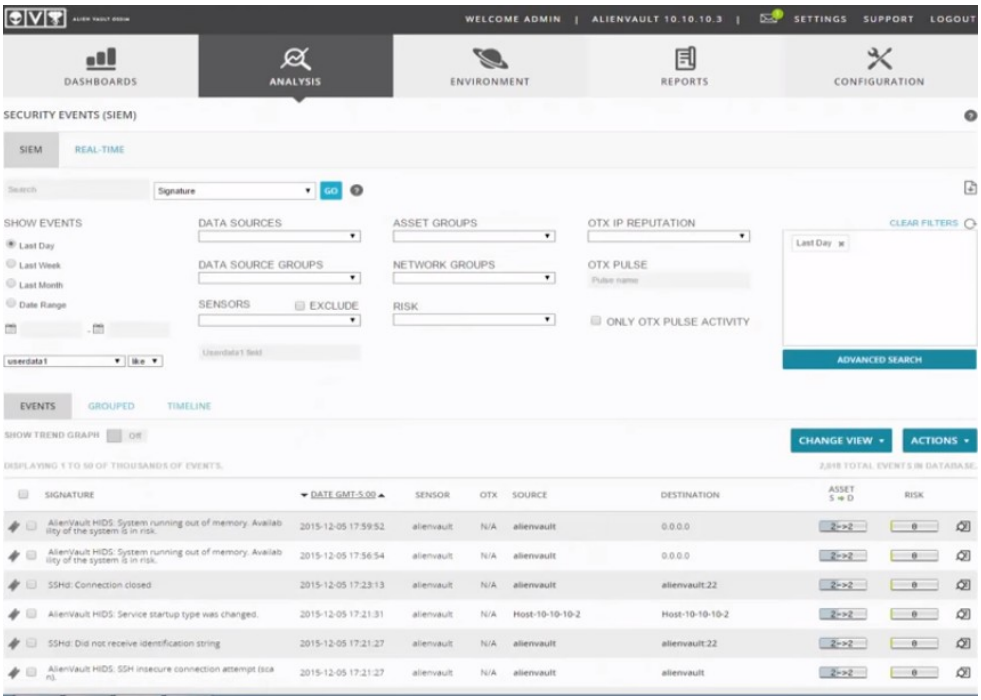
No mesmo menu, o sistema cria um banco de dados de ameaças onde os dados de ameaças são reunidos e correlacionados em grandes grupos e calcula quais são as maiores ameaças de rede, apresentando em forma de relatórios (Figura 25).

Figura 25: Relatório de Ameaças Detectadas



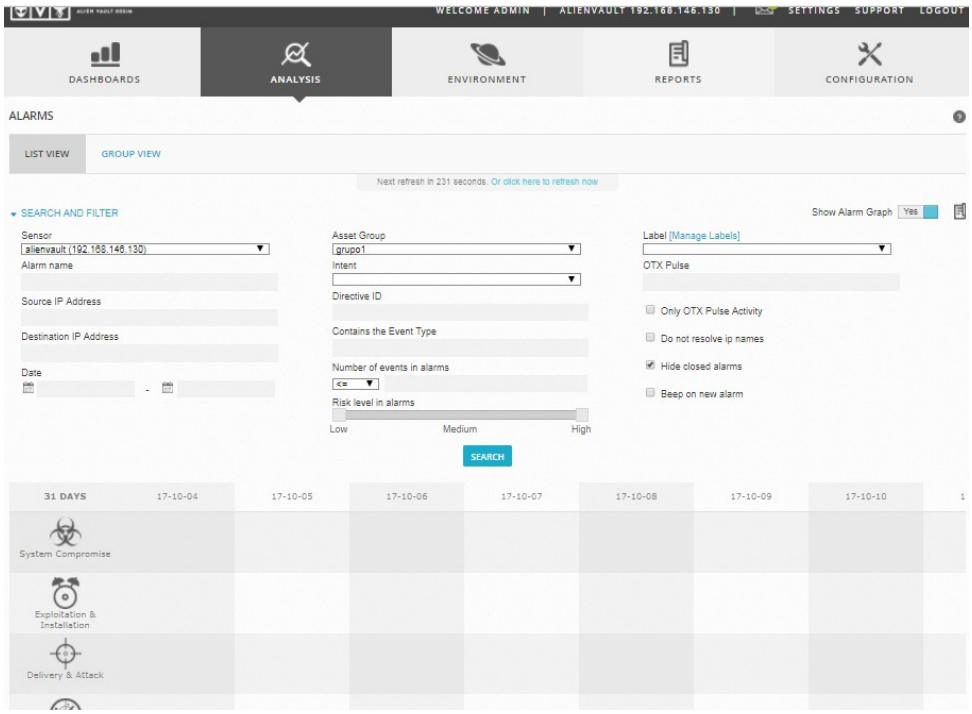
No menu Análises, opção Eventos de Segurança é possível consultar e filtrar os eventos de segurança ocorridos na rede. Os filtros podem ser realizados por período, sensores, os ativos, grupos de ativos e os riscos dentre outras opções (Figura 26).

Figura 26: Eventos de Segurança



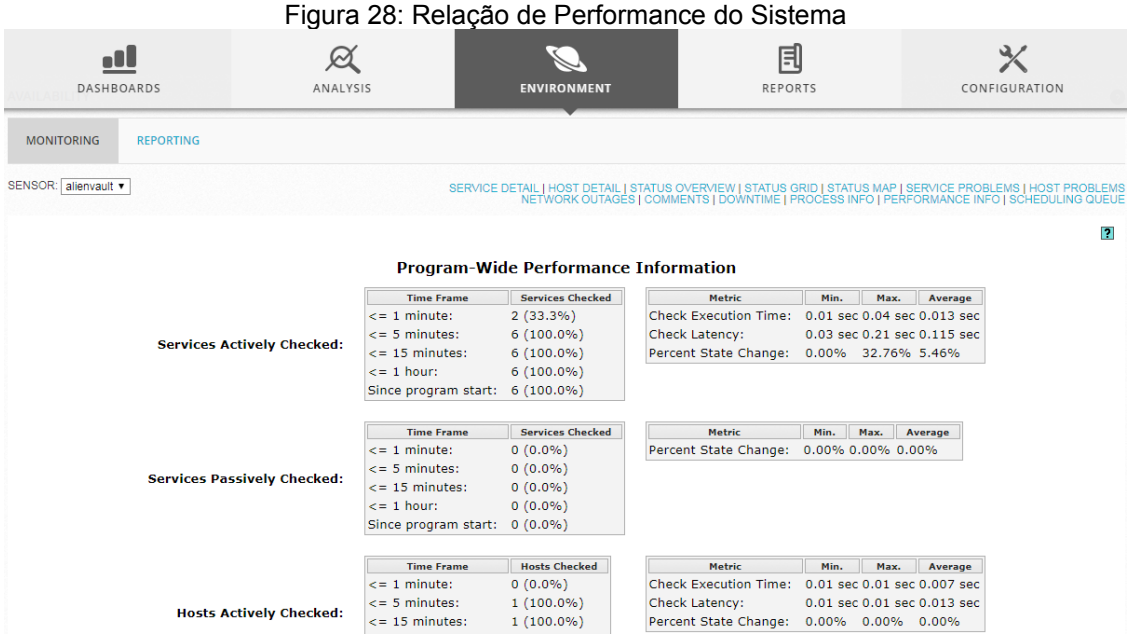
No menu Análises, opção Alarmes é configurar e consultar os alarmes de rede utilizando diversas opções de filtros e opções de alarmes conforme a Figura 27.

Figura 27: Alarmes de Rede



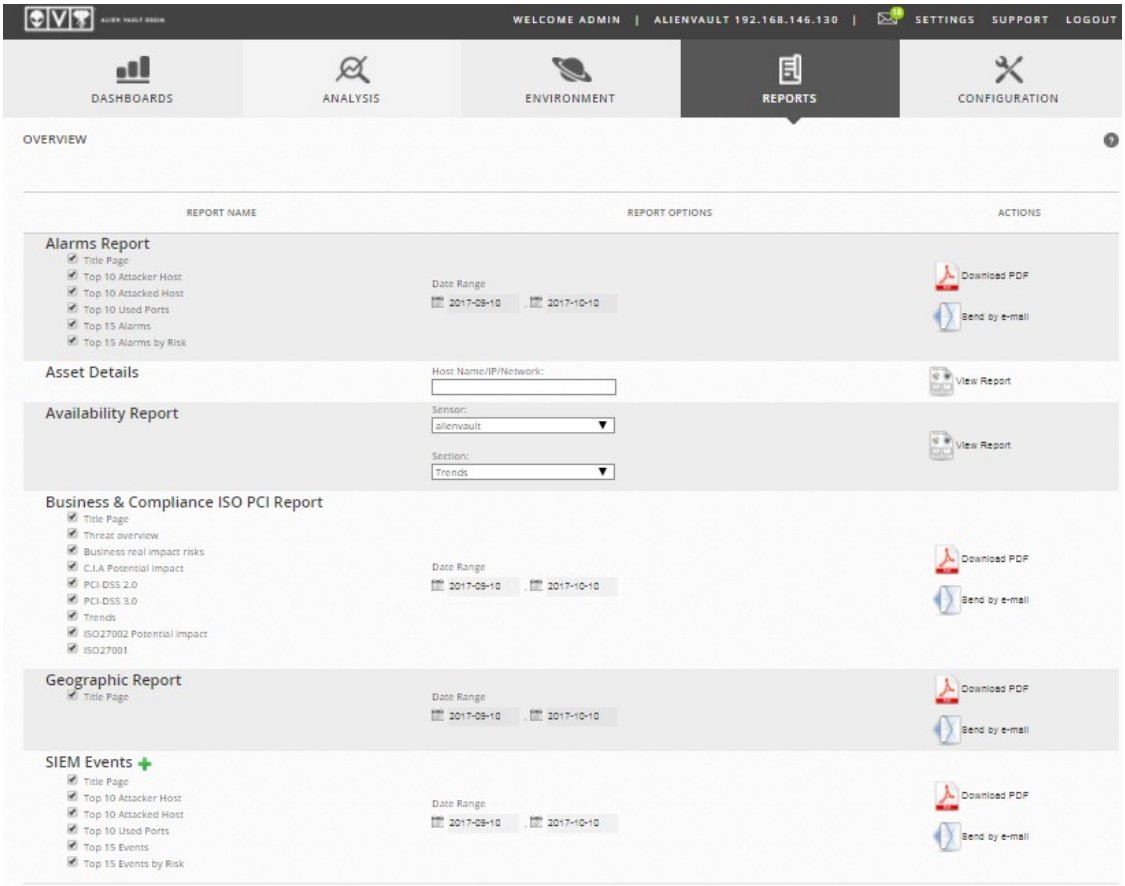
No menu Ambiente, opção Disponibilidade é possível analisar o desempenho do sistema. O software apresenta diversas opções de relatórios para o monitoramento interno do sistema. É possível gerar relatório de monitoramento como os detalhes de serviço, mapa de status, problemas de serviços, interrupções da rede, tempo de inatividade, informações de desempenho (Figura 28) e fila de agendamento.

Figura 28: Relação de Performance do Sistema



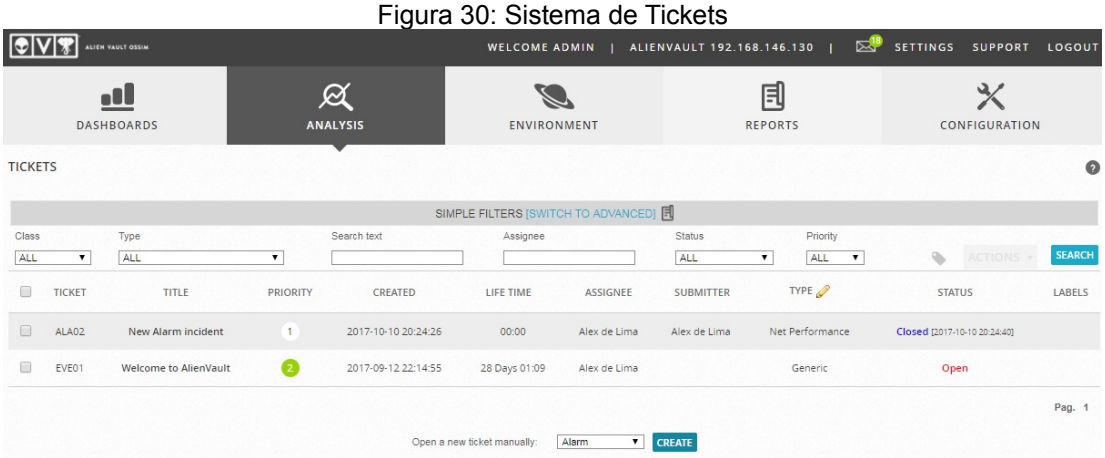
No menu Relatórios é encontrado uma grande variedade de relatórios de monitoramento da rede (Figura 29). Os possíveis relatórios pode-se citar: Eventos SGSI, Ativos, Alarmes, Ameaças, Vulnerabilidades e Tickets. Além disso, o sistema permite que vários filtros sejam aplicados nos relatórios de acordo com a necessidade do gerente de rede.

Figura 29: Relatórios de Monitoramento da Rede



O sistema também possui um sistema de tickets interno, onde é possível criar e fechar tickets de incidentes e problemas de rede (Figura 30).

Figura 30: Sistema de Tickets



4.2 EBIOS

Criado em 2006, EBIOS é de uma associação independente sem fins lucrativos, composta por especialistas e organizações, o Club Ebios. Essa associação apoia e aprimora a estrutura francesa de gestão da segurança desde 2003. Além de desenvolver o sistema Ebios, seu campo de ação se estende a todas as utilizações deste método e seus derivados no campo da gestão da segurança.

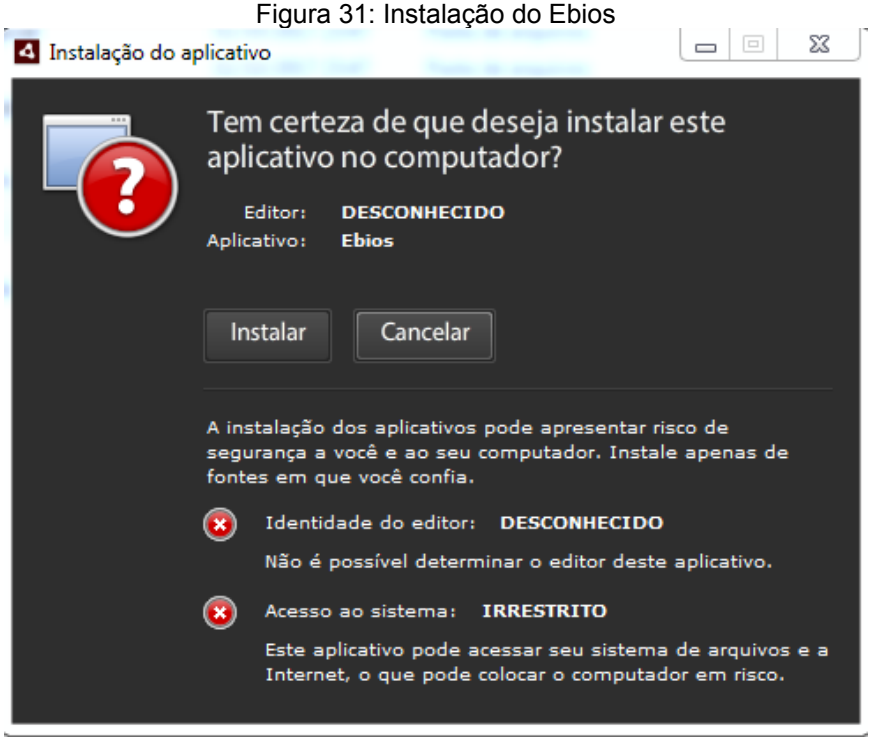
O Clube organiza reuniões periódicas para incentivar o intercâmbio de experiências, a homogeneização das práticas e a satisfação das necessidades dos usuários. É também um espaço para definir posições e influenciar debates nacionais e internacionais. EBIOS significa expressão de necessidades e identificação de objetivos de segurança. Ele é o método de gerenciamento da segurança publicado pela Agência de Segurança Nacional para Sistemas de Informação (ANSSI) e da Secretaria Geral de Defesa e Segurança Nacional (SGDSN).

EBIOS é um método de análise, avaliação e ação sobre segurança de sistemas de informação. Ele gera uma política de segurança adaptada às necessidades de uma organização. O método foi criado em 1995 e agora é mantido pelo ANSSI, um departamento do primeiro-ministro francês. Os cinco passos do método EBIOS são: Determinação do contexto; Requisitos de segurança; Estudo de risco; Identificação de metas de segurança; e Determinação dos requisitos de segurança.

Em sua primeira versão, o EBIOS foi focado em objetivos de segurança. Desde 2011, a DCSSI tomou conhecimento das melhorias nos padrões internacionais (ISO 27001) e adaptou o EBIOS a esta nova norma. Essas adaptações foram realizadas pois os métodos franceses não eram reconhecidos no exterior e não são adequados aos mercados internacionais. No entanto, a documentação do método está disponível apenas em francês.

O processo de instalação do software é bem tranquilo. O Ebios é um aplicativo independente desenvolvido em Java que funciona com documentos XML. Portanto, não importa qual plataforma o usuário usa os serviços Ebios, a única exigência é a instalação do software Adobe AIR. Esse software é um programa multiplataforma de ambiente e tempo de execução desenvolvida pela Adobe Systems para construir aplicações web e de segurança. Através do Adobe AIR é possível executar o instalador do Ebios conforme mostra a Figura 31.

Figura 31: Instalação do Ebios

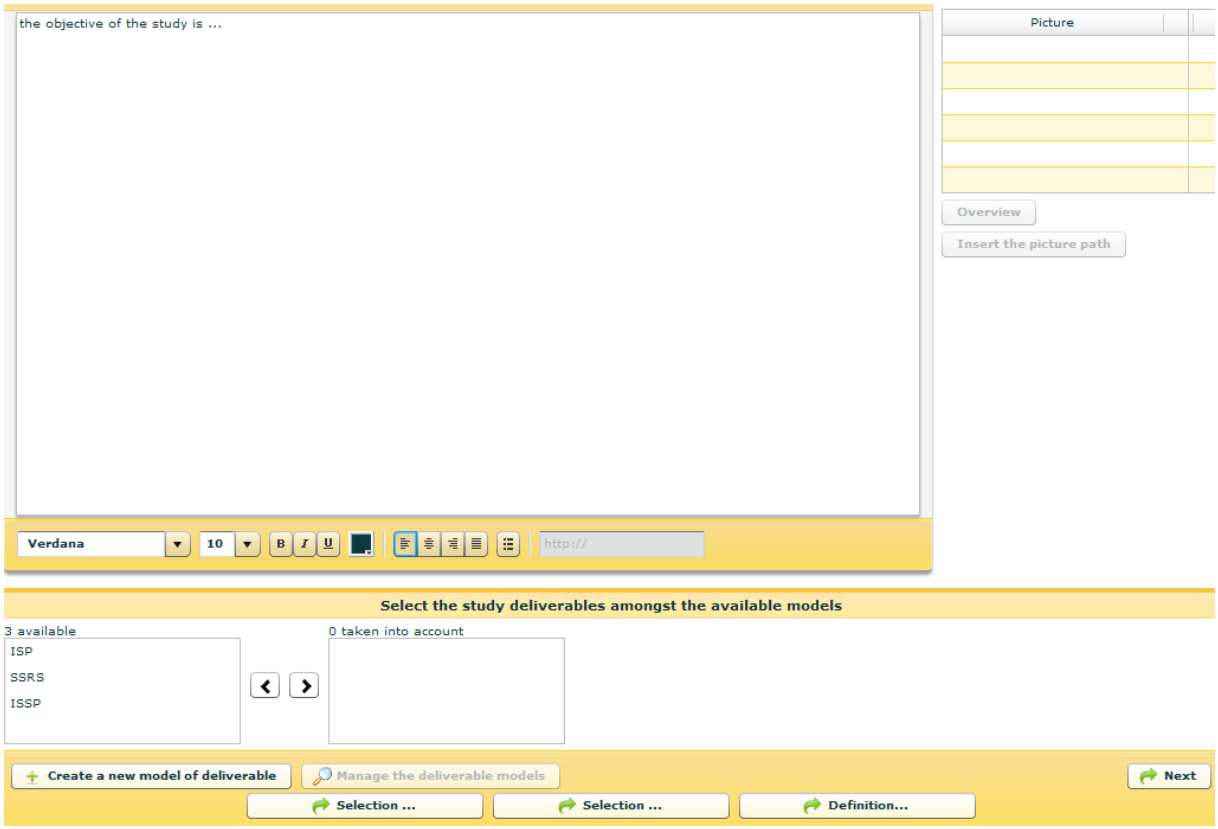


Após a instalação e execução do software onde é possível alterar o idioma, que inicialmente é Francês, para o Inglês (Figura 32). É possível também adicionar outros idiomas, baixando os pacotes na internet, mas o idioma Português ainda não está disponível.

Figura 32: Seleção de Idioma do Ebios

Inicialmente o software solicita se o usuário deseja criar um novo estudo ou abrir um existente. Após, o escopo do gerenciamento da segurança deve ser cadastrado (Figura 33).

Figura 33: Configuração do Estudo do Ebios



A próxima etapa é a seleção dos critérios para o gerenciamento da rede, denominada no Ebios de passos. Dentre os critérios disponíveis é possível citar a definição de critérios como análise do risco, identificação de ameaças, preparação de planos de ação dentre outras opções como é possível ver na Figura 34.

Figura 34: Configuração de Critérios de Gerenciamento

	Steps
☑	1.1.1 Scope the risks study
☑	1.1.2 Describe the general context
☑	1.1.3 Delimit the boundaries of the study
☑	1.1.4 Identify the parameters to be taken into account
☑	1.1.5 Identify the threat sources
☑	1.2.1 Define the security criteria and create the scales of needs
☑	1.2.2 Create a scale of seriousness
☑	1.2.3 Create a scale of likelihood
☑	1.2.4 Define the risk management criteria
☑	1.3.1 Identify the primary assets, their relations and their trustees
☑	1.3.2 Identify the supporting assets, their relations and their owners
☑	1.3.3 Determine the link between primary assets and supporting assets
☑	1.3.4 Identify the existing controls
☑	2.1.1 Analyse of all feared events
☑	2.1.2 Assess each feared events
☑	3.1.1 Analyse of all threat scenarios
☑	3.1.2 Assess each threat scenario
☑	4.1.1 Analyse the risks
☑	4.1.2 Assess the risks
☑	4.2.1 Choose the options for risk treatment
☑	4.2.2 Analyse the residual risks
☑	5.1.1 Determine the controls
☑	5.1.2 Analyse the residual risks
☑	5.1.3 Establish a statement of applicability
☑	5.2.1 Prepare an action plan and monitor the implementation of controls
☑	5.2.2 Analyse the residual risks

O software solicita o cadastramento dos membros da equipe de segurança (Figura 35) definindo suas responsabilidades (Figura 36).

Figura 35: Configuração de Membros

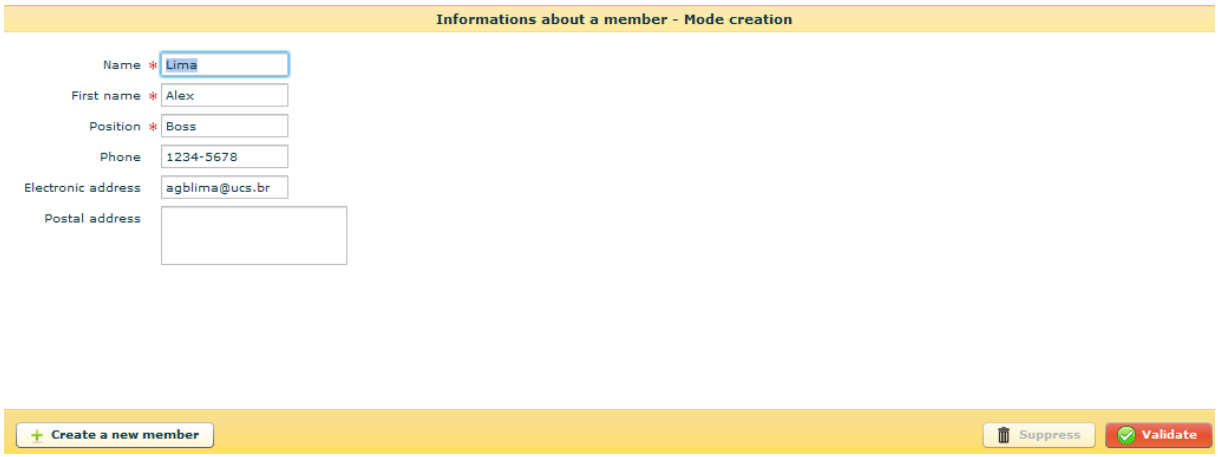
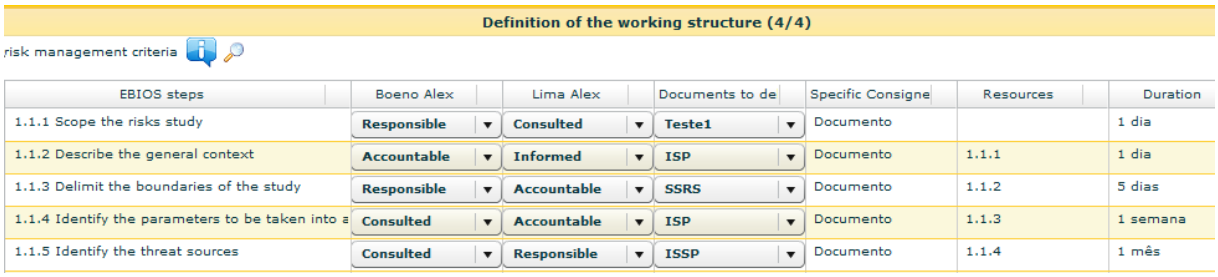


Figura 36: Definição de Estruturas



EBIOS steps	Boeno Alex	Lima Alex	Documents to de	Specific Consigne	Resources	Duration
1.1.1 Scope the risks study	Responsible	Consulted	Teste1	Documento		1 dia
1.1.2 Describe the general context	Accountable	Informed	ISP	Documento	1.1.1	1 dia
1.1.3 Delimit the boundaries of the study	Responsible	Accountable	SSRS	Documento	1.1.2	5 dias
1.1.4 Identify the parameters to be taken into a	Consulted	Accountable	ISP	Documento	1.1.3	1 semana
1.1.5 Identify the threat sources	Consulted	Responsible	ISSP	Documento	1.1.4	1 mês

Após as configurações iniciais, as informações sobre o SGSI podem ser incluídas no software (Figura 37). O menu 1.1 permite a definição do escopo e de contexto geral. O menu 1.2 é onde são definidos as métricas que o sistema utilizará para gerenciar a segurança, onde são definidos os critérios de segurança e escalas para identificar a proporção dos riscos e ameaças (Figura 38).

Figura 37: Tela Inicial do Ebios

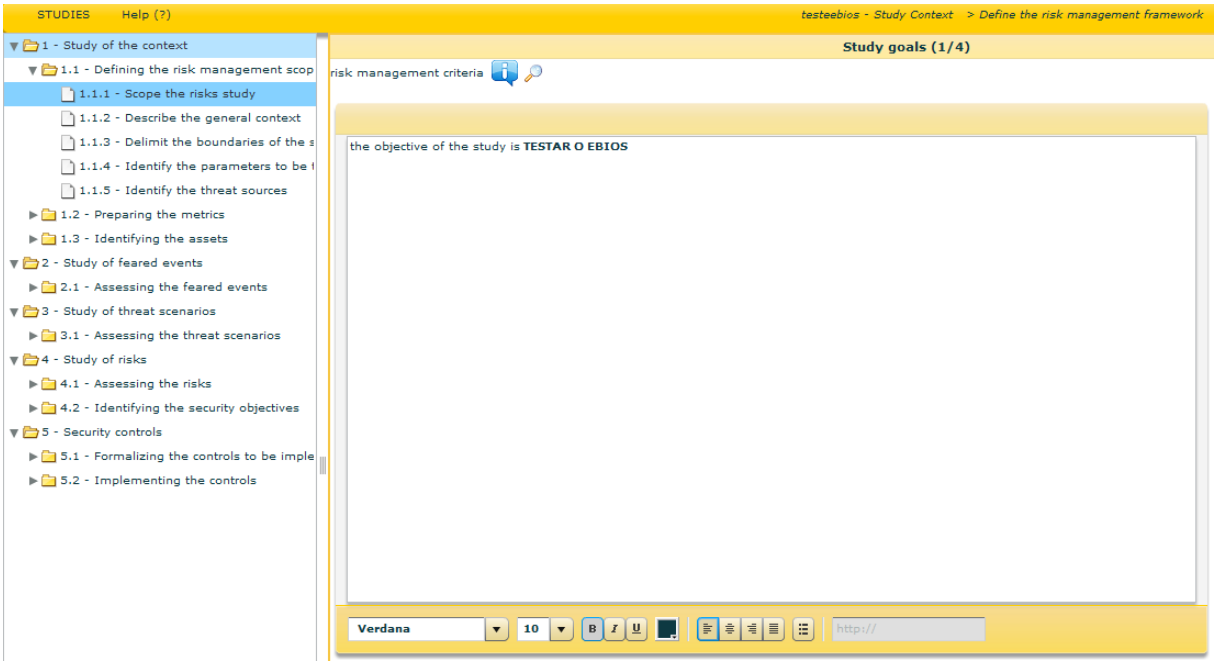
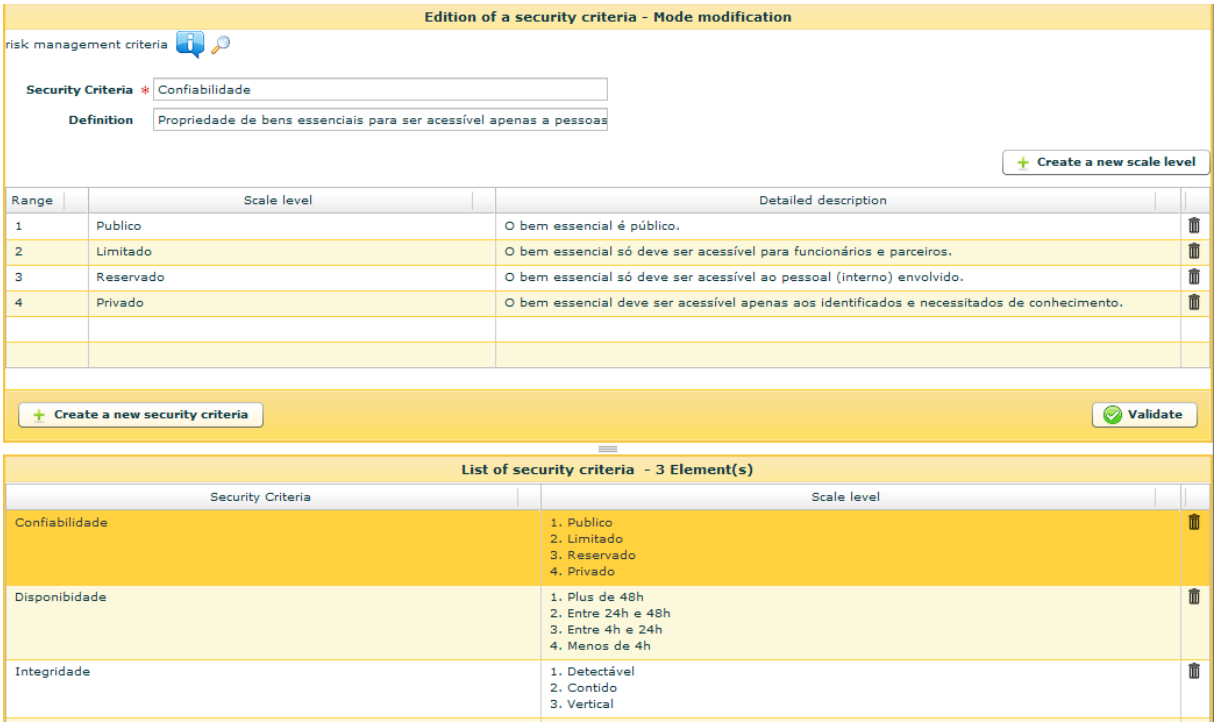


Figura 38: Critérios de Segurança



O menu 1.3 permite a definição dos ativos e as relações que existem entre eles. Onde são cadastrados os controles de segurança já existentes da organização (Figura 39). No menu 2.1 são realizados os cadastros e as avaliações dos eventos

temidos pela segurança da rede. Nesse passo é possível configurar o tempo de resposta para um possível evento, a sua gravidade e o seu impacto na rede. O software também permite gerar um relatório dos eventos (Figura 40).

Figura 39: Configuração dos Controles

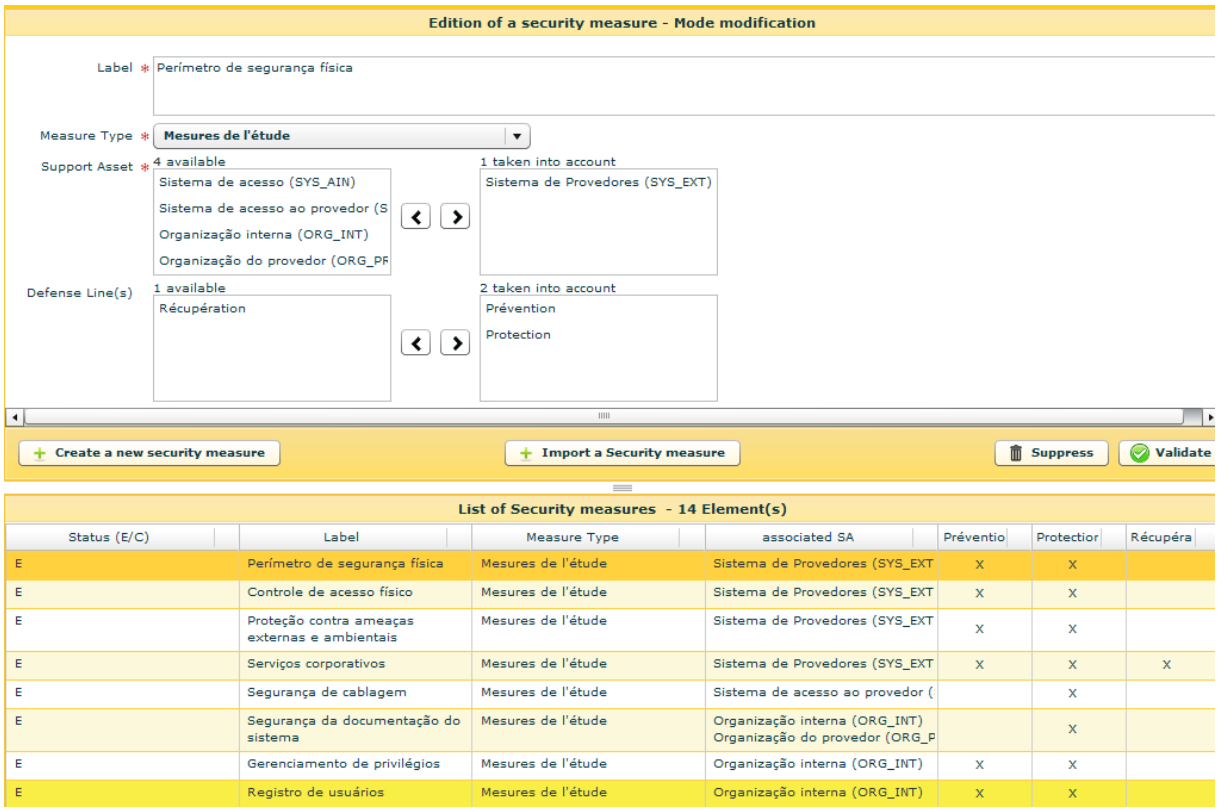
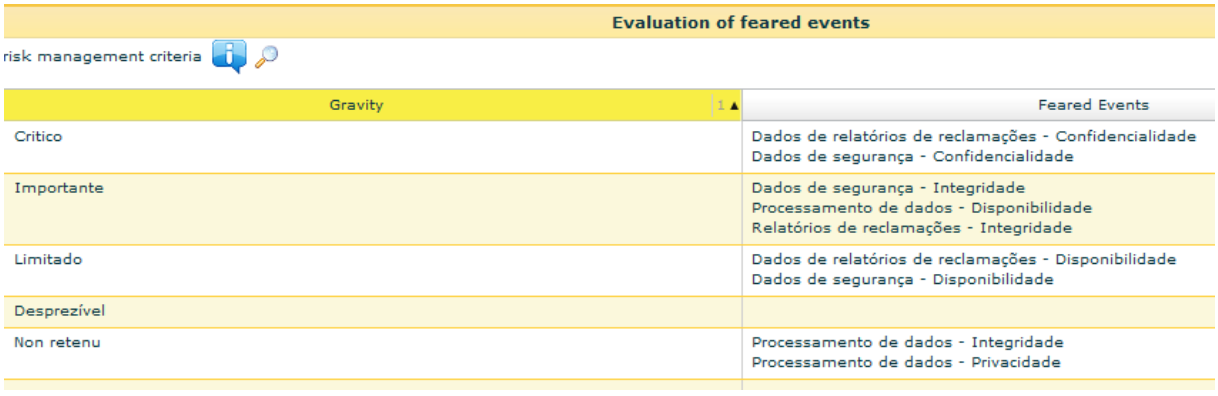


Figura 40: Configuração de Eventos



Através do menu 3.1 é possível efetuar os cadastros e as avaliações para os cenários de ameaças. Nesse momento é necessário a definição das ameaças, as possíveis fontes das ameaças e a probabilidade de que elas aconteçam. O software também permite gerar um relatório das ameaças (Figura 41).

O menu 4 trata basicamente dos riscos. O item 4.2 permite selecionar as opções para o tratamento dos riscos detectados na rede e analisar o risco residual e definir a melhor forma de tratá-lo (Figura 42 e 43).

Figura 41: Configuração de Ameaças

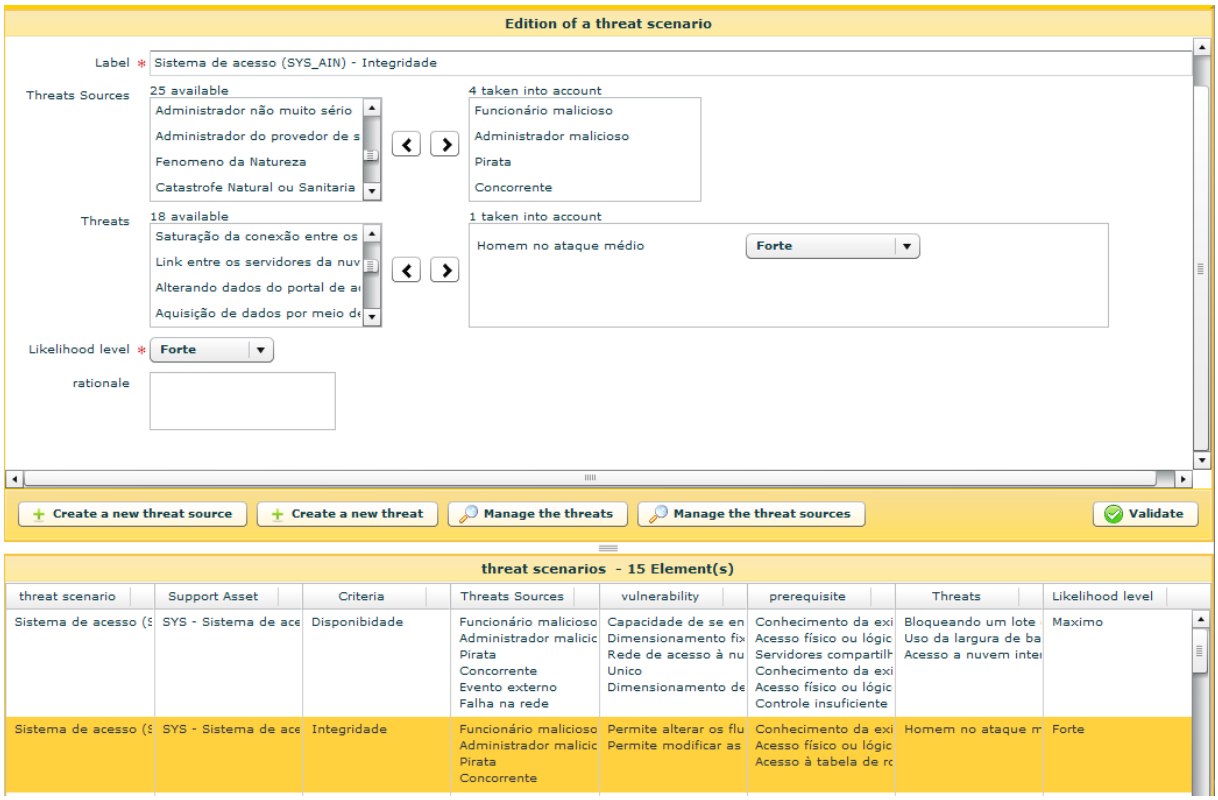


Figura 42: Configuração de Riscos

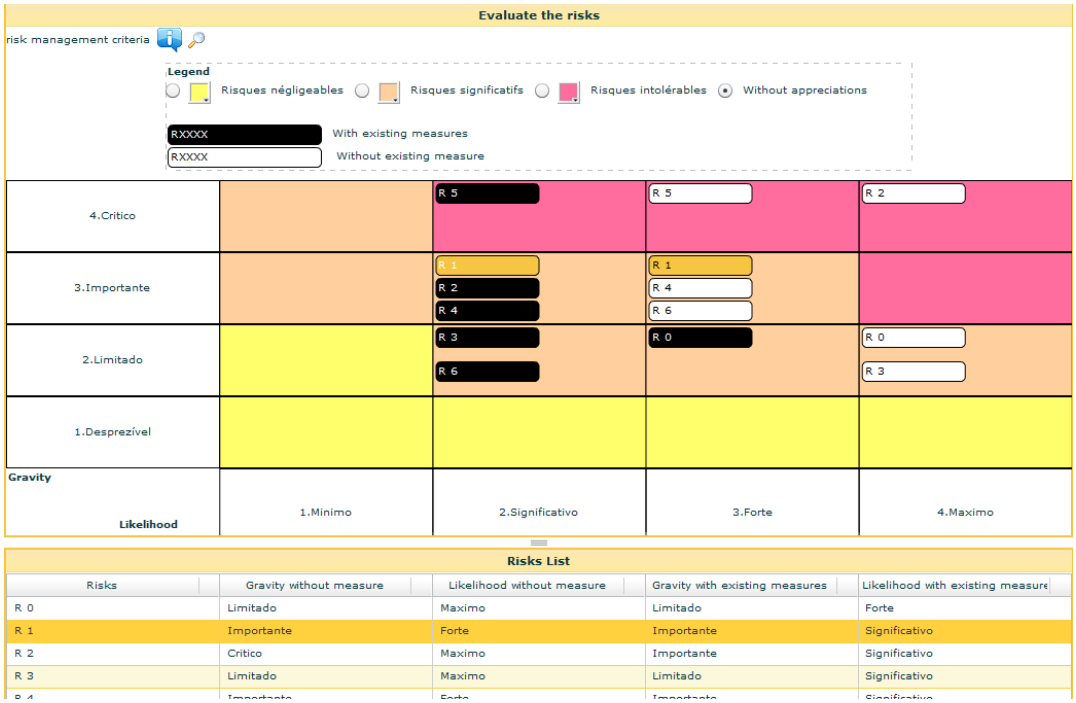
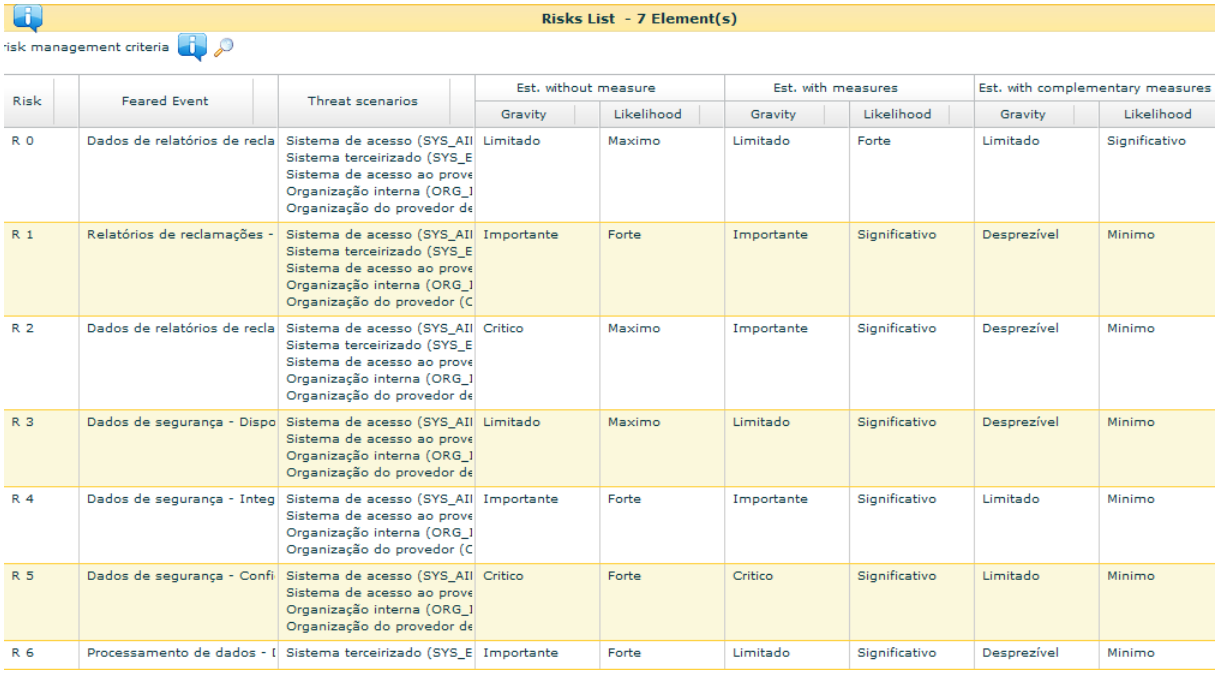


Figura 43: Relatório de Riscos



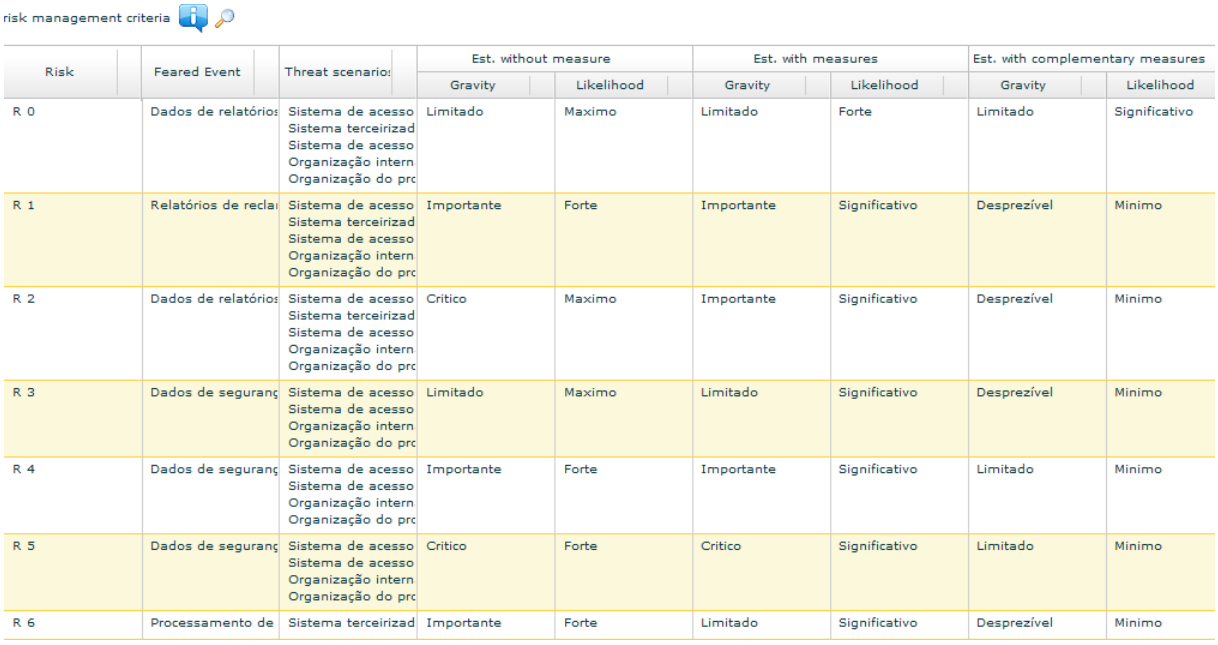
Risks List - 7 Element(s)

risk management criteria

Risk	Feared Event	Threat scenarios	Est. without measure		Est. with measures		Est. with complementary measures	
			Gravity	Likelihood	Gravity	Likelihood	Gravity	Likelihood
R 0	Dados de relatórios de recla	Sistema de acesso (SYS_AII Sistema terceirizado (SYS_E Sistema de acesso ao prove Organização interna (ORG_I Organização do provedor de	Limitado	Maximo	Limitado	Forte	Limitado	Significativo
R 1	Relatórios de reclamações -	Sistema de acesso (SYS_AII Sistema terceirizado (SYS_E Sistema de acesso ao prove Organização interna (ORG_I Organização do provedor (C	Importante	Forte	Importante	Significativo	Desprezível	Minimo
R 2	Dados de relatórios de recla	Sistema de acesso (SYS_AII Sistema terceirizado (SYS_E Sistema de acesso ao prove Organização interna (ORG_I Organização do provedor de	Critico	Maximo	Importante	Significativo	Desprezível	Minimo
R 3	Dados de segurança - Dispo	Sistema de acesso (SYS_AII Sistema de acesso ao prove Organização interna (ORG_I Organização do provedor de	Limitado	Maximo	Limitado	Significativo	Desprezível	Minimo
R 4	Dados de segurança - Integ	Sistema de acesso (SYS_AII Sistema de acesso ao prove Organização interna (ORG_I Organização do provedor (C	Importante	Forte	Importante	Significativo	Limitado	Minimo
R 5	Dados de segurança - Confi	Sistema de acesso (SYS_AII Sistema de acesso ao prove Organização interna (ORG_I Organização do provedor de	Critico	Forte	Critico	Significativo	Limitado	Minimo
R 6	Processamento de dados - I	Sistema terceirizado (SYS_E	Importante	Forte	Limitado	Significativo	Desprezível	Minimo

No menu 5 são cadastrados os controles de segurança utilizados na rede e a declaração de aplicabilidade desses controles. Após são cadastrados os planos de implementação e monitoramento desses controles (Figura 44).

Figura 44: Configuração do Plano de Ação



risk management criteria

Risk	Feared Event	Threat scenarios	Est. without measure		Est. with measures		Est. with complementary measures	
			Gravity	Likelihood	Gravity	Likelihood	Gravity	Likelihood
R 0	Dados de relatórios	Sistema de acesso Sistema terceirizad Sistema de acesso Organização intern Organização do prc	Limitado	Maximo	Limitado	Forte	Limitado	Significativo
R 1	Relatórios de reclar	Sistema de acesso Sistema terceirizad Sistema de acesso Organização intern Organização do prc	Importante	Forte	Importante	Significativo	Desprezível	Minimo
R 2	Dados de relatórios	Sistema de acesso Sistema terceirizad Sistema de acesso Organização intern Organização do prc	Critico	Maximo	Importante	Significativo	Desprezível	Minimo
R 3	Dados de segurança	Sistema de acesso Sistema de acesso Organização intern Organização do prc	Limitado	Maximo	Limitado	Significativo	Desprezível	Minimo
R 4	Dados de segurança	Sistema de acesso Sistema de acesso Organização intern Organização do prc	Importante	Forte	Importante	Significativo	Limitado	Minimo
R 5	Dados de segurança	Sistema de acesso Sistema de acesso Organização intern Organização do prc	Critico	Forte	Critico	Significativo	Limitado	Minimo
R 6	Processamento de	Sistema terceirizad	Importante	Forte	Limitado	Significativo	Desprezível	Minimo

5 AVALIAÇÃO DOS SOFTWARES OSSIM E EBIOS

Para realizar a avaliação dos softwares foram utilizados os critérios e as métricas definidas no capítulo 3. Foram definidos dois critérios de qualidade em uso e mais sete critérios de qualidade externa. Cada critério de qualidade externa possui subcaracterísticas, do qual foram selecionadas onze (Tabela 3).

Cada característica e/ou subcaracterística selecionada possui vínculo a uma métrica (Tabelas 4 e 5) auxiliando na mensuração das funcionalidades dos softwares. O peso de cada métrica foi definido na seção 3.3.

Após a avaliação dos softwares utilizando os critérios definidos, foi realizada a avaliação individual de cada software considerando a pontuação recebida em cada critério.

5.1 Adequação

Este critério é o de maior peso na avaliação dos softwares. O propósito da métrica é identificar o quão adequadas são as funções avaliadas. Ela avalia o número de funções que são adequadas para executar as tarefas especificadas, em comparação com o número de funções que foram avaliadas.

As funcionalidades foram previamente definidas com base nos requisitos da norma ABNT NBR ISO 27001. O software OSSIM não atingiu algumas funcionalidades como o cadastramento de tarefas e documentação. As demais funcionalidades foram atendidas pelo software. O EBIOS também não possui algumas das funcionalidades testadas como a correlação de eventos, acompanhamentos e documentação. As demais funcionalidades são atendidas pelo software. Um resumo das funcionalidades atendidas por cada um dos softwares encontra-se na Tabela 19.

Tabela 19: Funcionalidades Adequação

Funcionalidade	Satisfeitas	
	OSSIM	Ebios
Análise de Risco	X	X
Cadastramentos Sobre Tarefas		X
Cadastramentos de Controles	X	X
Cadastramentos Funcionais	X	X
Correlação do Evento	X	
Armazenamento dos Eventos	X	X
Acompanhamentos	X	
Documentação		

A adequação foi calculada utilizando a fórmula X = 1 - A / B, onde A representa o número de funcionalidades não atendidas e B o número de funções avaliadas (Tabela 19). Considerando que quanto mais próximo de 1 mais adequado é o software, o OSSIM (0,75) obteve um resultado melhor que o EBIOS (0,62) (Tabela 20).

Tabela 20: Critério 1

Característica	Subcaracterística	Métrica	Software	Interpretação	Resultado
Funcionalidade	Adequação	Adequação Funcional	OSSIM	X = 1 – 2 / 8	0,75
Funcionalidade	Adequação	Adequação Funcional	EBIOS	X = 1 – 3 / 8	0,62

5.2 Acurácia

Este critério tem como propósito identificar com que frequência os usuários finais encontram resultados com precisão inadequada. Pode-se citar como exemplos de resultados com precisão inadequada: relatórios emitidos e consultas realizadas entregues pelos softwares com imprecisão de dados.

Foram realizados diversos testes visando identificar a imprecisão dos softwares através dos casos de testes de número 3 (Aceitação de Riscos), 4 (Tratamento de Riscos), 5 (Cadastros), 6 (Correlacionar Eventos de Segurança), 8 (Métricas e Relatórios) e 9 (Análise de Desempenho) definidos na seção 3.4. Para

identificar a precisão dos resultados foram realizadas as tarefas descritas na Tabela 21.

Tabela 21: Tarefas Acurácia

Tarefas	Precisão	
	OSSIM	Ebios
Cadastro de Ativos	X	X
Cadastro de Ameaças	X	X
Cadastro de Controles Existentes	X	X
Cadastro de Vulnerabilidades	X	X
Cadastro das Consequências	X	X
Relação da Avaliação das Probabilidades e Consequências (Impacto)	X	X
Relação de Estimativa de Riscos	X	X
Relação da Escolha do Tipo de Tratamento a Ser Realizado	X	X
Relação da Recomendação de Controles	X	X
Relação da Análise e Avaliação de Riscos	X	X
Relação da Aceitação de Risco	X	X
Cadastros de Tarefas	X	X
Relação de Tratamento do Risco	X	X
Correlação dos Eventos de Segurança	X	
Relação do Armazenamento dos Eventos de Segurança	X	X

O teste do software OSSIM não apresentou nenhuma imprecisão nos resultados. O software EBIOS apresentou uma imprecisão, ao executar o caso de teste de número 6, correlacionar os eventos de segurança. O relatório de correlação dos eventos de segurança trouxe dados incoerentes com o que foi cadastrado.

A acurácia foi calculada utilizando a fórmula X = A / B, onde A representa o número de resultados com precisão inadequada e B o tempo em horas de operação do sistema. Considerando que o resultado quanto o mais próximo de 0 mais adequado, o OSSIM (0) obteve um resultado melhor que o EBIOS (0,03) nesse critério (Tabela 22).

Tabela 22: Critério 2

Característica	Subcaracterística	Métrica	Software	Interpretação	Resultado
Funcionalidade	Acurácia	Precisão	OSSIM	X = 0 / 30	0
Funcionalidade	Acurácia	Precisão	EBIOS	X = 1 / 30	0,03

5.3 Conformidade

Este critério identifica o quão compatível é a funcionalidade do produto com os regulamentos, padrões e convenções aplicáveis a este tipo de software. São contados o número de itens que exigem conformidade que foram atendidos e comparados com o número de itens que exigem conformidade na especificação que consta na norma ABNT NBR ISO 27001.

Foram testados os softwares através dos casos de teste de acordo com os itens de conformidade. O OSSIM teve 13 itens de conformidade satisfeitos e o EBIOS teve 16 itens (Tabela 23).

Tabela 23: Conformidades

Conformidades	**Satisfeitas**	
	OSSIM	**Ebios**
Contexto da Organização		X
Funções e Responsabilidades	X	X
Liderança e Comprometimento		X
Política		
Generalidades		
Avaliação de Risco SI	X	X
Tratamento de Risco SI	X	X
Objetivos da SI e Planejamento para Alcançar		
Recursos	X	X
Competência	X	X
Conscientização		
Comunicação		X
Controle de Informação Documentada		
Genérico		
Criação e Atualização	X	X
Planejamento e Controle Operacional	X	X
Avaliação de Risco	X	X
Tratamento de Risco	X	X
Monitorização, Medição, Análise e Avaliação	X	X
Auditoria Interna		
Revisão pela Gestão	X	X
Não Conformidade e Ações Corretivas	X	X
Melhoria Contínua	X	X

Este critério é calculado utilizando a fórmula X = 1 - A / B, onde A representa o número de conformidades não atendidas e B o número total de conformidades da norma. Considerando que quanto mais próximo de 1, mais adequado será o software, o OSSIM obteve um índice de 0,56 e o EBIOS um índice de 0,69 (Tabela 24).

Tabela 24: Critério 3

Característica	Subcaracterística	Métrica	Software	Interpretação	Resultado
Funcionalidade	Conformidade	Conformidade de funcionalidade	OSSIM	X = 1 - 10 / 23	0,56
Funcionalidade	Conformidade	Conformidade de funcionalidade	EBIOS	X = 1 - 7 / 23	0,69

5.4 Operacionalidade

Este critério tem o propósito de identificar o quão consistente é o componente da interface do usuário, através da observação do comportamento do usuário. É solicitado a opinião do usuário sobre os componentes de interface encontrados nos softwares testados.

Foram realizados diversos testes visando identificar a inconsistência dos componentes de interface dos softwares através dos casos de testes de número 3 (Aceitação de Riscos), 5 (Cadastros), 6 (Correlacionar Eventos de Segurança), 7 (Armazenamento dos Eventos de Segurança), 8 (Métricas e Relatórios) e 9 (Análise de Desempenho). Não foi encontrada nenhuma inconsistência de interface em ambos os softwares. Destaca-se o software EBIOS, que mesmo com a possibilidade de alterar o idioma do sistema, manteve a consistência.

A operacionalidade foi calculada utilizando a fórmula X = A / B, onde A representa o número de operações que o usuário encontrou inaceitavelmente inconsistente com a expectativa do usuário e B o tempo em horas de operação do sistema. Dessa forma, considerando que o resultado o quanto mais próximo de 0 mais adequado, tanto o OSSIM (0) quanto o EBIOS (0) foram perfeitos nesse critério (Tabela 25).

Tabela 25: Critério 4

Característica	Subcaracterística	Métrica	Software	Interpretação	Resultado
Usabilidade	Operacionalidade	Consistência operacional em uso	OSSIM	X = 0 / 30	0
Usabilidade	Operacionalidade	Consistência operacional em uso	EBIOS	X = 0 / 30	0

5.5 Atratividade

Este critério possui o propósito de identificar qual a capacidade de personalização da interface dos softwares, identificando qual a proporção de elementos de interface que podem ser personalizadas em aparência para a satisfação do usuário final. O teste é conduzido através da observação e o comportamento dos usuários com os componentes de interface encontrados.

Foram realizados diversos testes visando identificar a capacidade de personalização da interface dos softwares através dos casos de testes de número 1 (Parametrização do Sistema), 5 (Cadastros), 7 (Armazenamento dos Eventos de Segurança) e 8 (Métricas e Relatórios). Não foi identificado nenhuma possibilidade de personalizar a interface em ambos os softwares.

A atratividade foi calculada utilizando a fórmula X = A / B, onde A representa o número de elementos de interface personalizados na aparência para a satisfação do usuário e B o número de elementos de interface que o usuário deseja personalizar. Dessa forma, considerando que o resultado o quanto mais próximo de 1 mais adequado, tanto o OSSIM (0) quanto o EBIOS (0) foram más nesse critério (Tabela 26).

Tabela 26: Critério 5

Característica	Subcaracterística	Métrica	Software	Interpretação	Resultado
Usabilidade	Atratividade	Capacidade de personalização da interface	OSSIM	X = 0 / 2	0
Usabilidade	Atratividade	Capacidade de personalização da interface	EBIOS	X = 0 / 4	0

5.6 Adaptabilidade

Este critério tem o propósito de identificar se o usuário ou mantenedor do software pode facilmente adaptar o software ao ambiente encontrado e se o software é capaz de se adaptar ao ambiente de operação encontrado, mais especificamente se o software consegue se adaptar aos dispositivos de hardware e instalações de rede. É medido através da observação do comportamento do usuário ou do mantenedor quando o usuário está tentando adaptar o software ao ambiente de operação.

Este critério possui um caso de teste específico para si, caso de teste número 10 (Adaptabilidade), onde é testado se o software é capaz de executar em diversos sistemas operacionais, Foram realizados diversos testes visando identificar se o software se adapta ao ambiente de operação encontrado através dos casos de testes de número 1 (Parametrização do Sistema), 7 (Armazenamento dos Eventos de Segurança) e 8 (Métricas e Relatórios) e 9 (Análise de Desempenho).

O software OSSIM é um tipo de arquivo ISO com base em Linux, portanto não é possível utilizá-lo em outra plataforma que não Linux. O sistema exige uma memória RAM mínima de 2GB, porém para ter um bom desempenho é necessário alocar uma quantidade maior de memória RAM. O software EBIOS possui versão para executar tanto em Linux quanto em Windows. O EBIOS exige menores requisitos de hardware e não apresentou nenhum problema na execução do software (Tabela 27).

Tabela 27: Testes Adaptabilidade

Testes Adaptabilidade	**Satisfeitas**	
	OSSIM	**Ebios**
Executar Software no SO Linux	X	X
Executar Software no SO Windows		X
Executar Software na Rede Local	X	X
Executar Software no Host com 2GB de RAM Alocado		X
Executar Software no Host com 4GB de RAM Alocado	X	X
Executar Software no Host com 8GB de RAM Alocado	X	X
Executar Software no Host com 127GB HD Alocado	X	X
Executar Software no Host com 250GB HD Alocado	X	X

Este critério foi calculado utilizando a fórmula X = 1 - A / B, onde A representa o número de funções operacionais das quais as tarefas não foram concluídas ou não foram suficientes para atender a níveis adequados durante o teste operacional combinado com hardware ambiental e B o número total de funções que foram testadas.

O OSSIM não é compatível com o sistema operacional Windows e ele necessita uma memória RAM superior a 2GB para ser executado. Por outro lado, o EBIOS não apresentou problemas em sua execução. Considerando que quanto maior o resultado mais adequado o software, o EBIOS (1) obteve um resultado melhor que o OSSIM (0,75) nesse critério (Tabela 28).

Tabela 28: Critério 6

Característica	Subcaracterística	Métrica	Software	Interpretação	Resultado
Portabilidade	Adaptabilidade	Adaptabilidade ambiental do hardware	OSSIM	X = 1 - 2 / 8	0,75
Portabilidade	Adaptabilidade	Adaptabilidade ambiental do hardware	EBIOS	X = 1 - 0 / 8	1

5.7 Coexistência

Este critério tem o propósito de identificar com que frequência o usuário encontra restrições ou falhas inesperadas ao operar o software em simultâneo com outros softwares que o usuário geralmente usa.

Foram realizados diversos testes visando identificar a disponibilidade da coexistência dos softwares através dos casos de testes de número 2 (Análise e Avaliação de Risco), 6 (Correlacionar Eventos de Segurança), 9 (Análise de Desempenho), 10 (Adaptabilidade) e 11 (Coexistência). Ambos os softwares, OSSIM e EBIOS, não apresentaram nenhuma indisponibilidade, restrição ou falha ao operar em conjunto com outros softwares.

A coexistência foi calculada utilizando a fórmula X = A / B, onde A representa o número de restrições ou falhas inesperadas que o usuário enfrenta ao operar em simultâneo outro software, e B o tempo em horas de operação simultânea com outros softwares. Dessa forma, considerando que o resultado o quanto mais próximo

de 0 mais adequado, tanto o OSSIM (0) quanto o EBIOS (0) foram perfeitos nesse critério (Tabela 29).

Tabela 29: Critério 7

Característica	Subcaracterística	Métrica	Software	Interpretação	Resultado
Portabilidade	Coexistência	Coexistência disponível	OSSIM	X = 0 / 30	0
Portabilidade	Coexistência	Coexistência disponível	EBIOS	X = 0 / 30	0

5.8 Efetividade

Este critério tem o propósito de identificar qual é a frequência de erros apresentados pelos softwares.

Foram realizados diversos testes visando identificar a frequência de erros dos softwares através das tarefas identificadas nos casos de testes (seção 4.3) em conjunto com as definições do caso de uso (Anexo A) utilizado (Tabela 30).

Tabela 30: Tarefas Efetividade

Tarefas	Satisfeitas	
	OSSIM	Ebios
Identificação de Ativos	X	X
Identificação de Ameaças	X	X
Identificação de Controles Existentes	X	X
Identificação de Vulnerabilidades	X	X
Identificação das Consequências	X	X
Avaliação das Probabilidades e Consequências (Impacto)	X	X
Estimativa de Riscos	X	X
Escolha do Tipo de Tratamento a Ser Realizado	X	X
Recomendação de Controles	X	X
Análise e Avaliação de Riscos	X	X
Aceitação de Risco	X	X
Cadastros	X	X
Tratamento do Risco	X	X
Correlacionar Eventos de Segurança	X	
Armazenamento dos Eventos de Segurança	X	X

O teste do software OSSIM não apresentou nenhum erro em dezesseis tarefas completadas enquanto o software EBIOS apresentou um, ao tentar executar uma correlação dos eventos de segurança cadastrados.

A efetividade foi calculada utilizando a fórmula X = A / B, onde A representa o número de erros encontrados e B número de tarefas completadas pelo usuário. Dessa forma, considerando que o resultado quanto mais próximo de 0 mais adequado, o OSSIM (0) obtêm um resultado melhor que o EBIOS (0,1) nesse critério (Tabela 31).

Tabela 31: Critério 8

Característica	Métrica	Software	Interpretação	Resultado
Efetividade	Frequência de Erro	OSSIM	X = 0 / 16	0
Efetividade	Frequência de Erro	EBIOS	X = 1 / 16	0,1

5.9 Produtividade

Este critério tem o propósito de identificar quanto tempo demora para o usuário completar uma tarefa. É medido através de testes com o usuário, calculando através da divisão do tempo ocioso do usuário pelo tempo das tarefas completadas pelo usuário, assim obtendo o valor e qual o tempo de tarefa.

Foram realizados diversos testes visando identificar o tempo de tarefa dos softwares através das tarefas (Tabela 30) definidas com base nos casos de testes (seção 3.4). O teste do software OSSIM obteve um total de quatro horas ociosas durante a execução das tarefas completadas enquanto o software EBIOS apresentou o total de uma hora ociosa.

A produtividade foi calculada utilizando a fórmula X = A / B, onde A representa o tempo ocioso do usuário e B o tempo das tarefas completadas pelo usuário. Dessa forma, considerando que o resultado quanto mais próximo de 0 mais adequado, o EBIOS (0,03) obtêm um resultado melhor que o OSSIM (0,13) nesse critério (Tabela 32).

Tabela 32: Critério 9

Característica	Métrica	Software	Interpretação	Resultado
Produtividade	Tempo da Tarefa	OSSIM	X = 4 / 30	0,13
Produtividade	Tempo da Tarefa	EBIOS	X = 1 / 30	0,03

5.10 Resultados das Avaliações

Após a avaliação individual dos softwares utilizando os critérios e métricas selecionados, o resultado final das avaliações foi calculado. Para realizar o cálculo foi construída uma tabela com os critérios utilizados, o peso de cada critério (seção 3.3) para avaliação e os resultados dos critérios por software testado (Tabela 33).

Para calcular o valor total de um software, foi calculado o percentual do resultado de cada software por critério avaliado, colunas “OSSIM/Critério (%)” e “EBIOS/Critério (%)”. Depois este resultado foi calculado de acordo com o peso que cada critério possui, colunas “Total OSSIM (%)” e “Total EBIOS (%)”. Após foi somado o percentual total de cada critério, o que gerou o percentual total do software, o resultado mais alto na última linha da tabela (TOTAL %) representa o software que possui maior aderência a norma ABNT NBR ISO 27001.

Tabela 33: Avaliação dos Softwares

Critérios	**OSSIM / Critério (%)**	**EBIOS / Critério (%)**	**Peso (%)**	**Total OSSIM (%)**	**Total EBIOS (%)**
Adequação	75	62	**40**	30	24,8
Acurácia	100	97	**7,5**	7,5	7,3
Conformidade	56	69	**7,5**	4,2	5,2
Operacionalidade	100	100	**7,5**	7,5	7,5
Atratividade	0	0	**7,5**	0	0
Adaptabilidade	75	100	**7,5**	5,6	7,5
Coexistência	100	100	**7,5**	7,5	7,5
Frequência de Erro	100	90	**7,5**	7,5	6,7
Tempo da Tarefa	87	97	**7,5**	6,5	7,3
TOTAL (%)				**76,3**	**73,8**

Tendo em vista as análises realizadas, nenhum dos softwares avaliados está adequado totalmente aos critérios propostos, sobretudo, aquele julgado mais importante, a adequação funcional. Entretanto, o software que demonstrou melhores capacidades e, portanto, obteve o maior valor foi o OSSIM.

O OSSIM foi o que mostrou-se o mais preparado na maioria dos critérios, sendo estes critérios a adequação, acurácia e frequência de erro. O valor total do OSSIM se deve principalmente pelo software ter obtido maior média no critério

adequação funcional, assim, se mostrando o mais aderente aos requisitos funcionais que exige a norma ABNT NBR ISO 27001. Conclui-se então que embora ainda tenha pontos que poderiam ser melhorados o software se mostrou mais completo quanto as exigências da norma ABNT NBR ISO 27001.

O EBIOS obteve uma boa média também, sendo inclusive superior em alguns dos critérios como a conformidade, adaptabilidade e tempo de tarefa. Importante pontuar que tirando o critério de adequação, que era o que mais valia, o EBIOS possui pontuação maior que o OSSIM, ou seja, apesar de o software não ser o mais aderente as exigências da norma ABNT NBR ISO 27001 ainda é um software com bastante potencial.

6 CONCLUSÃO

Para que a segurança da informação seja devidamente implantada, é necessário que as organizações definam e implementem controles que sejam continuamente monitorados e analisados. Os SGSI possuem como base um programa estruturado para a implantação de procedimentos, diretrizes, políticas, orientações e normas para a proteção do conhecimento e da marca da organização. A ABNT/NBR 27001 descreve basicamente como desenvolver um SGSI como uma abordagem sistemática para a proteção e gestão das informações dessa organização.

O objetivo principal deste trabalho foi analisar e avaliar softwares SGSI com o intuito de identificar qual o software possui maior aderência com a norma ABNT NBR ISO/IEC 27001. Para chegar a esta conclusão e executar as avaliações das ferramentas, foi necessário o estudo de alguns conceitos de Segurança da Informação e SGSI. Para melhor tratar as questões de segurança e normalização também foram escolhidas algumas das principais normas da área de Segurança da Informação (ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27003 e ABNT NBR ISO/IEC 27004).

Foram selecionados alguns softwares para uma pré análise e dentre estes foram selecionados os softwares a serem testados (OSSIM e EBIOS). Para seguir um padrão na avaliação dos softwares foram selecionadas algumas normas que regem padrão para avaliação da qualidade de softwares (ABNT NBR ISO/IEC 25020 e ABNT NBR ISO/IEC 25030). Com base nos estudos das normas foi possível definir os critérios, métricas e casos de testes para a avaliação dos softwares, de acordo com as funcionalidades fundamentais definidas pela norma ABNT NBR ISO/IEC 27001.

Com o desenvolvimento do trabalho foi possível chegar a conclusão de que as normas de segurança e avaliação de softwares são um fator importante e que podem auxiliar na hora de escolher uma ferramenta de software para utilizar em uma organização. Com a ajuda das normas é possível desenvolver um plano de análise bem estruturado e profundo em busca de selecionar qual a melhor ferramenta para a sua organização.

Selecionar softwares SGSI de código aberto foi um pouco complicado pois a grande maioria dos softwares encontrados eram ferramentas pagas e foi necessário

fazer um filtro nas buscas. A fase da escolha dos softwares SGSI de código livre e a definição dos critérios e métricas de avaliação foram mais teóricas porém muito importantes para o desenvolvimento do trabalho.

Para o desenvolvimento do trabalho foi necessário instalar os softwares selecionados em um ambiente controlado. Os testes definidos foram realizados nas ferramentas selecionadas de acordo com os critérios e métricas definidos, buscando encontrar qual ferramenta atingi objetivo principal do trabalho.

O OSSIM apesar de ter sido o software que ficou com o melhor resultado nas avaliações, pode ser aprimorado. Ele possui alguns requisitos que não estão de acordo com as exigências da norma ABNT NBR ISO 27001. O software poderia ser mais atrativo, dando a possibilidade do usuário customizar a interface do sistema conforme a sua necessidade. Porém mesmo com a necessidade de algumas alterações, o sistema atingiu quase 80% na avaliação final, e 75% no critério de adequação das funcionalidades. O OSSIM também possui a sua versão paga, o SIEM, que possui funcionalidades a mais que a versão aberta e talvez tenha as funcionalidades que penalizaram o OSSIM nessa avaliação.

O EBIOS, apesar de ficar atrás do OSSIM na avaliação final, não deixa de ser uma boa opção para quem deseja implementar um SGSI na sua organização. O software necessita de alguns aprimoramentos, principalmente na área de adequação funcional e as conformidades do sistema de acordo com a norma ABNT NBR ISO 27001. Porém, apesar de ser um sistema menor que o OSSIM, ele é bem interessante e com uma boa base, principalmente para organizações que estejam iniciando nesse mercado do gerenciamento da segurança da informação.

Como possíveis trabalhos futuros, pode se considerar, já que todos os softwares utilizados são de código aberto, a incorporação de novos módulos nos softwares testados, acrescentando funções as quais os softwares deixaram a desejar nos testes efetuados.

REFERÊNCIAS

ALMEIDA, E. **Sistema de Gestão de Segurança da Informação (SGSI) – Parte I.** Disponível em: <http://www.tiespecialistas.com.br/2013/10/sistema-gestao-seguranca-informacao-sgsi-i/> Acesso em: 20 mar. 2017.

ALIENVAULT. **OSSIM**. Disponível em: <https://www.alienvault.com/products/ossim>. Acesso em: 11 jun. 2017.

ANTINARELLI, Alexandre. **CONSTRUINDO A GESTÃO ESTRATÉGICA SUSTENTÁVEL: UM ESTUDO SOBRE A EMPRESA MERCUR S/A.** 2013. 1 v. Tese (Doutorado) - Curso de Administração, Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2013.

ANTOLÍK, Štefan. **COMPARISON OF TOOLS FOR INFORMATION SECURITY MANAGEMENT SYSTEM.** 2013. Disponível em: <https://www.unob.cz/eam/Documents/Archiv/EaM_1_2013/Antolík.pdf>. Acesso em: 17 jun. 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 25000:2008:** Engenharia de software - Requisitos e avaliação da qualidade de produtos de software (SQuaRE) - Guia do SQuaRE. Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 25010:2011:** Engenharia de sistemas e software - Sistemas e software Requisitos de Qualidade e Avaliação (SQuaRE) - Modelos de qualidade de sistema e software. Rio de Janeiro, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 25020:2009:** Engenharia de software - Requisitos e avaliação da qualidade de produto de software (SQuaRE) - Guia e modelo de referência para medição. Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 25030:2008:** Engenharia de software - Requisitos e Avaliação da Qualidade de Produto de Software (SQuaRE) - Requisitos de qualidade. Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013:** Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisito. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2005:** Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27003:2011:** Tecnologia da informação - Técnicas de segurança - Diretrizes para implantação de um sistema de gestão da segurança da informação. Rio de Janeiro, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27004:2010:** Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Medição. Rio de Janeiro, 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2008:** Tecnologia da Informação: Técnicas de Segurança: Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008.

BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.** São Paulo: Atlas, 2008.

BOISOT, M. **Knowledge Assets.** Oxford: Oxford University Press, 1998.

CAMPONAR, L. O. C. M. C. **Micro e pequenas empresas: Caracteristicas estruturais e gerenciais.** 2004. Disponível em: <http://www.unifafibe.com.br/revistasonline/arquivos/hispecielemaonline/sumario/10/19042010081633.pdf >. Acesso em: 13 abr. 2017.

CAMPOS, A. **Sistema de segurança da informação:** controlando os riscos. Florianópolis: Visual Books, 2ª ed, 2007.

COMPUTER WORLD (Brasil). **Empresas precisam reavaliar estratégias de segurança.** 2017. Disponível em: <http://computerworld.com.br/empresas-precisam-reavaliar-estrategias-de-seguranca-afirma-cisco>. Acesso em: 08 mar. 2017.

ELASTICSEARCH. **ELK Stack**. Disponível em: <https://www.elastic.co/webinars/introduction-elk-stack>. Acesso em: 11 jun. 2017.

EY BRASIL (Brasil). **Crimes cibernéticos são a maior ameaça à sobrevivência das empresas.** 2013. Disponível em: <http://www.ey.com/br/pt/services/release_pesquisa_seguranca_informacao_ey>. Acesso em: 28 fev. 2017.

GALVÃO, M. **Fundamentos em segurança da informação**. São Paulo: Pearson Education do Brasil, 2015.

HERMANOWSKI, Damian. **Open Source Security Information Management System Supporting IT Security Audit.**2015. Systems Department, Military Communication Institute, Zegrze, 2015. Disponível em: <http://www.wil.waw.pl/art_prac/2015/pub_cybconfCybersec15_DH-OSSIM-ieee_REVIEW_RC05_ver_PID3720933.pdf>. Acesso em: 29 maio 2017.

KASPERSKY BRASIL (Brasil). **Brasil é lider em cibertaques na América Latina.** 2017. Disponível em: <https://blog.kaspersky.com.br/brasil-e-lider-em-cibertaques-na-america-latina/3754/>. Acesso em: 27 fev. 2017.

KUROSE, J. e ROSS, K. **Redes de computadores e a Internet: uma abordagem top-down.** São Paulo: Pearson Education do Brasil, 2013.

LLC, Security Onion Solutions. **Security Onion**. Disponível em: <https://securityonion.net/>. Acesso em: 11 jun. 2017.

MANOEL,S. S. **Governança de Segurança da Informação- Como criar oportunidades para seu negocio.** Editora Brasport, Rio de Janeiro, 2014.

McGEE, J.; PRUSAK, L. **Gerenciamento estratégico da informação:** aumente a competitividade e eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Tradução de Astrid Beatriz de Figueiredo. Rio de Janeiro: Elsevier, 1994.

MOURA, H. P.; ANDRADE, J. N. **Implantando a Gestão de Serviços de TI: Uma abordagem horizontal baseada no catálogo de serviços de TI**. Recife, 2007. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2008/0016.pdf>. Acesso em: 20 mar. 2017.

PREWIKKA, Prelude And. **Prelude OSS**. Disponível em: <https://www.prelude-siem.com/en/products/prelude-oss/>. Acesso em: 11 jun. 2017.

PWC BRASIL (Brasil). **Inovando e Transformando em Segurança Cibernética.** 2016. Disponível em: <http://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/2016/tl-gsiss16-pt.pdf>. Acesso em: 07 mar. 2017.

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

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. **Risk Management Guide for Information Technology Systems.** Gaithersburg: NIST – National Institute of Standards and Technology, 2002. 54p. (Special Publication 800-30). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: 27 fev. 2017.

TREND MICRO. **TURNING THE TABLES ON CYBER ATTACKS.** 2014. Disponível em: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-turning-the-tables-on-cyber-attacks.pdf>. Acesso em: 05 mar. 2017.

TSO, I. **O ciclo de vida dos serviços ITIL.** London: TSO: Figura 3 p. 2012.

TRYFONAS, Theo; ASKOXYLAKIS, Ioannis. **Human Aspects of Information Security**, Privacy, and Trust. Los Angeles: Springer, 2015.

OPEN SOURCE SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM: **Security Management**. Canadá: Admin Network And Security, 2014. Disponível em: <http://www.admin-magazine.com/Archive/2014/20/Open-Source-Security-Information-and-Event-Management-system>. Acesso em: 17 jun. 2017.

UPGUARD. **ALIENVAULT VS QRADAR.** 2017. Disponível em: <https://www.upguard.com/articles/alienvault-vs-qradar>. Acesso em: 15 jun. 2017.

VIANEZ, M. S.; SEGOBIA, R. H.; CAMARGO, V. **Segurança de Informação:** Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005. Revista de Informática Aplicada, São Caetano do Sul, n. 1, p. 33-44, 2008. Disponível em: http://seer.uscs.edu.br/index.php/revista_informatica_aplicada/article/view/307. Acesso em: 28 fev. 2017.

VERHEIJEN, V. T. **ITIL V3 Foundation Exam - The Study Guide.** First. Van Haren Publishing, Zaltbommel, 2008.

ZURIEL. **LOGalyze**. Disponível em: <http://www.logalyze.com/>. Acesso em: 11 jun. 2017.

ANEXO A

TRABALHO DE GESTÃO DE RISCOS - CONSTRUINDO A GESTÃO ESTRATÉGICA SUSTENTÁVEL: UM ESTUDO SOBRE A EMPRESA MERCUR S/A

Este trabalho utilizou como base para estudo de caso o trabalho desenvolvido na disciplina de Segurança da Informação, do ano 2016, do curso Bacharel em Sistemas da Informação da Universidade de Caxias do Sul feito pelos alunos Alex Gilmar Boeno de Lima e Fernando Loss Scopel. Ressaltando que foi utilizado apenas uma parte desse trabalho, que vai ser compactada nesse anexo.

1ª Etapa – Definição do Contexto

Ao analisar a organização é importante definir os elementos que caracterizam-na. A seguir vemos alguns desses itens para identificação:

Propósito da Organização:

Trabalhar para atender as necessidades humanas com o menor peso possível sobre animais, ambiente natural, pessoas e sociedade.

O negócio:

A empresa que atua na área da produção de derivados da borracha expandiu seus negócios atuando nos segmentos da Educação (stationery), Saúde (cuidados pessoais), Revestimentos e Negócios Internacionais.

A missão:

Definida como “Compromisso Institucional” é de “Unir pessoas e organizações para construir soluções sustentáveis”.

A visão do futuro:

A visão tem enfoque estratégico sobre o campo do “bem-estar”, sendo este conceituado a nível institucional como: “O mundo de um jeito bom para todo o mundo”.

Os valores:

Os valores da empresa são: atuar em função das pessoas, buscar soluções relevantes com simplicidade, ser ético em todos os relacionamentos, preservar para a posteridade e atuar em mercados éticos que valorizem a vida.

A estrutura organizacional:

A empresa possui uma estrutura organizacional diferenciada dos tradicionais modelos de organograma das empresas, menos verticalizada e composta da seguinte forma:

-Conselho de Administração, Diretor Geral e Facilitação que atuam na direção estratégica da empresa;

-E pelas demais áreas de Infraestrutura, Serviços Compartilhados, Cadeia de Suprimentos, Espaços de Aprendizagem, Clientes, PeD, Estratégia e Incubadora que atuam na coordenação das principais operações da empresa, através do formato de colegiado em substituição aos tradicionais cargos de gerência.

Quanto a segurança da informação fica sob responsabilidade do setor de Tecnologia da Informação.

O organograma:

As estratégias:

Os objetivos estratégicos organizacionais, definidos como “Direcionamentos Mercur”, são voltados para as dimensões do desenvolvimento sustentável e tem o

propósito de apoiar as ações e decisões da empresa nos âmbitos estratégico, tático e operacional.

Quanto a segurança da informação a principal estratégia da empresa é trabalhar sempre visando diminuir os riscos e evitar perdas ou danos.

Os produtos:

A empresa detém um portfólio de mais de 1,5 mil itens, dentre os quais: as tradicionais borrachas de apagar, colas, corretivos líquidos, tintas guache e tintas para artesanato, bolsas para água quente e gelo, joelheiras, tornozeleiras, bolas para pilates, muletas, bengalas, andadores e uma extensa linha de pisos e revestimentos de borracha, como pisos táteis e pisos para playgrounds.

Os parceiros:

A empresa incentiva à busca da melhoria contínua dos fornecedores por meio de parcerias com os fornecedores-chave. Parceiros são aqueles fornecedores que compartilham o envolvimento com a qualidade, custo, logística, meio ambiente, tecnologia, serviços e questões financeiras.

Todos os parceiros passam pelo treinamento de integração a empresa, que inclui um overview sobre as normas de segurança da empresa que todos tem de seguir.

Os terceiros:

Além da força de trabalho, estão distribuídas por empresas prestadoras de serviços, com supervisão própria, 70 pessoas atuando como terceiros em atividades de apoio como refeitório, limpeza e segurança, sem a supervisão direta e que não estão associadas aos processos principais do negócio da empresa.

Todos os terceiros passam pelo treinamento de integração a empresa, que inclui um overview sobre as normas de segurança da empresa que todos tem de seguir.

As instalações:

A organização tem a gestão ambiental como um de seus principais desafios para o futuro. Para que as interferências sejam mínimas, o conceito de sustentabilidade deve ser aplicado desde a ocupação física do ambiente.

Nossas instalações são construídas sob demanda e no conceito "green building", de forma a promover o uso responsável de água, energia e outros recursos, além da redução de dejetos, poluentes e degradação ambiental. Estes

conceitos são considerados desde a escolha dos materiais da edificação até o seu uso e manutenção.

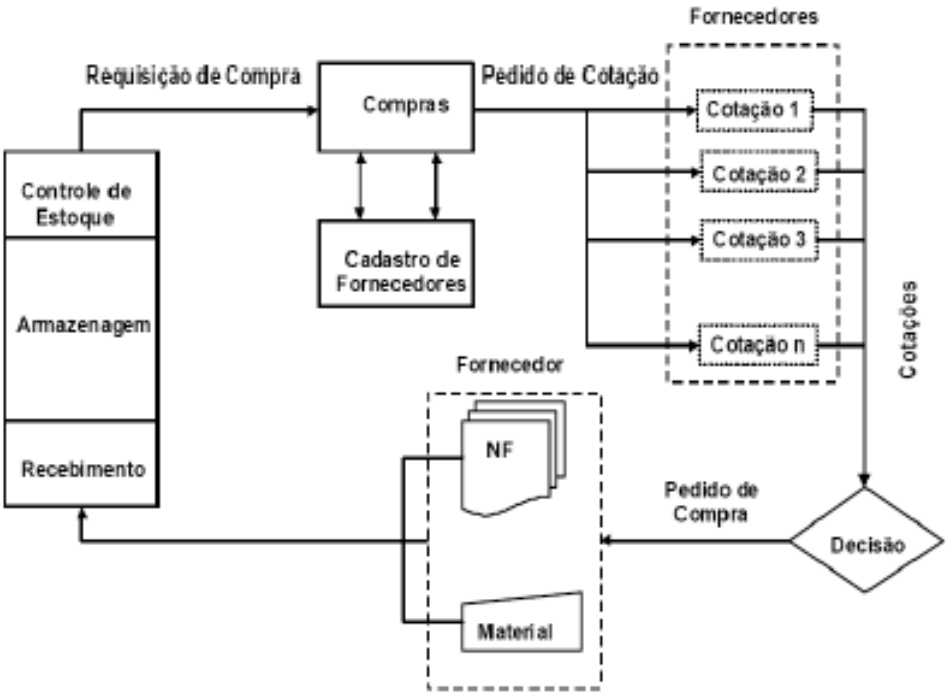
Os nossos servidores ficam dentro de uma “sala cofre” localizada no setor de TI aonde possuímos um ambiente climatizado e com sistema de prevenção de incêndio.

Os funcionários:

A empresa emprega diretamente cerca de 650 funcionários. Adicionalmente todos os funcionários são orientados sobre as Políticas de Segurança da Informação, as quais estão baseadas na Política Global em segurança, quanto à proteção aos Sistemas de Informação, Hardware e Equipamentos de Telecomunicação.

Todos os funcionários passam pelo treinamento de integração a empresa, que inclui um overview sobre as normas de segurança da empresa que todos tem de seguir. Adicionalmente os funcionários que tem acesso direto aos computadores da empresa passam por um outro treinamento que apresentam as normas de segurança tecnológicas.

Escopo



Processo de compra:

O processo de compra inicia-se a partir da seleção de fornecedores; caso eles ou ele não estiverem cadastrados é necessário acionar a etapa de validação dos testes e amostras dos produtos que serão fornecidos. Tendo esta etapa de cadastro ok, é requisitado a cotação para os fornecedores. Possuindo as cotações será passado para o processo análise e decisão, este consiste em definir quais das cotações será mais viável para empresa levando em conta as necessidades atuais e confirmação da compra. Recebido o XML, é recebido a mercadoria, está é feita a conferência pela equipe de descarregamento, e seguida é dada a entrada dos produtos via sistema e locado no local de armazenagem. Conforme ocorre o andamento de produção levando em conta a perspectiva de vendas, quando o estoque chega perto da margem de requisição de compra da matéria prima é disparado para o setor de compras que repete o ciclo.

- Sistema ERP
- Equipe de Recebimento
- Equipe de Compras
- Processo do negócio
- Sistema telefônico
- Mail de fornecedores
- Infraestrutura
- Mobilidade

Papeis e Responsabilidades da equipe:

Equipe de Compras: Realizam processo de cotação e compra.

Equipe de Descarregamento: Realizam conferência e recepção da mercadoria.

Equipe de Almoxarifado: Realiza processo de organização e controle de estoque.

2ª Etapa – Identificação dos Ativos

ATIVOS	NEGÓCIOS RELACIONADOS	IMPORTÂNCIA DO ATIVO
Sistema ERP	Compras	Alta
Fornecedores	Compras	Alta

Servidor de e-mails	Compras/Recebimento	Médio
Dados de compras	Compras	Alta
Gerente de Compras	Compras	Alta
Compradores	Compras	Médio
Servidor	Todos	Alta
Desktops compras	Compras	Alta
Desktop do gerente de compras	Compras	Alta
Desktops almoxarifado	Almoxarifado	Médio
Serviço de telefonia/internet	Compras/Recebimento	Alta
Serviço de energia	Compras/Recebimento	Alta
Prédios	Todos	Alta
Estrutura de armazenagem estoque	Almoxarifado	Médio
Anotações/rascunhos	Todos	Alta
Pessoal Recebimento	Recebimento	Alta
Pessoal Almoxarifado	Almoxarifado	Alta
Dados ERP	Compras	Alta
Estrutura telefônica interna	Compras	Alta
Estrutura telefônica interna almoxarifado	Todos	Médio
Estrutura elétrica interna	Todos	Alta
Estrutura de rede interna	Compras/Recebimento	Alta
Processo de compra de materiais	Compras	Alta
Processo de cadastro fornecedor	Compras	Alta
Processo de recebimento de mercadoria	Recebimento	Alta
Processo de controle de estoque	Almoxarifado	Alta

3ª Etapa – Identificação de Ameaças

Ativo	**Ameaça**	**Tipo**	**Fonte de Ameaça**
Sistema ERP	Violação das condições de uso do sistema	Falhas Técnicas	Código com falhas de segurança
Sistema ERP	Defeito de software	Falhas Técnicas	Código com falhas de segurança
Servidor de e-mails	Falha no equipamento	Falhas técnicas	Defeito de fábrica ou má manutenção
Servidor de e-mails	Fogo	Dano Físico	Indicio de incêndio
Servidor de e-mails	Uso não autorizado de equipamento	Ações não autorizadas	Pessoa mal intencionada
Dados do servidor de e-mail	Furto de dados	Ação não autorizada	Hacker
Dados do servidor de e-mail	Comprometimento dos dados	Ações não autorizadas	Pessoa mal intencionada
Dados de compras	Furto de dados	Ação não	Hacker

		autorizada	
Gerente de Compras	Indisponibilidade de Recursos Humanos	Falta de recurso	Doença
Compradores	Indisponibilidade de Recursos Humanos	Falta de recurso	Doença
Desktops compras	Falha de equipamento	Falha Técnica	Descarga elétrica
Desktops compras	Furto de equipamento	Ação não autorizada	Pessoa mal intencionada
Servidor(empresa)	Falha no equipamento	Falhas técnicas	Defeito de fábrica ou má manutenção
Servidor(empresa)	Fogo	Dano Físico	Indicio de incêndio
Servidor(empresa)	Uso não autorizado de equipamento	Ações não autorizadas	Pessoa mal intencionada
Desktop do gerente de compras	Falha de equipamento	Falha Técnica	Descarga elétrica
Desktop do gerente de compras	Furto de equipamento	Ação não autorizada	Pessoa mal intencionada
Desktops almoxarifado	Falha de equipamento	Falha Técnica	Descarga elétrica
Desktops almoxarifado	Furto de equipamento	Ação não autorizada	Pessoa mal intencionada
Serviço de telefonia/internet	Interrupção do suprimento de telefonia/internet	Paralisação de serviços essenciais	Acidente
Serviço de energia	Interrupção do suprimento de energia	Paralisação de serviços essenciais	Blackout

4ª Etapa – Identificação dos Controles Existentes

Ativo	**Descrição do controle**	**Situação do**	**Controle**	**Situação da implementaçã o**
Planejado		**Existente**		
Sistema ERP	Contrato de manutenção do software	X		Adequado
Servidor de e-mails	Manutenção periódica	X		Adequado
Servidor de e-mails	Extintor	X		Precisa de Revisão
Dados do servidor de e-mail	Backup de dados	X		Adequado
Dados do servidor de e-mail	Firewall/antivírus	X		Adequado
Dados de compras	Controle de acesso por usuários	X		Adequado
Desktops compras	Controle de acesso por usuários	X		Adequado

Desktops compras	Alarme empresa	X	Adequado
Servidor(empresa)	Extintor	X	Precisa de Revisão
Servidor(empresa)	Controle de acesso por usuários	X	Adequado
Desktop do gerente de compras	Manutenção periódica	X	Adequado
Desktop do gerente de compras	Alarme empresa	X	Adequado
Desktops almoxarifado	Manutenção periódica	X	Adequado
Desktops almoxarifado	Alarme empresa	X	Adequado
Serviço de energia	Gerador	X	
Serviço de telefonia/internet	Contrato de estabilidade	X	
Prédios	Extintor	X	
Estrutura de armazenagem estoque	Extintor	X	Precisa de Revisão

5° - Identificação de Vulnerabilidades

Ativo	**Vulnerabilidade**	**Ameaça**	**Controles**
Sistema ERP	Inexistência de controle eficaz de atualização	Violação das condições de uso do sistema	Contrato de manutenção do software
Sistema ERP	Software Imaturo	Defeito de software	Contrato de manutenção do software
Servidor de e-mails	Inexistência de manutenção periódica	Falha no equipamento	Manutenção Periódica
Servidor de e-mails	Sensibilidade ao fogo	Fogo	Extintor
Servidor de e-mails	Inexistência de controle de acesso eficiente	Uso não autorizado de equipamento	Controle de acesso por usuários
Dados do servidor de e-mail	Inexistência de mecanismos de proteção	Invasão	Firewall/antivírus
Dados do servidor de e-mail	Inexistência de back- up dos dados	Problemas de manipulação	Backup de dados
Dados de compras	Inexistência de mecanismos de proteção	Furto de dados	Controle de acesso por usuários
Gerente de Compras	Treinamento insuficiente	Indisponibilidade de Recursos Humanos	Treinamento pessoa substituta de função
Compradores	Treinamento insuficiente	Indisponibilidade de Recursos Humanos	Treinamento pessoa substituta de função

Desktops compras	Falta de uma rotina de substituição periódica	Falha de equipamento	Manutenção periódica
Desktops compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamento	Alarme empresa
Servidor(empresa)	Falta de uma rotina de substituição periódica	Falha no equipamento	Manutenção periódica
Servidor(empresa)	Material não resistente ao fogo ou falta de proteção contra.	Fogo	Extintor
Servidor(empresa)	Inexistência de controle de acesso eficiente	Uso não autorizado de equipamento	Controle de acesso por usuários
Desktop do gerente de	Falta de uma rotina de	Falha de equipamento	Manutenção periódica

6° - Identificação das consequências

Ativo	**Incidente**	**Consequências**
Sistema ERP	Erro em atualização	Vulnerabilidade do sistema
Servidor de e-mails	Falha no Equipamento	Equipamento Avariado
Servidor de e-mails	Fogo	Servidor avariado
Servidor de e-mails	Acesso indevido	Vulnerabilidade no servidor
Dados do servidor de e-mail	Invasão	Furto de dados
Dados do servidor de e-mail	Perda dos dados	Retrabalho
Dados de compras	Invasão	Furto de dados
Gerente de Compras	Indisponibilidade do RH	Quebra do processo
Compradores	Indisponibilidade do RH	Escassez de mão de obra
Desktops compras	Falha no equipamento	Equipamento Avariado
Desktops compras	Furto do equipamento	Perda de informações
Servidor(empresa)	Falta de uma rotina de substituição periódica	Falha no equipamento
Servidor(empresa)	Material não resistente ao fogo ou falta de proteção contra.	Fogo
Servidor(empresa)	Inexistência de controle de acesso eficiente	Uso não autorizado de equipamento
Desktop do gerente de compras	Falta de uma rotina de substituição periódica	Falha de equipamento
Desktop do gerente de compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamento
Desktops almoxarifado	Falta de uma rotina de	Falha de equipamento

	substituição periódica	
Desktops almoxarifado	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamento
Serviço de telefonia/internet	Sensível a fenômenos meteorológicos ou acidentes.	Interrupção do suprimento de telefonia/internet
Serviço de energia	Sensível a fenômenos meteorológicos ou acidentes.	Interrupção do suprimento de energia
Prédios	Inexistência de mecanismos de proteção	Fogo
Prédios	Inexistência de mecanismos de proteção	Fenômeno Meteorológico
Estrutura de armazenagem estoque	Forte impacto	Acidente Grave
Estrutura de armazenagem estoque	Fogo	Equipamento Avariado
Materiais de Escritório	Recuperação de mídia ou documentos reciclados ou descartados	
Materiais de Escritório	Fogo	Perda de material
Pessoal Recebimento	Treinamento insuficiente	Indisponibilidade de Recursos Humanos

7° - Avaliação das Probabilidades e Consequências (Impactos)

Ativo	**Vulnerabilidade**	**Probabilidade**	**Impacto**
Sistema ERP	Inexistência de controle eficaz de atualização	Média	Média (1B)
Sistema ERP	Software Imaturo	Baixa	Baixa (1C)
Servidor de e-mails	Inexistência de manutenção periódica	Média	Média (2B)
Servidor de e-mails	Sensibilidade ao fogo	Alta	Alta (1A e 2A)
Servidor de e-mails	Inexistência de controle de acesso eficiente	Média	Média (2B)
Dados do servidor de e-mail	Inexistência de mecanismos de proteção	Média	Média (2B)
Dados do servidor de e-mail	Inexistência de back- up dos dados	Baixa	Alta (1A e 2A)
Dados de compras	Inexistência de mecanismos de proteção	Baixa	Alta (2A)
Gerente de Compras	Treinamento insuficiente	Média	Alta (2A)

Compradores	Treinamento insuficiente	Média	Média (2B)
Desktops compras	Falta de uma rotina de substituição periódica	Média	Baixa (1C,2C)
Desktops compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Baixa	Baixa (2C)
Servidor(empresa)	Falta de uma rotina de substituição periódica	Média	Baixa(2C)
Servidor(empresa)	Material não resistente ao fogo ou falta de proteção contra.	Alta	Alta(1A e 2A)
Servidor(empresa)	Inexistência de controle de acesso eficiente	Média	Média(2B)
Desktop do gerente de compras	Falta de uma rotina de substituição periódica	Baixa	Baixa (1C e 2C)
Desktop do gerente de compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Baixa	Baixa (1C e 2C)
Desktops almoxarifado	Falta de uma rotina de substituição periódica	Baixa	Baixa(1C)
Desktops almoxarifado	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Baixa	Baixa (1C e2C)
Serviço de telefonia/internet	Sensível a fenômenos meteorológicos ou acidentes.	Alta	Alta(1A e 2A)
Serviço de energia	Sensível a fenômenos meteorológicos ou acidentes.	Alta	Alta(1A e 2A)
Prédios	Inexistência de	Média	Alta (1A, 3A)

	mecanismos de proteção		

8° - Estimativa de Riscos

Ativo	**Vulnerabilidade**	**Probabilidade**	**Impacto**	**Riscos**
Sistema ERP	Inexistência de controle eficaz de atualização	Média	Média (1B)	4
Sistema ERP	Software Imaturo	Baixa	Baixa (1C)	2
Servidor de e-mails	Inexistência de manutenção periódica	Média	Média (2B)	4
Servidor de e-mails	Sensibilidade ao fogo	Alta	Alta (1A e 2A)	6
Servidor de e-mails	Inexistência de controle de acesso eficiente	Média	Média (2B)	4
Dados do servidor de e-mail	Inexistência de mecanismos de proteção	Média	Média (2B)	4
Dados do servidor de e-mail	Inexistência de backup dos dados	Baixa	Alta (1A e 2A)	4
Dados de compras	Inexistência de mecanismos de proteção	Baixa	Alta (2A)	4
Gerente de Compras	Treinamento insuficiente	Média	Alta (2A)	5
Compradores	Treinamento insuficiente	Média	Média (2B)	4
Desktops compras	Falta de uma rotina de substituição periódica	Média	Baixa (1C,2C)	3
Desktops compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Baixa	Baixa (2C)	2
Servidor(empresa)	Falta de uma rotina de substituição periódica	Média	Baixa(2C)	3
Servidor(empresa)	Material não resistente ao	Alta	Alta(1A e 2A)	6

	fogo ou falta de proteção contra.			
Servidor(empresa)	Inexistência de controle de acesso eficiente	Média	Média(2B)	4
Desktop do gerente de compras	Falta de uma rotina de substituição periódica	Baixa	Baixa (1C e 2C)	2
Desktop do gerente de compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Baixa	Baixa (1C e 2C)	2
Desktops almoxarifado	Falta de uma rotina de substituição periódica	Baixa	Baixa(1C)	2
Desktops almoxarifado	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Baixa	Baixa (1C e2C)	2
Serviço de telefonia/internet	Sensível a fenômenos meteorológicos ou acidentes.	Alta	Alta(1A e 2A)	6
Serviço de energia	Sensível a fenômenos	Alta	Alta(1A e 2A)	6

9° - Escolha do tipo de tratamento a ser realizado

Ativo	**Vulnerabilidade**	**Tipo de tratamento para o risco**
Sistema ERP	Inexistência de controle eficaz de atualização	Tratar
Sistema ERP	Software Imaturo	Retenção
Servidor de e-mails	Inexistência de manutenção periódica	Tratar
Servidor de e-mails	Sensibilidade ao fogo	Tratar
Servidor de e-mails	Inexistência de controle de acesso eficiente	Tratar
Dados do servidor de e-mail	Inexistência de mecanismos de proteção	Tratar
Dados do servidor de e-mail	Inexistência de backup dos dados	Tratar

Dados de compras	Inexistência de mecanismos de proteção	Retenção
Gerente de Compras	Treinamento insuficiente	Tratar
Compradores	Treinamento insuficiente	Tratar
Desktops compras	Falta de uma rotina de substituição periódica	Tratar
Desktops compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Retenção
Servidor(empresa)	Falta de uma rotina de substituição periódica	Tratar
Servidor(empresa)	Material não resistente ao fogo ou falta de proteção contra.	Retenção
Servidor(empresa)	Inexistência de controle de acesso eficiente	Tratar
Desktop do gerente de compras	Falta de uma rotina de substituição periódica	Tratar
Desktop do gerente de compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Retenção
Desktops almoxarifado	Falta de uma rotina de substituição periódica	Retenção
Desktops almoxarifado	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Retenção
Serviço de telefonia/internet	Sensível a fenômenos meteorológicos ou acidentes.	Retenção
Serviço de energia	Sensível a fenômenos meteorológicos ou acidentes.	Tratar

10° - Recomendação de Controles

Ativo	**Vulnerabilidade**	**Controles recomendados**
Sistema ERP	Inexistência de controle eficaz de atualização	Implementação de rotinas de backup
Sistema ERP	Software Imaturo	Aplicação de testes pré-instalação
Servidor de e-mails	Inexistência de manutenção periódica	Implementação de rotinas de backup / Instalar servidor espelho
Servidor de e-mails	Sensibilidade ao fogo	Detectores de fumaça / Mecanismo de retirada do oxigênio da sala / Utilização de gases

		inibidores de combustão
Servidor de e-mails	Inexistência de controle de acesso eficiente	Política de controle de acesso
Dados do servidor de e-mail	Inexistência de mecanismos de proteção	Implementação de rotinas de backup/ Implantação de manutenção preventiva e corretiva periódica
Dados do servidor de e-mail	Inexistência de backup dos dados	Implementação de rotinas de backup
Dados de compras	Inexistência de mecanismos de proteção	Implementação de rotinas de backup / Implantação de manutenção preventiva e corretiva periódica
Gerente de Compras	Treinamento insuficiente	Treinamento
Compradores	Treinamento insuficiente	Treinamento
Desktops compras	Falta de uma rotina de substituição periódica	Implantação de manutenção preventiva e corretiva periódica
Desktops compras	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Implementação de rotinas de backup
Servidor(empresa)	Falta de uma rotina de substituição periódica	Implantação de manutenção preventiva e corretiva periódica
Servidor(empresa)	Material não resistente ao fogo ou falta de proteção contra.	Detectores de fumaça / Mecanismo de retirada do oxigênio da sala / Utilização de gases inibidores de combustão
Servidor(empresa)	Inexistência de controle de acesso eficiente	Política de controle de acesso
Desktop do gerente de compras	Falta de uma rotina de substituição periódica	Implantação de manutenção preventiva e corretiva periódica
Desktop do gerente de compras	Inexistência de mecanismos de proteção física no prédio, portas e	Implementação de rotinas de backup