UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS

UNIDADE ACADÊMICA DE EDUCAÇÃO CONTINUADA

ESPECIALIZAÇÃO EM GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO BASEADA EM PADRÕES INTERNACIONAIS

Everton Gamba Lermen

ANÁSE DE RISCOS DE SEGURANÇA DA INFORMAÇÃO EM REDES WI-FI EM UMA INSTITUIÇÃO DE ENSINO – ABNT NBR ISO/IEC 27005:2011

São Leopoldo

2015

EVERTON GAMBA LERMEN

ANÁSE DE RISCOS DE SEGURANÇA DA INFORMAÇÃO EM REDES WI-FI EM UMA INSTITUIÇÃO DE ENSINO – ABNT NBR ISO/IEC 27005:2011

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do título de Especialista em Governança de Tecnologia da Informação, pelo curso de Pós-Graduação Lato Sensu em Governança de Tecnologia da Informação da Universidade do Vale do Rio dos Sinos – UNISINOS.

Orientadora: Profa. Dra. Margrit Reni Krug

São Leopoldo

2015

RESUMO

Este trabalho tem por objetivo verificar como é realizada a gestão de segurança de redes Wi-Fi em uma Instituição de Ensino Superior e, sugerir melhorias com base na norma ABNT NBR ISO/IEC 27005:2011. Para que este estudo tivesse êxito, foi realizada uma análise dos documentos e procedimentos existentes, uma observação da operação do ambiente e entrevistas com colaboradores de representatividade na área. Com as informações obtidas pela análise documental e da observação do ambiente, foi realizada a análise, avaliação e sugerido tratamentos com base na norma ABNT NBR ISO/IEC 27005:2011. Os resultados foram apresentados e validados pelos colaboradores participantes das entrevistas com o intuito de melhorar a gestão de risco e segurança da informação na Instituição.

Palavras-chave: Segurança da Informação. Gestão de Risco. Rede Wi-Fi. ISO/IEC 27005.

ABSTRACT

This work aims to verify how the Wi-Fi network security management in a Higher Education Institution is accomplished and, suggest improvements based on standard ISO/IEC 27005:2011. For the success of this study, an analysis of existing documents and procedures were performed. Also, an observation of the operations in the environment and interviews with representative employees in the area were conducted. With the information obtained by document analysis and environment monitoring, the assessment/analysis was performed as well as treatment recommendations based on the standard ISO/IEC 27005:2011. The results were presented and validated by the employees, chosen to participate in the interviews, in order to improve risk management and security information in the Institution.

Keywords: Security Information. Risk Management. Wi-Fi Network. ISO/IEC 27005.

LISTA DE FIGURAS

Figura 1 - Normas que influenciaram a criação da ISO/IEC 27005 ..... **13**

Figura 2 - O processo de gestão de risco da ABNT NBR ISO/IEC 27005:2011 ..... **14**

Figura 3 - Atividade de tratamento do risco da ABNT NBR ISO/IEC 27005:2011 ..... **19**

Figura 4 - Diagrama lógico do acesso a rede Wi-Fi **27**

Figura 5 - Diagrama físico de acesso a rede Wi-Fi **28**

Figura 6 - Fluxo do processo de instalação de um novo Access Point **29**

Figura 7 - Novo fluxo do processo de instalação de um novo Access Point **36**

LISTA DE QUADROS

Quadro 1 - Matriz de Risco **32**

Quadro 2 - Classificação de Risco **32**

Quadro 3 - Análise de Riscos **33**

Quadro 4 - Priorização dos riscos **34**

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

AP – Access Point

BS – British Standard

CPF – Cadastro de Pessoa Física

EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité

IEC – International Electrotechnical Commission

IES – Instituição de Ensino Superior

ISO – International Organization for Standardization

MAC – Media Access Control Address

NAC – Network Access Control

NBR – Norma Brasileira

TI – Tecnologia da Informação

WAP2 – Wi-Fi Protected Access II

SUMÁRIO

1 INTRODUÇÃO 9
1.1 DEFINIÇÃO DO PROBLEMA 10
1.2 OBJETIVOS 11
1.2.1 Objetivo Geral 11
1.2.2 Objetivos Específicos 11
1.3 JUSTIFICATIVA 12

2 GESTÃO DE RISCOS: NORMA ABNT NBR ISO/IEC 27005:2011 13
2.1 DEFINIÇÃO DO CONTEXTO 15
2.2 PROCESSO DE AVALIAÇÃO DE RISCOS 16
2.3 TRATAMENTO DO RISCO 18
2.4 ACEITAÇÃO DO RISCO 20
2.5 COMUNICAÇÃO E CONSULTA DO RISCO 21
2.6 MONITORAMENTO E ANÁLISE CRÍTICA DE RISCOS 22

3 MÉTODOS E PROCEDIMENTOS 23
3.1 DELINEAMENTO DA PESQUISA 23
3.2 DEFINIÇÃO DA ÁREA E PARTICIPANTES DA PESQUISA 24
3.3 TÉCNICAS DE COLETA DE DADOS 24
3.4 TÉCNICAS DE ANÁLISE DE DADOS 25

4 ESTUDO DE CASO 26
4.1 DESCRIÇÃO DO AMBIENTE 26
4.2 PRÁTICA DE GESTÃO DE SEGURANÇA 31
4.3 ANÁLISE E AVALIAÇÃO DOS RISCOS 31
4.4 TRATAMENTO DOS RISCOS 34
4.5 VALIDAÇÃO DA ANÁLISE E TRATAMENTO DOS RISCOS 37

5 CONSIDERAÇÕES FINAIS 39

REFERÊNCIAS 41

APENDICE A – ROTEIRO DE ENTREVISTA 43

1 INTRODUÇÃO

O mercado de educação está cada vez mais dinâmico e competitivo e, as Instituições de Ensino Superior (IES), apesar de possuírem características específicas que as diferenciam de outras organizações, também acabam por enfrentar riscos à continuidade de seus negócios.

A importância crescente da tecnologia da informação nas organizações e o aumento das ameaças e dos riscos a que essas informações estão submetidas, tornaram a gestão de riscos de TI uma preocupação constante no dia-a-dia da operação.

Sendo organizações que possuem características específicas, os riscos enfrentados pelas IES também possuem suas peculiaridades, o que traz a necessidade de adequar o sistema de gestão de riscos para esta realidade, visando aumentar a segurança da gestão, conhecendo melhor os eventos que podem impedir cumprimento das metas e, consequentemente, aumentar as chances de atingirem seus objetivos. (SEDREZ e FERNANDES, 2011).

O problema levantado neste trabalho é a instalação/ampliação da cobertura Wi-Fi nas IES, sendo realizada, na grande maioria das vezes, para atender as reivindicações dos alunos por uma melhor conectividade, mas também, muitas vezes, sendo realizada sem uma análise dos riscos que esta ação pode trazer à continuidade da operação.

O objetivo geral desta monografia, verificar como é realizada a gestão de segurança de Redes Wi-Fi em uma IES e, sugerir melhorias com base na ABNT NBR ISO/IEC 27005:2011.

> Neste contexto, a gestão de riscos assume um papel de fundamental importância na adoção de medidas de proteção adequadas das informações críticas da IES. Sem o uso de instrumentos de gestão adequados, não há garantias do emprego correto dos investimentos e das medidas apropriadas de proteção. (OHTOSHI, 2008, p. 15).

Este trabalho está estruturado em cinco capítulos contando com esta introdução. O segundo capítulo apresenta a gestão de risco pela norma ABNT NBR ISO/IEC 27005:2011. O capítulo três apresenta a metodologia aplicação para elaboração. O quarto capítulo traz o estudo de caso e, o quinto e último capítulo fecha com as considerações finais.

1.1 DEFINIÇÃO DO PROBLEMA

Boa parte das Instituições de ensino superior do Brasil disponibilizam acesso à Internet ou mesmo a recursos internos como, portais, Intranet, arquivos, entre outros ao seu corpo docente e discente através de conexão Wi-Fi.

Este meio de acesso permite, por meio de instalação de pontos de acessos espalhados pelos campi, uma maior conectividade e acesso a informação, bem como uma redução da complexa estrutura necessário para entrega de um cabeamento físico – rede *wire*.

Os pontos de acesso são normalmente instalados em locais de grande concentração e atividade interna, como biblioteca, auditório e praça de alimentação. "A Fundação Armando Álvares Penteado (FAAP) investiu em uma rede wireless com maior amplitude, que cobre toda a instituição". (IT PRO: CARREIRA, 2008).

Seu uso pedagógico e cada vez mais estimulado pelas Instituições. "Aplicações pedagógicas e prestação de serviço à comunidade motivam universidade cearense a implantar rede sem fio em todo seu campus". (APRENDER VIRTUAL, 2015).

Universidades como a Unifor de Fortaleza realizou seu primeiro piloto, disponibilizando Wi-Fi e no centro de convivência em 2005 e, em pouco mais de um ano, já estava com cobertura total do campus. A Faculdade de Comunicação Social da Pontifícia Universidade Católica do Rio Grande do Sul (FAMECOS-PUCRS) em 2001 implantou acesso Wi-Fi com o objetivo de oferecer acesso aos alunos e professores e facilitar a transmissão de vídeo entre as salas. (PASSEIWEB, 2015).

Além de possibilitar o uso pedagógico, estimulado pelas Instituições, ela pode ser foco de problema quando não gerenciada de forma segura, como acesso a conteúdo impróprio, tentativas de invasão/ataques externos ou internos aos ativos da Instituição.

Apesar de pouco divulgado, as Instituições de ensino são alvos de ataques que buscam desde a forma mais simples, conhecida como pichação, até outros mais elaborados com o objetivo de tirar o serviço do ar ou mesmo realizar o roubo de informações. Alguns casos

como os da Universidade Federal de Pernambuco[1], da Universidade Federal do Rio de Janeiro[2] e da Universidade de Brasília[3], ilustram o problema.

Este trabalho se propõe a analisar como é feita a gestão de segurança sobre rede wireless em uma Instituição de ensino e sugerir melhorias com base na ABNT NBR ISO/IEC 27005:2011.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O objetivo geral deste trabalho foi realizar uma análise de como era realizada a gestão de segurança de Redes Wi-Fi em uma Instituição de Ensino, para posteriormente sugerir melhorias com base na ABNT NBR ISO/IEC 27005:2011.

1.2.2 Objetivos Específicos

Partindo do objetivo geral, foram estabelecidos os seguintes objetivos específicos:

- Descrever as práticas de gestão de segurança de Redes Wi-Fi atualmente implantadas.
- Analisar e Avaliar os riscos com base na ISO/IEC 27005.
- Propor ações para tratamento dos riscos.

[1] Universidade Federal de Pernambuco sofre ataque hacker.
http://blogs.ne10.uol.com.br/mundobit/2015/01/05/site-da-ufpe-sofreu-ataque-hacker/
[2] Universidade Federal do Rio de Janeiro tem páginas invadidas.
http://oglobo.globo.com/rio/paginas-da-ufrj-na-internet-sao-invadidas-por-hacker-que-afirma-ser-muculmano-15082134
[3] Universidade de Brasília tem notícias alteradas em seu site em onda de ataque.
http://ultimosegundo.ig.com.br/brasil/hackers+comandam+onda+de+ataques+pelo+quarto+dia+consecutivo/n1597046555189.html

1.3 JUSTIFICATIVA

A Instituição estudada vem ampliando ano a ano suas instalações físicas, com novas unidades, novos prédios, novos equipamentos. Este investimento tem como objetivo oferecer, pelo lado acadêmico, ao seu corpo docente, uma melhor experiência de aprendizado. Paralelamente, pelo lado administrativo, a Instituição é cobrada pelas áreas de *Compliance* e Auditoria a manter e aprimorar seus controles de segurança.

O dilema do Departamento de TI é: Como atender as demandas da área acadêmica, sem fragilizar os controles acordados junto a área administrativa? Isto fez com que a TI voltasse seus olhares, com mais atenção a Gestão de Riscos e Segurança da Informação e também as demais normas da família ABNT NBR ISO/IEC 27000.

A rede Wi-Fi foi escolhida para esta primeira análise, devido a investimentos em sua renovação e ampliação nos campi.

O autor deste trabalho atua junto à Instituição, objeto deste estudo, como Especialista em Infraestrutura, ficando envolvido diretamente em todo o processo.

2 GESTÃO DE RISCOS: NORMA ABNT NBR ISO/IEC 27005:2011

A gestão de riscos de segurança é um processo sistemático da gestão organizacional, que auxilia a identificar as necessidades da organização em relação aos requisitos de segurança da informação, buscando desta forma uma aplicação equilibrada de controles de segurança, com base em um perfil de risco. (FERNANDES, 2009). É considerada uma das etapas mais importantes da gestão da segurança da informação que, quando adequadamente implantado, permite a melhoria contínua da tomada de decisão e do desenvolvimento da organização. (OHTOSHI, 2008).

Segundo Schauer (2007), a ISO/IEC 27005 é o resultado de diversas outras normas e métodos. A Figura 1 apresenta os normas que influenciaram a sua criação.

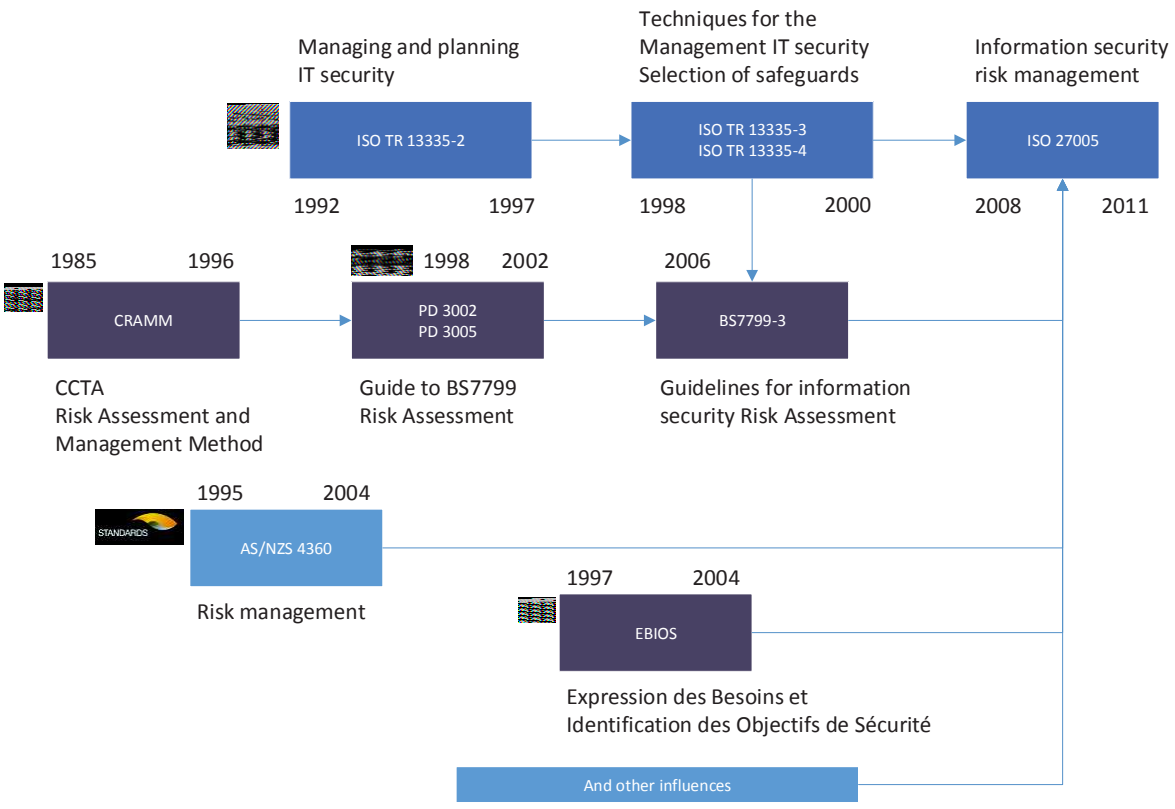

Figura 1 – Normas que influenciaram a criação da ISO/IEC 27005

Fonte: Elaborado pelo autor com base em Schauer (2007).

A ISO/IEC 2005 sofreu influências da ISO 13335-3, que apresenta um modelo de gestão de risco desde 1992 com o início da normalização da segurança em tecnologia de informação. A *British Standard* BS 77990-3 possui função similar à da ISO/IEC 27005 e, sua série de normas foi a base da família 27000. O método EBIOS criado pelo Ministério de

Defesa francês, contribuiu com a ideia da divisão do processo de avaliação de riscos em atividades e subatividades. Ainda teria sofrido, segundo Schauer (2007), influências de outras fontes que não puderam ser identificadas. (SILVA, 2009).

A norma ABNT NBR ISO/IEC 27005:2011 fornece diretrizes para o processo de gestão de riscos de segurança da informação, que consiste na 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.

A Figura 2 apresenta o fluxo do processo de gestão de gestão de risco adotado pela norma.

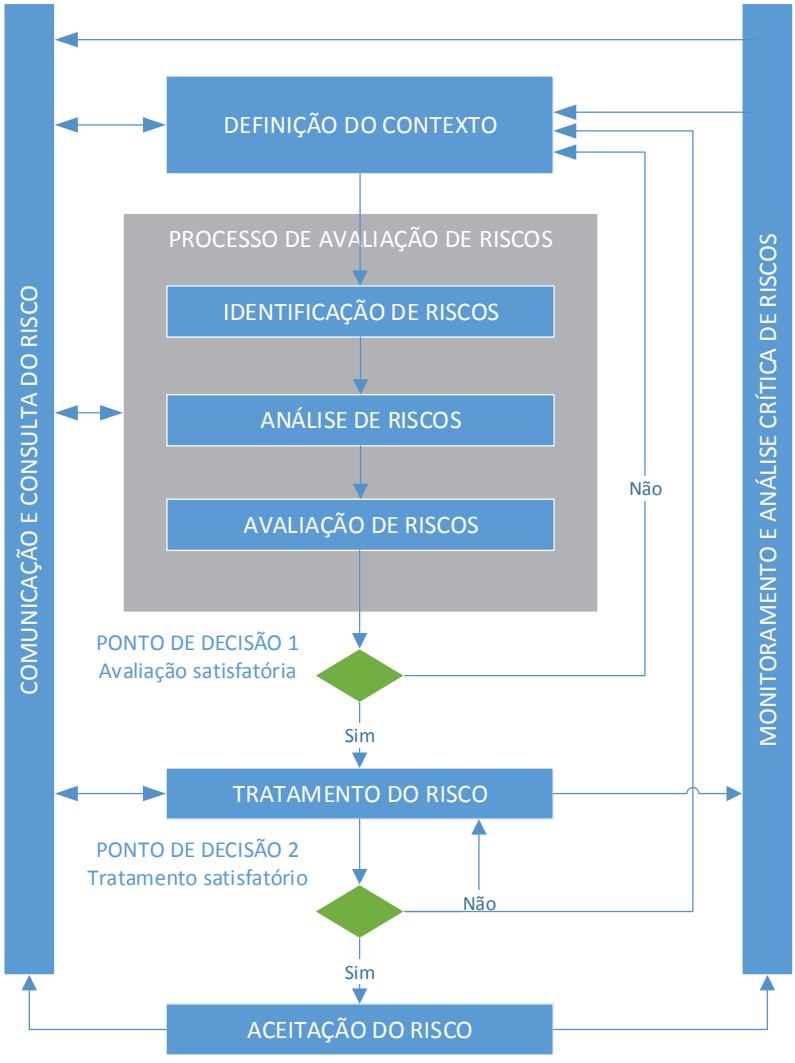

Figura 2 – O processo de gestão de risco da ABNT NBR ISO/IEC 27005:2011

Fonte: ABNT NBR ISO/IEC 27005 (2011)

O processo de gestão de risco é contínuo e pode ser iterativo com a avaliação de riscos e/ou na atividade de tratamento do risco.

Um enfoque iterativo no processo de avaliação de riscos é adotado, assim a cada repetição é possível aprofundar e detalhar mais a avaliação. Nesta mesma linha, se o tratamento do risco não resultar em um nível que seja aceitável, um tratamento adicional precisa ser trabalhado ou ainda uma nova interação com o processo de avaliação de riscos precisa ser realizada.

As sessões a seguir detalham os processos apresentados na norma ABNT NBR ISO/IEC 27005:2011.

2.1 DEFINIÇÃO DO CONTEXTO

Na definição do contexto são definidos os parâmetros gerais da gestão de riscos os quais envolvem desde os critérios básicos para abordagem, avaliação, impacto e aceitação dos riscos até o escopo e organização. Tanto os fatores externos como internos devem ser considerados e, é essencial determinar o propósito da gestão de riscos de segurança da informação, pois este impacta em todo o processo.

O critério para abordagem depende do escopo e dos objetivos da gestão de riscos desejado na organização. Para avaliação, é importante considerar o valor estratégico para o negócio; a criticidade dos ativos envolvidos; requisitos legais e regulatórios, bem como as obrigações contratuais; a importância da disponibilidade, confidencialidade e integridade e; as percepções e consequências negativas a valor de mercado, a imagem e a reputação.

Critérios de impacto devem ser desenvolvidos e especificados com base no dano ou custo causado à organização em decorrência de um evento de segurança da informação, levando em consideração nível de classificação do ativo; ocorrências de violação; operações afetadas; perda de oportunidades; não cumprimento de prazos; dano à reputação e; violação de requisitos legais, regulatórios ou contratuais.

Os critérios para aceitação dos ricos estão fortemente associados a política, metas e objetivos da organização. Neste critério, é importante que a organização defina sua própria escala do nível de aceitação do risco e que itens como operações; tecnologia; finanças e; fatores sociais e humanitários sejam considerados.

O escopo e limites garantem que todos os ativos relevantes sejam considerados no processo de avaliação de riscos. É importante também que justificativas para qualquer exclusão de ativos do escopo sejam apresentadas.

Por fim, uma organização apropriada deve estabelecer e manter as responsabilidades sobre os processos de gestão de riscos de segurança e garantir que estes sejam aprovados pelos gestores responsáveis.

2.2 PROCESSO DE AVALIAÇÃO DE RISCOS

O processo de avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades existentes ou possíveis de existir, identifica os controles atuais e seus efeitos sobre o risco apontado, determina as consequências possíveis e, por fim, prioriza os riscos, ordenando-os conforme os critérios de avaliação de riscos estabelecidos previamente na definição do contexto.

Este processo é composto por três atividades: identificação dos riscos, análise dos riscos e avaliação dos riscos. “Se as informações obtidas forem suficientes para tomar as medidas necessárias para a redução dos riscos a níveis aceitáveis, inicia-se o tratamento dos riscos. Caso contrário, inicia-se nova análise/avaliação de riscos, incluindo uma revisão do contexto estabelecido inicialmente” (OHTOSHI, 2008, p. 29).

Dentre as definições de risco, a apresentada pela ABNT NBR ISO/IEC 31000:2009, é que o risco é o efeito da incerteza nos objetos. O risco é uma condição inerente a toda organização, sendo acompanhado de fatores que podem afeta-lo positivamente, de forma a mitiga-lo ou ainda negativamente, fazendo com que este risco que materialize. “É importante saber que o risco é uma possibilidade, situação que difere ao perigo, pois, perigo é a origem de uma perda. Portanto, na análise e avaliação de riscos, os fatores e os próprios riscos devem ser tratados para que os perigos não se concretizem” (PIAZZA, 2015, p. 4).

Para tanto, é fundamental que os riscos sejam identificados, quantificados ou descritos qualitativamente, tendo priorização conforme critérios de avaliação em relevância as definições da organização, através de sua alta gestão.

O propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial, deixando claro o como, onde e por que dela acontece. É importante que

todos os ativos que fazem parte do escopo sejam identificados e, quanto maior o grau de detalhamento, maior também será a quantidade geral de informações reunidas durante o processo de avaliação de riscos.

Um ativo é algo que tem valor para a organização e que, portanto, requer proteção. Para a identificação dos ativos convém que se tenha em mente que um sistema de informação compreende mais do que *hardware* e *software* (ABNT NBR ISO/IEC 27005, 2011).

A identificação das ameaças é a segunda etapa da identificação de riscos. Uma ameaça tem o potencial de comprometer ativos e, consequentemente, todo uma organização. Ela por ser de origem natural ou humana, podendo ser acidental ou intencional.

A terceira etapa é a identificação dos controles existentes. Esta etapa tem por objetivo evitar custos e trabalho desnecessários e, assegurar que os mesmos estão funcionando corretamente pois, um controle que não funciona como esperado, pode provocar o surgimento de uma vulnerabilidade. A eficiência de um controle pode ser medida pela redução causada a probabilidade de ocorrência da ameaça, pelo grau de facilidade de exploração de uma vulnerabilidade ou, pelo impacto causado pelo incidente.

Como penúltima etapa tem-se a identificação das vulnerabilidades, a qual tem como base uma relação das ameaças conhecidas, dos ativos e dos controles existentes. É importante destacar que, a presença de uma vulnerabilidade não causa prejuízo por si só, é necessário existir uma ameaça para explora-la logo, uma vulnerabilidade sem ameaça, pode não requerer a implementação de um controle.

Por fim, a identificação das consequências, busca identificar os prejuízos ou mesmo consequências para a organização, em decorrência de um cenário de incidente.

As cinco etapas citadas anteriormente estão relacionadas à atividade de identificação dos riscos. A próxima atividade é a de análise de riscos. Ela possui quatro etapas, na qual a primeira é a de escolha da metodologia.

Uma metodologia para análise de riscos pode ser qualitativa, quantitativa ou ainda, uma combinação de ambas. Na prática, a análise qualitativa é mais frequentemente utilizada, devido ao seu menor grau de complexidade e custo de realização.

A segunda etapa é de avaliação das consequências, e leva em consideração a relevância dos ativos e do impacto para o negócio. A relevância do ativo (valoração) é baseada na criticidade e importância deste ativo para a realização dos objetivos de negócio da

organização. Já o impacto pode ser expresso de forma qualitativa ou quantitativa, porém um método para designar valores monetários pode fornecer informações mais relevantes para a tomada de decisões.

Como terceira etapa tem-se a avaliação da probabilidade dos incidentes, na qual cenários de incidentes são apresentados com base na identificação da ameaça, dos ativos afetados, das vulnerabilidades exploradas e das possíveis consequências para o negócio. É incluído também todos os controles existentes e seu grau de eficácia.

A última etapa é a determinação do nível de risco, utilizando também métodos quantitativos ou qualitativos. Pode designar valores para a probabilidade e consequências de um risco, bem como considerar o custo-benefício. O risco estimado é uma combinação da probabilidade de um cenário de incidente e suas consequências.

Como última atividade tem-se a avaliação de riscos. É importante que o critério utilizado seja consistente com o contexto. As decisões tomadas durante esta atividade são baseadas principalmente no nível de risco aceitável, mas convém também que as consequências, probabilidade e grau de confiança da identificação e análise de riscos, sejam considerados.

2.3 TRATAMENTO DO RISCO

Na atividade de tratamento do risco, as medidas para reduzir os riscos previamente identificados são selecionadas e implantadas de modo a manter os níveis de risco em patamares aceitáveis estabelecidos pelo critério de risco (OHTOSHI, 2008).

A norma apresenta quatro opções para o tratamento do risco: modificação, retenção, ação de evitar e compartilhamento. A Figura 3 ilustra esta atividade de tratamento do risco dentro do processo de gestão de risco apresentado na Figura 2.

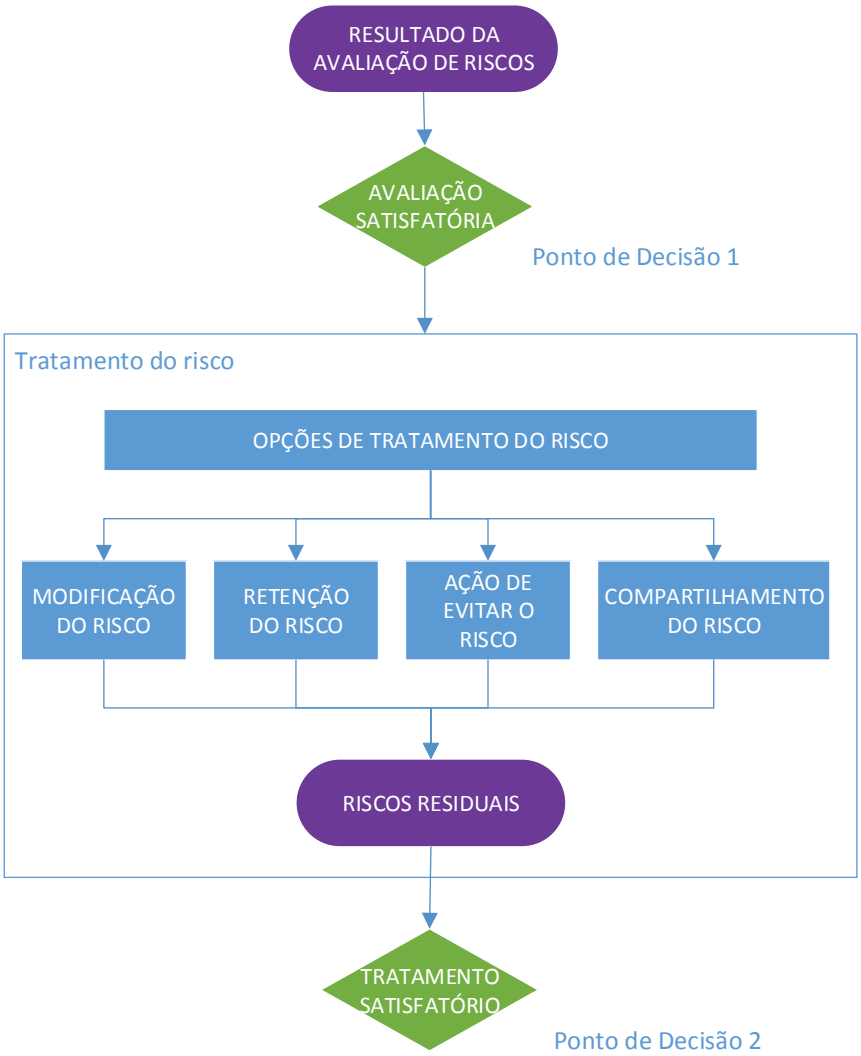

Figura 3 - Atividade de tratamento do risco da ABNT NBR ISO/IEC 27005:2011

Fonte: ABNT NBR ISO/IEC 27005 (2011)

É importante que as opções de tratamento do risco sejam escolhidas não somente com base no resultado obtido no processo de avaliação de riscos, mas também considerando os custos estimados para sua implementação e o retorno esperado. Cabe destacar também que as quatro opções não são mutuamente exclusivas, ou seja, podem ser combinadas de modo a trazer o melhor benefício para a Instituição.

A opção de modificação do risco busca, por meio da inclusão, exclusão ou mesmo alteração de controles, apresentar um risco residual que possa ser reavaliado e então considerado aceitável. Com base nos controles selecionados pode-se obter diferentes tipos de proteção como: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização. Cabe considerar o custo do controle em relação ao ativo protegido. É importante destacar também que existem restrições

que podem afetar a seleção de controles e, dentre elas estão as: temporais, financeiras, técnicas, operacionais, culturais, éticas, ambientais, legais, de recursos humanos e facilidade de uso.

Uma segunda opção para o tratamento do risco é realizar a sua retenção e, sua escolha deve ser tomada com base na avaliação de riscos. Caso o nível de risco atenda aos critérios de aceitação, não há necessidade de se implementar controles adicionais, ocorrendo desta forma a retenção do risco.

A terceira opção da atividade de tratamento do risco é a ação de evitar. Isto se dá pela eliminação da atividade ou condição que dava origem a este risco. Esta opção deve ser considerada quando o risco for muito elevado, assim como os custos para implementação de outros tratamentos excedam os benefícios.

Como quarta e última opção tem-se o compartilhamento do risco, que busca envolver uma entidade externa que possa gerencia-lo de forma mais eficaz. Este compartilhamento pode ser feito por um seguro que cubra as consequências ou pela contração de um parceiro que tem o papel de monitorar e tomar ações proativas. Pode-se destacar dois pontos importantes desta opção de tratamento do risco. O primeiro, é que ela pode criar novos riscos ou modificar riscos existentes, podendo ser necessário um novo tratamento do risco. O segundo é que apesar de compartilhar a responsabilidade de gerenciamento do risco, a responsabilidade legal pelo impacto causado não é compartilhada.

2.4 ACEITAÇÃO DO RISCO

A aceitação do risco, consiste em entender e trabalhar com ele independente do seu nível de criticidade e, a decisão por aceitar um risco deve ser formalmente registrada, juntamente com a responsabilidade pela decisão.

Os critérios adotados para aceitação do risco podem ser complexos e ir muito além de apenas determinar se um risco residual está acima ou abaixo dos limites pré-definidos. Os critérios devem ser revistos, caso o nível de um risco residual pode atenda aos critérios previamente estabelecidos para aceitação do risco. Em não sendo possível rever os critérios para a aceitação do risco, o responsável deve justificar sua decisão por passar por cima dos critérios normais estabelecidos para a aceitação do risco.

2.5 COMUNICAÇÃO E CONSULTA DO RISCO

A comunicação do risco tem como objetivo alcançar o consenso sobre como os riscos devem ser gerenciados. É fundamental o compartilhamento das informações sobre os riscos entre os responsáveis de decisão e as demais partes interessadas. Esta comunicação deve incluir, entre outras, informações sobre a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos.

Uma comunicação eficaz é fundamental, primeiramente porque pode refletir nas decisões tomadas, em segundo, para assegurar um bom entendimento entre os responsáveis pela implementação da gestão de riscos, e aqueles com interesses reais de direito.

> A gestão de riscos pode ter diversas partes interessadas. Estas partes devem ser identificadas e seus papéis e responsabilidades delimitados na fase de Comunicação do Risco. É importante desenvolver um plano de comunicação que permita a cada uma destas partes conhecer o andamento do processo e fornecer subsídios para seu desenvolvimento. (BRANDÃO e FRAGA, 2008, p. 12).

A percepção do risco pode variar devido a diferenças de suposições, conceitos, necessidades, interesses e preocupações das partes interessadas quando lidam com o risco. As partes interessadas farão julgamentos sobre a aceitabilidade do risco, tendo como base suas próprias percepções. Neste caso, é essencial garantir que estas percepções também sejam identificadas e documentadas.

Por fim, conforme a normal ABNT NBR ISO/IEC 27005:2011 (2011, p. 31) convém que a comunicação do risco seja realizada a fim de:

a) Fornecer garantia do resultado da gestão de riscos da organização
b) Coletar informações sobre os riscos
c) Compartilhar os resultados do processo de avaliação de riscos e apresentar o plano de tratamento do risco
d) Evitar ou reduzir tanto a ocorrência quanto as consequências das violações de segurança da informação que aconteçam devido à falta de entendimento mútuo entre os responsáveis pela decisão e as partes interessadas
e) Dar suporte ao processo decisório
f) Obter novo conhecimento sobre a segurança da informação

g) Coordenar com outras partes e planejar respostas para reduzir as consequências de um incidente

h) Dar aos responsáveis pela decisão e às partes interessadas um senso de responsabilidade sobre riscos

i) Melhorar a conscientização

2.6 MONITORAMENTO E ANÁLISE CRÍTICA DE RISCOS

O monitoramento considera o risco como um elemento não estático, ou seja, com características mutáveis. As ameaças, as vulnerabilidades, a probabilidade ou as consequências podem mudar rapidamente, sem qualquer indicação prévia e, é neste cenário que o monitoramento constante se faz necessário.

É fundamental que os riscos e seus fatores como valores dos ativos, impactos, ameaças, vulnerabilidades e probabilidade de ocorrência sejam monitorados e analisados de forma crítica, com o objetivo de identificar, o mais rapidamente possível, eventuais mudanças no contexto da Instituição e para manter uma visão geral dos riscos.

Novas ameaças, vulnerabilidades e mudanças na probabilidade ou nas consequências podem alterar a situação dos riscos considerados aceitáveis. O monitoramento constante e a análise crítica podem contribuir para a melhoria do processo de gestão de riscos. Convém que não somente as atividades de monitoramento de riscos sejam repedidas regularmente, mas também que as opções escolhidas para o tratamento do risco sejam periodicamente revistas.

3 MÉTODOS E PROCEDIMENTOS

3.1 DELINEAMENTO DA PESQUISA

De acordo com Vergara (2007), os tipos de pesquisa podem ser definidos por dois critérios básicos: quanto aos fins e quanto aos meios. Quanto aos fins, a pesquisa foi do tipo aplicada, pois ainda segundo Vergara (2007) é motivada pela necessidade de resolver problemas que já existam na prática, seja de forma imediata, ou não. Tem, portanto, finalidade prática, ao contrário da pesquisa pura, motivada basicamente pela curiosidade intelectual do pesquisador e situada, sobretudo no nível da especulação.

Quanto aos meios, esta pesquisa foi bibliográfica e também um estudo de caso. Bibliográfica, pois abordou a gestão de risco sob a ótica da ABNT NBR ISO/IEC 27005:2011, analisando a Instituição escolhida. Também foi um estudo de caso, pois o conhecimento adquirido no estudo bibliográfico foi utilizado em uma aplicação experimental em uma Instituição de Ensino Superior, com vistas a observar os aspectos relacionados à gestão de segurança da informação, com escopo restrito a rede Wi-Fi, realizando análise e avaliação dos riscos e propondo ações para tratamento.

As ações propostas foram submetidas à avaliação dos participantes da pesquisa. A estratégia de pesquisa adotada caracterizou-se por ser um estudo de caso único. Yin (2010) defende que o estudo de caso é um conjunto de questões substantivas que refletem a investigação real, ou seja, quando se quer verificar algum conceito em uma situação.

Entretanto, um trabalho de pesquisa pode ser classificado também quanto a sua natureza ou abordagem. Este trabalho possui natureza qualitativa, pelo fato de ser caracterizada pela interpretação dos fenômenos e atribuição de significados atribuídos pelo autor, não fazendo uso de métodos e técnicas estatísticas (GIL, 2010).

3.2 DEFINIÇÃO DA ÁREA E PARTICIPANTES DA PESQUISA

A pesquisa foi realizada com membros da área de TI da Instituição como: Operações, Controles Internos e *Compliance*. Estes colaboradores foram escolhidos pelo fato de possuírem poder nas decisões relacionadas à tecnologia, segurança e processos.

Para participar da entrevista (APÊNDICE A), foram selecionados o Coordenador de Operações de TI, responsável pelas áreas de *Service Desk* e Suporte, a Analista de Controles Internos, responsável pela elaboração das políticas e procedimentos que envolvem TI e o Gerente de *Compliance* de TI, responsável por garantir que as Instituições da Rede estão seguindo com as políticas e procedimentos adotados.

3.3 TÉCNICAS DE COLETA DE DADOS

Os dados aqui apresentados foram coletados pelo autor deste trabalho durante o seu dia-a-dia na Instituição. O autor, como participante ativo das decisões sobre o tema e escopo, tem acesso aos dados e materiais aqui citados.

Quanto ao estudo de caso, foram utilizados para coleta de dados as seguintes fontes:

a) Análise de documentos – o estudo dos documentos relacionados à Instituição, além dos requisitos de *Compliance* aos quais a mesma está sujeita, para que o estudo da gestão de segurança da informação possa se dar de forma adequada, considerando suas particularidades. Os documentos analisados foram:
    - Procedimento Controle de Acesso Lógico (v4.0);
    - Procedimento Gestão de Mudanças (v5.0);
    - Procedimento Equipamento Notebook e Tablet (v1.0); e
    - Procedimento Dispositivos Moveis – Celular (v1.0).
b) Observação direta – observações no ambiente, com o objetivo de verificar a efetividade das ações de segurança da informação, como também as eventuais ausências de medidas e procedimentos relativos a esta segurança.

c) Entrevistas – foram realizadas entrevistas individuais no mês de junho de 2015. As mesmas foram realizadas conforme disponibilidade de tempo de cada um dos participantes, tendo como objetivo identificar as percepções de cada um sobre o cenário atual e validar ações propostas neste trabalho. Cada uma das entrevistas foi realizada pessoalmente e teve duração de 40 minutos. As respostas dos entrevistados foram sendo registradas simultaneamente pelo autor.

3.4 TÉCNICAS DE ANÁLISE DE DADOS

Após realizada avaliação do cenário atual, os dados coletados foram confrontados com as recomendações apresentadas na ABNT NBR ISO/IEC 27005:2011, com a técnica de análise de conteúdo. A análise de conteúdo é

> (...) um conjunto de técnicas de análise das comunicações visando obter, por procedimentos sistemáticos e objetivos de descrição dos conteúdos das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção / recepção (variáveis inferidas) destas mensagens. (BARDIN, 1977, p. 42)

Os resultados obtidos após a execução do fluxo do processo de gestão de gestão de risco, foram apresentados aos participantes durante a entrevista, de modo que estes avaliassem a proposta e expusessem suas considerações. As opiniões dos participantes da entrevista foram coletadas individualmente e analisadas de forma consolidada.

4 ESTUDO DE CASO

Este capítulo dedica-se a descrever o ambiente; apresentar a prática de gestão de segurança atualmente aplicadas na Instituição; traz também a análise, avaliação e tratamento dos riscos com base na norma ABNT NBR ISO/IEC 27005:2011; e fecha com a avaliação dos dados das entrevistas.

4.1 DESCRIÇÃO DO AMBIENTE

A Instituição oferece atualmente acesso Wi-Fi em todos os seus Campi. A cobertura é abrangente, não ficando restrita as salas de aulas, mas podendo ser acessível de áreas comuns como restaurantes, auditórios, pátios, estacionamento e, em alguns casos, alguns metros fora das dependências do campus.

A tecnologia utilizada oferece uma gerência de forma centralizada e, o acesso dos alunos à rede Wi-Fi é realizado via um portal de autenticação, também chamado de *Captive Portal*[4]. Apenas com um usuário/senha previamente cadastrados na base de autenticação é possível ingressar na rede.

O acesso pode ser realizado todos os dias da semana, sem restrição quanto ao horário de conexão, ou seja, a rede Wi-Fi tem seu acesso disponibilizado 24x7. Não é fornecido acesso anônimo, mas a comunidade pode obter acesso mediante um portal, no qual é realizado o cadastro prévio com nome, CPF e data de expiração. Com estes dados, um usuário e senha são gerados e a conta fica ativa dentro da data de expiração.

Dados de acesso, como horário, usuário, ponto de acesso, endereço MAC, endereço IP, endereço web, são armazenados e possibilitam o rastreamento caso necessário. Esta navegação passa por um sistema de Firewall que pode bloquear determinados sites, conforme política interna da Instituição. As etapas descritas até então podem ser observadas no fluxo apresentado pela Figura 4.

---

[4] *Captive Portal* é uma página Web que usuários necessitam visualizar, interagir e autenticar, antes do acesso a rede ser concedido. (TECHTARGET01, 2015).

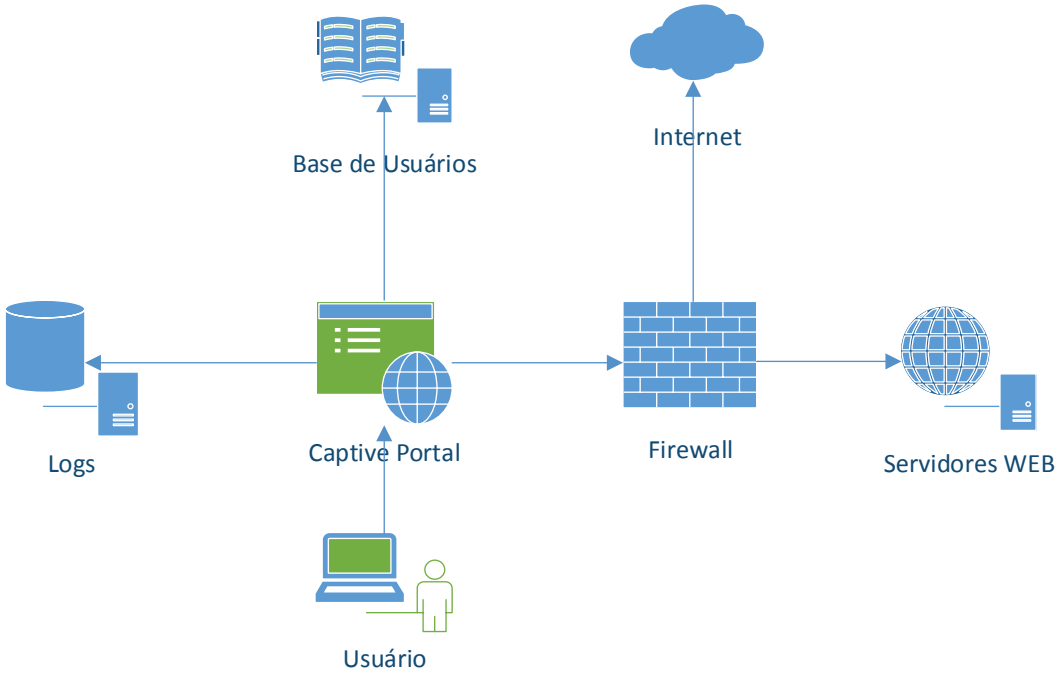

Figura 4 – Diagrama lógico do acesso a rede Wi-Fi.

Fonte: Elaborado pelo autor (2015).

O ambiente Wi-Fi foi projetado como uma rede isolada das demais redes da Instituição, permitindo acesso à Internet e aos portais públicos. Este projeto também impede que os computadores e dispositivos móveis como *smartphones* e *tablets* tenham acesso entre si.

Complementando o fluxo apresentado pela Figura 4, o diagrama físico de rede apresentado na Figura 5, busca exemplificar as conexões e os ativos de redes envolvidos no ambiente Wi-Fi da Instituição.

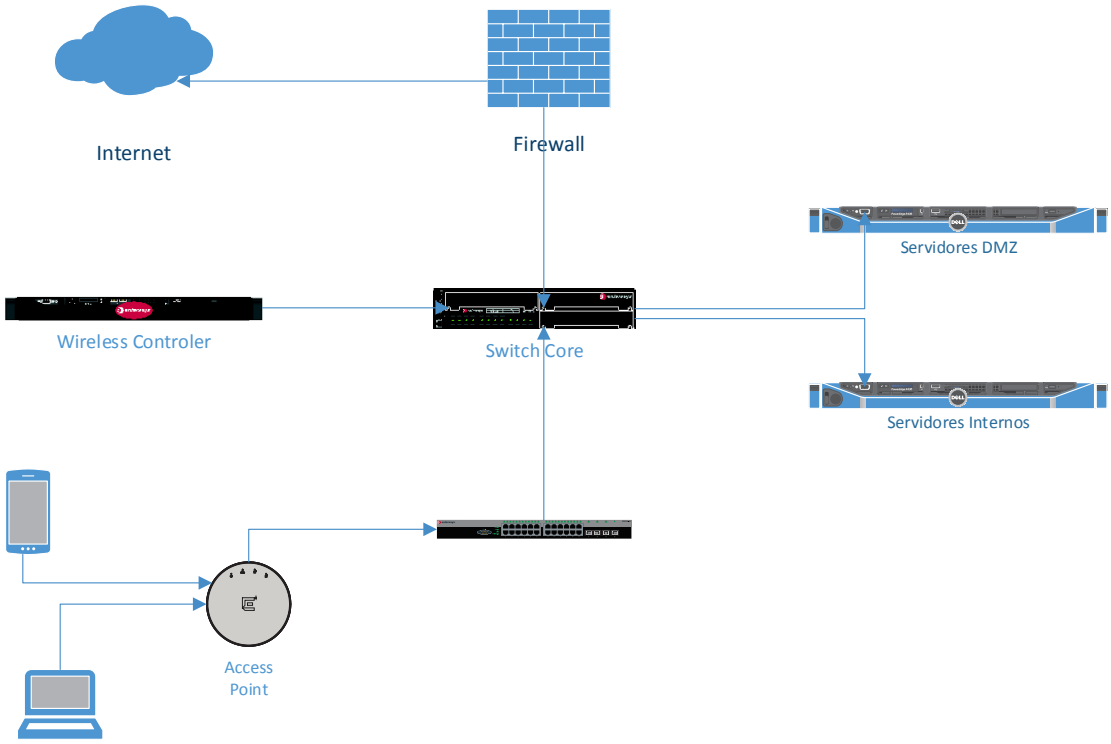

Figura 5 – Diagrama físico de acesso a rede Wi-Fi.

Fonte: Elaborado pelo autor (2015)

A instalação física inicial de cada *Access Point* foi definida com base em um *Site Survey*[5]. Esta análise indicou o melhor local para instalação, levando também em consideração o número de usuários suportados por cada equipamento e as áreas de cobertura desejadas, de modo a evitar pontos de sombra. A Figura 6 busca representar este fluxo como trabalhado hoje.

[5] S*ite survey*, algumas vezes também chamado de RF *site survey* ou *wireless survey*, é o processo de projeto e planejamento de uma rede wireless, de modo a entregar uma solução que forneça cobertura, boa taxa de transferência de dados, capacidade de atender o volume de usuários e também a possibilidade de *roaming*. (WIKIPEDIA01, 2015).

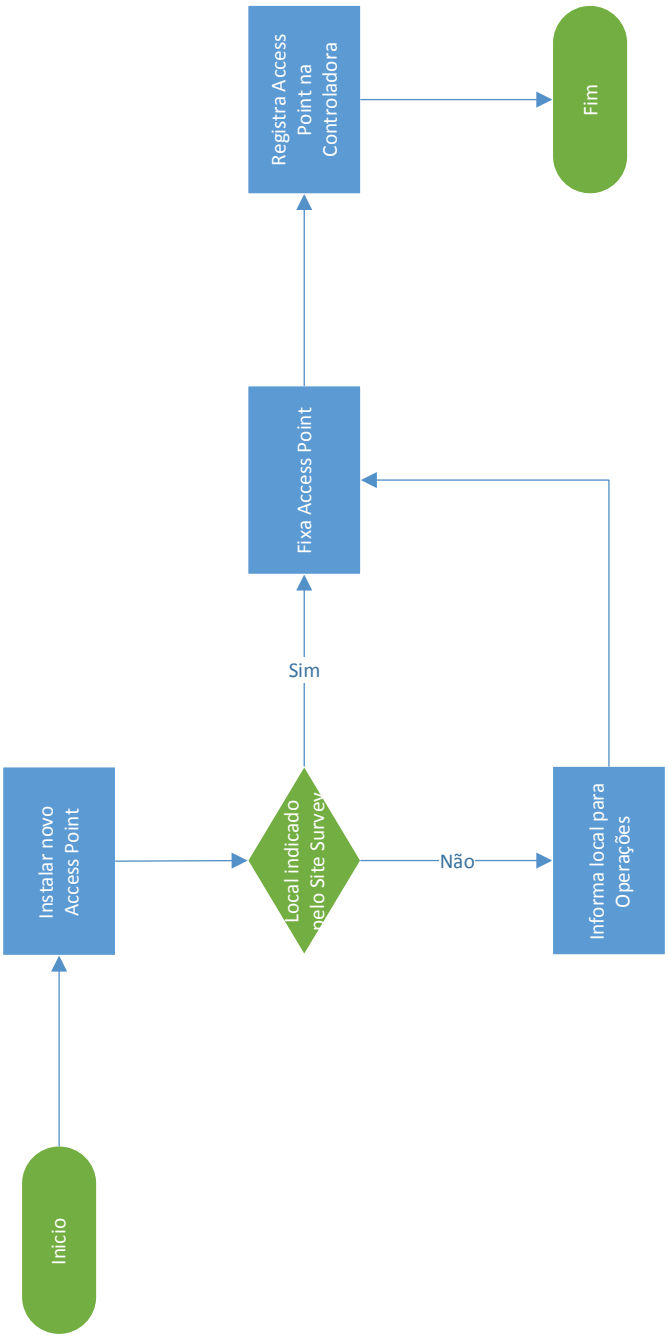

Figura 6 – Fluxo do processo de instalação de um novo *Access Point*.

Fonte: Elaborador pelo autor (2015)

Apesar das informações apresentadas até então representarem o padrão de configuração, durante a observação foram identificadas algumas exceções que podem gerar risco a Instituição.

Mesmo a rede Wi-Fi sendo isolada, permitindo acesso apenas à Internet e aos portais públicos, existem casos em que liberações foram feitas para possibilitar o acesso a recursos

internos e de conteúdo considerado sensível. Não foi possível constatar se todas as liberações foram aprovadas, o que indica um desvio/falha do procedimento de gestão de mudança.

Outro ponto importante está ligado a autenticação dos usuários. Mesmo o usuário sendo nominal, de forma que se pode rastrear o dono da conta utilizada para autenticação, mas ocorre que atualmente, a configuração definida no ambiente, não impede que um mesmo usuário acesse mais de um dispositivo simultaneamente. Também foram identificadas exceções para eventos abertos que ocorrem nos campi, onde um mesmo usuário e senha são criados especificamente para o evento e divulgado para todos os participantes. Esta exceção e seus controles compensatórios não estão descritos no procedimento de controle de acesso lógico.

Pode-se observar também que, mesmo com dados de acesso sendo armazenados, o histórico para auditoria é não superior a 24 horas. Desta forma, pode não ser possível rastrear um acesso que tenha realizado uma tentativa de ataque, seja ela bem-sucedida ou não.

Existem também duas outras redes Wi-Fi criadas que não utilizam o *Captive Portal* como método de autenticação, mas sim uma chave de acesso no padrão WPA2[6]. Estas redes possuem um perfil específico e foram criadas para atender a necessidade de duas disciplinas, nas quais os equipamentos não são compatíveis com o método via *Captive Portal* e, que também precisam trocar informações entre si. A chave gerada para estas redes é de conhecimento da equipe de suporte de TI, responsável por digita-la nos dispositivos que precisam ingressar nestas redes.

O último ponto diz respeito a instalação dos pontos de acesso que, apesar da realização de um *Site Survey* indicar o melhor ponto de instalação, foi possível identificar que em alguns casos o equipamento não está instalado no lugar recomendado e que, quando necessária esta realocação, a documentação não se encontrava atualizada.

[6] WPA2 é um protocolo de segurança e um programa de certificação de segurança desenvolvido pela Wi-Fi Alliance para garantir a segurança de rede *wireless* de computadores. (WIKIPEDIA02, 2015).

4.2 PRÁTICA DE GESTÃO DE SEGURANÇA

A Instituição possui em seu organograma uma área de auditoria interna, que trabalha a gestão da segurança, em conjunto com as demais áreas da TI (Desenvolvimento, Infraestrutura, Suporte e *Service Desk*).

As polícias e procedimentos ficam publicadas na Intranet para consulta dos colaboradores. Já os alunos obtêm acesso à política de acesso de Wi-Fi, no portal de autenticação (*Captive Portal*)

Os documentos internos analisados para este cenário foram:

a) Procedimento Controle de Acesso Lógico (v4.0)

b) Procedimento Gestão de Mudanças (v5.0)

c) Procedimento Equipamento *Notebook* e *Tablet* (v1.0)

d) Procedimento Dispositivos Móveis – Celular (v1.0)

A área de infraestrutura tem a responsabilidade de garantir que as políticas e procedimentos sejam seguidos.

Dependendo do recurso computacional, a área de Controles Internos realiza ações de auditoria, que variam em períodos (mensal, trimestral ou semestral). Os resultados são enviados para validação da equipe de *Compliance* que afere se os controles estão sendo executados conforme proposto e se continuam efetivos.

4.3 ANÁLISE E AVALIAÇÃO DOS RISCOS

Com base na análise realizada no ambiente, foi adotado um enfoque de alto nível e uma abordagem qualitativa para definição do nível de risco.

No enfoque de alto nível, os ativos, ameaças, probabilidade, impacto e consequentemente os riscos, serão abordados de uma perspectiva mais ampla. Com o uso de

uma abordagem qualitativa, se define o Nível de Risco[7] (NR) multiplicando o Nível de Impacto (NI), Nível de Probabilidade (NP) e Nível de Ameaça (NA).

Para simplificar o valor resultante do produto NI x NP x NA, os níveis muito baixo (MB) e muito alto (MA) não foram considerados para o Nível de Impacto e o Nível de Probabilidade. O Quadro 1 apresenta a Matriz de Risco e o valor obtido possibilita identificar o nível de risco conforme o Quadro 2.

NA (Nível da Ameaça)		Baixo (1)			Média (2)			Alto (3)		
NP (Nível de Probabilidade)		B (1)	M (2)	A (3)	B (1)	M (2)	A (3)	B (1)	M (2)	A (3)
NI (Nível de Impacto)	B (1)	1	2	3	2	4	6	3	6	9
	M (2)	2	4	6	4	8	12	6	12	18
	A (3)	3	6	9	6	12	18	9	18	27

Quadro 1 - Matriz de Risco

Fonte: Adaptado pelo autor com base na ABNT NBR ISO/IEC 27005 (2011)

Nível do Risco	Valor do Risco
Risco Baixo	Entre 1 e 6
Risco Médio	Entre 8 e 12
Risco Alto	Entre 18 e 27

Quadro 2 - Classificação de Risco

Fonte: Elaborado pelo autor com base na ABNT NBR ISO/IEC 27005 (2011)

Considerando as informações aqui presentadas e também a descrição do ambiente, foi elaborada a matriz de análise de risco, vista no Quadro 3 a seguir.

[7] Fórmula: NR = NI x NP x NA

Análise de Riscos								
Identificação					Estimativa			
ID	Ativo	Vulnerabilidade	Ameaça	Impacto	NI	NP	NA	NR
NR01	Firewall	Inexistência de um controle eficaz de mudança	Alteração de configuração sem aprovação	Comprometimento/Indisponibilidade dos serviços	3	1	3	9
NR02	Infraestrutura	Documentação desatualizada	Erro durante o uso	Comprometimento/Indisponibilidade dos serviços	3	3	1	9
NR03	Controladora Wireless	Múltiplos logins de um mesmo usuário em diferentes dispositivos.	Não identificação da pessoa vinculada ao usuário em caso de solicitação legal	Perda de confiabilidade	3	3	2	18
NR04	Controladora Wireless	Acesso não autenticado utilizando chave de acesso WPA2	Não identificação da pessoa vinculada ao usuário em caso de solicitação legal	Perda de confiabilidade	2	2	2	8
NR05	Controladora Wireless	Tempo reduzido de retenção de logs	Não identificação da pessoa vinculada ao usuário em caso de solicitação legal	Perda de confiabilidade	3	3	2	18
NR06	Controladora Wireless	Equipamento sem redundância / Ponto único de falha	Falha do equipamento	Indisponibilidade do serviço	1	2	1	2
NR07	Controladora Wireless	Acesso permitido entre dispositivos conectados via chave de acesso WPA2	Roubo de informação	Perda da confidencialidade Passível de ação penal	3	2	3	18
NR08	Controladora Wireless	Acesso fora do horário comercial e de operação da TI	Não identificação da pessoa vinculada ao usuário em caso de solicitação legal	Comprometimento/Indisponibilidade dos serviços	2	3	2	12
NR09	Servidores	Acesso a conteúdo sensível	Roubo de informação	Perda da confidencialidade Passível de ação penal	3	2	3	18

Quadro 3 - Análise de Riscos

Fonte: Elaborado pelo autor com base na ABNT NBR ISO/IEC 27005 (2011)

Ao final foi verificado que a análise e avaliação dos riscos gerou resultados satisfatórios, não sendo necessária uma nova interação do processo de gestão de riscos com o objetivo de se obter um maior detalhamento.

A lista gerada e apresentada no Quadro 3, foi priorizada conforme seu nível de risco e impacto para tratamento, na atividade de tratamento dos riscos apresentada a seguir.

4.4 TRATAMENTO DOS RISCOS

Os riscos identificados na fase de análise e avaliação foram priorizados e seu resultado pode ser verificado no Quadro 4, que traz os riscos ordenados segundo a ordem prioridade para tratamento.

Prioridade	ID	Vulnerabilidade	NR
1	NR09	Acesso a conteúdo sensível	18
2	NR03	Múltiplos *logins* de um mesmo usuário em diferentes dispositivos	18
3	NR05	Tempo reduzido de retenção de logs	18
4	NR07	Acesso permitido entre dispositivos conectados via chave de acesso WPA2	18
5	NR08	Acesso fora do horário comercial e de operação da TI	12
6	NR01	Inexistência de um controle eficaz de mudança	9
7	NR02	Documentação desatualizada	9
8	NR04	Acesso não autenticado utilizando chave de acesso WPA2	8
9	NR06	Equipamento sem redundância / Ponto único de falha	2

Quadro 4 - Priorização dos riscos

Fonte: Elaborado pelo autor com base na ABNT NBR ISO/IEC 27005 (2011)

Com exceção do risco com ID NR06, que se encontrava dentro do nível de risco aceitável e foi tratado utilizando o critério de retenção, todos os demais foram tratados pela opção de modificação do risco, visando trazê-lo para níveis aceitáveis. As ações consideradas para estes riscos estão descritas:

a) Bloqueio imediato da regra que permite o acesso a partir da rede Wi-Fi aos portais internos.

b) Ativação do protocolo 802.1x[8] para rede Wi-Fi, possibilitando atribuição de endereçamento IP com base no usuário autenticado.

c) Restringir para 4 o número máximo de dispositivos em que um mesmo usuário pode estar conectado.

d) Restringir acesso entre 0h e 6h.

e) Ativar autenticação por endereço MAC para os dispositivos que não possuem suporte a *Captive Portal*.

f) Ativar NAC[9], permitindo o ingresso na rede via WPA2, apenas se o equipamento estiver com firewall ativado.

g) Aprimorar o procedimento de gestão de mudanças.

h) Adequar o procedimento de controle de acesso lógico.

Buscando exemplificar, o fluxo do processo de instalação de um novo ponto de acesso foi redesenhado e apresentado na Figura 7 de maneira a garantir que siga o processo de gestão de mudança e para que a documentação seja atualizada.

[8] 802.1x é um padrão IEEE para acesso autenticado à rede cabeada e sem fio. O protocolo melhora a segurança fornecendo suporte para identificação centralizada de usuário, autenticação e gerenciamento dinâmico de chaves. (MICROSOFT, 2015).

[9] NAC, também chamado de controle de admissão de rede, é um método que reforça a segurança de uma rede, restringindo a disponibilidade dos recursos para os terminais clientes que não estejam em conformidade com a política de segurança definida. (TECHTARGET02, 2015).

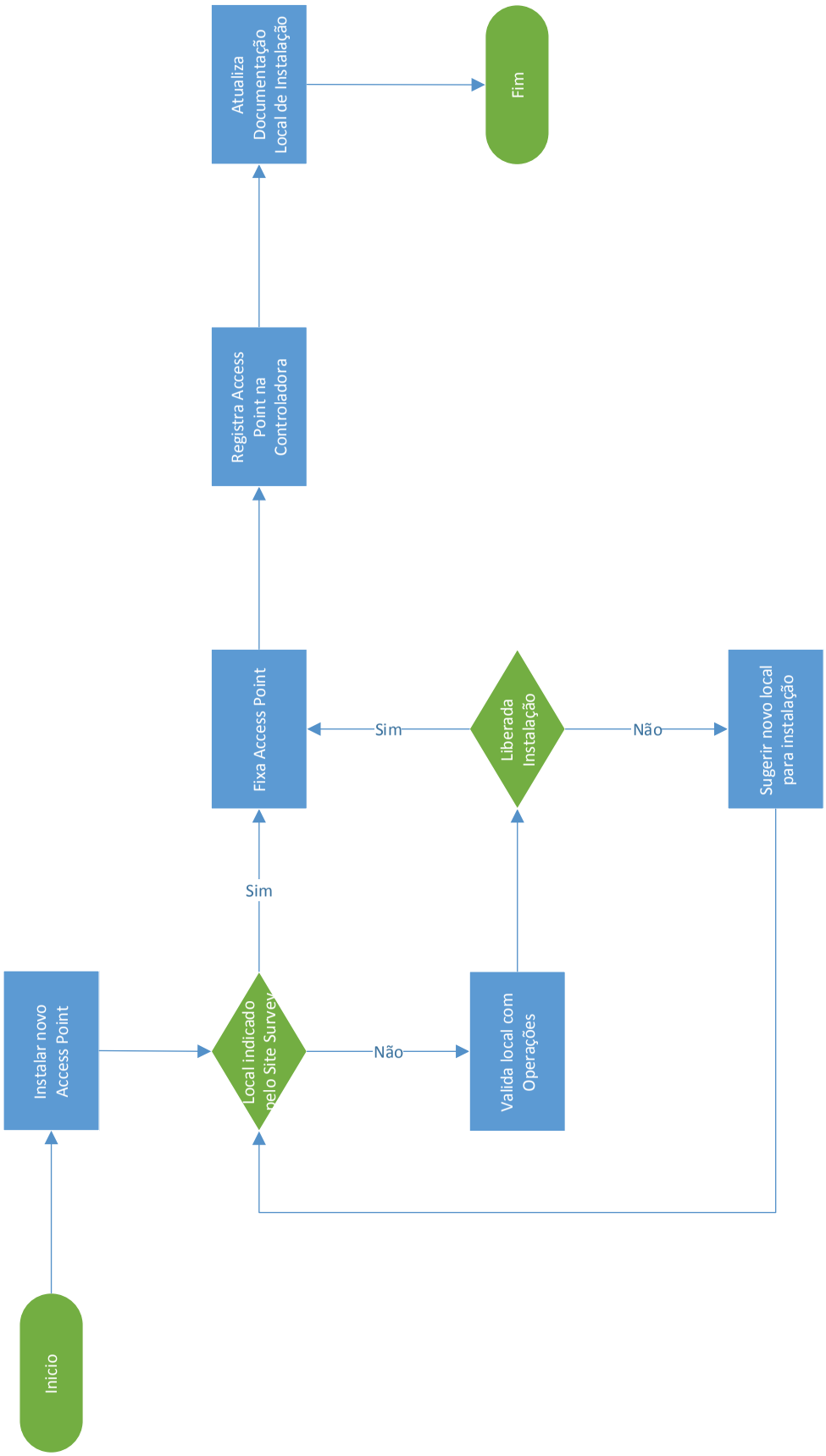

Figura 7 – Novo fluxo do processo de instalação de um novo *Access Point*

Fonte: Elaborado pelo autor (2015).

Neste novo fluxo foram incorporados a validação/aprovação, por parte da área de Operações, para instalação de um AP fora do local indicado pelo *Site Survey*. Sem esta aprovação, o equipamento não é instalado. Outro ponto importante é a atualização da documentação para futuras consultas.

As demais ações utilizadas para tratamento dos riscos levantados, estão associadas a ajustes de configuração e implantação de novas funcionalidades no ambiente, assim como aprimoramento e criação de controles para monitoramento dos procedimentos de gestão de mudança e controle de acesso lógico.

4.5 VALIDAÇÃO DA ANÁLISE E TRATAMENTO DOS RISCOS

Todas as informações levantadas do ambiente, bem como a análise, avaliação e tratamento dos riscos proposto foram apresentados para conhecimento e consideração do Coordenador de Operações, da Analista de Controles Internos e do Gerente de *Compliance*.

Ao se apresentar as informações, buscou-se deixa claro o escopo ao qual ela estava restrita e, que o trabalho seguiu as recomendações da ABNT NBR ISO/IEC 27005:2011 para realizar a análise, avaliação e o tratamento dos riscos.

Iniciando pelo ambiente, todos consideraram que a Instituição está passando por um momento importante de adaptação e que os controles e procedimentos precisam ser ajustados. O Gerente de *Compliance* exemplificou este momento de adaptação e busca do aprimoramento, destacando o recente cargo criado e ocupado pela Analista de Controles Internos. Foi citado também pelo Coordenador de Operações e pela Analista de Controles Internos que ações de engajamento da equipe para seguir os procedimentos e também as ações de auditoria para identificar possíveis falhas na execução dos mesmos.

O Coordenador de Operações demonstrou certa surpresa, mas salientou que os pontos de exceção apresentados do ambiente podem sem corrigidos com ajustes de configuração e dos procedimentos.

Seguindo com a apresentação, foi mostrado o quadro de análise de riscos no qual o Gerente de *Compliance* reforçou a importância do trabalho e solicitou mais controle a equipe e que os fluxos dos processos devem ser seguidos. Novamente todos concordaram com os riscos apresentados e, o Coordenador de Operações e a Analista de Controle Internos

basearam sua resposta fazendo referência à base de chamados atendidos pelas áreas de Suporte e *Service Desk* e, pelas evidências coletadas durante auditoria, respectivamente.

Analisando o tratamento dos riscos propostos, o Coordenador de Operações concordou com as ações e salientou que apenas é preciso ajustar as configurações e seguir os procedimentos já existentes para garantir a segurança do ambiente. A Analista de Controles Internos concordou positivamente com o tratamento proposto e, o Gerente de *Compliance* gostaria que o risco NR06, apesar de baixo, também fosse tradado, mas entendeu que para isto exige um investimento não provisionado no orçamento do ano.

Finalizando a apresentação, todos destacaram novamente a relevância do trabalho e da escolha do escopo proposto para realização do mesmo. O Coordenador de Operações já gostaria de iniciar esta mesma análise, com enfoque de alto nível, para os demais serviços e ativos da Instituição. Um ponto levantado pelo Gerente de *Compliace* é a importância da etapa de monitoramento da ABNT NBR ISO/IEC 27005:2011, que não foi foco do trabalho apresentado. Ele gostaria de ver a atividade de monitoramento na análise de risco quando realizada para os demais serviços de ativos da Instituição.

5 CONSIDERAÇÕES FINAIS

Entende-se que este trabalho abordou um tema importante para as Instituições de Ensino Superior relacionado à gestão de riscos. Como citado no início, o mercado educacional é dinâmico e competitivo. As IES possuem características que as diferenciam de outras organizações e, consequentemente, abordagens para a gestão de risco e da segurança da informação precisam estar alinhados a esta realidade.

Uma realidade percebida nas IES é a propagação das redes Wi-Fi. Cada vez mais as Instituições estão melhorando, ampliando e fazendo uso das redes Wi-Fi em seus Campi. Este é um recurso considerado essencial pelos estudantes que circulam pelas dependências da Instituição. Sendo essencial para os alunos, a área acadêmica tende a priorizar sua ampliação. Como consequência, a área de TI tem a responsabilidade de atender estas solicitações, possibilitando o uso cada vez mais disseminado da rede Wi-Fi por dispositivos móveis, garantindo a segurança no que diz respeito a informação – da Instituição e dos alunos que fazem uso deste recurso.

Entende-se também que os objetivos propostos, estabelecidos em seu início foram cumpridos. O objetivo de analisar a prática de gestão da segurança foi alcançado através da verificação de documentos e procedimentos aplicados e na observação direta da operação. Atendeu-se também aos objetivos de aplicar a metodologia da norma ABNT NBR ISO/IEC 27005:2011 para analisar, avaliar e tratar os riscos identificados gerando, a partir da matriz de risco, o quadro de análise de risco e o quadro de priorização de riscos.

O autor deste trabalho, fazendo uso dos conhecimentos adquiridos ao longo do curso, mais especificamente do módulo de Gestão de Riscos em Segurança da Informação – ISO 27005; de seu conhecimento do ambiente acadêmico e por estar à frente de projetos associados à infraestrutura, objetivou verificar como estava sendo realizada a gestão de segurança da rede Wi-Fi em uma IES, sugerindo melhorias com base na norma ABNT NBR ISO/IEC 27005:2011.

Um ponto importante, que vem a corroborar sobre a relevância deste trabalho, foi a validação, junto a colaboradores representativos da Instituição, da análise, avaliação e tratamentos propostos. Estes colaboradores expressaram suas opiniões ao responder a entrevista (APÊNDICE A), concordando e contribuindo com as informações levantadas do

ambiente, sobre o resultado obtido com a aplicação da norma e sobre a importância desta ação para o momento ao qual se encontra a Instituição.

Buscando aplicar este trabalho, uma das sugestões é realizar uma nova análise e avaliação dos riscos, obtendo assim os riscos residuais após os tratamentos propostos. Outro ponto importante é realizar as etapas de monitoramento e comunicação dos riscos, visando ter um melhor acompanhamento futuro e alinhamento das áreas quanto aos riscos existentes. Por fim, aplicar a metodologia de gestão de risco, proposta pela norma ABNT NBR ISO/IEC 27005:2011, ao demais projetos e ativos da Instituição.

REFERÊNCIAS

ABNT NBR ISO/IEC 27005. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. 2011.

ABNT NBR ISO/IEC 31000. Gestão de riscos – Princípios e diretrizes. 2009.

APRENDER VIRTUAL. Apresenta texto sobre rede sem fio é realidade nas universidades. Disponível em <http://www.aprendervirtual.com.br/noticiaInterna.php?ID=77&IDx=134>. Acesso em: 18 mai. 2015.

BRANDÃO, José E. M. S.; FRAGA, Joni S. Gestão de Riscos de Segurança. In: Maziero, Carlos Alberto; Gaspary, Luciano Paschoal; Weber, Raul Fernando. (Org.). *Minicursos / VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2008, p. 1-43.

FERNANDES, Jorge H. C. *Introdução à Gestão de Riscos de Segurança da Informação*. 2009-2011. Desenvolvido em atendimento ao plano de trabalho do Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC 2009-2011. Brasília, 2009.

GIL, Antônio C. *Como Elaborar Projetos de Pesquisa*. 5.ed. São Paulo: Atlas, 2010.

IT PRO: CARREIRA. Apresenta texto sobre universidades que oferecem redes Wi-Fi para estudantes. Disponível em <http://pos.faap.br/clipping/wifi/wifi.htm>. Acesso em: 18 mai. 2015.

MICROSOFT. Apresenta texto explicativo sobre 802.1X. Disponível em <https://technet.microsoft.com/en-us/library/cc759077(v=ws.10).aspx>. Acesso em: 30 jul. 2015.

MUNDOBIT. Apresenta texto sobre ataque hacker sofrido pela UFPE em seu site. Disponível em <http://blogs.ne10.uol.com.br/mundobit/2015/01/05/site-da-ufpe-sofreu-ataque-hacker>. Acesso em: 23 mai. 2015.

OGLOBO. Apresenta texto sobre invasão por hacker na página da UFRJ. Disponível em <http://oglobo.globo.com/rio/paginas-da-ufrj-na-internet-sao-invadidas-por-hacker-que-afirma-ser-muculmano-15082134>. Acesso em 23 mai. 2015.

OHTOSHI, Paulo H. *Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005*. Monografia (Especialização em Gestão de Segurança da Informação Comunicações) – Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2008. (mimeo)

PASSEIWEB. Apresenta texto sobre uso da Internet sem fio amplia possibilidades pedagógicas. Disponível em <http://www.passeiweb.com/estudos/sala_de_aula/atualidades/uso_da_internet_sem_fio_amplia_possibilidades_pedagogicas>. Acesso em: 18 mai. 2015.

PIAZZA, Maurício R. Norma ABNT NBR ISO/IEC 27.005 Gestão de Riscos da Segurança da Informação como base para a Gestão de Riscos Corporativos. Disponível em < http://www.prevenirperdas.com.br/portal/attachments/article/326/Artigo_%20ISO%2027%20005.pdf>. Acesso em 11 mai. 2015.

SCHAUER, Hervé. *Méthode de gestion des risques ISO27005*. Netfocus, 2009, Bruxelles. Disponível em <http://www.hsc.fr/ressources/presentations/netclu09-27005/netclu09-27005.pdf> Acesso em 30 jul. 2015

SEDREZ, Célia S.; FERNANDES, Francisco C. Gestão de Risco nas Universidades e Centros Universitários do Estado de Santa Catarina. *Revista de Gestão Universitária na América Latina*, Florianópolis, Edição especial 2011, p.70-93, 2011.

SILVA, Pedro J. S. *Análise/Avaliação de Riscos de Segurança da Informação para a Administração Pública Federal: Um Enfoque de Alto Nível Baseado na ISO/IEC 27005*. Monografia (Especialização em Gestão de Segurança da Informação Comunicações) – Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2009. (mimeo).

TECHTARGET01. Apresenta texto explicativo sobre captive portal. Disponível em < http://searchmobilecomputing.techtarget.com/definition/captive-portal>. Acesso em: 30 jul. 2015

TECHTARGET02. Apresenta texto explicativo sobre NAC. Disponível em < http://searchnetworking.techtarget.com/definition/network-access-control>. Acesso em: 30 jul. 2015

ULTIMOSEGUNDO. Apresenta texto sobre onda de ataques hacker. Disponível em < http://ultimosegundo.ig.com.br/brasil/hackers+comandam+onda+de+ataques+pelo+quarto+dia+consecutivo/n1597046555189.html>. Acesso em: 23 mai. 2015.

VERGARA, Sylvia C. *Projetos e relatórios de pesquisa em administração*. 9. ed São Paulo: Atlas, 2007.

WIKIPEDIA01. Apresenta texto explicativo sobre site survey. Disponível em <https://en.wikipedia.org/wiki/Wireless_site_survey>. Acesso em: 30 jul. 2015.

WIKIPEDIA02. Apresenta texto explicativo sobre WPA2. Disponível em <https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access>. Acesso em: 30 jul. 2015.

YIN, Robert K. *Estudo de Caso: Planejamento e Métodos*. 4.ed. Porto Alegre: Bookman, 2010.

APENDICE A – ROTEIRO DE ENTREVISTA

a) Tendo como base o levantamento do ambiente apresentado, qual a sua percepção em relação a prática da gestão de segurança da Instituição? Leve em consideração para sua resposta os procedimentos e controles existes.

b) Qual sua avaliação da apresentação da análise e avalição dos ricos levantados, seguindo a ABNT NBR ISO/IEC 27005:2011? Você concorda ou discorda dos riscos levantados? Por quê?

c) Como você avalia o tratamento dos riscos propostos, considerando o escopo e os critérios utilizados?

d) Em sua opinião, esta análise poderia ser aplicada para um escopo mais abrangente da Instituição? Por quê?