PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO UTILIZANDO ISO 27005 E VULNERABILIDADES

VITOR BITTENCOURT GABRIEL

GOIÂNIA
2021

VITOR BITTENCOURT GABRIEL

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO UTILIZANDO ISO 27005 E VULNERABILIDADES

Trabalho de Conclusão de Curso apresentado à Escola Politécnica, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.

Orientadora:

Profa. Dra. Solange Da Silva

GOIÂNIA

2021

VITOR BITTENCOURT GABRIEL

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO UTILIZANDO ISO 27005 E VULNERABILIDADES

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Ciência da Computação, e aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, em 02/12/2021.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca Examinadora:

_____

Orientadora: Profa. Dra. Solange Da Silva

_____

Prof. Me. Rafael Leal Martins

_____

Prof. Me. Gustavo Siqueira Vinhal

GOIÂNIA

2021

RESUMO

O objetivo geral deste TCC foi o de apresentar estudos de caso de empresas que aplicaram a norma ISO 27005 em um sistema de SGSI e realizar uma análise das vulnerabilidades, seguindo uma das ferramentas disponíveis (no caso, foi usado o *Wireshark*). Em relação aos procedimentos metodológicos, esta pesquisa, segundo a natureza, é um resumo de assunto e quanto aos seus objetivos, é exploratória. Quanto aos procedimentos técnicos é uma pesquisa bibliográfica, documental e experimental. Nos estudos realizados foi observado que as empresas estão protegendo suas informações usando: combinação das técnicas ISSO 27005 com a NIST SP 800-30 revisão 1. Assim, geram uma escala de probabilidade geral e avaliação dos riscos que, por fim, com auxílio de uma ferramenta de identificação de riscos, cria, a partir daquela combinação, uma tabela de avaliação e os métodos de resolução dos riscos encontrados. Algumas empresas não têm colocado em prioridade o SGSI em suas rotinas, deixando em risco o seu sistema e empresa como um todo. Os estudos realizados permitiram concluir que a norma ISO 27005 não é um padrão imposto, mas sim uma recomendação de boas práticas. Ela ajuda a proteger as informações da empresa ou organização que a aplica em suas políticas de segurança. Além disso, com a implementação realizada com o *Wireshark*, pode-se verificar o uso das ferramentas de vulnerabilidades para diagnosticar problemas e avaliar desempenho, possibilitando a tomada de medidas apropriadas.

Palavras-chave: ISO 27005. Sistema de Gestão de Segurança da Informação. Vulnerabilidades. Segurança de Dados. Gestão de Riscos.

ABSTRACT

This TCC's overall objective was to present case studies of companies that have applied an ISO 27005 standard to an SGSI system and perform a vulnerability analysis following one of the available tools (in this case, used Wireshark). Regarding the methodological procedures, this research according to its nature is a summary of the subject, as for the objectives, it is exploratory. As for the technical procedures, it is a bibliographical, documental, and experimental research. The studies carried out showed that companies are protecting their information using: combination of ISO 27005 techniques with a NIST SP 800-30 revision 1. Thus, they generate a general probability scale and risk assessment that, finally, with the help of a risk identification tool, creation, from combination risks, an assessment table, and methods of solving the risks found. Some companies didn't prioritize the SGSI in their routines, putting their system and company at risk. The studies carried out make it possible to fulfill that the ISO 27005 norm is not a standard, but a recommendation of good practices. It helps protect the information of the company or organization that enforces its security policies. Furthermore, with the implementation carried out with Wireshark, the use of vulnerability tools to diagnose problems and assess performance can be verified, enabling the taking of appropriate measures.

Keywords: ISO 27005. Information Security Management System. Vulnerability. Data Security. Risk management.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE MATRIZES

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APT	*Advanced Persistent Threat*
GCF	*Greenbone Community Feed*
GSF	*Greenbone Security Feed*
IDS	*Intrusion Detection System* ou Sistema de Detecção de Intrusão
IEC	*International Electrotechnical Commission* ou Comissão Eletrotécnica Internacional
ISO	*International Organization for Standardization* ou Organização Internacional de Normalização
ISRM	*Information Security Risk Management* ou Gestão de Riscos de Segurança da Informação.
NBR	Norma Brasileira
NIST	*National Institute of Standards and Technology* ou Instituto Nacional de Padrões e Tecnologia
NVT	*Network Vulnerability Tests* ou Testes de Vulnerabilidade de Rede ou
SGSI	Sistema de Gestão de Segurança da Informação ou *Information Security Management System*
SITP	Sistema Integrado de Transporte Público
SP	*Special Publication* ou Publicação Especial
TCC	Trabalho de Conclusão de Curso
WEB	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Os dados são considerados como patrimônio de grande valor para a empresa e que através de suas características e qualidades se define em uma informação segura, de modo que ao gerar informações devemos fazer com que os dados tenham todos os requisitos relacionados e definidos como fundamentais para eles (CHINELATO, 2008).

Dados são observações documentadas ou resultados da medição, a disponibilidade dos dados oferece oportunidades para a obtenção de informações, obtendo-os pela percepção através dos sentidos (por exemplo, observação) ou pela execução de um processo de medição (UNICAMP, 2021).

Conforme o art. 4°, inciso I, da Lei nº 12.527/2011, informações são dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, registrados em qualquer suporte ou formato.

A classificação da informação se dá de acordo com os negócios da empresa, quanto mais importante a informação, mais medida de segurança será necessário para a sua proteção. Cada empresa classifica sua informação de acordo com seus negócios, deverá ser revista, avaliadas ou atualizadas as informações, mantendo em seu banco de dados somente as necessárias e eliminando o que está em excesso (CHINELATO, 2008).

A análise de ameaças mostra como explorar a fraqueza do sistema para atingir seus objetivos. Identifica ameaças e define uma política de mitigação de risco para uma arquitetura, funcionalidade e configuração (STANGO, 2009).

> Vulnerabilidades são pontos fracos em um sistema ou em seu design que permitem a um intruso para executar comandos, acessar dados não autorizados e / ou conduzir ataques de negação de serviço. Vulnerabilidades podem ser encontradas em várias áreas, eles podem ser pontos fracos no hardware do sistema ou software, deficiências nas políticas e procedimentos usados nos sistemas e fraquezas dos próprios usuários do sistema (ABOMHARA, 2015).

As etapas da análise de vulnerabilidade são: avaliação de risco, avaliação de vulnerabilidades e tratamento do risco.

O risco é a união da chance de um evento indesejado ocorrer e suas consequências para a organização e na segurança da informação, este risco ocorre nas tecnologias envolvidas, nos processos em execução e nas pessoas que interagem com eles. Os riscos de segurança da informação são a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, assim prejudicando a organização (BEZERRA, 2013).

As atividades de gestão de riscos identificam as informações necessárias para a identificação de riscos e processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência (ABNT NBR ISO/IEC 27005, 2019).

De acordo com Bezerra (2013), a norma da Associação Brasileira de Normas Técnicas (ABNT) Norma Brasileira (NBR) Organização Internacional para Padronização (ISO)/ Comissão Eletrotécnica Internacional (IEC) 27005 apresenta um sistema de gestão de riscos de segurança da informação com foco em tecnologia da informação, ela esclarece como gerenciar riscos de segurança da informação. É a entrada para todas as informações sobre a organização relevantes para a definição do contexto da gestão de riscos de segurança da informação (ABNT NBR ISO/IEC 27005, 2019).

Esta norma descreve todo o processo necessário para o Sistema de Gestão de Segurança da Informação (SGSI) e as atividades necessárias para a perfeita execução da gestão, também apresenta práticas para gestão de riscos da segurança da informação, as técnicas nela descritas seguem o conceito, os modelos e os processos globais especificados na norma ABNT NBR ISO/IEC 27001, além de apresentar a metodologia de avaliação e tratamento dos riscos requeridos pela mesma norma (BEZERRA, 2013).

As ferramentas pesquisadas, que podem ser usadas para os controles propostos pela norma 27005 são: *Scanner* de vulnerabilidade *OpenVAS; Nexpose Community; Nessus Vulnerability Scanner; Vulnerability Manager Plus e Wireshark.*

É relevante estudar este tema, pois na área de segurança da informação possui diversas técnicas para implementar suas normas, porém no Brasil não existe um padrão para as aplicações. É importante apresentar estudos de caso para divulgar o uso na norma ISO 27005 nas empresas no Brasil e no mundo. Os Documentos Técnicos ABNT, assim como as Normas Internacionais (ISO e IEC), são voluntários e não incluem requisitos contratuais, legais ou estatutários (ABNT NBR ISO/IEC 27005, 2019). Além disso, a questão da pandemia do Covid-19 causou uma demanda maior, pois os contatos físicos tornaram-se virtuais. Isso implica em maior segurança dos dados.

Diante deste contexto, este trabalho de conclusão de curso visa responder a seguinte questão de pesquisa: **- Como as empresas estão protegendo suas informações em relação a ISO 27005 no SGSI (estudos de casos) e como utilizar uma ferramenta de análise de vulnerabilidades?**

O objetivo geral deste trabalho é apresentar estudos de casos de empresas que aplicaram a norma ISO 27005 em um sistema de SGSI e realizar uma análise das vulnerabilidades seguindo uma das ferramentas disponíveis.

Os objetivos específicos são:

- Estudar a norma ISO 27005.
- Mapear os estudos de casos do Brasil e do mundo.
- Mapear as ferramentas para identificar as vulnerabilidades de uma empresa.
- Realizar uma análise de vulnerabilidades usando algumas das ferramentas existentes.

Em relação aos procedimentos metodológicos, esta pesquisa segundo a natureza é resumo de assunto, quanto aos objetivos é exploratória. Quanto aos procedimentos técnicos é uma pesquisa bibliográfica, documental e experimental.

Espera-se que os resultados obtidos neste trabalho possam contribuir:

- Mostrando a importância de aplicar um SGSI para proteção de dados.
- Apresentando o resultado de algumas empresas que estão aplicado a norma 27005 no SGSI.
- Divulgando a norma 27005 e a importância de usá-la.
- Apresentando algumas das ferramentas de análise de vulnerabilidades.
- Mostrando alguma implementação das ferramentas de análise de vulnerabilidades.

Esta monografia está estruturada da seguinte maneira:

Neste Capítulo é apresentada a introdução com o contexto do trabalho, a questão de pesquisa, objetivos e resultados esperados. O Capítulo 2 traz o referencial teórico com conceitos e definições e trabalhos relacionados com o tema. No Capítulo 3 estão descritos os procedimentos metodológicos para atingir o objetivo geral. O Capítulo 4 contém os estudos de casos de empresas que utilizaram políticas de segurança, usando a ISO 27005, seus resultados e análise dos resultados obtidos. O Capítulo 5 traz a análise e implementação da ferramenta *Wireshark*, que foi escolhida para uma implementação para monitorar a segurança de uma rede. O Capítulo 6 traz as análises dos resultados obtidos ao longo da pesquisa. Por fim, o Capítulo 7 apresenta a conclusão e sugestões de trabalhos futuros.

2 REFERENCIAL TEÓRICO

2.1 CONCEITOS E DEFINIÇÕES

Este capítulo traz uma introdução sobre a Norma ISO 27005 em relação as suas atividades de gestão de risco, sobre vulnerabilidade, análise de vulnerabilidade e as ferramentas utilizadas nesse estudo para implementação.

2.2 NORMA ISO 27005

A ISO 27005 é um padrão conhecido de SGSI, as tarefas da ISO 27005 incluem a identificação, avaliação e priorização de riscos (ABNT NBR ISO/IEC 27005, 2019).

Uma organização cria, coleta e processa uma quantidade significativa de informação em diversos formatos durante o prazo de gerenciamento de segurança, o SGSI deve ser um processo recorrente composto por fases que, quando implementado apropriadamente, permite a melhoria contínua nas tomadas de decisões e desempenho (AGRAWAL, 2017).

Na fase de implementação, ISO 27005 pode ser combinada com outras normas ou diretrizes para atender os requisitos organizacionais em relação ao SGSI (FIKRI, 2019).

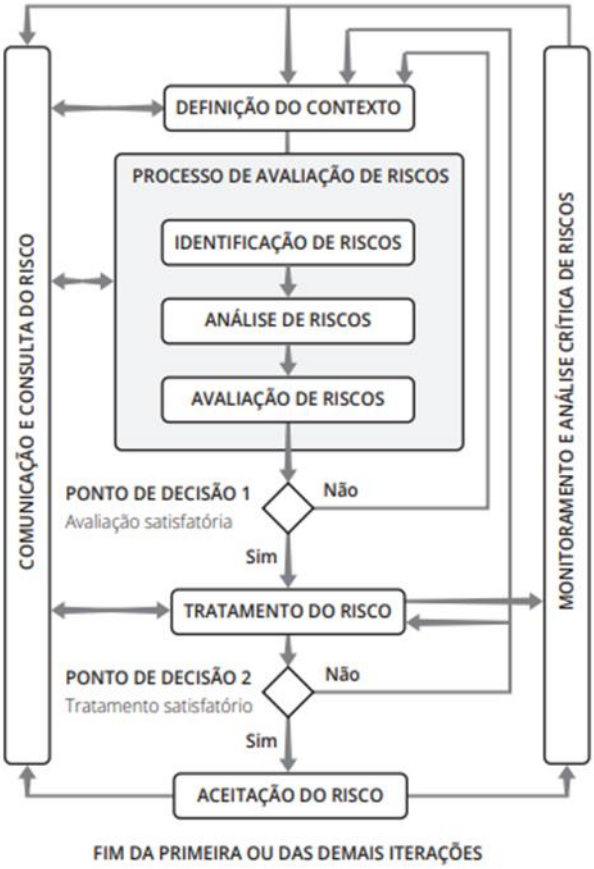
Conforme a ABNT NBR ISO/IEC 27005, 2019 as atividades de gestão de riscos de segurança da informação são descritas nas seguintes seções:

— Definição do contexto,
— Processo de avaliação de riscos,
— Tratamento do risco,
— Aceitação do risco,
— Comunicação e consulta do risco,
— Monitoramento e análise crítica de riscos.

As atividades de gestão de riscos identificam as informações necessárias para a identificação de riscos e processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência (ABNT NBR ISO/IEC 27005, 2019).

A Figura 1 mostra o processo iterativo de avaliação de risco e/ou atividades de tratamento de risco do padrão.

Figura 1 - Processo de gestão de riscos de segurança da informação



Fonte: ABNT NBR ISO/IEC 27005, 2019.

De acordo com a Figura 1, o contexto estabelecido é avaliado primeiro e, em seguida, é realizada a avaliação de risco.

Uma visão iterativa na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição, minimizando o tempo e o esforço na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possa ser adequadamente avaliados (ABNT NBR ISO/IEC 27005, 2019).

Se informações suficientes forem fornecidas para determinar as ações necessárias para modificar os riscos a um nível aceitável, o tratamento do risco é finalmente seguido. Se as informações não forem suficientes, outra iteração é realizada com um contexto revisado. A atividade de aceitação de risco deve assegurar que os riscos residuais sejam explicitamente aprovados pelos diretores da organização (YOO, 2018).

O tratamento do risco envolve um processo cíclico para avaliar um tratamento do risco, decidir se os níveis de risco residual são aceitáveis, gerar um novo tratamento do risco

se os níveis de risco não forem aceitáveis e avaliar a eficácia do tratamento (ABNT NBR ISO/IEC 27005, 2019).

Conforme a ABNT NBR ISO/IEC 27005:2019 o processo de avaliação de riscos descreve o risco qualitativamente e capacita os gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos. O processo de avaliação de riscos consiste nas seguintes atividades:

— Identificação de riscos,

— Análise de riscos,

— Avaliação de riscos.

Também de acordo com ABNT NBR ISO/IEC 27005:2019, a identificação de riscos determina o que pode causar uma perda potencial e mostrar como, onde e por que a perda pode acontecer. Também inclui os riscos, cujas fontes estejam ou não sob controle da organização, mesmo que a origem ou a causa dos riscos não seja evidente.

Um ativo, identificado como: (A1, A2, ..., An), é algo que possui valor para a organização e que requer proteção. A identificação dos ativos deve ser feita com detalhamento, apresentando informações necessárias para o processo de avaliação de riscos (ABNT NBR ISO/IEC 27005, 2019).

Uma ameaça, identificada como: (T1, T2, ..., Tn), tem o potencial de comprometer ativos. As ameaças podem ser de origem natural ou humana, ser acidentais ou intencionais. São identificadas como: genéricas, específicas e por classe (ABNT NBR ISO/IEC 27005, 2019).

2.3 VULNERABILIDADE E RISCO

A vulnerabilidade são falhas no sistema ou design que concede ao intruso acesso não autorizados para conduzir ataques ao serviço. Podem ser encontradas, tanto nas áreas do *hardware* ou *software* do sistema, procedimentos usados e pelos próprios usuários (ABOMHARA, 2015).

A análise de vulnerabilidade é um processo de identificação, documentação e redução das ameaças de segurança, propondo uma nova abordagem na caracterização do sistema. Mostra como podem explorar a fraqueza do sistema para atingir seus objetivos (STANGO, 2009).

Setiawan, Pradana e Putra (2017) dizem que o risco é uma combinação da ocorrência de um evento inesperado com a possibilidade do evento. O gerenciamento de risco é um

processo de identificação, estimativa e identificação de etapas para reduzir o risco em um nível aceitável.

De acordo com Fikri et al (2019) um dos focos do gerenciamento de risco atual é o gerenciamento de risco para segurança da informação, sendo a ISO 27005 um padrão utilizado na implementação gestão de riscos de segurança da informação ou *Information Security Risk Management* (ISRM).

A ISRM deve ser um processo contínuo e recorrente, composto por fases que, quando implementadas corretamente, oferecem a melhoria na tomada de decisões e no desempenho (AGRAWAL, 2017).

Na implementação do processo de gestão de riscos utiliza-se referências e padrões para a sustentabilidade de seus processos. O mais importante na resolução das dificuldades em relação ao risco está na atenção da construção, melhoria e gerenciamento do nível de confiança antes, durante e após a ocorrência de um incidente (FIKRI, 2019).

A ISO 27005 envolve informações relacionadas à organização, sendo a criação, coleta e processamento de informações durante a atividade de gerenciamento de riscos de segurança da informação (AGRAWAL, 2017).

2.4 FERRAMENTAS

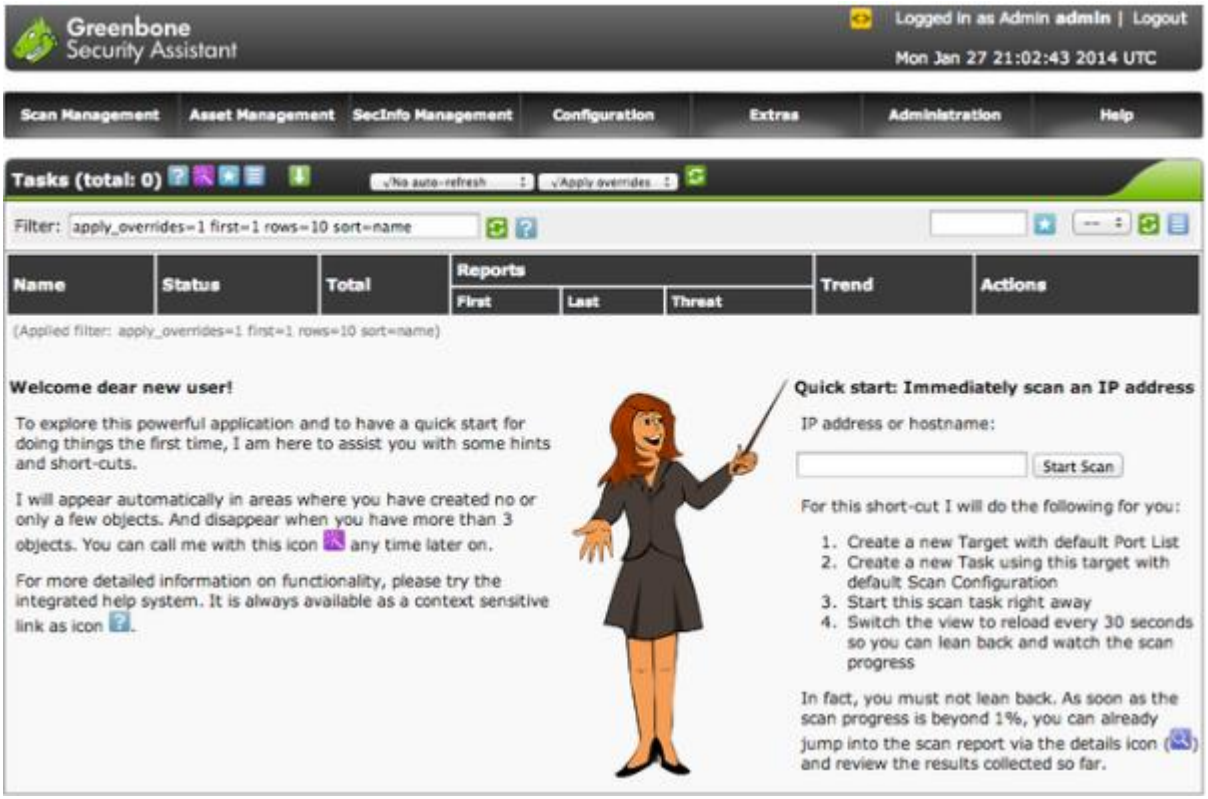
Esta seção trata-se das ferramentas *Scanner* de vulnerabilidade *OpenVAS*, *Nexpose Community*, *Nessus Vulnerability Scanner*, *Vulnerability Manager Plus* e *Wiresha*rk.

2.4.1 *Scanner* de vulnerabilidade *OpenVAS*

O OpenVAS foi desenvolvido pela empresa alemã *Greenbone Networks,* em 2006, com sua sede em Osnabruque. É um *framework* baseado em serviços e ferramentas para avaliação de vulnerabilidades. Sendo um *scanner* de vulnerabilidade seus recursos incluem testes não autenticados e autenticados, protocolos industriais e de Internet de alto e baixo nível, ajuste de desempenho para varreduras em grande escala e uma poderosa linguagem de programação interna para implementar qualquer tipo de teste de vulnerabilidade. O objetivo é aprender como seus servidores são protegidos contra vetores de ataque conhecidos (OPENVAS, 2021).

O *scanner* obtém os testes de detecção de vulnerabilidades de um *feed* que tem um longo histórico e atualizações diárias. O *scanner* principal *OpenVAS Scanner* é um mecanismo de varredura completo que executa testes de vulnerabilidade ou *Vulnerability Tests* (VT) contra sistemas de destino, mostrado na Figura 2.

Figura 2 – Tela Inicial *OpenVAS*



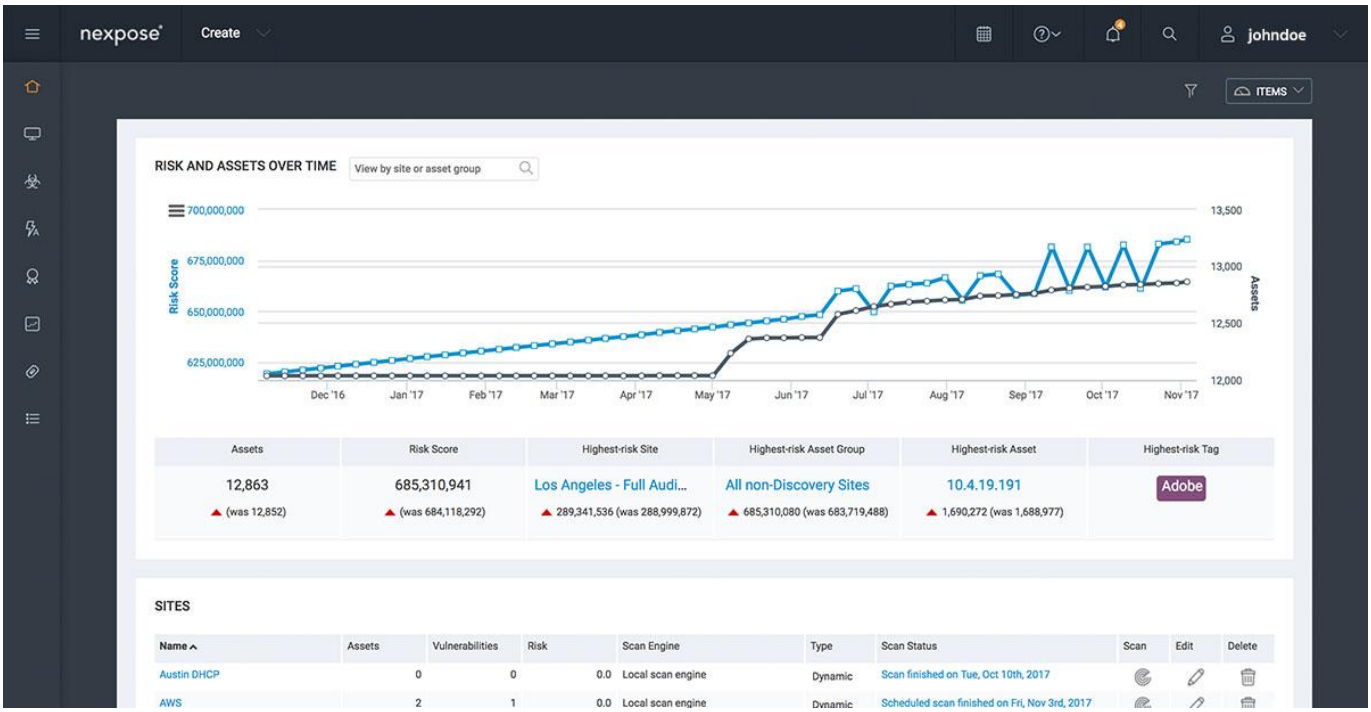
Fonte: Silva, 2021.

Ele usa *feeds* abrangentes e atualizados diariamente: o *Greenbone Security Feed* (GSF) comercial completo e extenso ou o *Greenbone Community Feed* (GCF), disponível gratuitamente (GREENBONE, 2021).

2.4.2 *Nexpose Community*

O Nexpose, ilustrado na Figura 3, foi desenvolvido pela empresa estadunidense *Rapid7*, em 2016, com sua sede em Boston. É uma solução de gerenciamento de vulnerabilidade local, que ajuda a reduzir exposição a ameaças. Permite que avalie e responda às mudanças em seu ambiente em tempo real e priorizando riscos em vulnerabilidades, configurações e controles. Com o avanço e aumento das violações de dados, sua superfície de ataque muda constantemente (NEXPOSE, 2021).

Figura 3 – Tela Inicial *Nexpose Community*



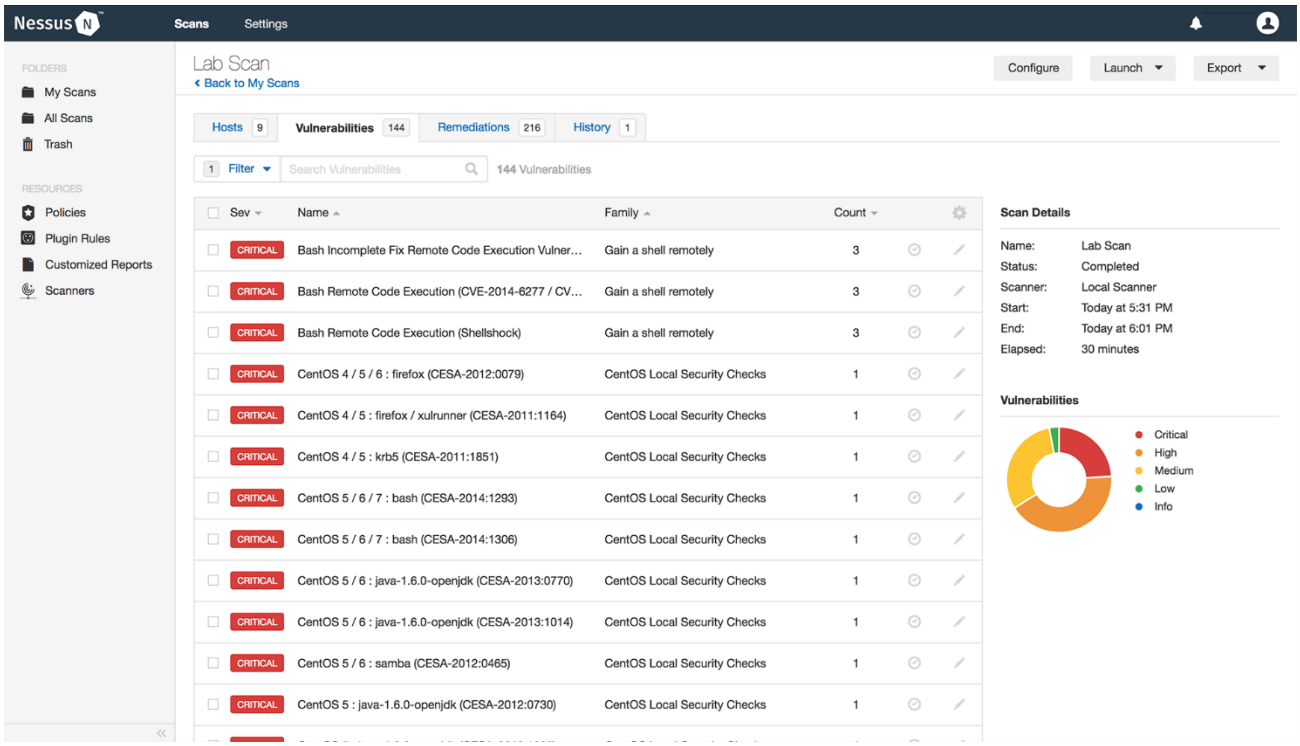
Fonte: Rapid7, 2021.

A *Nexpose* auxilia o usuário a entender a superfície de ataque da empresa, focar no que importante e criar melhores resultados de segurança. Identifica os serviços ativos da empresa, portas abertas e aplicativos em execução em cada máquina e tenta encontrar vulnerabilidades que podem existir com base nos atributos dos serviços e aplicativos conhecidos (RAPID7, 2021).

2.4.3 *Nessus Vulnerability Scanner*

O aplicativo *Nessus*, ilustrado na Figura 4, foi desenvolvido pelo americano Renaud Deraison, em 1998. Em seguida, criou o *Tenable Network Security*, em 2002, com sua sede em Columbia, para comercializá-lo. É uma ferramenta de verificação de segurança remota, que verifica um computador e emite um alerta se descobrir alguma vulnerabilidade que pode usar para obter acesso a qualquer computador conectado à rede. Ele executa mais de 1200 verificações, testando se algum desses ataques poderia ser usado para invadir o computador ou danificá-lo (TENABLE, 2021).

Figura 4 – Tela Inicial *Nessus Vulnerability Scanner*



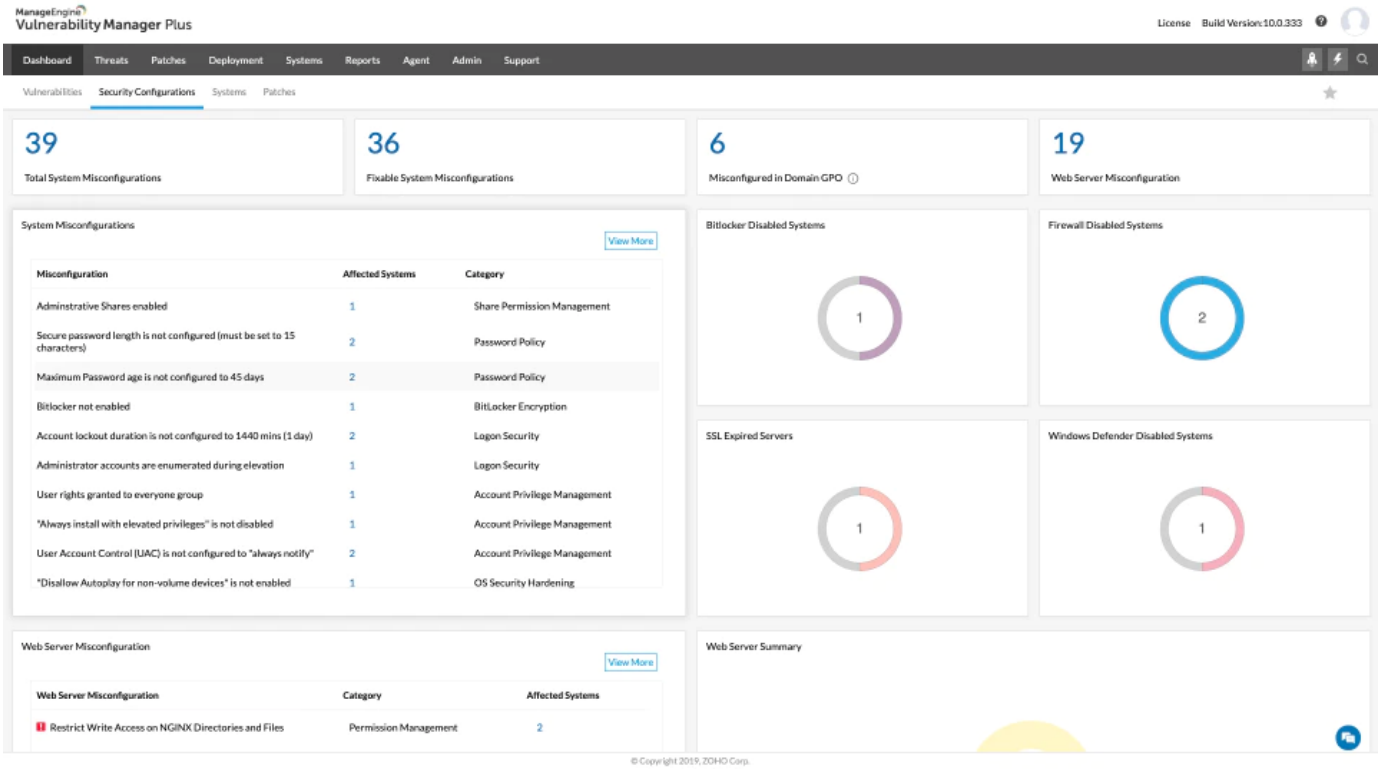
Fonte: Tenable, 2021.

Essa ferramenta testa cada porta de um computador, determinando qual serviço está sendo executado. Em seguida verifica o serviço para garantir que não haja vulnerabilidades que possam ser usadas em um ataque malicioso. É chamado de "*scanner* remoto" porque não precisa ser instalado em um computador para testar esse computador. Ao invés disso, pode ser instalado em apenas um computador e testar em quantos computadores for necessário (WENDLANDT, 2021).

2.4.4 *Vulnerability Manager Plus*

O *Vulnerability Manager Plus*, mostrado na Figura 5, foi desenvolvido pela empresa multinacional indiana *ManageEngine*, uma divisão da ZOHO *Corporation*, fundada em 1996, com sua sede em Chennai. É um software integrado de gerenciamento de ameaças e vulnerabilidades, que oferece recursos abrangentes de varredura, avaliação e correção de vulnerabilidades em todos os terminais de uma rede, a partir de um console centralizado (ACSOFTWARE, 2021).

Figura 5 – Tela Inicial *Vulnerability Manager Plus*



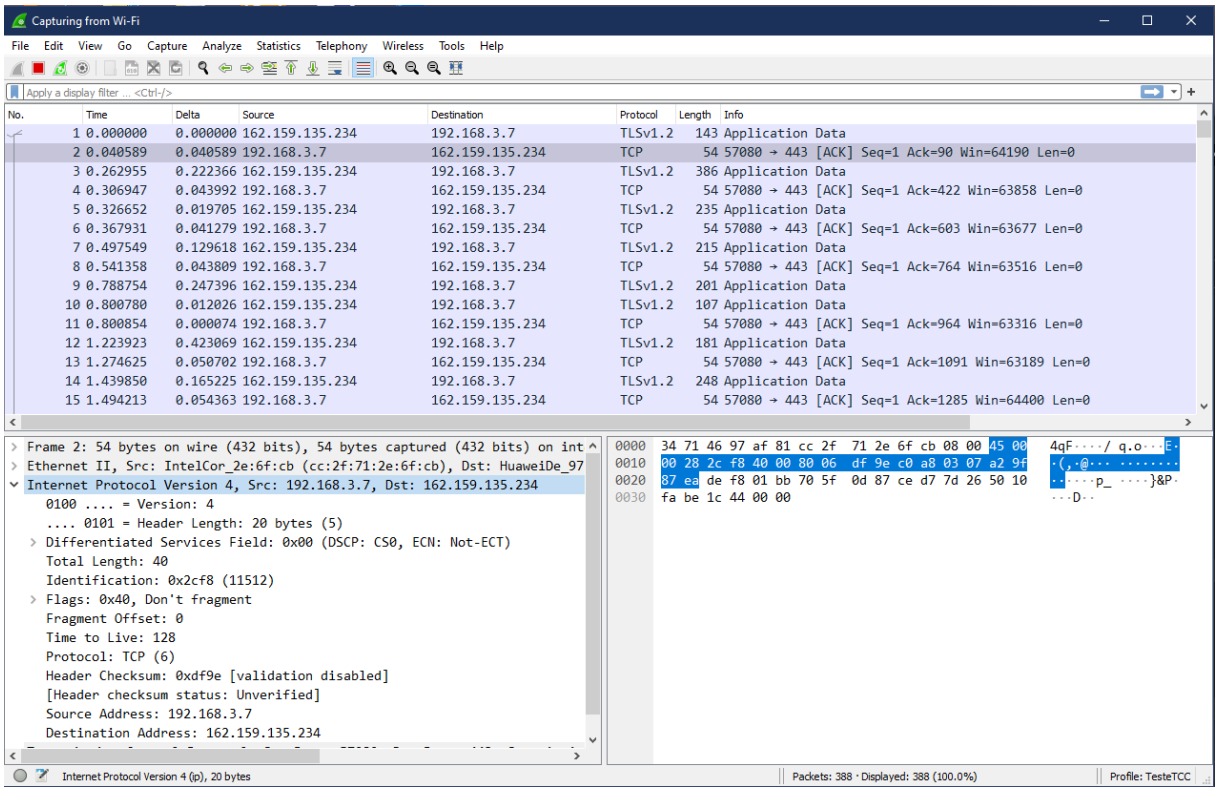
Fonte: ManageEngine, 2021.

Funciona em uma arquitetura cliente-servidor. O servidor, que está localizado no local do cliente tem um banco de dados integral. Este é mantido atualizado com as últimas varreduras e informações de correção por meio da sincronização periódica com o banco de dados de vulnerabilidade central, localizado no site da empresa ZOHO *Corporation*. O console da Rede mundial de computadores ou *World Wide Web* (WEB) é o centro do gerenciamento de vulnerabilidades. Ele permite que se monitore a conduta de segurança de uma empresa e execute todas as tarefas em qualquer lugar, a qualquer hora (MANAGEENGINE, 2021).

2.4.5 *Wireshark*

O desenvolvimento do *Wireshark*, ilustrado na Figura 6, é a continuação de um projeto iniciado pelo estadunidense Gerald Combs, em 1998, seu desenvolvimento avança devido às contribuições voluntárias de especialistas em rede ao redor do mundo, pois é *Open Source*. O *Wireshark* é um analisador de protocolo de rede local, que captura e analisa o tráfego de rede e o organiza por protocolos. Auxilia no monitoramento, para que seja verificado o que está acontecendo na rede. É a ferramenta padrão usada em muitas empresas comerciais e sem fins lucrativos, agências governamentais e instituições educacionais (WIRESHARK, 2021).

Figura 6 - Tela Inicial *Wireshark*



Fonte: Autoria própria.

Para Petters (2020), o *Wireshark* possui um rico conjunto de recursos que captura o tráfego da rede local e armazena esses dados para análise *offline*. Também captura o tráfego de rede de Ethernet, Bluetooth, *Wireless* (IEEE. 802.11), *Token Ring*, conexões *Frame Relay* dentre outros. Permite que seja filtrado o log antes do início da captura ou durante a análise do tráfego, para que se possa restringir e zerar o que está procurando no rastreamento da rede.

Os filtros do *Wireshark* são um dos principais motivos pelos quais ele se tornou a ferramenta padrão para análise de pacotes porque eles permitem a visualização da captura, do modo que o usuário preferir, para resolver os problemas em estudo (SHARPE, 2021).

3 PROCEDIMENTOS METODOLOGICOS

Este capítulo traz os procedimentos metodológicos usados para atingir o objetivo geral.

Quanto à natureza esta pesquisa se trata de um resumo de assunto, usado para sistematizar uma área de conhecimento, indicando sua evolução histórica e estado, pois explica a área de estudo do projeto, tratando de estudos de caso sobre o uso da ISO 27005 nas empresas (WAZLAWICK, 2014).

Quanto ao objetivo esta pesquisa é exploratória, aquela em que o autor não tem necessariamente uma hipótese ou objetivo definido em mente. As pesquisas exploratórias têm como propósito proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses (GIL, 2017).

Na pesquisa exploratória, examina-se um conjunto de fenômenos, buscando anomalias que não sejam ainda conhecidas e que possam ser a base para uma pesquisa mais elaborada uma vez que tem como finalidade desenvolver, esclarecer, modificar ideias e conceitos para estudos posteriores (WAZLAWICK, 2014).

Quantos aos procedimentos técnicos é uma pesquisa bibliográfica e documental, para a coleta de dados, com a utilização de livros, artigos, jornais e similares (GIL, 2017). Além disso, também é uma pesquisa experimental.

A pesquisa documental, por outro lado, consiste na análise de documentos ou dados que não foram ainda sistematizados e publicados, ou seja, a pesquisa documental busca encontrar informações e padrões em documentos ainda não tratados sistematicamente (WAZLAWICK, 2014).

A pesquisa bibliográfica resulta no estudo de artigos, teses, livros e outras publicações disponibilizadas por editoras e indexadas, mas não produz conhecimento novo, apenas propõe ao pesquisador informações que ele ainda não possuía (GIL, 2017). Para Wazlawick (2014) os passos utilizados para a pesquisa bibliográfica são:

i. Listar os títulos de periódicos e eventos relevantes para o tema de pesquisa e os títulos de periódicos gerais em computação que eventualmente possam ter algum artigo na área do tema de pesquisa.
ii. Obter a lista e todos os artigos publicados nos últimos cinco anos (ou mais) nesses veículos. O material foi buscado na plataforma de periódicos da CAPES, na plataforma *Z-Library* (z-lib.org) e sites autorais.
iii. Selecionar dessa lista aqueles títulos que tenham relação com o tema de pesquisa.

iv. Ler o abstract desses artigos e, em função da leitura, classificá-los como relevância “alta”, “média” ou “baixa”.

v. Ler os artigos de alta relevância e fazer fichas de leitura anotando os principais conceitos e ideias aprendidos. Anotar também títulos de outros artigos possivelmente mencionados na bibliografia de cada artigo (mesmo que com mais de cinco anos) e que pareçam relevantes para o trabalho de pesquisa. Incluir esses artigos na lista dos que devem ser lidos (inicialmente o abstract e, se for relevante, o artigo todo).

vi. Dependendo do caso, ler também os artigos de relevância média e baixa, mas iniciando sempre pelos de alta relevância. Listar os títulos de periódicos e eventos relevantes para o tema de pesquisa nos últimos cinco anos nesses veículos.

Os passos acima foram seguidos para realizar a revisão bibliográfica, para realizar o estudo de casos e adquirir os demais conhecimentos escritos nos capítulos desta monografia.

Uma pesquisa experimental depende de um objeto de estudo, variáveis que podem manipulá-lo, formas de controle das variáveis e formas de observação dos efeitos que as variáveis produzem no objeto (GIL,2017).

A pesquisa experimental caracteriza-se pela manipulação de um aspecto da realidade pelo pesquisador. Implica que o pesquisador sistematicamente provocará alterações no ambiente a ser pesquisado, de forma a observar se cada intervenção produz os resultados esperados (WAZLAWICK, 2014).

Para Gil (2017) os passos utilizados para a pesquisa experimental são:

i. Formulação do problema**; Como as empresas estão protegendo suas informações em relação a ISO 27005 no SGSI (estudos de casos) e como utilizar uma ferramenta de análise de vulnerabilidades?**

ii. Construção das hipóteses; não se aplica

iii. Operacionalização das variáveis; não se aplica

iv. Definição do plano experimental; resume o que será feito

v. Determinação dos sujeitos; não se aplica

vi. Determinação do ambiente; utiliza-se o ambiente de rede local. Com a versão *Wireshark* 3.4.10, em um sistema operacional *Windows* 10.

vii. Coleta de dados; a análise e implementação da ferramenta *Wireshark*, mostrando o seu funcionamento e simulando sua utilidade dentro de uma rede local de computadores, com a versão *Wireshark* 3.4.10, em um sistema

operacional *Windows* 10, simulando um caso simples de Sniffing de rede. Também contendo cenários de testes feito para casos especificos, *Advanced Persistent Threat* (APT), dos autores Bullock e Parker (2017).

viii. Análise e interpretação dos dados; os resultados obtidos são mostrados no Capítulo 5, montando sua estrutura e o conteúdo trabalhado. Além de, ter sua análise no Capítulo 6.

ix. Redação do relatório; toda a pesquisa realizada foi registrada nesse presente TCC.

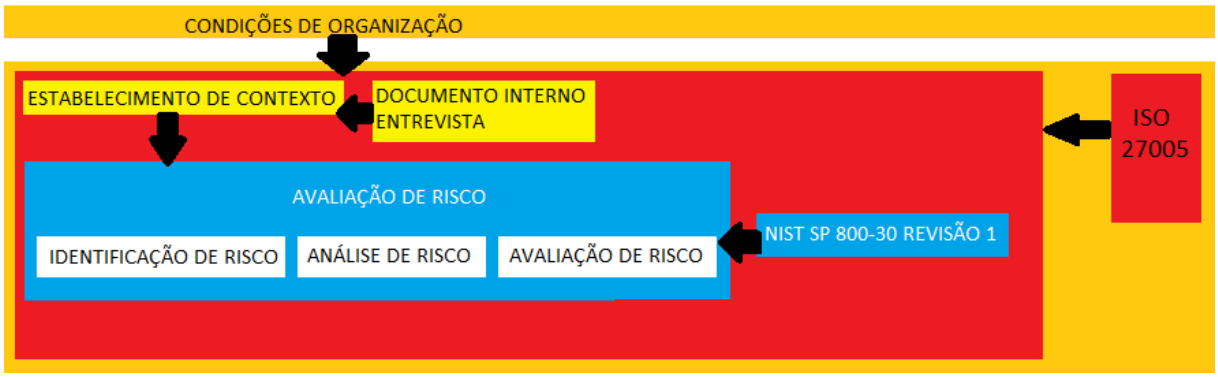
4 ESTUDOS DE CASO

Este capítulo contém os estudos de casos de empresas que utilizaram políticas de segurança, usando a ISO 27005, com a análise dos resultados obtidos. As empresas citadas tiveram seus nomes alterados pelos autores para manter o anonimato das mesmas.

4.1 AGÊNCIA ABC – INDONÉSIA

Este estudo de caso foi escrito por Fikri et al (2019), que estudaram a otimização da avaliação de risco, combinando NIST SP 800-30 revisão 1 com a ISO 27005, em empresas sem fins lucrativos. Tudo isso foi realizado para explicar sobre como usar a combinação das técnicas mencionadas, mostrado na Figura 7, e facilitar sua implementação, visando responder à questão de pesquisa: Esta abordagem pode ser utilizada em uma organização comum ou não? O objeto de pesquisa foi a Agência ABC, uma organização com fins lucrativos, com seu sistema de informação ZZZ, onde são operados em organizações de grande escala por toda a região.

Figura 7 - Conceito de Análise



Fonte: Adaptado de Fikri et al, 2019.

A gestão de risco é um processo de identificação, estimativa e etapas para reduzir o risco em um nível aceitável, como mostra a Tabela 1. Na implementação de um processo de gestão de risco, utiliza-se vários padrões e referências para sua construção, melhoria e gestão do nível de confiança antes, durante, e após a ocorrência de um incidente.

Tabela 1 - Escala de Avaliação - Probabilidade Geral

PROBABILIDADE DE INICIAÇÃO OU OCORRÊNCIA DE EVENTO DE AMEAÇA	PROBABILIDADE DE EVENTO DE AMEAÇA RESULTAR EM IMPACTOS ANTECIPADOS				
	MUITO BAIXO (0)	BAIXO (2)	MODERADO (5)	ALTO (8)	MUITO ALTO (10)
MUITO BAIXO (0)	MUITO BAIXO	MODERADO	ALTO	MUITO ALTO	MUITO ALTO
BAIXO (2)	MUITO BAIXO	MODERADO	MODERADO	ALTO	MUITO ALTO
MODERADO (5)	MUITO BAIXO	BAIXO	MODERADO	MODERADO	ALTO
ALTO (8)	MUITO BAIXO	BAIXO	BAIXO	MODERADO	MODERADO
MUITO ALTO (10)	MUITO BAIXO	MUITO BAIXO	MUITO BAIXO	BAIXO	BAIXO

Fonte: Adaptado de Fikri et al, 2019.

Na fase de implementação, a ISO 27005 pode ser combinada com outras normas ou diretrizes para atender às necessidades em relação à gestão de riscos de segurança. Espera-se que outros padrões ou diretrizes aprimorem o processo de gerenciamento de riscos, com base na segurança da informação, de modo que a NIST SP 800-30 revisão 1 possa ser usada como complemento ao processo de avaliação de risco e aplicada à estrutura de gerenciamento de risco da ISO 27005, visto na Tabela 2.

Tabela 2 - Matriz de Risco

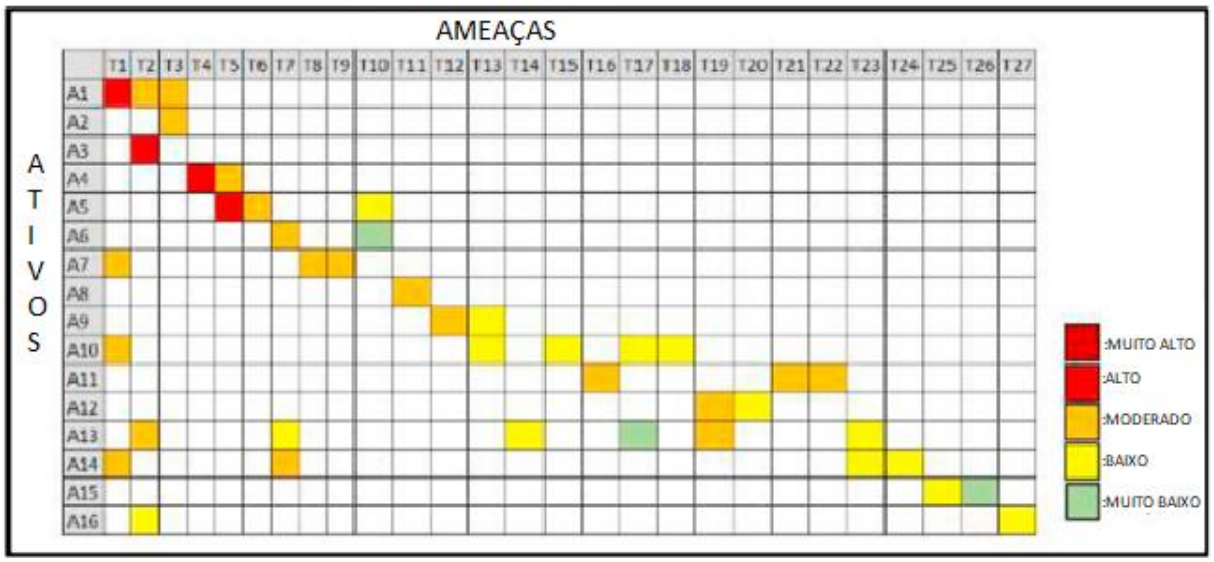
PROBABILIDADE GERAL	NÍVEL DE IMPACTO				
	MUITO BAIXO (0)	BAIXO (2)	MODERADO (5)	ALTO (8)	MUITO ALTO (10)
MUITO BAIXO (0)	ACEITAR	MITIGAÇÃO	MITIGAÇÃO	MITIGAÇÃO	MITIGAÇÃO
BAIXO (2)	ACEITAR	MITIGAÇÃO	MITIGAÇÃO	MITIGAÇÃO	MITIGAÇÃO
MODERADO (5)	ACEITAR	MITIGAÇÃO	MITIGAÇÃO	MITIGAÇÃO	MITIGAÇÃO
ALTO (8)	ACEITAR	ACEITAR	MITIGAÇÃO	MITIGAÇÃO	MITIGAÇÃO
MUITO ALTO (10)	ACEITAR	ACEITAR	ACEITAR	MITIGAÇÃO	MITIGAÇÃO

Fonte: Adaptado de Fikri et al, 2019.

Os processos utilizados na pesquisa foram: técnica de coleta de dados, técnica de validação de dados, técnica de análise de dados, análise da implementação da técnica de

combinação, avaliação de risco (Identificação de ativos, identificação de ameaças, identificação de controles existentes e identificação de vulnerabilidades), análise de risco, avaliação de risco, discussão e conclusão, como pode-se ver na Matriz 1.

Matriz 1 - Prioridade de Risco



Fonte: Adaptado de Fikri et al, 2019.

Tendo o resultado positivo, essa técnica pode ser aplicada em uma organização comum. Assim, se pode implementar esta nova técnica como uma ferramenta alternativa para avaliação de risco de segurança da informação.

4.2 INSTITUTO XYZ – INDONÉSIA

Setiawan, Pradana e Putra (2017) propõem implementar um projeto de gerenciamento de risco de segurança da informação em aplicativos de dados de comunicação no Instituto XYZ.

O Instituto XYZ opera serviços de comunicação para sub organizações sob ele, tendo o foco a comunicação com o sistema de rede para relatórios e informações, sendo estas restritas e confidenciais. Assim, o processo de gerenciamento de risco oferece a proteção do sistema e dados da organização, com objetivo de identificação, avaliação e tratamento de risco que acontece na comunicação, como mostrado no Quadro 1.

Quadro 1 - Matriz de Risco

PROBABILIDADE GERAL	NÍVEL DE IMPACTO				
	MUITO BAIXO	BAIXO	MODERADO	ALTO	MUITO ALTO
MUITO ALTO	ACEITAR	MITIGAR	MITIGAR	MITIGAR	MITIGAR
ALTO	ACEITAR	MITIGAR	MITIGAR	MITIGAR	MITIGAR
MODERADO	ACEITAR	MITIGAR	MITIGAR	MITIGAR	MITIGAR
BAIXO	ACEITAR	ACEITAR	MITIGAR	MITIGAR	MITIGAR
MUITO BAIXO	ACEITAR	ACEITAR	ACEITAR	MITIGAR	MITIGAR

Fonte: Adaptado de Setiawan, Pradana e Putra, 2017.

Ocorrem vulnerabilidades e ameaças em seus sistemas de informação e redes. Para implementar o projeto usaram da estrutura ISO 27005 e NIST SP 800-30 revisão 1 para avaliação de risco e ISO 27002, ilustrado na Figura 8, como referência para plano de tratamento de risco de desenvolvimento.

Figura 8 - Referencial Teórico da Pesquisa

Fonte: Adaptado de Setiawan, Pradana e Putra, 2017.

Juntando a ISO 27005 e NIST SP 800-30 revisão 1 como critérios básicos, os resultados obtidos nesta empresa foram analisados por uma ferramenta para avaliação de risco e organizados em uma tabela, como ilustrado no Quadro 2.

Quadro 2 - Prioridade do Risco

Prioridade	Cenário de Risco	Nível de Risco	Prioridade	Cenário de Risco	Nível de Risco	Prioridade	Cenário de Risco	Nível de Risco
1	A1,T1	Mitigar	25	A11,T9	Mitigar	49	A10,T1	Aceitar
2	A1,T2	Mitigar	26	A6,T1	Mitigar	50	A10,T2	Aceitar
3	A3,T5	Mitigar	27	A7,T1	Mitigar	51	A24,T16	Aceitar
4	A7,T8	Mitigar	28	A7,T1	Mitigar	52	A24,T21	Aceitar
5	A8,T8	Mitigar	29	A8,T1	Mitigar	53	A25,T23	Aceitar
6	A8,T6	Mitigar	30	A16,T13	Mitigar	54	A26,T22	Aceitar
7	A22,T19	Mitigar	31	A17,T1	Mitigar	55	A26,T23	Aceitar
8	A23,T19	Mitigar	32	A17,T14	Mitigar	56	A26,T24	Aceitar
9	A16,T1	Mitigar	33	A18,T1	Mitigar	57	A27,T22	Aceitar
10	A2,T1	Mitigar	34	A20,T17	Mitigar	58	A27,T23	Aceitar
11	A11,T1	Mitigar	35	A29,T16	Mitigar	59	A27,T24	Aceitar
12	A11,T6	Mitigar	36	A29,T25	Mitigar	60	A28,T23	Aceitar
13	A6,T7	Mitigar	37	A21,T18	Mitigar	61	A29,T21	Aceitar
14	A6,T6	Mitigar	38	A30,T26	Mitigar	62	A13,T2	Aceitar
15	A18,T7	Mitigar	39	A31,T26	Mitigar	63	A14,T1	Aceitar
16	A18,T15	Mitigar	40	A30,T27	Mitigar	64	A14,T2	Aceitar
17	A20,T16	Mitigar	41	A31,T27	Mitigar	66	A15,T12	Aceitar
18	A9,T2	Mitigar	42	A12,T1	Aceitar	65	A15,T11	Aceitar
19	A5,T1	Mitigar	43	A12,T2	Aceitar	67	A18,T11	Aceitar
20	A5,T2	Mitigar	44	A13,T1	Aceitar	68	A19,T1	Aceitar
21	A4,T6	Mitigar	45	A20,T6	Aceitar	69	A19,T11	Aceitar
22	A1,T3	Mitigar	46	A21,T6	Aceitar	70	A21,T17	Aceitar
23	A15,T10	Mitigar	47	A22,T20	Aceitar	71	A25,T22	Aceitar
24	A2,T4	Mitigar	48	A23,T20	Aceitar	72	A28,T24	Aceitar

Fonte: Adaptado de Setiawan, Pradana e Putra, 2017.

O tratamento dos riscos fornece meios para eliminar o risco do processo de comunicação. O resultado do tratamento do risco e as recomendações para controle está apresentando no Quadro 3.

Quadro 3 - Tratamento de Risco e Estratégias de Resolução de Risco

Cenários de Risco		**Tratamento de Risco**	
		Recomendações de controle	**PIC**
AI-T1 A16-T1		Logout automático com tempo limite de sessão	Sub Diretoria de Desenvolvimento
A6-T1	A17-T1	Restrições às redes públicas	Sub Diretoria Operacional
A11-T1 A8-T6		Verificações de segurança e triagem de aplicativos periodicamente	Sub Diretoria Operacional
A2-T1	A5-T1	Gerenciamento de senhas	Sub Diretoria Operacional
A1-T2		Avaliar testes de aplicativos	Sub Diretoria de Desenvolvimento
A2-T4 A29-T25		Tecnologia da informação, segurança da informação e treinamento em criptografia para pessoal	Sub Diretoria de Desenvolvimento
A1-T3 A2-T4		Implementação do BCP/DRP em redes de comunicação de dados	Sub Diretoria de Desenvolvimento
A3-T5	A11-T6	Aquisição de software antivírus	Escritório Regional
A11-T9	A4-T6	Aquisição do sistema operacional mais recente	Escritório Regional
A6-T7 A6-T6		Implementação da função hash no armazenamento de senhas	Sub Diretoria de Desenvolvimento
A18-T7 A7-T6	A18-T1	Aplicação de criptografia no armazenamento de dados e armazenamento de banco de dados	Sub Diretoria de Desenvolvimento
A8-T8	A18-T15	Criação de servidor de backup	Sub Diretoria de Desenvolvimento
A7-T8		Sistema de gerenciamento de rede melhorado	Sub Diretoria Operacional
A22-T19	A23-19	Aplicativo firewall no PC	Sub Diretoria Operacional
A17-T14		Monitoramento de aplicativos com sistema de log	Sub Diretoria Operacional
A7-T1	A8-T1	Autorização de função	Sub Diretoria Operacional

A31-T27		Implementação de procedimentos da segurança da informação	Sub Diretoria de Desenvolvimento
A20-T16 A31-T26	A30-T26	Maior conscientização sobre a segurança da informação	Sub Diretoria de Desenvolvimento
A5-T2		Acesso remoto ao dispositivo	Sub Diretoria de Desenvolvimento
A15-T10		Implementação de assinatura digital	Sub Diretoria de Desenvolvimento
A16-T13		Implementação da padrões de reserva de comunicação	Sub Diretoria de Desenvolvimento
A20-T17	A9-T2	Manutenção de dispositivos de comunicação	Sub Diretoria de Desenvolvimento
A30-T27		Procedimento de uso da rede	Sub Diretoria de Desenvolvimento
A21-T18		Implementação da segurança física	Sub Diretoria Operacional
A29-T16		Implementação de uma política de escrivaninha e tela limpa	Sub Diretoria Operacional

Fonte: Adaptado de Setiawan, Pradana e Putra, 2017.

Como resultado do projeto, foi possível combinar a ISO 27005 com outras diretrizes, de modo que a compatibilidade com a NIST SP 800-30 revisão 1 ocorreu. Assim, pelo fato de não possuir guia para apresentar o processo de incidente em cenários de risco, permitiu a avaliação dos riscos de segurança para os sistemas de informação da empresa.

4.3 SISTEMA INTEGRADO DE TRANSPORTE PÚBLICO (SITP) – COLÔMBIA

Felipe, Andrés e Raúl (2019) apresentam um estudo de caso no sistema integrado de transporte público (SITP), anteriormente conhecido como Transmilenio S.A., um dos maiores e mais sofisticados sistemas de transporte da Colômbia. A entrada no sistema é feita através de cartões inteligentes sem contato, frequentemente apresentando vulnerabilidades e riscos por meio deste método de pagamento no momento da entrada no sistema de transporte. Esta investigação contrasta e avalia os riscos do uso dos diferentes cartões sob NTC / ISO 27005. Foca na segurança da informação em ativos, nomeadamente nas etapas de identificação de ameaças, vulnerabilidades e riscos dos cartões utilizados no sistema, da mesma forma que a

utilização da informação pública encontrada no sistema de transporte do site para o funcionamento do sistema de gestão de risco na organização.

Os resultados alcançados permitiram detectar e contrastar os riscos, como mostrados na Figura 9 e Quadro 4, associados à utilização de cada um dos cartões que têm vindo a ser utilizados por esta entidade.

Figura 9 - Critérios de Avaliação de Risco

NÍVEL DE RISCO	PONTUAÇÃO
BAIXO	1 A 2
MEDIANO	3 A 4
ALTO	5 A 12
EXTREMO	15 A 25

Fonte: Adaptado de Felipe, Andrés e Raúl, 2019.

Quadro 4 - Probabilidade de Eventos

NÍVEL	DESCRIÇÃO	DEFINIÇÃO
1	Raramente	Pode ocorrer apenas em circunstâncias excepcionais (incomum ou anormais)
2	Improvável	Pode ocorrer esporadicamente
3	Possível	Isso pode acontecer em algumas circunstâncias
4	Frequente	Pode ocorrer na maioria das circunstâncias
5	Quase Certo	Acontece na maioria das circunstâncias

Fonte: Adaptado de Felipe, Andrés e Raúl, 2019.

A metodologia proposta na norma NTC / ISO 27005 tem sido aplicada nos diferentes *heat-maps*. Isso evidencia a probabilidade e o impacto no caso de uma ameaça explorar uma vulnerabilidade, dada a avaliação de risco da solução proposta.

Neste estudo, foram usados dois cartões eletrônicos, conhecidos como carteira e cliente frequente tipo *MIFARE® classic* e *MIFARE digite key® plus*.

A metodologia para o desenvolvimento do projeto de pesquisa foi baseada na norma NTC / ISO 27005, segurança da informação de ativos, especificamente na fase de avaliação de risco incluindo identificação, estimativa e avaliação. Utilizando da documentação pública do Transmilenio S.A., adquiriram informações sobre o funcionamento do sistema de gestão de riscos (avaliação de impacto e probabilidade, nível de severidade, critérios de aceitação e *heat-maps*). Na fase de avaliação de risco, os fatores revisados foram: identificação de ativos, ameaças, controles existentes, vulnerabilidades, consequências e no desenvolvimento do

projeto de pesquisa. A estimativa de risco, como mostrado no Quadro 5, foi revisada pelas etapas do NTC / ISO 27005: tipo semi-qualitativo, avaliação de consequências, incidentes e nível de estimativa.

Quadro 5 - Critérios de Avaliação e Aceitação de Risco

ID	RISCO	NÍVEL DO RISCO	NÍVEL DE SEGURANÇA	CRÍTERIO DE ACEITAÇÃO
RSK-12	Perda da confidencialidade da chave criptografada para um setor, devido ao curto comprimento da chave atribuída por setor, produto da manipulação de software	20	EXTREMO	NÃO TOLERAVEL
RSK-07	Perda de confidencialidade da chave criptografada da indústria, eles entendem a chave para um setor resultante do mau funcionamento do software	16	EXTREMO	NÃO TOLERAVEL
RSK-09	Perda de confidencialidade da chave criptografada da indústria, produto da manipulação com software	16	EXTREMO	NÃO TOLERAVEL
RSK-10	Perda de integridade da informação, produto de manipulação de software	16	EXTREMO	NÃO TOLERAVEL
RSK-14	Perda de integridade das informações do cartão, falta de aleatoriedade nos números únicos gerados, produto de mau funcionamento do software	16	EXTREMO	NÃO TOLERAVEL
RSK-33	Perda da confidencialidade das informações pessoais dos usuários, levando as informações contidas em cartões de crédito, realizando algum tipo de transação online resultante de uso não autorizado	16	EXTREMO	NÃO TOLERAVEL
RSK-35	Perda de integridade nas transações, para a prática de atos de clonagem, fraude ou modificações decorrentes do uso indevido ou de interrupções de comunicação	16	EXTREMO	NÃO TOLERAVEL

Fonte: Adaptado de Felipe, Andrés e Raúl, 2019.

Aos cartões *mifare* clássicos, ocorre alta probabilidade de riscos (90%), como ilustrado na Matriz 2. E no cartão *mifare plus* a probabilidade de ocorrer esses riscos foi reduzida em 40%, como mostra a Matriz 3.

Matriz 2 - Mapa de risco do cartão *Mifare* Clássico

		IMPACTO				
		Insignificante 1	Menor 2	Moderado 3	Maior 4	Catástrofico 5
PROBABILIDADE	Quase certo 1		RSK-13		RSK-12	
	Frequente 2		RSK-08 - RSK-11 RSK-15 - RSK-16		RSK-10 - RSK-14 RSK-07	
	Possível 3		RSK-05 - RSK-06 RSK-17 - RSK-18 RSK-19 - RSK-21		RSK-02 - RSK-03 RSK-20	
	Improvavel 4		RSK-04		RSK-01	
	Raramente 5					

Fonte: Fonte: Adaptado de Felipe, Andrés e Raúl, 2019.

Matriz 3 - Mapa de Risco do cartão *Mifare Plus*

		IMPACTO				
		Insignificante 1	Menor 2	Moderado 3	Maior 4	Catástrofico 5
PROBABILIDADE	Quase certo 1					
	Frequente 2					
	Possível 3					
	Improvavel 4		RSK-08 - RSK-11 RSK-13		RSK-07 - RSK-09 RSK-10 - RSK-12	
	Raramente 5		RSK-15 - RSK-19 RSK-21		RSK-14 - RSK-20	

Fonte: Adaptado de Felipe, Andrés e Raúl, 2019.

Como resultado foi respondida à questão da pesquisa de referência: **Se aplicar o padrão NTC / ISO 27005, pode os pontos fortes e fracos dos diferentes tipos de cartões**

inteligentes que foram usados como meio de pagamento ser encontrados no sistema de transporte de Bogotá D.C., Transmilenio S.A.?

Ao comparar os cartões *mifare plus* com o mifare *classic*, menos riscos foram evidenciados no *mifare plus*, devido as atividades que os geraram desapareceram (falha no código de erro de autenticação). A probabilidade de ocorrência de vulnerabilidades observadas e justificadas puderam ser reduzidas, devido a atual análise, resultando em *heat-maps* que destacam a avaliação de risco para os cartões *mifare* clássico e *mifare plus*.

Os autores concluíram que a aplicação e regulagem de uma gestão de riscos com foco na segurança da informação com um padrão adequado as suas necessidades, tomando como referência a norma NTC / ISO 27005, garante progresso e execução do objetivo. Além disso, traz o aumento da chance de sucesso e impacto positivo em uma organização.

5 ANÁLISE DA FERRAMENTA *WIRESHARK* E IMPLEMENTAÇÃO

Este capítulo contém a análise da ferramenta *Wireshark*, que foi escolhida para realizar uma implementação do caso *Sniffing* em uma rede local para monitorar sua segurança.

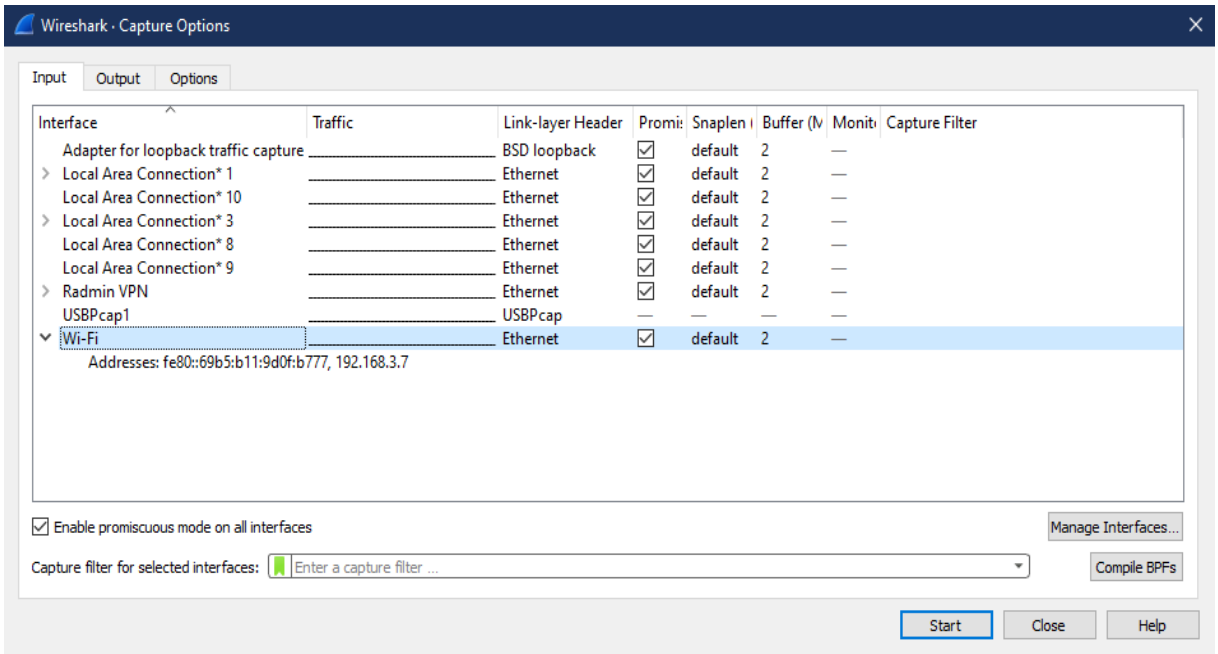
Esta ferramenta foi escolhida devido seu fácil acesso e suporte, além de ser um *software Open Source*. Isso significa que qualquer pessoa pode utilizá-lo gratuitamente, podendo ser modificado e distribuído, para qualquer finalidade.

A simulação foi realizada dentro de uma rede local de computadores, com a versão *Wireshark* 3.4.10, em um sistema operacional *Windows* 10, simulando um caso simples de Sniffing de rede. Também contém cenários de testes feito para casos especificos, APT, dos autores Bullock e Parker, 2017.

No *Sniffing* , também conhecido como farejar, normalmente só pode ver o tráfego de rede originado do computador, destinado ao computador ou tráfego de *broadcast*. Sendo assim, efetua monitoramento do tráfego de Internet em tempo real, capturando todos os dados que entram e saem de um computador.

Para começar a farejar, o *Wireshark* deve ser iniciado e usada a opção seção de captura na tela inicial, como mostrada na Figura 10.

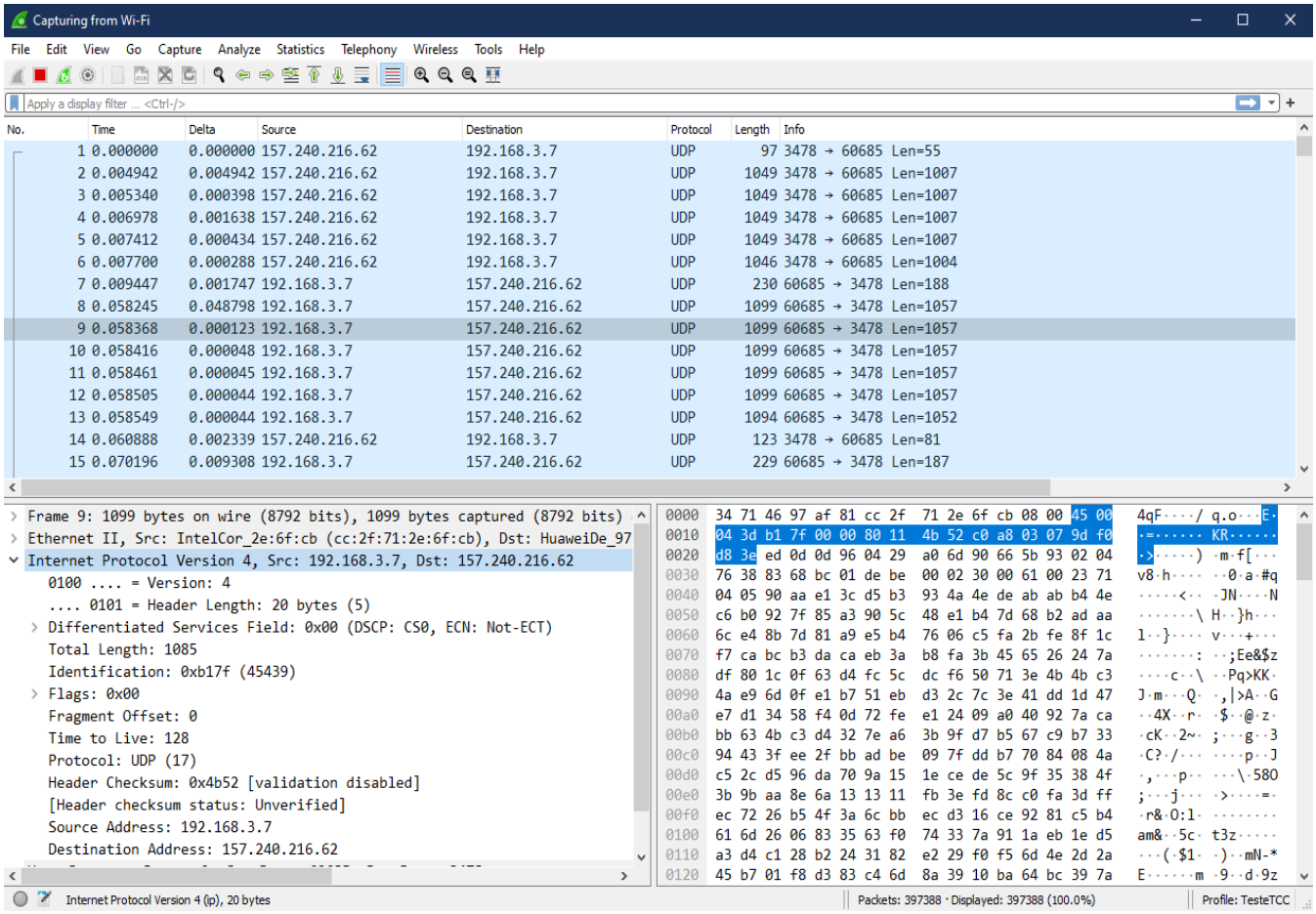
Figura 10 – Lista de Captura de Interfaces



Fonte: Autoria própria.

Para uma captura basica foi selecionado o modo Wi-Fi, com as opções padrões. Em seguida iniciou-se em *promiscuous mode* e começou a farejar o tráfego. Após iniciar, apareceu tráfego no monitor. Conforme mostrado na Figura 11, os pacotes foram capturados e exibidos nos primeiros segundos da detecção. Ao clicar no pacote número 9, no painel *Packet List*, apareceu uma divisão do pacote no painel *Packet Details*.

Figura 11 – Novo Tráfego



Fonte: Autoria própria.

O pacote de exemplo que o painel *Packet List* destaca qual pacote está sendo mostrado. O *Packet Details* do pacote mostra dentro do pacote por meio das subárvores aplicáveis. Expandir uma subárvore, "*Internet Protocol Version 4*", no *Packet Details* do pacote mostra os endereços IP de origem e destino do pacote, bem como vários sinalizadores e outras informações de cabeçalho IPv4.

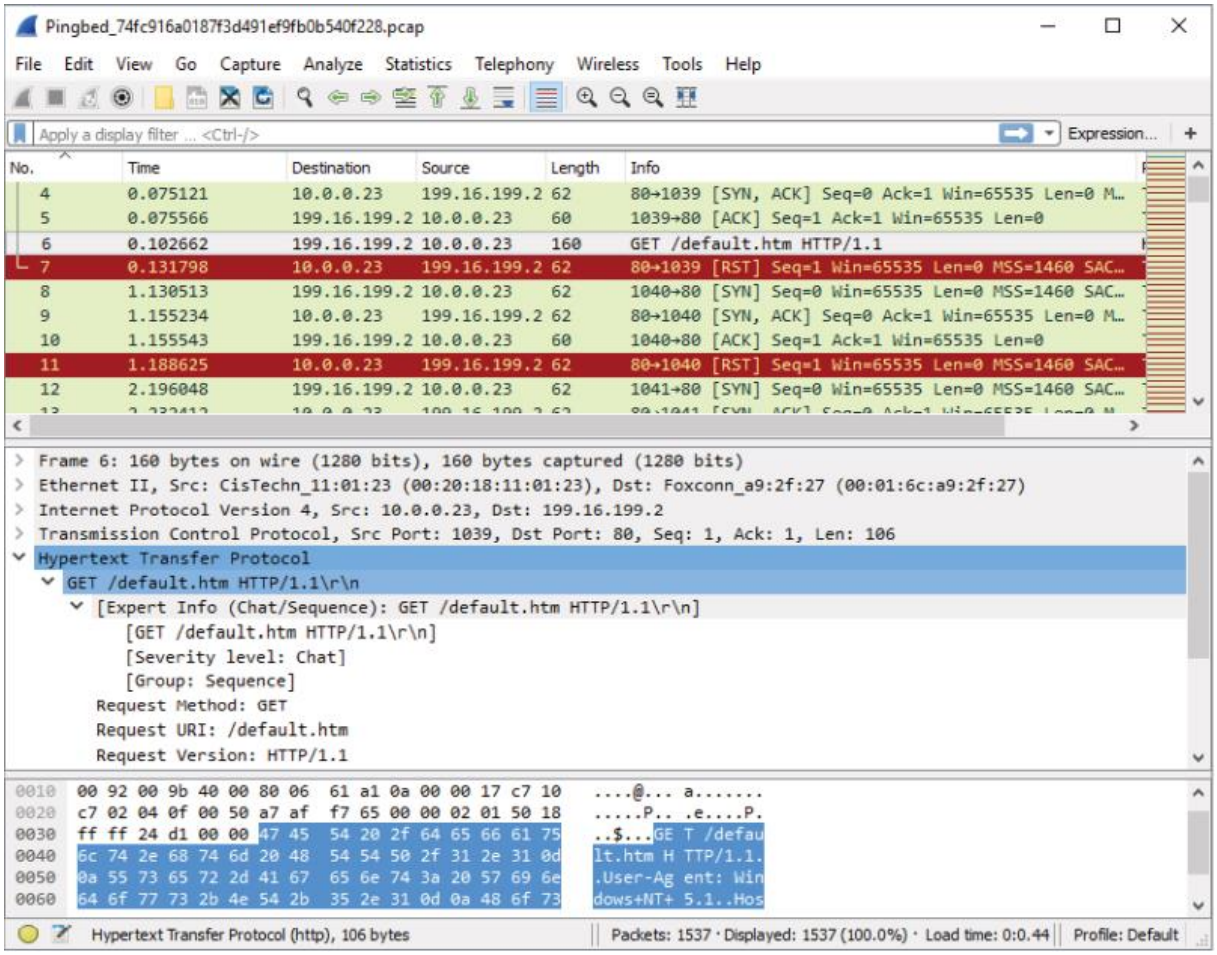
Neste caso, é observado que se pode usar do *Sniffing* para diagnosticar problemas e avaliar desempenho, possibilitando a tomada de medidas apropriadas. Também utilizado para

coletar o tráfego de toda a rede, ou aplicar um filtro para avaliar pacotes com tipos específicos de dados.

Para os cenários de testes dos autores Bullock e Parker (2017), são mostrados os casos APT:*Pingbed* e APT:*Gh0st*. De acordo com estes autores, o APT é uma categoria generalizada do comportamento do *malware*. Assim que é inserido o reconhecimento é iniciado à medida que o invasor procura dados ou usuários valiosos. O *malware* pode se espalhar ou se replicar para facilitar o reconhecimento.

Exemplo de APT Win32/*Pingbed*: A Figura 12 é uma captura de tela do *Wireshark* mostrando o tráfego capturado do *Pingbed*.

Figura 12 – *Pingbed*

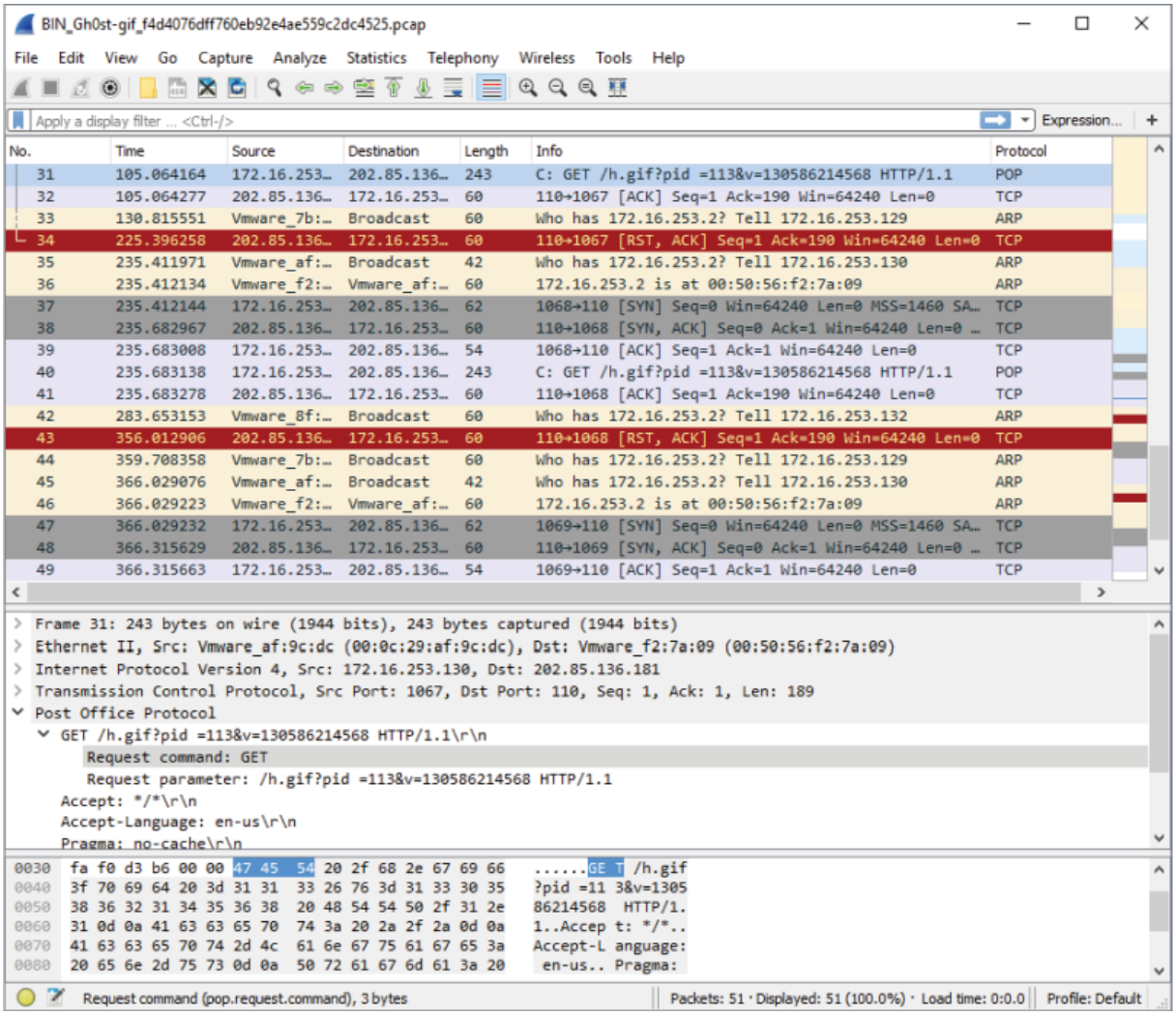


Fonte: BULLOCK J.; PARKER J., 2017.

Observe as chamadas persistentes para o IP remoto via 80 / tcp do sistema com cavalo de Tróia (10.0.0.23), o método GET para recuperar *default.htm* e, em seguida, a conexão fechada (sinalizador RST).

Exemplo APT *Gh0st*: A Figura 13 é uma captura de tela do *Wireshark* mostrando o tráfego capturado de *Gh0st*.

Figura 13 – *Gh0st*



Fonte: BULLOCK J.; PARKER J., 2017.

Observe as chamadas persistentes para o IP remoto via 80 / tcp do sistema com cavalo de Troia (172.16.253.130), o método GET para recuperar *h.gif* e a conexão fechada (sinalizador RST) - cada conexão de SYN para RST cronometrada para levar 120 segundos.

Esta implementação permitiu mostrar o monitoramento da Internet, em tempo real, e suas possiveis ameaças e riscos.

Além disso, foi possível confirmar o uso do *Wireshark* para diagnosticar problemas e avaliar desempenho, possibilitando a tomada de medidas apropriadas. Pode-se confirmar o que foi detectado ou suspeitado, também detectar o que um Sistema de Detecção de Intrusão (IDS) suspeita para decidir entre tráfego malicioso e uma bandeira falsa.

6 ANÁLISE DOS RESULTADOS OBTIDOS E DISCUSSÃO

Este capítulo contém a análise dos resultados obtidos ao longo da pesquisa, perante os estudos sobre a norma, os estudos de caso e sobre a ferramenta escolhida, *Wireshark* e seu funcionamento.

Em relação a norma ISO 25007, é um padrão conhecido de SGSI, em que suas tarefas incluem a identificação, avaliação e priorização de riscos. Suas atividades são descritas como: Definição do contexto, Processo de avaliação de riscos, Tratamento do risco, Aceitação do risco, Comunicação e consulta do risco e Monitoramento e análise crítica de riscos.

Voltando para a vulnerabilidade e riscos, o processo de avaliação de riscos descreve o risco qualitativamente e habilita a priorização dos riscos de acordo com a sua gravidade ou outro critério estabelecido. O processo consiste nas atividades de: Identificação de riscos, Análise de riscos e Avaliação de riscos.

A vulnerabilidade são falhas no sistema ou design que concede ao intruso acesso não autorizados para conduzir ataques ao serviço. A análise de vulnerabilidade é um processo de identificação, documentação e redução das ameaças de segurança, propondo uma nova abordagem na caracterização do sistema.

O risco é uma combinação da ocorrência de um evento inesperado com a possibilidade do evento. O gerenciamento de risco é um processo de identificação, estimativa e identificação de etapas para reduzir o risco em um nível aceitável. Na implementação do processo de gestão de riscos utiliza-se referências e padrões para a sustentabilidade de seus processos.

Os estudos dos casos das empresas, apresentados neste trabalho, conseguiram implementar as normas pesquisadas e, assim, propor um meio para resolução dos riscos identificados em cada uma delas.

No caso da Agência ABC – Indonésia, houve o estudo da otimização da avaliação de risco, combinando NIST SP 800-30 revisão 1 com a ISO 27005, em empresas sem fins lucrativos. Tudo isso foi realizado para explicar sobre como usar a combinação das técnicas mencionadas e facilitar sua implementação. Tendo o resultado positivo, visto que essa técnica pode ser aplicada em uma organização comum. Assim, se pode aplicar esta nova técnica como uma ferramenta alternativa para avaliação de risco de segurança da informação.

No caso do Instituto XYZ – Indonésia, desenvolveram um projeto de gerenciamento de risco de segurança da informação em aplicativos de dados de comunicação no próprio instituto. Para implementar o projeto usaram da estrutura ISO 27005 e NIST SP 800-30 revisão 1 para avaliação de risco e ISO 27002, como referência para plano de tratamento de

risco de desenvolvimento. Como resultado, foi possível combinar a ISO 27005 com outras diretrizes, de modo que a compatibilidade com a NIST SP 800-30 revisão 1 ocorreu. Assim, permitiu a avaliação dos riscos de segurança para os sistemas de informação da empresa

No Estudo de caso do SITP – Colômbia, eles apresentam um estudo de caso no sistema integrado de transporte público (SITP), um dos sistemas de transporte da Colômbia. Este estudo contrasta e avalia os riscos do uso dos diferentes cartões sob NTC / ISO 27005, focado na segurança da informação em ativos. Os resultados alcançados permitiram detectar e contrastar os riscos, associados à utilização dos cartões utilizados. Foi concluído que a aplicação e regulagem de uma gestão de riscos com foco na segurança da informação com um padrão adequado as suas necessidades, tomando como referência a norma NTC / ISO 27005, garante progresso e execução do objetivo. Além disso, traz o aumento da chance de sucesso e impacto positivo em uma organização.

Além desta parte teórica, este trabalho fez um experimento prático de teste de vulnerabilidade, usando, dentre as ferramentas estudadas, o *Wireshark*. Utiliza-se o ambiente de rede local, simulando uma empresa pequena. Com a versão *Wireshark* 3.4.10, em um sistema operacional *Windows* 10.

Diante a implementação dos testes realizados, mostra-se a análise e implementação da ferramenta *Wireshark*, utilizado para coletar o tráfego de toda a rede, ou aplicar um filtro para avaliar pacotes com tipos específicos de dados. Assim, é possível monitorar o tráfego de internet em tempo real, capturando todos os dados que entram e saem de um computador.

Analisando os exemplos de testes, pode-se verificar o uso do *Wireshark* para diagnosticar problemas e avaliar desempenho, possibilitando a tomada de medidas apropriadas. Pode-se confirmar o que foi detectado ou suspeitado, também detectar o que um Sistema de Detecção de Intrusão (IDS) suspeita para decidir entre tráfego malicioso e uma bandeira falsa.

7 CONCLUSÃO

A questão de pesquisa que norteou este trabalho de conclusão de curso foi: **- Como as empresas estão protegendo suas informações em relação a ISO 27005 no SGSI (estudos de casos) e como utilizar uma ferramenta de análise de vulnerabilidades?**

O objetivo geral deste TCC foi o de apresentar estudos de caso de empresas que aplicaram a norma ISO 27005 em um sistema de SGSI e realizar uma análise das vulnerabilidades seguindo uma das ferramentas disponíveis (no caso, foi usado o *Wireshark*).

Nos estudos de casos das empresas foi observado que elas estão protegendo suas informações usando: combinação das técnicas ISO 27005 com a NIST SP 800-30 revisão 1. Assim, geram uma escala de probabilidade geral e avaliação dos riscos que, por fim, com auxílio de uma ferramenta de identificação de riscos, cria, a partir daquela combinação, uma tabela de avaliação e os métodos de resolução dos riscos encontrados.

Algumas empresas não têm colocado em prioridade o SGSI em suas rotinas, deixando em risco o seu sistema e empresa como um todo. De modo que a convergência de suas normas com a ISO 27005 e afins, ajudam a identificar os problemas presentes na segurança e mostram um método para solução desse problema.

Os estudos realizados permitiram concluir que a norma ISO 27005 não é um padrão imposto, mas sim uma recomendação de boas práticas. Ela ajuda a proteger as informações da empresa ou organização que a aplica em suas políticas de segurança.

Além disso, com a implementação realizada neste trabalho, pode-se verificar o uso das ferramentas de vulnerabilidades para diagnosticar problemas e avaliar desempenho, possibilitando a tomada de medidas apropriadas. Dessa forma, busca-se confirmar uma suspeita para decidir entre tráfego malicioso e uma bandeira falsa.

Para continuidade deste trabalho, sugere os seguintes trabalhos futuros:

- Realizar estudos envolvendo as demais ferramentas;
- Implementar as ferramentas em uma empresa de pequeno ou grande porte.

REFERÊNCIAS

ACSOFTWARE. ***Software* de gerenciamento de vulnerabilidades**. 2021. Disponível em: <https://acsoftware.com.br/detalhes_do_software.php?item=105&software_gerenciamento_vulnerabilidades>. Acesso em: 30 de setembro de 2021.

AGRAWAL, Vivek. *A Framework for the Information Classification in ISO 27005 Standard*. In: *International Conference on Cyber Security and Cloud Computing*, 4, 2017, Nova York. **IEEE**. Nova York: IEEE, 2017. p. 264-269.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT – NBR ISO/IEC 27005:2019. **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. 3. ed. Rio de Janeiro: ABNT, 2019.

BEZERRA, Edson Kowask. **Gestão de Riscos de TI NBR 27005**. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2013.

BULLOCK, Jessey.; PARKER, Jeff T. ***Wireshark® for Security Professionals: Using Wireshark and the Metasploit® Framework***. Indianapolis: *John Wiley & Sons*, 2017.

CHINELATO, João Filho. **O&M integrado à informática**. 13 Ed: Rio de Janeiro, 2008.

FELIPE, Mojica S. I.; ANDRÉS, L. V. S.; RAÚL, B. G. *Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp D.C Colombia*. In: *Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)*, 1, 2019, Bogotá. **IEEE**. Bogotá: IEEE, 2019. p. 1-6.

FIKRI, Muhamad A.; PUTRA, F. A.; SURYANTO, Y.; RAMLI, K. *Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency*. In: *Information Systems International Conference*, 5, 2019, Surabaya. ***Procedia Computer Science***. Surabaya: Elsevier, 2019. p. 1206-1215.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa.** 6. ed. São Paulo: Atlas, 2017.

GREENBONE. ***History of the OpenVAS project***. 2021. Disponível em: <https://greenbone.github.io/docs/background.html#history-of-the-openvas-project>. Acesso em: 30 de setembro de 2021.

MANAGEENGINE. ***Vulnerability Manager Plus***. 2021. Disponível em: <https://www.manageengine.com/br/vulnerability-management/>. Acesso em: 30 de setembro de 2021.

NEXPOSE. ***Nexpose Vulnerability Scanner***. 2021. Disponível em: <https://www.rapid7.com/products/nexpose/>. Acesso em: 30 de setembro de 2021.

OPENVAS. ***OpenVAS - Open Vulnerability Assessment Scanner***. 2021. Disponível em: <https://www.openvas.org>. Acesso em: 30 de setembro de 2021.

PETTERS, Jeff. ***How to Use Wireshark: Comprehensive Tutorial + Tips***. 2020. Disponível em: <https://www.varonis.com/blog/how-to-use-wireshark/>. Acesso em: 30 de setembro de 2021.

RAPID7, ***PRODUCT BRIEF***. 2021. Disponível em: <https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-nexpose-product-brief.pdf>. Acesso em: 30 de setembro de 2021.

SETIAWAN, Hermawan; PRADANA, A. R.; PUTRA, F. A. *Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A case study at communication data applications of XYZ institute*. In: *International Conference on Information Technology Systems and Innovation (ICITSI)*, 1, 2017, Bandung. **IEEE**. Bandung: IEEE, 2017. p. 251-256.

SHARPE, Richard; WARNICKE, E.; LAMPING, U. ***Wireshark User's Guide - Version 3.7.0***. 2021. Disponível em:<https://www.wireshark.org/docs/wsug_html_chunked/>. Acesso em: 15 de outubro de 2021.

SILVA, Fabio. ***OpenVas – Scanner de Vulnerabilidades***. 2021. Disponível em: <https://fabiosilva.com.br/2021/03/07/openvas-scanner-de-vulnerabilidades/>. Acesso em: 30 de setembro de 2021.

STANGO, Antonietta; PRASAD, N. R.; KYRIAZANOS, D. M. *A Threat Analysis Methodology for Security Evaluation and Enhancement Planning*. In: *International Conference on Emerging Security Information, Systems and Technologies*, 3, 2009, Atenas. **IEEE**. Atenas: IEEE, 2009. p. 262-267.

TENABLE. ***NESSUS Professional***. 2021. Disponível em: <https://www.tenable.com/lp/campaigns/19/try-nessus/?utm_campaign=gs-%7b11596512476%7d-%7b116641139201%7d-%7b537515898416%7d_00021181_fy21q1&utm_promoter=tenable-hv-brand-00021181&utm_source=google&utm_term=nessus%20vulnerability%20scanner&utm_medium=cpc&utm_geo=latam&gclid=Cj0KCQjwtMCKBhDAARIsAG-2Eu-r5BIXp0NIDlirEs3a0XVEoP-O4qGDdh4KBuirSLRG023JOOCHPo0aAjOYEALw_wcB>. Acesso em: 30 de setembro de 2021.

UNICAMP. **O QUE SÃO DADOS?** 2021. Disponível em: <https://www.ime.unicamp.br/~hildete/dados.pdf>. Acesso em: 25 de abril de 2021.

WAZLAWICK, Raul Sidnei. **Metodologia de Pesquisa para Ciência da Computação**. 2 ed. Rio de Janeiro: Elsevier, 2014.

WENDLANDT, Dan. ***Nessus: A security vulnerability scanning tool***. 2021. Disponível em: <https://www.cs.cmu.edu/~dwendlan/personal/nessus.html>. Acesso em: 30 de setembro de 2021.

WIRESHARK. ***Wireshark***. 2021. Disponível em: < https://www.wireshark.org>. Acesso em: 30 de setembro de 2021.

YOO, Sang G.; PATIÑO, S.; ARROYO, R.; SOLÍS, E. F. *ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005*. In: *International*

Conference on eDemocracy & eGovernment (ICEDEG), 5, 2018, Ambato. **IEEE**. Ambato: IEEE, 2018. p. 75-82.