CENTRO UNIVERSITÁRIO CARIOCA – UNICARIOCA

GUILHERME DIAS LUTZ
MARIO SERGIO CARDOSO GOMES
WELLINGTON SEVERINO DA SILVA

SEGURANÇA DA INFORMAÇÃO E ANÁLISE DE RISCOS

RIO DE JANEIRO
2011

GUILHERME DIAS LUTZ
MARIO SERGIO CARDOSO GOMES
WELLINGTON SEVERINO DA SILVA

SEGURANÇA DA INFORMAÇÃO E ANÁLISE DE RISCOS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Carioca, como requisito para conclusão do curso de Redes de Computadores.

Orientador: Prof. Sergio dos Santos Cardoso Silva MSc

RIO DE JANEIRO
2011

Lutz, Guilherme Dias
Segurança da informação e análise de riscos / Guilherme Dias Lutz, Mario Sergio Cardoso Gomes e Wellington Severino da Silva. Rio de Janeiro, 2011.
f.

Orientador: Sérgio dos Santos Cardoso Silva

Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores) – Centro Universitário Carioca, Rio de Janeiro, 2011.

1. Segurança da informação. 2.Informação – Riscos e vulnerabilidade. I. Silva, Sérgio dos Santos Cardoso,Prof. Orient. II.Título.

CDU 004.056

GUILHERME DIAS LUTZ
MARIO SERGIO CARDOSO GOMES
WELLINGTON SEVERINO DA SILVA

SEGURANÇA DA INFORMAÇÃO E ANÁLISE DE RISCOS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Carioca, como requisito para conclusão do Curso Superior de Redes de Computadores.

Aprovada em 2011

Banca Examinadora

_____

Prof. Sergio dos Santos Cardoso Silva MSc - Orientador
Centro Universitário Carioca

_____

Prof. Anderson Fernandes P. dos Santos, DSc
Instituição a que pertence

_____

Prof. Mario Antonio Monteiro, MSc
Centro Universitário Carioca

Dedicamos este trabalho aos nossos familiares e amigos que ao longo desta nossa jornada nos apoiaram e deram forças para subir neste novo degrau de nossas vidas.

AGRADECIMENTOS

À Deus, por nossas vidas.

À nossas esposas que nos apoiaram durante as muitas horas dedicadas à este trabalho de conclusão de curso.

Ao nosso orientador Sérgio Cardoso pela excelente administração do trabalho, pelos ensinamentos transmitidos, e pela amizade conquistada durante toda nossa vida acadêmica.

Aos nossos amigos e amigas que contribuíram de alguma forma para a construção deste estudo.

RESUMO

No início deste trabalho, na parte teórica, será apresentada uma introdução, explicando como surgiu a necessidade de realizar-se a gerência dos riscos como forma de antecipação aos desvios de informações ou ataques. Após a introdução, serão abordadas explicações conceituais sobre Segurança da Informação, o porquê de sua necessidade, tipos de ameaças, atacantes e o funcionamento do processo de Gestão de Riscos. Neste último, serão levantadas explicações sobre cada uma das fases do processo, além de uma descrição sobre as melhores práticas para gerenciar o ambiente de forma a prevenir ataques.

Na parte prática do trabalho, será detalhado um estudo de caso – por questões de segurança e idoneidade, optou-se por não divulgar o nome da Instituição que serviu como base para este estudo, já que todas as suas vulnerabilidades serão expostas. Nesta etapa, será detalhada toda a implantação dos processos de gerência de riscos, passando pelas fases de definição do contexto, análise/avaliação dos riscos (englobando os processos de identificação e estimativa), tratamento, aceitação, comunicação e monitoramento dos riscos. A fase de definição do contexto servirá como referência para todo o resto do processo. Nela serão descritos todos os critérios definidos pela alta direção da Instituição que servirão como base para todos os pontos de decisão do projeto. Em seguida, tendo estes critérios já definidos, será realizada a identificação, análise e avaliação dos riscos encontrados, passando pela fase de aceitação e comunicação dos riscos. Finalizando, será implementada a fase de monitoramento dos riscos, onde os riscos deverão ser verificados de maneira contínua.

Palavras chave:

Riscos, Vulnerabilidade e Ameaça.

ABSTRACT

At the beginning of this work, in the theoretical part, it shall be presented an introduction explaining how the need arose to make the management of risks as a way to anticipate hijacks or attacks. After the introduction, we shall discuss conceptual explanations on Information Security, why of it needs, types of threats, attackers and the operation of the process of Management Of Risks. In the last topic, we shall arise explanations about each stage processes besides the descriptions of the best practices to management the environment to prevent attacks.

In the practical part of the work, it will have a detail case study – because of issues related about security, concerns and our good standing, the name of the Institution that was used as base of our work will not be published, otherwise all the vulnerabilities could be expose. In this stage will be detailed all the implementation of procedures for risk management, passing though definition of the context, analysis / risk assessment (requiring the process of identification and estimate risks), treatment, acceptance, communication and monitoring risks. The definition stage of this context will be use as a reference for all the process. Here will be describe all the steps defined by the high administration of the Institution in order to serve as the base for all decision points of this project. Forward, having all criteria defined, there will be made a identification, analysis and assessment of the risks, passing through risk acceptance and communication. Finally, the frequently implementation of the risk monitoring as a preventive way to avoid hijackers.

Hint words:

Risks, vulnerability and hijack.

LISTA DE ILUSTRAÇÕES

Figura 1 - Categorias de ameaças 18
Figura 2 - Processo da gestão de riscos de Segurança da Informação 24
Figura 3 - Fonte de informação de Ameaças 26
Figura 4 - A atividade de tratamento o risco 31
Figura 5 - Diagrama da rede do instituto 38

LISTA DE TABELAS

Tabela 1 - Qualificação dos Riscos 27
Tabela 2 - Quantificação dos riscos 27
Tabela 3 - Matriz de relacionamentos: Ameaças x Impactos x Probabilidades 28
Tabela 4 - Priorização dos riscos para tratamento. 29
Tabela 5 - Matriz de relacionamento dos riscos da área de Recursos Humanos 40
Tabela 6 - Priorização dos riscos para Tratamento. 41
Tabela 8 - Matriz de relacionamento dos riscos da área de Controle de Acessos 42
Tabela 9 - Priorização dos riscos para tratamento. 44
Tabela 10 - Matriz de relacionamento dos riscos da área de TIC 45
Tabela 11 - Matriz de relacionamento de riscos comuns aos três setores. 46
Tabela 12 - Priorização dos riscos para tratamento. 46
Tabela 13 - Tratamento do risco da área de RH. 48
Tabela 14 - Tratamento do risco da área Controle de Acessos 48
Tabela 15 - Tratamento do risco TIC 49

SUMÁRIO

LISTA DE ABREVIATURAS E SÍMBOLOS 12

1 INTRODUÇÃO 13

1.1 OBJETIVO GERAL 15
1.2 ORGANIZAÇÃO 15

2 CONCEITOS BÁSICOS DE SEGURANÇA 16

2.1 SEGURANÇA DA INFORMAÇÃO 16
2.2 A NECESSIDADE DA SEGURANÇA 17
2.3 AMEAÇAS 17
2.4 TIPOS DE ATACANTES 19
2.5 POLÍTICA DE SEGURANÇA 21
2.6 NORMAS ISO 27005 E ISO 31000 22

3 GESTÃO DE RISCOS 23

3.1 ANÁLISE DE RISCOS 25
3.1.1 ANÁLISE DE IMPACTOS, PROBABILIDADE DE AMEAÇAS E PRIORIZAÇÃO DOS RISCOS 26
3.2 TRATAMENTO DE RISCOS DE SEGURANÇA 29
3.2.1 Tratamento de riscos de segurança em Recursos Humanos 32
3.2.2 Tratamento de riscos de segurança de acesso 32
3.2.3 Tratamento de riscos de segurança Tecnologia da Informação e Comunicação (TIC) 34
3.3 ACEITAÇÃO DE RISCOS 35
3.4 COMUNICAÇÃO DO RISCO 35

4 ESTUDO DE CASO: SOLUÇÃO DE ESTRUTURAÇÃO DA SEGURANÇA DA INFORMAÇÃO COM ANÁLISE E GESTÃO DE RISCOS DO INSTITUTO DE EDUCAÇÃO E PESQUISA 36

4.1 DEFINIÇÃO DO CONTEXTO 36
4.1.1 FUNÇÕES E ESTRUTURAS DA ORGANIZAÇÃO 36
4.1.2 AMBIENTE ATUAL 37
4.1.3 ESCOPO DO PROJETO 38
4.1.4 CRITÉRIO PARA AVALIAÇÃO DOS RISCOS E CRITÉRIOS DE IMPACTO 39
4.1.5 CRITÉRIOS PARA A ACEITAÇÃO DO RISCO 40
4.2 ANÁLISE/AVALIAÇÃO DE RISCOS 40
4.2.1 ANÁLISE/AVALIAÇÃO DE RISCOS DA ÁREA DE RECURSOS HUMANOS 40
4.2.2 ANÁLISE/AVALIAÇÃO DE RISCOS DA ÁREA DE CONTROLE DE ACESSOS 42
4.2.3 ANÁLISE/AVALIAÇÃO DE RISCOS DA ÁREA DE TIC 45
4.3 COMUNICAÇÃO DO RISCO 47
4.4 TRATAMENTO DOS RISCOS 47
4.4.1 TRATAMENTO DOS RISCOS DA ÁREA DE RECURSOS HUMANOS 47
4.4.2 TRATAMENTO DOS RISCOS DA ÁREA DE CONTROLE DE ACESSOS 48
4.4.3 TRATAMENTO DOS RISCOS DA ÁREA DE TIC 49
4.5 RISCO RESIDUAL 50
4.6 ACEITAÇÃO DOS RISCOS 50
4.7 MONITORAMENTO DO RISCO 50

5 CONCLUSÃO E TRABALHO FUTURO 51

ANEXO 1 52
REFERÊNCIA 55

LISTA DE ABREVIATURAS E SÍMBOLOS

ABREVIATURAS

ARPA	-	*Advanced Research Projects Agency*
ARPANET	-	*Advanced Research Projects Agency Network*
MILNET	-	*Military Network*
TI	-	Tecnologia da Informação
TIC	-	Tecnologia da Informação e Comunicação
GPO	-	*Group Police Object*
ABNT -	-	Associação Brasileira de Normas Técnicas
NBR	-	Norma Brasileira
ISO	-	*International Standartization Organization*
IEC	-	*International Engineering Consortium*
WEB	-	Abreviatura de *World Wide Web*
MSN	-	*Microsoft Network*

1 INTRODUÇÃO

Até o início da década de 60, quando se falava em “informação”, logo era possível imaginar algo registrado em papel, na memória de determinada pessoa, ou, no máximo, em computadores centralizados (sem acesso externo). Entretanto, nesta época, alguns pesquisadores, de Universidades americanas, iniciaram o desenvolvimento de trabalhos buscando a interligação de computadores. Esta ideia animou o governo americano, que planejava utilizar esta nova tecnologia em programas militares com o objetivo de descentralizar a informação, criando assim a ARPA (*Advanced Research Projects Agency*).

Na época da Guerra Fria, ainda com o nome de ARPANET, esta comunicação foi aprimorada e implementada pelos militares, descentralizando os computadores responsáveis pela distribuição da informação para manter a comunicação entre as bases militares dos Estados Unidos, mesmo que o Pentágono fosse destruído por ataques inimigos. Isso porque, na antiga infraestrutura, existia um computador central, localizado no Pentágono, por onde passavam todas as informações, o que aumentava o risco de vulnerabilidade da comunicação.

Com o fim da Guerra Fria, os militares acreditavam não haver necessidade de manter, somente sobre sua gerência, toda aquela infraestrutura. Como havia um grande interesse de cientistas em seu uso, a ARPANET foi dividida em duas redes: a MILNET, que permaneceu sobre o controle dos militares, e a nova ARPANET, cujo acesso foi liberado aos cientistas, o que permitiria o acesso às Universidades locais e, sucessivamente, às Universidades de outros países. Com isso, usuários domésticos também passaram a ter acesso àquela rede, até que mais de cinco milhões de pessoas já estavam conectadas.

Algum tempo depois, com o surgimento de vários protocolos e serviços incorporados a essa rede, ela foi ficando mais robusta e atraente, com inúmeras funcionalidades, passando a não só a pesquisadores e universitários, como também às pessoas comuns, com pouco ou nenhum conhecimento de informática. Com toda essa diversidade de conteúdo e facilidade de acesso, logo foi possível perceber que, através da Internet, seria possível movimentar negócios lucrativos de forma direta, com surgimento de e-commerces e as lojas virtuais, ou de forma indireta, otimizando a comunicação e as transações das organizações.

Quando criada, o principal objetivo da ARPANET era prover disponibilidade de dados; além disso, seu uso era restrito aos militares. Com isso, não se pensou, em um primeiro momento, na implementação de segurança lógica já que, por se encontrar em um ambiente militar, teoricamente, ela já estava segura. Como acontece em qualquer cenário que envolva ”pessoas”, existem aquelas que obtêm conhecimento e o utilizam da forma correta – normalmente, no que diz respeito à “Tecnologia da Informação” (TI), este é um profissional de segurança de TI e/ou entusiasta da área, contribuindo com melhorias – e aquelas que o utiliza de forma inadequada, os chamados “atacantes”, que aproveitam-se do conhecimento adquirido e da pouca segurança da rede para invadir e/ou atacar servidores de bancos, empresas e comércios eletrônicos em geral, seja “à serviço” de empresas concorrentes, ou, simplesmente, pela sensação de “poder” em quebrar uma segurança previamente implantada. Por conta desta bipolaridade de ações, da valorização da informação e da dependência das organizações em relação aos serviços tecnológicos, hoje se trava uma “guerra virtual” entre os atacantes e os profissionais de Segurança de TI, uma guerra transparente aos “olhos” de um usuário comum, mas que ocorre com freqüência neste mundo virtual.

Diferentemente de algum tempo atrás, quando a Segurança da Informação acontecia de forma passiva – configurando os sistemas da maneira correta (mantendo-os sempre atualizados, analisando o comportamento da rede, verificando se havia alterações que pudessem caracterizar ataques etc.) – hoje é necessário que, além disso, sejam tomadas medidas preventivas para conter os ataques, analisando os riscos antecipadamente e evitando, ao máximo, a paralisação dos serviços da organização. Em função disto, existe um crescente interesse das organizações em saber o quanto suas informações, bens, entre outros dados importantes, estão expostos às ameaças (explicadas e exemplificadas no capítulo 2.3), capazes de causar inoperância em seus serviços. Para que seja possível ter uma mensuração dos riscos, podendo tratá-los, preparar planos de recuperação, entre outras medidas, é necessário que seja efetuada a gerência dos mesmos, cujo qual, neste trabalho, serão abordados os processos necessários para que esta gerência seja eficaz.

1.1 Objetivo Geral

Este trabalho tem como objetivo mostrar o conceito de segurança da informação e a importância de controlar os riscos envolvidos nesta área. Serão vistas as técnicas da análise de riscos e as formas de tratamento além de mostrar todo o processo do gerenciamento de riscos;

Especificamente, este projeto possui os seguintes objetivos:

- fazer uma abordagem teórica sobre segurança da informação;
- descrever tipos de ameaças, vulnerabilidades e atacantes;
- mostrar um estudo sobre a gerência e análise de riscos;
- mostrar uma implementação prática do processo de gerência de riscos, utilizando os padrões de processos mostrados nas normas NBR ISO/IEC 27001 e 27005.

1.2 Organização

O presente trabalho está organizado em 5 capítulos.

No capítulo 2 estão sendo descritos os conceitos básicos de segurança e suas propriedades básicas de confidencialidade, integridade e disponibilidade. Além disso, neste capítulo encontram-se explicações sobre ameaças, tipos de atacantes e políticas de segurança.

O capítulo 3 compreende a gestão de riscos, onde será mostrado todo o processo de análise/avaliação, tratamento, aceitação e comunicação dos riscos.

No capítulo 4 encontra-se um estudo de caso onde foi descrito todo o processo de implantação da gerência de riscos em um determinado instituto. Neste processo implantado, foram seguidos à risca todos os processos sugeridos pela norma ABNT NBR ISO_IEC 27005.

No último capítulo, capítulo 5, foi descrita uma conclusão de todo o trabalho.

2 CONCEITOS BÁSICOS DE SEGURANÇA

2.1 Segurança da Informação

A segurança da informação é um conjunto de medidas que tem como objetivo a proteção de dados e informações empresariais e pessoais, controlando o risco de revelação ou alteração por pessoas não autorizadas.

A segurança da informação deve ser implantada em todas as áreas da empresa, para minimizar qualquer fraqueza que possa ser explorada comprometendo a segurança de sistemas ou informações.

Segundo Kurose & Ross (2006), podemos identificar as seguintes propriedades desejáveis para segurança da informação:

- Confidencialidade, que compreende a proteção de dados transmitidos contra acessos não autorizados, envolvendo medidas como controle de acesso e criptografia.
- Autenticidade, ou seja, origem e destino podem verificar, com segurança a autentica identificação da outra parte envolvida na comunicação, com o objetivo de confirmar que a outra parte é realmente quem alega ser. A origem e o destino são usuários, dispositivos ou processos.
- Integridade, toda a Informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
- Não repúdio, previne uma origem ou destino de negar a transmissão de mensagem, quando a mensagem e enviada o destino pode provar que foi realmente enviada por determinada origem e vice-versa.
- Disponibilidade determina que recursos estejam disponíveis para acesso por entidades autorizadas sempre que solicitados, representando a proteção contra perdas.
- Controle de acesso trata de limitar e controlar o acesso lógico e físico, com o objetivo de proteger os recursos contra acessos não autorizados, por meio de identificação, autenticação e autorização.

2.2 A necessidade da segurança

A segurança da informação é um ponto crítico para a sobrevivência das organizações. Vários são os problemas envolvidos, tendo em vista que a sociedade atual depende das informações armazenadas nos sistemas computacionais para tomadas de decisões em negócios, órgãos do governo etc.

É necessário garantir a confiabilidade e segurança da organização e combater os ataques causados por vírus, hackers e outros, o que está se tornando cada vez mais comum e acontecendo de forma incrivelmente sofisticada..

Muitas organizações não estão preparadas para garantir a segurança da informação. É necessário escolher controles que permitam a implantação da segurança, mas para que os resultados sejam alcançados é necessária à participação de todos os funcionários da organização, e possivelmente a participação dos fornecedores, clientes e diretoria.

Algumas organizações pensam estar garantindo a segurança da informação quando compram softwares como *firewall*, antivírus, *antispyware* e os instalam nos computadores. Imaginam que assim estarão protegendo os dados da organização, entretanto ” Segurança da Informação” é algo muito mais complexo do que isso, como poderá ser visto mais adiante.

2.3 Ameaças

A ameaça existe quando uma vulnerabilidade pode ser explorada por um atacante, causando algum tipo de dano aos ativos. Quando este dano é causado, caracteriza-se um Incidente.

Há quatro categorias de ameaças possíveis. A figura 1 mostra o fluxo normal das informações de uma origem para um destino realçado na cor verde, e as quatro categorias de ameaças na segurança.

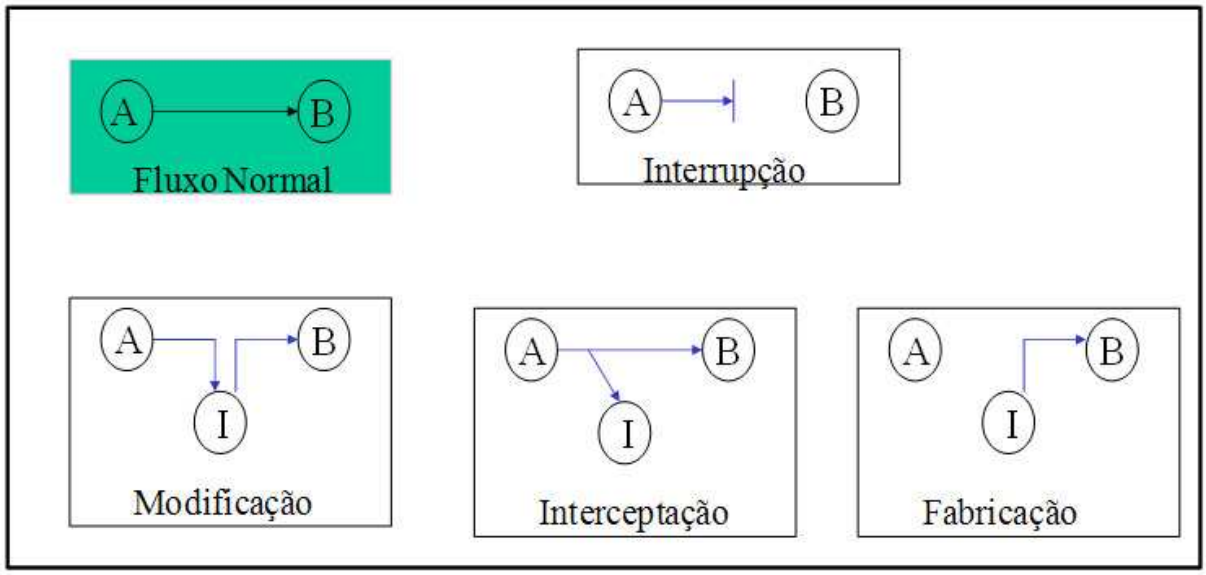

Figura 1 – Categorias de ameaças

Fonte: *Stallings, W. Network Security Essentials*, 2000.

- Interrupção: através desta um ativo é destruído ou torna-se indisponível, o que caracteriza um ataque contra a disponibilidade. Por exemplo, a destruição de um disco de armazenamento de dados.
- Interceptação: quando o ativo é acessado por alguém sem autorização, o que caracteriza um ataque contra a confidencialidade. Por exemplo, cópia não autorizada de arquivos e programas.
- Modificação: quando o ativo é acessado sem autorização e ainda alterado, o que caracteriza um ataque contra a autenticidade. Por exemplo, mudar os valores de um arquivo de dados.
- Fabricação: uma parte não autorizada insere objetos falsificados em um ativo, o que caracteriza um ataque contra autenticidade. Por exemplo, a adição de registros em um arquivo.

2.4 Tipos de Atacantes

O termo genérico usado para denominar aquele que realiza um ataque a um sistema computacional é *hacker*. Mas essa definição não é totalmente verdadeira, pois dependendo da intenção com que o atacante faz uma invasão, ele pode ser chamado de *hacke*r ou *cracker.*

Segundo Nakamura & Geus (2003), *hackers,* pela definição da palavra, “são aqueles que usam de seus conhecimentos para invadir sistemas, não com o intuito de causar danos às suas vítimas, mas sim como uma forma de testar os seus limites e habilidades”.

O termo “*hacker*“ tem origem na expressão *“to hack”,* e a tradução mais próxima é a palavra “fuçador”. Ao contrário dos “*hackers”,* os “*crackers*“ são pessoas de conhecimento e habilidades em computação que invadem sistemas com o objetivo de roubar informações e causar danos às suas vítimas, seja para ter retorno financeiro ou simplesmente para divertimento malicioso.

Além dessas definições de “*crackers*” e “*hackers*”, existem diferentes tipos de atacantes, e eles são classificados de acordo com o seu conhecimento e intenções ao realizarem invasões a sistemas. Abaixo serão listadas algumas definições de atacantes:

- *Script Kiddies*: é um termo depreciativo usado em referência a grupos *de crackers* inexperientes. São também conhecidos como *newbies*, ou iniciantes, e são responsáveis por trazer diversos problemas a empresas e organizações. Eles são inexperientes e normalmente usam ferramentas da internet sem saber exatamente o que estão fazendo.

- *Cyberpunks*: é a combinação de cibernética e *punk*. São aqueles que realizam suas invasões por puro divertimento e desafio. Geralmente são os responsáveis por encontrar vulnerabilidades em sistemas e divulgá-las na internet, causando vários malefícios a organizações de todos os tipos. Usam seu conhecimento "acima da média" para realizar protestos contra a sistemática vigente das grandes corporações, sob a forma de vandalismo, causando prejuízos sem ter qualquer ganho pessoal.

- *Insiders*: são os responsáveis por ataques de dentro da própria rede interna de uma organização, sendo aqueles que causam os maiores prejuízos, com fraudes financeiras e abusos nas redes internas. Os *insiders* geralmente são funcionários descontentes com seu trabalho, além de serem os principais causadores da espionagem industrial, que é considerada uma nova modalidade de crime.

- *White-Hats* ([1]): usam seus conhecimentos para explorar problemas de segurança e aplicar as correções necessárias, agindo sempre dentro da lei. Normalmente são contratados pelas empresas para fazer testes e simulações a fim de medir o nível de segurança das redes. São comparados a policiais que buscam falhas em sistemas a fim de corrigi-las. É comum encontrá-los ministrando palestras sobre segurança de sistemas ou trabalhando em empresas para garantir a segurança.

- *Black-Hats*[2]: também conhecidos como *full fledged* ou *crackers*, eles usam seus conhecimentos em benefício próprio e, geralmente, estão ligados a atividades ilícitas, como roubar informações secretas de organizações. Ações como quebrar a segurança de um programa, ou seja, fazer com que o programa não precise ser mais pago, são comuns dos *Black-Hats.* Ao contrário do *White-Hats*, os *Black-Hats* são hackers criminosos.

---

[1] C*hapéus brancos*, em tradução literal.
[2] C*hapéus pretos*, em tradução literal.

2.5 Política de Segurança

Para que a gerência de riscos seja eficaz, é necessário criar e implementar uma política de segurança que tenha como objetivo guiar a utilização e o tratamento das informações. Ela agirá na proteção dos ativos da corporação, sejam eles informação, hardware, aplicativos ou sistemas e deverá estar integrada com objetivos e negócios da empresa.

A norma ABNT NBR ISO/IEC 17799:2005 nos mostra como estabelecer uma política de segurança da informação:

> "Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização."

Uma política de segurança, quando bem orientada e integrada aos negócios da empresa, ajuda na análise e avaliação dos riscos. A diretoria terá maior facilidade na visualização dos riscos envolvidos e conseguirá tomar uma decisão mais precisa em relação às medidas preventivas.

Ao se elaborar uma política de segurança da informação, deve-se levar em consideração que ela será lida por todos os funcionários da empresa, pelos estagiários, pelos contratados, por seguranças patrimoniais, pelos diretores e gerentes e até mesmo pelos funcionários da limpeza e manutenção. Todos devem receber as instruções rotineiramente para que a política de segurança da informação seja absorvida e posta em prática, em todas as áreas da companhia. Estas áreas devem interagir para manter a harmonia na proteção dos ativos da corporação.

Desta forma, a linguagem deve ser clara, objetiva e, sempre que possível, referenciar outras normas ou padrões adotados. Esta prática tem a finalidade de tornar mais fácil a leitura, deixando a política com um conteúdo menor e tornando-a

mais segura em caso de desvio. Inclusive, caso isso aconteça, será mais difícil obter todas as normas ou padrões previamente referenciados. A impressão deste tipo de documento também é um item que pode ser bloqueado, dificultando a exteriorização das normas de forma indevida.

A política, uma vez definida, deve ser divulgada a todos, utilizando a estrutura que a empresa disponibiliza. Basicamente, os métodos utilizados para divulgação são:

- Uso da intranet para divulgar novos procedimentos;
- Uso de GPOs (*Group Police Object*) para difundir mensagens importantes;
- Palestras;
- Campanhas de segurança da informação online.

Com uma política de segurança bem orientada, atualizada e divulgada, os incidentes de segurança diminuirão e a gestão de riscos será facilitada a fim de tornar os ativos da corporação mais seguros ou menos suscetíveis aos ataques e desvios de informações de caráter sigilos.

2.6 Normas ISO 27005 e ISO 31000

Para a realização deste trabalho será utilizada, como guia, a norma ISO 27005, que fornece as diretrizes para o gerenciamento dos riscos pertinentes à segurança da informação (SI). Esta norma dá sustentação aos conceitos especificados na ISO 27001:2005, a norma de requisitos de sistemas de gestão da SI, além de auxiliar na implementação e certificação de tais sistemas de gestão.

Em 13 de novembro de 2009, foi publicada oficialmente a norma ISO 31000, que foi desenvolvida por um grupo de especialistas representantes de mais de 30 países, visando criar um guia que fosse mais completo, no que diz respeito à gerência de riscos como um todo. Ou seja, a criação desta nova norma não objetivou concorrer com a norma ISO 27005, já que esta última é específica para a gerência de riscos de Segurança da Informação.

3 GESTÃO DE RISCOS

As informações são ativos[3] que possuem atividades dinâmicas, sendo transferidas a todo instante. Elas passam por transformações, sendo atualizadas, modificadas, apagadas, acrescidas e transmitidas.

Uma boa forma de gerir os riscos é identificar os ativos para posteriormente definir-se a proteção adequada à sua integridade, disponibilidade e confidencialidade. A correta classificação das informações, por exemplo, ajuda a controlar a divulgação dos dados, dificultando o envio inadequado do material para fora da empresa ou para pessoas estranhas ao setor.

Na figura 2 é apresentada uma visão de como funciona o processo da gestão de riscos de segurança da informação segundo a ABNT NBR ISO/IEC 27005. O processo tem seis grupos de atividades:

- Definição do contexto: responsável pela definição do ambiente, escopo, critérios de avaliação etc. Nessa etapa é importante que a equipe que administra a gestão de risco conhecerá todas as informações sobre a organização.
- Análise e Avaliação de riscos: permite que sejam identificados os riscos para que sejam determinadas as ações necessárias a fim de reduzi-los a um nível aceitável.
- Tratamento do risco: a partir dos resultados obtidos na análise e avaliação do risco são definidos os controles para o seu tratamento.
- Aceitação do risco: esta atividade visa assegurar quais são os riscos aceitos pela organização, e quais são aqueles que, por algum motivo, não serão tratados ou tratados parcialmente.
- Comunicação do risco: nesta etapa são feitas as comunicações dos riscos e é definida a forma que como eles mesmos serão tratados para todas as áreas e seus gestores.

[3] Considera-se ativo tudo o que tem valor para a empresa e que precisa ser protegido.

- Monitoramento e análise crítica: são atividades de acompanhamento dos resultados, implantação de controles e de análise crítica para melhoria do processo de gestão de riscos.

O ciclo de vida da gestão de risco se desenvolve de maneira incremental, ocorre uma sucessão de iterações, e cada uma delas libera um resultado para a seguinte, minimizando tempo e esforço.

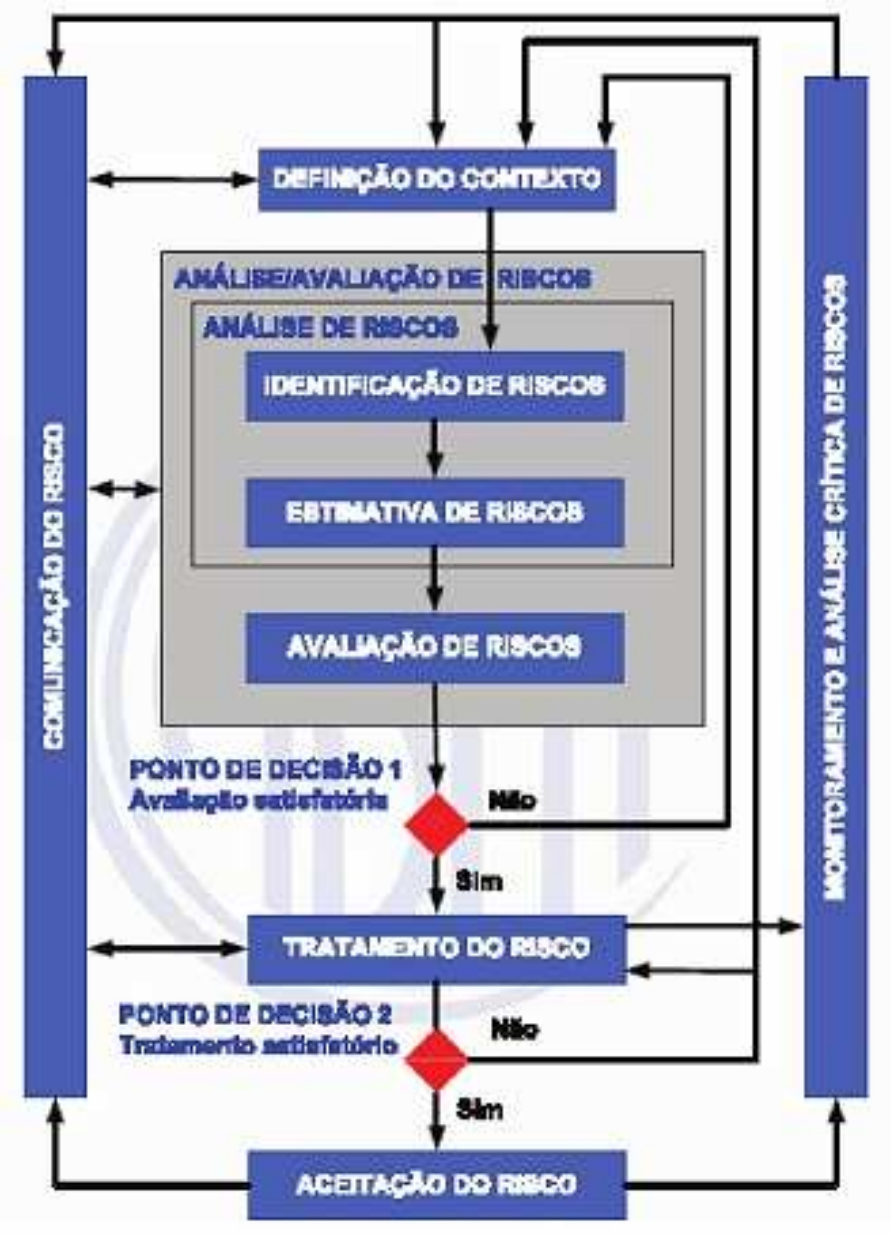

Figura 2-Processo da gestão de riscos de Segurança da Informação
Fonte: ABNT NBR ISSO/IEC 27005:2008

3.1 Análise de Riscos

Nesta fase, são identificados e descritos os eventos que poderão causar prejuízos à empresa, como: roubo e desvio de informações, ataques de engenharia social, ameaças naturais, entre inúmeras outras ameaças.

Identificar o risco é associar a identificação de dois fatores: os ativos e as ameaças. Relacionar as ameaças e as vulnerabilidades e traçar com estes dados um mapa de riscos facilitará a elaboração de um plano de controle, qualificando e quantificando os riscos para um efetivo tratamento.

- Identificação dos ativos: uma forma de definir e controlar os ativos da empresa é estabelecer um sistema de controle. Cada ativo deve ter seu usuário e/ou um responsável pelo seu uso. Com este controle, o ativo poderá ser rastreado caso alguma ameaça o atinja e, quando o risco for tratado, possa haver facilidade da área responsável em reagir da melhor forma, a fim de garantir a menor perda possível.

- Identificação das ameaças: identifica as ameaças existentes, elaborando uma relação daquelas que podem explorar vulnerabilidades da organização, facilitando assim a busca pelo risco existente. Existem fontes de informações de ameaças que podem ser pesquisadas até mesmo na internet, como empresas de antivírus e instituições do governo de diversos países. Na figura 3, segue um exemplo de um site que disponibiliza informações sobre ameaças:

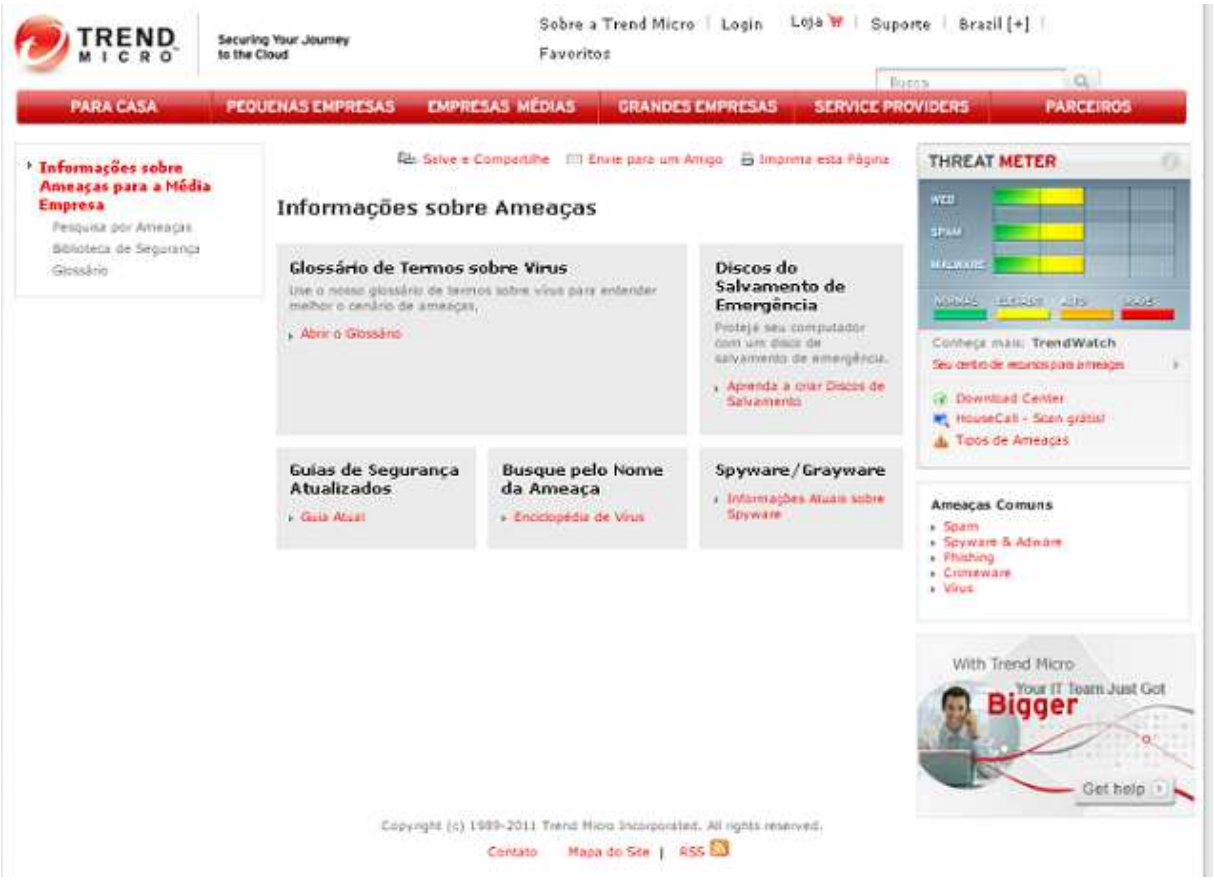

Figura 3-Fonte de informação de Ameaças
Fonte: Site da Trend Micro

A análise de riscos deve medir as ameaças, vulnerabilidades e impactos, de modo que o resultado possa servir para determinar as medidas de segurança adequadas, considerando custos, requisitos de proteção e facilidades de uso. Em termos quantitativos, esta análise pode ser considerada para assegurar que os custos com as medidas preventivas e corretivas não sejam elevados.

3.1.1 Análise de Impactos, Probabilidade de Ameaças e Priorização dos Riscos

Impacto é toda a consequência sofrida por uma organização ao ser atingida por uma ameaça. Considerando, por exemplo, controles de acesso implantados inadequadamente, à organização pode sofrer impactos como alteração não autorizada de dados e aplicativos, divulgação não autorizada de informações e roubo de informações, por isso é importante analisar os impactos, utilizando uma gestão de riscos adequada ao negócio.

Utilizando a categorização sugerida pela equipe que está realizando este estudo, na tabela 1, é possível qualificar o nível de risco de acordo com as consequências resultantes ao negócio da empresa. Cada nível é medido por um valor de 0 a 5, demonstrando as consequências financeiras sobre os negócios da empresa.

Tabela 1- Qualificação dos Riscos

Nível de risco	Valor	Descrição
Extremo	5	Efeitos desastrosos que comprometem a sobrevivência da organização
Altíssimo	4	Efeitos desastrosos, mas que não comprometem a sobrevivência da organização.
Alto	3	Grande perda financeira e de clientes
Médio	2	Sistemas indisponíveis por um período de tempo, podendo causar atraso na entrega de algum serviço.
Baixo	1	Efeito pouco significativo que não afeta os processos de negócio
Irrelevante	0	Impacto irrelevante

Da mesma forma que os impactos foram classificados, pode-se tomar como base a classificação da probabilidade de determinado risco afetar a organização. A tabela 2 mostra como podem ser atribuídos valores para quantificar o risco tomando como base a probabilidade de ocorrência das ameaças.

Tabela 2- Quantificação dos riscos

Valor	Definição
5	Ocorrer diariamente
4	Ocorrer pelo menos uma vez por semana
3	Ocorrer pelo menos uma vez por mês
2	Ocorrer pelo menos uma vez por ano
1	Ocorrer menos de uma vez por ano
0	Improvável de ocorrer

A tabela 3 exemplifica uma maneira simples de relacionamento entre ameaças, impactos e probabilidades, onde para cada vulnerabilidade e ameaça na

organização são medidos os impactos e as probabilidades de ocorrência. São utilizadas as categorias de 0 a 5 para cada item, conforme os exemplos mostrados anteriormente. O valor da coluna “GRAU DE RISCO”, é o resultado da soma das colunas “PROBABILIDADE” e “IMPACTO”, que será utilizado para descrever a ordem de priorização do tratamento do risco, de acordo com o seu valor (que poderá ser de 0 a 10) e sua importância para organização.

Tabela 3-Matriz de relacionamentos: Ameaças x Impactos x Probabilidades

	VULNERABILIDADES	AMEAÇAS	PROBABILIDADE (0 a 5)	IMPACTO (0 a 5)	GRAU DE RISCO (0 a 10)
SETOR 1	Uma falha de segurança encontrada	O que pode explorar uma falha	5	4	9
SETOR 2	Uma falha de segurança encontrada	O que pode explorar uma falha	5	3	8
SETOR 3	Uma falha de segurança encontrada	O que pode explorar uma falha	3	3	6

A tabela 4 mostra um exemplo utilizado para listar a priorização do tratamento dos riscos, levando em consideração os valores observados na tabela 3. Ou seja, quanto maior for o valor referente ao grau de risco (probabilidade + impacto), maior será a priorização para o seu tratamento.

A identificação dos riscos pode ser feita levando em consideração os diversos setores da empresa. Nesse caso, a ordem de prioridade dos setores da organização deverá ser demonstrada como, por exemplo: 1º - setor 1, 2º - setor 2, 3º - setor 3 . Logo, se houver uma igualdade no grau de riscos distintos em setores diferentes, a prioridade será maior de acordo com a prioridade de cada setor.

Caso exista a mesma vulnerabilidade em setores diferentes, pode ser adicionada, a esta matriz de relacionamento, a coluna “SETOR DETERMINANTE” que será referente ao setor que a vulnerabilidade apresentou o maior grau de risco. Nesse

caso, deverá ser levado em consideração, para a ordem de tratamento, o “setor determinante” de cada vulnerabilidade.

Tabela 4-Priorização dos riscos para tratamento.

INDICE	VULNERABILIDADES	AMEAÇAS	SETOR DETERMINANTE	ANALISE/ AVALIAÇÃO DO RISCO	GRAU DE RISCO (0 a 10)
1º	Uma falha de segurança encontrada	O que pode explorar uma falha	Setor onde ocorre o maior grau de risco	O risco será descrito e analisado de acordo com o estudo feito sobre prejuízo à organização, caso a ameaça explore a falha encontrada	9
2º	Uma 2ª falha de segurança encontrada	O que pode explorar uma falha	Setor onde ocorre o maior grau de risco	O risco será descrito e analisado de acordo com o estudo feito sobre prejuízo à organização, caso a ameaça explore a falha encontrada	5
3º	Uma 3ª falha de segurança encontrada	O que pode explorar uma falha	Setor onde ocorre o maior grau de risco	O risco será descrito e analisado de acordo com o estudo feito sobre prejuízo à organização, caso a ameaça explore a falha encontrada	2

3.2 Tratamento de Riscos de Segurança

O tratamento tem o objetivo de auxiliar na redução dos riscos previamente identificados, até um nível aceitável para os negócios da empresa.

A figura 2 descreve o processo completo da gestão de riscos, onde podem ser vistos os pontos de decisão, direcionando o fluxo de acordo com a resposta escolhida.

O fluxo da figura 4 mostra em detalhes o processo de tratamento do risco, onde os pontos de decisão 1 e 2 tomam como verdadeira a sentença apenas para ilustrar o caminho por onde o risco poderá ser reduzido, retido, evitado ou ter sua responsabilidade transferida.

Desta forma, após serem obtidos os resultados da análise/avaliação como satisfatórios, o risco segue para ser tratado e terá quatro opções de tratamento onde mais de uma opção poderá ser escolhida para um mesmo risco conforme o caso, segundo a norma ISO/IEC 27005:2005:

- Redução do risco – consiste em diminuir a probabilidade da ameaça até que o risco residual seja aceitável, como efetuar, por exemplo, as atualizações dos aplicativos,
- Retenção do risco – é basicamente aceitar o risco quando a ameaça não é relevante a ponto de ser válido investir no tratamento – o impacto não será relevante aos objetivos do negócio.
- Evitar o risco – esta ação é executada quando o risco é elevado e podem ser tomadas medidas preventivas para que ele não ocorra dentro da corporação. Por exemplo: sabe-se que os comunicadores instantâneos como o MSN *Messenger* são fontes para entrada de vírus. Desta forma, o aplicativo pode ser bloqueado e publicado na política de segurança a proibição do seu uso, tornando passível de punição o funcionário que infringir a regra.
- Transferência do risco – é a ação que transfere a responsabilidade de tratar este risco para outra empresa a fim de obter técnicas específicas de controle.

Mesmo com todas estas medidas de tratamento, ainda poderão existir riscos residuais que serão novamente avaliados para que seja possível diagnosticar se o processo de tratamento foi satisfatório. Sendo positivo, o risco residual será aceito e seguirá o fluxo, conforme figura 2, mostrada anteriormente.

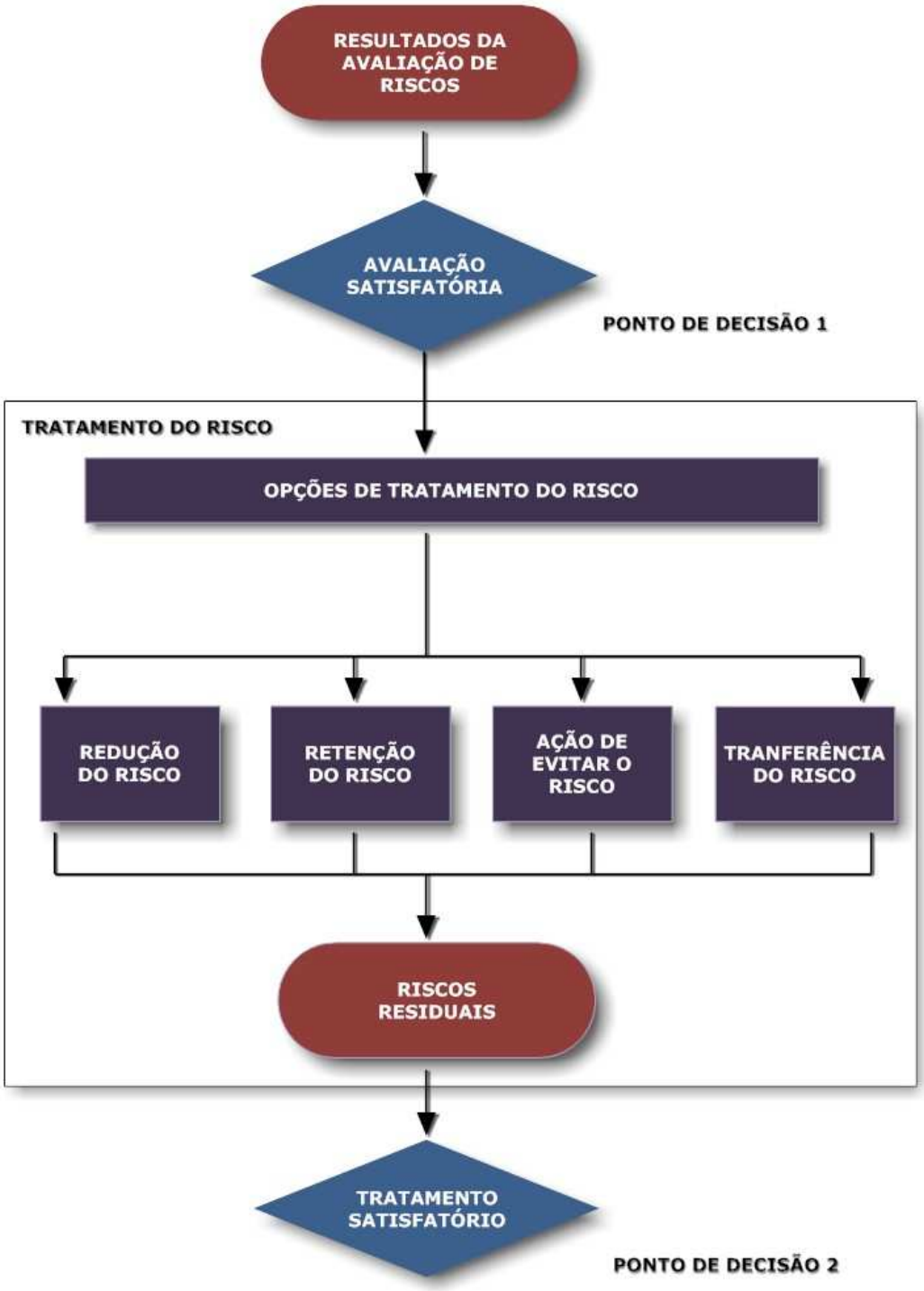

Figura 4-A atividade de tratamento o risco
Fonte: ABNT ISO/IEC 27005:2005

Algumas áreas podem ser consideradas essenciais para a organização, sendo necessária uma maior preocupação com os riscos e impactos causados pelas ameaças para garantir a segurança de seus ativos O tratamento dos riscos

referentes aos recursos humanos, à segurança dos acessos e às comunicações devem ser realizados de forma prioritária.

Nas próximas sessões, serão explicados estes três tipos de tratamento.

3.2.1 Tratamento de riscos de segurança em Recursos Humanos

Quem utiliza e transforma a informação são as pessoas que trabalham na empresa. Desta forma, deve ser cautelosa a ação para minimizar os riscos de segurança na área humana.

Educar, conscientizar e treinar os funcionários é uma tarefa bastante complexa, já que implica na mudança de hábitos dos envolvidos.

O sucesso no tratamento deste tipo de risco depende da correta avaliação do risco. É necessário verificar se ele foi ocasionado por uma falha na segurança de recursos humanos e se há necessidade de tratamento. Confirmada a falha, segue-se para o tratamento, como mostra o fluxo da figura 2. Dependendo das escolhas, o monitoramento avaliará se o risco poderá ser aceito, ou se deve ser realizada uma nova avaliação de acordo com os critérios estabelecidos para identificar os riscos.

Mesmo existindo regras de uso das informações e dos ativos da empresa ou por mais que uma boa política de segurança iniba o usuário de utilizar o equipamento de maneira incorreta, sempre poderá existir o risco de algum usuário ignorar as regras e utilizar os ativos de maneira indevida.

3.2.2 Tratamento de riscos de segurança de acesso

Acessar a empresa significa atingir física ou logicamente os ativos que estão disponíveis ao funcionamento da atividade organizacional.

Existem vários riscos diretamente ligados ao mau uso do controle de acesso da empresa. A inexistência de controles de acesso afeta diretamente a segurança, aumenta os riscos e expõe a empresa a impactos que podem ser desastrosos, considerando os aplicativos e informações críticas aos negócios.

Para as escolhas e decisões tomadas no tratamento, devem ser levadas em conta: a eficácia dos controles, o valor de uma divulgação não autorizada de determinada informação, os possíveis danos em equipamentos e perdas financeiras.

Algumas práticas são recomendadas para diminuir os riscos de acessos não autorizados e os impactos causados pela vulnerabilidade existente na área, por exemplo:

- Restringir e monitorar o acesso a recursos críticos.
- Utilizar criptografia adequada.
- Não armazenar senhas em logs.
- Conscientizar os usuários para que não divulguem suas senhas.
- Dar acesso apenas às atividades necessárias aos funcionários.
- Identificar funcionários e visitantes.
- Controlar a entrada e saída de equipamentos.
- Supervisionar a atuação da equipe de limpeza, manutenção e vigilância.

Além disso, alguns dos riscos relacionados ao controle de acesso indevido são:

- Alteração não autorizada de dados e aplicativos
- Divulgação não autorizada de informação
- Introdução de códigos maliciosos
- Roubo de equipamentos
- Atos de vandalismo

Que podem causar os seguintes impactos:

- ❖ Perdas financeiras decorrentes de fraudes, restaurações etc.
- ❖ Comprometer plano de continuidade dos negócios.
- ❖ Perdas financeiras.
- ❖ Facilidades para ataques contra sistemas de controles de acesso

3.2.3 Tratamento de riscos de segurança Tecnologia da Informação e Comunicação (TIC)

As áreas de TIC envolvem uma série de ativos dentro da empresa e, para garantir um bom controle, poderão existir sistemas para supervisioná-los a fim de garantir sua localização. Uma das formas de controle mais utilizadas, com o objetivo de proteger seus ativos, é a realização de inventário dos mesmos. Este inventário consiste basicamente de uma identificação dos ativos e um cadastro em base de dados relacionando quem os utiliza, o setor onde são encontrados, entre outras informações que podem ser úteis para a organização.

Estes ativos podem ser descriminados como microcomputadores, notebooks, impressoras locais e de rede, scanners, e equipamentos da área de telecomunicações como telefones, fax, cabeamentos de rede, hubs, switches, roteadores, entre outros.

Além dos ativos físicos, citados anteriormente, para garantir a segurança das áreas de TIC, deverá ser considerada a adequação aos requisitos de comunicação da empresa. Esta segurança é imprescindível para garantir a confidencialidade, confiabilidade e a disponibilidade da comunicação, uma vez que as informações estão em constante ameaça de alteração e/ou roubo.

O anexo 1 mostra uma lista com exemplos de vulnerabilidades e ameaças para ajudar a identificar os riscos nos cenários que estarão em análise.

3.3 ACEITAÇÃO DE RISCOS

O objetivo é determinar os critérios a serem considerados para indicar se um risco é aceitável ou não para a organização.

Um risco é considerado aceitável quando, por exemplo, após a avaliação, é considerado baixo ou quando seu tratamento representa custos viáveis para a organização. Entretanto, aceitar um risco significa tratá-lo já que, antes de ser aceito, ele passou por uma análise prévia. Para determinar se um risco é aceitável ou não, alguns aspectos devem ser levados em conta:

- Requisitos legais e de segurança;
- Objetivos do negócio;
- Relação custo x beneficio para a aquisição e implementação de medidas de segurança em relação aos riscos que devem ser reduzidos.

3.4 COMUNICAÇÃO DO RISCO

Esta é a última, porém não menos importante fase do processo de gestão de riscos. Nesta etapa os riscos já foram identificados e analisados. A comunicação do risco é de extrema utilidade, pois, além de deixar todos os envolvidos cientes dos riscos existentes, compartilha as responsabilidades de cada pessoa com os demais. Com o compartilhamento de responsabilidades sobre o risco, faz-se uma pressão sobre o setor responsável por decidir sobre a aceitação do risco ou a liberação de verbas para que seja efetuado o tratamento, agilizando o processo de gestão e diminuindo muito (ou até mesmo isentando) a responsabilidade da equipe de gestão de riscos, caso ocorra um incidente. Uma maneira muito comum de comunicação dos riscos, visando deixar o cenário claro para todos os usuários da empresa, é fazer campanhas de conscientização de segurança, diminuindo, bastante, a probabilidade de danos causados por falta de conhecimento sobre o assunto.

4 ESTUDO DE CASO: SOLUÇÃO DE ESTRUTURAÇÃO DA SEGURANÇA DA INFORMAÇÃO COM ANÁLISE E GESTÃO DE RISCOS DO INSTITUTO DE EDUCAÇÃO E PESQUISA

Este estudo de caso visa a implementação de um modelo de sistema de gestão da segurança da informação preparado para analisar criticamente e minimizar qualquer fraqueza que possa ser explorada em um instituto de pesquisa com o objetivo de estabelecer processos e procedimentos, seguindo a norma ABNT NBR ISO/IEC 27005, para controlar os riscos.

O nome do instituto permanecerá em sigilo, pois estas informações podem denegrir a sua vulnerabilidade e comprometer a segurança.

O Instituto mantém um programa de Pós-Doutoramento que desenvolve pesquisas em temáticas supervisionadas por pesquisadores. Para tanto, conta com um núcleo consolidado e reconhecido de pesquisadores-doutores, bolsistas de produtividade em pesquisa. Também aborda amplos programas de mestrado, doutorado e pós-graduação em ciência da informação.

4.1 Definição do Contexto

4.1.1 Funções e Estruturas da Organização

A organização é separada em três departamentos, secretaria (que engloba o setor administrativo) com 20 usuários, setor de pesquisas com 20 usuários e um laboratório para uso dos alunos com 30 computadores.

A hierarquia do Instituto compõe-se da seguinte maneira:

- Dois (02) Diretores – que compõem a parte mais alta na hierarquia (a alta Direção) e ficam alocados na Secretaria. Responsáveis por tomar as decisões mais críticas.

- Quatro (04) Coordenadores – responsáveis pelas tomadas de decisões mais cotidianas.

- Quatro (04) secretárias e 10 funcionários do administrativo –usuários que compõem o setor da Secretaria. Trabalham com informações críticas, mas que não interferem nas tomadas de decisão da Instituição.
- Vinte (20) pesquisadores –além de efetuarem pesquisas tecnológicas, são professores. Na maior parte do tempo, ficam no setor de Pesquisas, mas, nos horários de aula, utilizam equipamentos nos laboratórios.
- Alunos –usuários dos equipamentos nos laboratórios.

Existe somente um funcionário de TI para toda a empresa, logo, todas as responsabilidades pertinentes à área ficam sobre sua responsabilidade.

4.1.2 Ambiente Atual

A organização não possui nenhum tipo de controle de acessos (físicos e lógicos) ou proteção contra roubo de informações. O treinamento adequado dos funcionários para correta utilização dos equipamentos de TI é ineficiente e as políticas de segurança são inexistentes.

A topologia de rede utilizada é em árvore e não são adotados padrões para uma rede gerenciável e centralizada. Além disso, inúmeros problemas são encontrados, como:

- Centralização de informação;
- Os controles de acesso são inexistentes;
- Rotinas de backup não existem;
- Não existem rotinas de contingência;
- Os ativos de redes tais como roteadores, *switches* e modem, não estão em *racks* ou armários que possibilitem a sua proteção física. Estão no chão ou sobre a mesa;
- O software antivírus dos computadores está desatualizado;
- A rede não está segmentada em VLANs a fim de separar cada departamento.

A figura 05 mostra o diagrama da estrutura da rede.

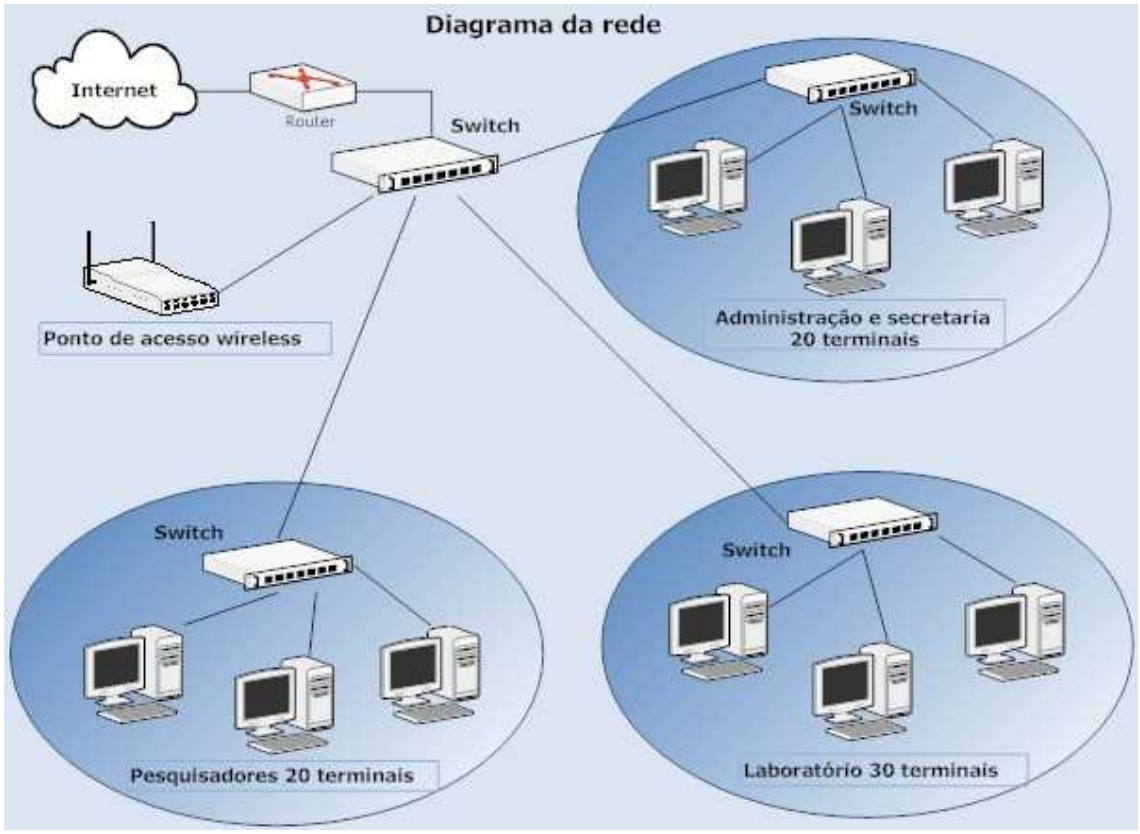

Figura 5-Diagrama da rede do instituto

4.1.3 Escopo do Projeto

O escopo do projeto compreende todos os ativos encontrados nos 3 setores da organização: Secretaria, Setor de pesquisas e laboratórios. Para implementar o processo de Gestão de Riscos no Instituto, deverão ser realizados os processos de análise/avaliação dos riscos, tratamento dos riscos e aceitação dos riscos, de forma individual, em cada uma das áreas de atuação: Recursos Humanos, Controle de Acessos (físicos e lógicos) e TIC.

Os processos realizados em cada área de atuação seguirão os critérios definidos nas seções a seguir.

4.1.4 Critério para Avaliação dos Riscos e Critérios de Impacto

Para a alta Direção do Instituto, maiores interessados na redução dos riscos existentes, a implantação do processo de Gestão de Riscos terá uma enorme importância, já que hoje existe uma perda muito grande de confiabilidade devido aos constantes desvios de informação. Além da perda de confiabilidade, no que diz respeito ao mercado, o Instituto considera uma perda imensurável os desvios de informações financeiras, de processos internos e até de pesquisas que poderiam ser vinculadas ao Instituto e acabam desviadas para outras Instituições. Visto isso, chegou-se à conclusão que o grau de prioridade das áreas, na ordem de tratamento dos riscos, é respectivamente: Secretaria (que engloba, também, o setor administrativo), Setor de Pesquisas e Laboratórios.

Para fazer a mensuração dos riscos, será criada uma tabela que levará em consideração, além do grau de prioridade dos setores, os critérios de preenchimento explicados anteriormente na tabela 3, que poderão ser definidos, dependendo da necessidade, da seguinte forma:

- Riscos com valor de 1 a 3 serão considerados “Baixos”.
- Riscos com valor de 4 a 6 serão considerados “Médios”.
- Riscos com valor de 7 a 10 serão considerados “Altos”.

Estas definições (Baixos, Médios e Altos) poderão ser utilizadas como base para a definição da aceitação (ou não aceitação) do risco, descrita na próxima seção.

A ordem de priorização do risco será descrita em uma tabela que servirá como saída da fase de análise/avaliação e, consequentemente, como entrada para a fase de tratamento do risco. O modelo a ser seguido para listar ordenadamente estas vulnerabilidades, de acordo com sua prioridade, deverá respeitar os padrões de preenchimento exemplificados na tabela 4.

4.1.5 Critérios para a aceitação do risco

Foi definido, juntamente com a alta direção do Instituto, que os riscos considerados “Baixos” poderão ser aceitos diretamente pela equipe que gerencia os riscos. Os Riscos considerados “Médios” deverão ser levados aos Coordenadores do Instituto para que sejam avaliados e decidido se eles serão aceitos ou encaminhados para o devido tratamento. Já os riscos considerados “Altos” deverão ser encaminhados para a Alta Direção para que seja definida, juntamente com a equipe que gerencia os riscos, a forma de tratamento a ser adotada para a minimização dos mesmos.

4.2 Análise/Avaliação de Riscos

4.2.1 Análise/Avaliação de Riscos da Área de Recursos Humanos

Na análise, constatou-se que existem muitas vulnerabilidades referentes a recursos humanos no Instituto. Estas vulnerabilidades vão desde a inexistência de políticas de uso de equipamentos, causando riscos considerados médios para o Instituto, até a constatação de que existe poucos recursos humanos de TI para suprir às demandas geradas por incidentes, que também ocorrem, em alguns casos, devido ao uso incorreto de equipamentos, que é outra vulnerabilidade encontrada no local.

A tabela 05 apresenta as vulnerabilidades e ameaças, mensurando os riscos e levando em consideração o impacto e a probabilidade de ocorrência do incidente.

Tabela 5-Matriz de relacionamento dos riscos da área de Recursos Humanos

	VULNERABILIDADES	AMEAÇAS	PROBABILIDADE	IMPACTO	RISCO
SECRETARIA	Poucos Recursos Humanos na área de TI	Demora na correção de Problemas impactantes no negócio	5	4	9
	Uso incorreto de software e/ou hardware	Danos aos equipamentos de TI	3	3	6
	Treinamento insuficiente e falta de conscientização em segurança	Roubo de informações	3	5	8
	Inexistência de políticas para uso correto de equipamentos	Uso não autorizado de equipamentos	4	3	7
SETOR DE PESQUISAS	Poucos Recursos de TI	Demora na correção de Problemas	5	3	8
	Uso incorreto de software e/ou hardware	Danos aos equipamentos de TI	2	3	5
	Treinamento insuficiente e falta de conscientização em segurança	Roubo de informações	2	4	6

	Inexistência de políticas para uso correto de equipamentos	Uso não autorizado de equipamentos	3	3	6
LABORATÓRIOS	Poucos Recursos de TI	Demora na correção de Problemas	3	3	6
	Uso incorreto de software e/ou hardware	Danos aos equipamentos de TI	5	2	7
	Treinamento insuficiente e falta de conscientização em segurança	Roubo de informações	5	1	6
	Inexistência de políticas para uso correto de equipamentos	Uso não autorizado de equipamentos	5	3	8

Com o resultado da tabela anterior, foi criada a tabela 06, que segue o padrão de tabela informado na definição do contexto, listando as vulnerabilidades e ameaças por ordem de prioridade no tratamento do risco, sendo realizada uma análise detalhada de cada risco. Esta tabela servirá como guia de entrada na fase de tratamento do risco de Recursos Humanos, que abordaremos na seção 4.4.1.

Tabela 6-Priorização dos riscos para Tratamento.

INDICE	VULNERABILIDADES	AMEAÇAS	SETOR DETERMINANTE	ANALISE DO RISCO	GRAU DE RISCO (0 a 10)
1º	Poucos Recursos Humanos de TI	Demora na correção de Problemas	SECRETARIA	Este é um risco com alta probabilidade de ocorrência e que necessita de ação imediata. Como só existe um recurso de TI, um problema grave pode não ser solucionado prontamente.	9
2º	Treinamento insuficiente e falta de conscientização em segurança	Roubo de informações	SECRETARIA	Este é um risco que pode trazer prejuízos imensuráveis para a Instituição, uma vez que informações importantes podem ser roubadas. Como o setor determinante foi a Secretaria, esta vulnerabilidade terá prioridade no tratamento levando-se em conta outras vulnerabilidades com o mesmo Grau de Risco.	8
3º	Inexistência de políticas para uso correto de equipamentos	Uso não autorizado de equipamentos	LABORATÓRIOS	Este é um risco que possui enorme probabilidade de ocorrência. Como não existe nenhuma política explicitando como e para que fins devam ser utilizados os equipamentos, muitos funcionários e, principalmente alunos, podem fazê-los maneira incorreta, gerando danos irreparáveis,	8

4º	Uso incorreto de software e/ou hardware	Danos aos equipamentos de TI	LABORATÓRIOS	Apesar de esta vulnerabilidade ter um baixo grau de impacto, a probabilidade de que ela ocorra, podendo causar indisponibilidade em vários equipamentos deixando alunos e professores ociosos.	7

4.2.2 Análise/Avaliação de riscos da área de Controle de Acessos

Ao analisar o controle de acesso dos departamentos da Secretaria, Pesquisa e Laboratório, foram identificadas vulnerabilidades e ameaças que têm o potencial de comprometer os ativos do Instituto. Como há uma série de riscos relacionados à inexistência de controles de acesso, os impactos podem ser desastrosos considerando os aplicativos e as informações críticas, inviabilizando a continuidade do negócio.

Durante as ações para identificação dos riscos, foi montada a tabela 07 onde serão analisadas as vulnerabilidades e ameaças de acordo com o seu grau de prioridade e impacto ao negócio.

Tabela 7-Matriz de relacionamento dos riscos da área de Controle de Acessos

	VULNERABILIDADES	AMEAÇAS	PROBABILIDADE	IMPACTO	RISCO
SECRETARIA	Inexistência de firewall para controle de acesso as portas	Invasão de hackers e vírus	5	4	9
	Download e upload não controlado	Defeito e alteração de software	5	3	8
	Processo de logon inexistente	Uso não autorizado de recursos da rede	5	4	9
	Inexistência de mecanismo de autenticação de usuário	Forjamento de direitos	5	4	9
	Inexistência de chaves para acesso à rede sem fio	Uso não autorizado de recursos da rede	4	4	8
	Documentações críticas sem proteção	Forjamento de direitos	5	4	9

	Trabalho não supervisionado de pessoas da limpeza ou de terceirizados	Furto de mídias ou documentos contendo informações	5	3	8
	Inexistência de identificação de funcionários, terceiros e alunos	Uso não autorizado de equipamentos, roubo de informações e equipamentos	4	3	7
	Inexistência de monitoramento dos ambientes vinte e quatro horas	Uso não autorizado de equipamentos, roubo de informações e equipamentos	4	3	7
	Inexistência de catracas eletrônicas para restrição de acesso nas entradas aos locais	Uso não autorizado de equipamentos, roubo de informações e equipamentos	3	3	6
	Ativos de rede, roteadores, switches e modem sem proteção	Falha nos equipamentos	5	4	9
SETOR DE PESQUISAS	Inexistência de firewall para controle de acesso às portas	Invasão de hackers e vírus	5	5	10
	Download e upload não controlado	Defeito e alteração de software	4	4	8
	Processo de logon inexistente	Uso não autorizado de recursos da rede	4	4	8
	Inexistência de mecanismo de autenticação de usuário	Forjamento de direitos	4	4	8
	Inexistência de chaves para acesso à rede sem fio	Uso não autorizado de recursos da rede	3	2	5
	Documentações críticas sem proteção	Forjamento de direitos	4	3	7
	Trabalho não supervisionado de pessoas da limpeza ou de terceirizados	Furto de mídias ou documentos contendo informações	4	3	7
	Inexistência de identificação de funcionários, terceiros e alunos	Uso não autorizado de equipamentos, roubo de informações e equipamentos	4	3	7
	Inexistência de monitoramento dos ambientes vinte e quatro horas	Uso não autorizado de equipamentos, roubo de informações e equipamentos e processamento ilegal de dados	3	4	7
	Inexistência de catracas eletrônicas para restrição de acesso nas entradas aos locais	Uso não autorizado de equipamentos, roubo de informações e equipamentos	3	2	5
	Ativos de rede, roteadores, switches e modem sem proteção	Falha nos equipamentos	4	2	6
LABORATÓRIOS	Inexistência de firewall para controle de acesso as portas	Invasão de hackers e vírus	4	4	8
	Download e upload não controlado	Defeito e alteração de software	3	3	6

	Trabalho não supervisionado de pessoas da limpeza ou de terceirizados	Furto de médias ou documentos contendo informações	3	2	5
	Inexistência de identificação de funcionários, terceiros e alunos.	Uso não autorizado de equipamentos, roubo de informações e equipamentos.	3	2	5
	Inexistência de chaves para acesso à rede sem fio	Uso não autorizado de recursos da rede	3	2	5
	Inexistência de monitoramento dos ambientes vinte e quatro horas	Uso não autorizado de equipamentos, roubo de informações e equipamentos e processamento ilegal de dados.	4	3	7
	Inexistência de catracas eletrônicas para restrição de acesso nas entradas aos locais	Uso não autorizado de equipamentos, roubo de informações e equipamentos.	3	2	5
	Ativos do laboratório, computador, mouse teclado e projetor sem proteção.	Uso não autorizado de equipamentos, roubo de informações e equipamentos.	4	2	6

Com o resultado da tabela anterior, foi criada a tabela 08, que segue o padrão de tabela informado na definição do contexto.

Tabela 8-Priorização dos riscos para tratamento.

INDICE	VULNERABILIDADES	AMEAÇAS	SETOR DETERMINANTE	ANALISE DO RISCO	GRAU/ RISCO (0 a 10)
1º	Inexistência de firewall para controle de acesso às portas	Invasão de hackers e vírus	Pesquisa	Tráfego de dados entre computador e Internet sem controle, acarretando propagação de vírus facilidade na invasão da rede	10
2º	Processo de logon inexistente	Uso não autorizado de recursos da rede	Secretaria	Obtenção de acesso aos dados e aplicativos sem autorização	9
3º	Inexistência de mecanismo de autenticação de usuário	Forjamento de direitos	Secretaria	Alteração não autorizada de dados e aplicativos, divulgação não autorizada e introdução de códigos maliciosos	9
4º	Ativos de rede, roteadores, switches e modem sem proteção	Falha nos equipamentos e roubo	Secretaria	Dados aos equipamentos podendo parar toda comunicação da rede, acarretando perdas financeiras	9
5º	Inexistência de monitoramento dos ambientes vinte e quatro horas	Uso não autorizado de equipamentos, roubo de informações e equipamentos e processamento ilegal de dados	Pesquisa	Pode acarretar roubo de equipamentos, atos de vandalismo, roubo de documentos e dados restritos	8
6º	Trabalho não supervisionado de pessoas da limpeza ou de terceirizados	Furto de mídias ou documentos contendo informações	Secretaria	Pode acarretar roubo de equipamentos, atos de vandalismo, roubo de documentos e dados restritos	8
7º	Download e upload não controlado	Defeito e alteração de software	Secretaria	Acesso a conteúdo malicioso, o usuário pode instalar sem querer programas espiões, o negócio pode ser colocado em posição vulnerável	8

				por colaboradores que se envolvem em atividades ilegais na Web	
8º	Inexistência de chaves para acesso à rede sem fio	Uso não autorizado de recursos da rede	Secretaria	Facilidade para que terceiros leiam seus e-mails ou descubram senhas e outras informações sigilosas, usem secretamente a conexão Wi-Fi e tenham acesso a todo ambiente de rede.	8
9º	Inexistência de catracas eletrônicas para restrição de acesso nas entradas aos locais	Uso não autorizado de equipamentos, roubo de informações e equipamentos	Secretaria	Pode acarretar roubo de equipamentos, atos de vandalismo, roubo de documentos e dados restritos	7
10º	Inexistência de identificação de funcionários, terceiros e alunos	Uso não autorizado de equipamentos, roubo de informações e equipamentos	Secretaria	Pode acarretar roubo de equipamentos, atos de vandalismo, roubo de documentos e dados restritos	7

4.2.3 Análise/Avaliação de riscos da área de TIC

A área de TIC foi analisada nos setores da empresa e constatou-se a existência de riscos de vários níveis que podem gerar indisponibilidade de recursos como, por exemplo, uma parada total da rede de dados. A integridade também corre o risco de ser afetada, pois os dados podem ser modificados ou perdidos, devido à inexistência de serviços básicos como serviço de impressão centralizado, servidores de arquivos, padronização de proteção individual como firewall e antivírus.

Os riscos associados aos setores foram descritos e organizados na tabela 09. Para as vulnerabilidades cuja análise foi comum aos 3 setores, foi criada a tabela 10. Nestas, os riscos serão analisados de acordo com a probabilidade e impacto ao negócio.

Tabela 9-Matriz de relacionamento dos riscos da área de TIC

	VULNERABILIDADES	AMEAÇAS	PROBABILIDADE	IMPACTO	RISCO
SECRETARIA	Distribuição irregular do cabeamento de rede	Falha na transmissão de dados	3	2	5
	Conexões de rede mal feitas	Falha na transmissão de dados	3	2	5
	Sistema operacional desatualizado	Comprometimento dos dados	3	2	5

	Impressões não recolhidas expostas no dispositivo de impressão	Furto de informação	4	2	6
SETOR DE PESQUISAS	Distribuição irregular do cabeamento de rede	Falha na transmissão de dados	3	2	5
	Conexões de rede mal feitas	Falha na transmissão de dados	3	2	5
	Concentrador de rede exposto (fora do rack)	Falha na transmissão de dados	5	2	7
	Sistema operacional desatualizado	Comprometimento dos dados	3	2	5
LABORATÓRIOS	Distribuição irregular do cabeamento de rede	Falha na transmissão de dados	3	2	5
	Conexões de rede mal feitas	Falha na transmissão de dados	3	2	5
	Concentrador de rede exposto (fora do rack)	Falha na transmissão de dados	5	2	7
	Sistema operacional desatualizado	Comprometimento dos dados	3	2	5

Tabela 10-Matriz de relacionamento de riscos comuns aos três setores.

	VULNERABILIDADES	**AMEAÇAS**	**PROBABILIDADE**	**IMPACTO**	**RISCO**
COMUM	Antivírus desatualizado	Comprometimento dos dados	5	2	7
	Procedimento inexistente para instalação de softwares.	Abuso de direitos	5	2	7
	Uso não controlado de software.	Defeito de software.	3	2	5
	Concentrador de rede exposto (fora do rack)	Falha na transmissão de dados	5	2	7

Com o resultado da tabela anterior, foi criada a tabela 08, que segue o padrão de tabela informado na definição do contexto.

Tabela 11-Priorização dos riscos para tratamento.

INDICE	VULNERABILIDADES	AMEAÇAS	SETOR DETERMINANTE	ANALISE DO RISCO	GRAU/ RISCO (0 a 10)
1º	Concentrador de rede exposto (fora do rack)	Falha na transmissão de dados	COMUM	O risco nesta vulnerabilidade é a extensão do impacto que pode atingir todo um setor ou mesmo toda a rede, dependendo do switch que for afetado.	7
2º	Procedimento inexistente para instalação de softwares.	Abuso de direitos e defeito de software.	COMUM	Risco de disponibilidade da informação por falha no software.	7
3º	Antivírus desatualizado	Comprometimento da integridade e disponibilidade dos dados	COMUM	Risco de infecções por códigos maliciosos que podem comprometer a integridade e a disponibilidade da informação.	7
4º	Impressões não recolhidas expostas no dispositivo de	Furto de informação	SECRETARIA	Uma impressão que foi esquecida na impressora pode afetar a confidencialidade da informação, pois	6

	impressão			pessoas não autorizadas podem furtar o documento.	
5º	Uso não controlado de software.	Defeito de software.	COMUM	Risco de disponibilidade da informação por falha no funcionamento do software.	5
6º	Distribuição irregular do cabeamento de rede	Falha na transmissão de dados	SECRETARIA	Este é um risco que pode acarretar impacto de paralisação do tráfego de dados na rede causando interrupção de trabalhos que pode ser um simples cadastro de notas dos alunos ou mesmo uma operação financeira.	5
7º	Conexões de rede mal feitas	Falha na transmissão de dados	SECRETARIA	Este risco pode afetar o tráfego de dados na rede paralisando algumas operações simples como lançamento das notas dos alunos, o que geraria retrabalho na digitação dos dados, como também pode afetar uma operação financeira. Porém este risco pode ser pontual, ou seja, atingir um ou outro usuário.	5
8º	Sistema operacional desatualizado	Falha na integridade dos dados	SECRETARIA	O fabricante disponibiliza periodicamente atualizações para cobrir falhas de segurança que podem comprometer o funcionamento e a segurança do sistema operacional	5

4.3 Comunicação do Risco

Com o intuito de compartilhar a responsabilidade sobre os riscos encontrados e realizar as tomadas de decisão para efetuar o tratamento, foram comunicados aos responsáveis (Alta direção e Coordenadores) todas as vulnerabilidades e riscos encontrados na fase de análise.

4.4 Tratamento dos Riscos

O tratamento dos riscos neste projeto será realizado de maneira uniforme de acordo com os riscos levantados em cada área de atuação, ou seja, o tratamento será realizado de forma a gerar reflexos em todo o Instituto, englobando os três setores: Secretaria, Setor de Pesquisas e Laboratório.

Serão apresentados, nas seções seguintes, os planos de ação para tratar cada risco que foi descrito na seção 4.2. Este plano será organizado por um índice que corresponderá à prioridade obtida por cada risco em sua respectiva área.

4.4.1 Tratamento dos Riscos da área de Recursos Humanos

Seguindo a ordem de priorização de tratamento descrita na tabela 12, seguem as sugestões de tratamento para cada risco da área de RH:

Tabela 12-Tratamento do risco da área de RH.

INDICE	VULNERABILIDADES	OPÇÃO DE TRATAMENTO	TRATAMENTO SUGERIDO	GRAU/ RISCO (0 a 10)
1º	Poucos Recursos Humanos de TI	REDUÇÃO DO RISCO	Contratação de, pelo menos, mais dois profissionais capacitados para auxiliar nos problemas referentes a TI, totalizando três funcionários nesta área.	7
2 º	Treinamento insuficiente e falta de conscientização em segurança	REDUÇÃO DO RISCO	Efetuar treinamento em segurança da informação para todos os funcionários, conscientizando-os sobre os riscos, periodicamente.	7
3 º	Inexistência de políticas para uso correto de equipamentos	REDUÇÃO DO RISCO	Criar uma política de segurança que guie os usuários para a utilização correta de equipamentos, softwares e informações, incluindo a responsabilidade de cada um. Inclusive, caso necessário, explicitar punições caso as regras não sejam cumpridas.	7
4 º	Uso incorreto de software e/ou hardware	REDUÇÃO DO RISCO	Efetuar treinamento dos usuários sobre como utilizar corretamente os softwares e os hardwares da Instituição. Este tratamento, juntamente com uma política de segurança, poderá reduzir drasticamente esta vulnerabilidade.	6

4.4.2 Tratamento dos Riscos da área de Controle de Acessos

Seguindo a ordem de priorização de tratamento descrita na tabela 13, seguem as sugestões de tratamento para cada risco da área de Controle de Acessos:

Tabela 13-Tratamento do risco da área Controle de Acessos

ÍNDICE	VULNERABILIDADES	OPÇÃO DE TRATAMENTO	TRATAMENTO SUGERIDO	GRAU/ RISCO (0 a 10)
1 º	Inexistência de firewall para controle de acesso as portas	REDUÇÃO DO RISCO	Implantar um Firewall com todas as portas bloqueadas, liberar somente as portas necessárias para realização das atividades	10
2 º	Processo de logon inexistente	EDUÇÃO DO RISCO	Processo de logon. Para obter acesso aos dados e aplicativos, o processo envolve a utilização de um User ID e uma senha. Para dificultar uma invasão, o limite de tentativas é de três, caso as tentativas sejam incorretas a conta do usuário será bloqueada.	9

3 º	Inexistência de mecanismo de autenticação de usuário	REDUÇÃO DO RISCO	Para autenticação do usuário, o sistema solicitará User ID e senha mais o crachá, que também é um cartão inteligente.	9
4 º	Ativos de rede, roteadores, switches e modem sem proteção	REDUÇÃO DO RISCO	Os ativos de redes servidores, roteadores, switches e modem estão organizados em racks em uma sala com acesso restrito somente à equipe de segurança – o acesso à sala é feito por autenticação biométrica em conjunto com o crachá.	9
5 º	Inexistência de monitoramento dos ambientes vinte e quatro horas	REDUÇÃO DO RISCO	Monitorando dos ambientes vinte e quatro horas por dia através de câmeras de vigilância.	8
6 º	Trabalho não supervisionado de pessoas da limpeza ou de terceirizados	REDUÇÃO DO RISCO	Supervisão da equipe de limpeza, que é terceirizada.	8
7 º	Download e upload não controlado	REDUÇÃO DO RISCO	Restringir o acesso á internet e bloquear o download e upload.	8
8 º	Inexistência de chaves para acesso á rede sem fio	REDUÇÃO DO RISCO	A autenticação na rede sem fio é feita através de um servidor RADIUS utilizando certificados digitais.	8
9 º	Inexistência de catracas eletrônicas para restrição de acesso nas entradas dos locais	REDUÇÃO DO RISCO	Uso de catracas eletrônicas para a restrição de acesso nas entradas dos locais.	7
10 º	Inexistência de identificação de funcionário, terceiros e alunos	REDUÇÃO DO RISCO	Identificação de todos os funcionários, pesquisadores, alunos e visitantes por meio de crachá, que devem sempre ser usados em locais visíveis.	7

4.4.3 Tratamento dos Riscos da área de TIC

A tabela 14 indica a opção de tratamento utilizada e a sugestão para tratar o risco.

Tabela 14-Tratamento do risco TIC

ÍNDICE	VULNERABILIDADES	OPÇÃO DE TRATAMENTO	TRATAMENTO SUGERIDO	GRAU/ RISCO (0 a 10)
1 º	Concentrador de rede exposto (fora do rack)	REDUÇÃO DO RISCO	Organizar os equipamentos em salas específicas se possível de modo estruturado.	7
2 º	Procedimento inexistente para instalação de softwares.	REDUÇÃO DO RISCO	Elaborar documentações que possibilitem a instalação de softwares de forma segura.	7
3 º	Antivírus desatualizado	REDUÇÃO DO RISCO	Implementar um sistema centralizado de defesa contra vírus ou mesmo um critério para agendar as atualizações.	7

4 º	Impressões não recolhidas expostas no dispositivo de impressão	REDUÇÃO DO RISCO	Definir normas para utilização de material impresso evitando deixa-los à disposição com a utilização de salas de pool de impressão.	6
5 º	Uso não controlado de software.	REDUÇÃO DO RISCO	Elaborar uma lista de aplicativos de uso autorizado na empresa.	5
6 º	Distribuição irregular do cabeamento de rede	REDUÇÃO DO RISCO	Organizar o cabeamento de dados e voz para evitar o bloqueio da passagem ou rompimento dos cabos.	5
7 º	Conexões de rede mal feitas	REDUÇÃO DO RISCO	Verificar as conexões e fazer as devidas correções.	5
8 º	Sistema operacional desatualizado	REDUÇÃO DO RISCO	Elaborar um plano para distribuir as atualizações de forma centralizada evitando erro no sistema operacional.	5

4.5 Risco Residual

Após implementar o tratamento sugerido em cada risco, deve-se atentar quanto à eficácia de cada um e aos resultados obtidos de forma a assegurar que o tratamento tenha reduzido o risco a um nível satisfatório. Para tanto, é necessário que seja feita uma nova análise no risco residual de cada vulnerabilidade.

4.6 Aceitação dos Riscos

Como é possível observar através das opções de tratamento das seções anteriores, em nenhum dos riscos analisados escolheu-se a opção de retenção, ou seja, a aceitação do risco por parte da Alta Direção (nos riscos considerados altos) ou dos Coordenadores (nos riscos considerados médios). Como nenhum dos riscos identificados obteve grau de risco “baixo”, nenhum deles foi retido diretamente. É sugerido, pela equipe que está realizando este processo, que após a análise dos riscos residuais, caso os mesmos encontrem-se com grau de risco “baixo”, seja formalizada, com a alta direção do Instituto, a aceitação destes riscos.

4.7 Monitoramento do Risco

O monitoramento do risco também deverá ser implementado para verificar se houve alterações nos riscos analisados e avaliados previamente. Além de identificar possíveis mudanças no grau de cada risco, é sugerido, pela equipe que está realizando este processo, que seja verificado constantemente o surgimento de novos riscos e possíveis extinções de riscos identificados anteriormente.

CONCLUSÃO E TRABALHO FUTURO

Este trabalho apresentou um estudo sobre a análise de risco em segurança da informação sob os aspectos da norma ABNT NBR ISO/IEC 27005 e 27001 e sua aplicabilidade em um ambiente acadêmico cuja denominação foi ocultada por motivos de segurança.

Foi abordado inicialmente o conceito da segurança da informação com suas características básicas e a necessidade da sua implementação para que uma organização tenha seus ativos protegidos das ameaças e dos invasores e atacantes.

Toda organização empresarial tem seus objetivos de negócio que precisam ser atingidos para assim ter sucesso no empreendimento. Com o negócio em atividade poderão surgir interesses dos concorrentes para obterem informações internas da empresa. Pode haver uma ameaça interna de funcionários revoltos ou insatisfeitos e degradar os ativos ou repassar informações confidenciais.

Para minimizar estas ações foi comentado no capítulo da gestão e análise de riscos da segurança da informação como todo o processo funciona. O propósito foi estabelecer uma maneira flexível, porém sistemática para manter um baixo grau de risco no ambiente a se proteger.

Os riscos então foram identificados e priorizados para serem tratados a fim de serem anulados, reduzidos, transferidos ou mesmo aceitos pela organização.

De qualquer forma a organização está sempre em plena mudança, pois os negócios podem ser alterados, os objetivos e valores mudam.

Concluindo o estudo foi mostrado uma implementação prática de todo o processo de gestão e análise de riscos onde se pôde constatar que a essência deste ciclo é possuir um monitoramento constante para que possa adequar as mudanças aos novos riscos que assim forem identificados.

Como trabalho futuro é indicada a continuidade do processo de gestão de riscos, após serem implementadas as formas de tratamentos sugeridas, a fim de reavaliar os riscos, retendo-os quando necessário e identificando riscos futuros.

ANEXO 1

Tabela 1-Exemplo de vulnerabilidades
Fonte: NORMA ABNT ISO/IEC 27005

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Hardware	Manutenção insuficiente/Instalação defeituosa de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia
	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento
	Sensibilidade à radiação eletromagnética	Radiação eletromagnética
	Inexistência de um controle eficiente de mudança de configuração	Erro durante o uso
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Armazenamento não protegido	Furto de mídia ou documentos
	Falta de cuidado durante o descarte	Furto de mídia ou documentos
	Realização de cópias não controlada	Furto de mídia ou documentos
Software	Procedimentos de teste de *software* insuficientes ou inexistentes	Abuso de direitos
	Falhas conhecidas no *software*	Abuso de direitos
	Não execução do "*logout*" ao se deixar uma estação de trabalho desassistida	Abuso de direitos
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados	Abuso de direitos
	Inexistência de uma trilha de auditoria	Abuso de direitos
	Atribuição errônea de direitos de acesso	Abuso de direitos
	Software amplamente distribuído	Comprometimento dos dados
	Utilizar programas aplicativos com um conjunto errado de dados (referentes a um outro período)	Comprometimento dos dados
	Interface de usuário complicada	Erro durante o uso
	Documentação inexistente	Erro durante o uso
	Configuração de parâmetros incorreta	Erro durante o uso
	Datas incorretas	Erro durante o uso

Rede	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de usuários	Forjamento de direitos
	Tabelas de senhas desprotegidas	Forjamento de direitos
	Gerenciamento de senhas mal feito	Forjamento de direitos
	Serviços desnecessários permanecem habilitados	Processamento ilegal de dados
	Software novo ou imaturo	Defeito de *software*
	Especificações confusas ou incompletas para os desenvolvedores	Defeito de *software*
	Inexistência de um controle eficaz de mudança	Defeito de *software*
	Download e uso não controlado de *software*	Alteração do *software*
	Inexistência de cópias de segurança (*back-up*)	Alteração do *software*
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento
	Inexistência de evidências que comprovem o envio ou o recebimento de mensagens	Repúdio de ações
	Linhas de Comunicação desprotegidas	Escuta não autorizada
	Tráfego sensível desprotegido	Escuta não autorizada
	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor e do receptor	Forjamento de direitos
	Arquitetura insegura da rede	Espionagem à distância
	Transferência de senhas em claro	Espionagem à distância
	Gerenciamento de rede inadequado (quanto à flexibilidade de roteamento)	Saturação do sistema de informação
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Recursos humanos	Ausência de recursos humanos	Indisponibilidade de recursos humanos
	Procedimentos de recrutamento inadequados	Destruição de equipamento ou mídia
	Treinamento insuficiente em segurança	Erro durante o uso
	Uso incorreto de *software* e *hardware*	Erro durante o uso
	Falta de conscientização em segurança	Erro durante o uso
	Inexistência de mecanismos de monitoramento	Processamento ilegal de dados
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de mídia ou documentos
	Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de equipamento

Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e aposentos	Destruição de equipamento ou mídia
	Localização em área suscetível a inundações	Inundação
	Fornecimento de energia instável	Interrupção do suprimento de energia
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamentos
Organização	Inexistência de um procedimento formal para o registro e a remoção de usuários	Abuso de direitos
	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)	Abuso de direitos
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros	Abuso de direitos
	Inexistência de procedimento de monitoramento das instalações de processamento de informações	Abuso de direitos
	Inexistência de auditorias periódicas (supervisão)	Abuso de direitos
	Inexistência de procedimentos para a identificação e análise/avaliação de riscos	Abuso de direitos
	Inexistência de relatos de falha nos arquivos (*logs*) de auditoria das atividades de administradores e operadores	Abuso de direitos
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Acordo de nível de serviço (SLA - da sigla do termo em inglês) inexistente ou insuficiente	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de procedimento de controle de mudanças	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de um procedimento formal para o controle da documentação do SGSI	Comprometimento dos dados
	Inexistência de um procedimento formal para a supervisão dos registros do SGSI	Comprometimento dos dados
	Inexistência de um processo formal para a autorização das informações disponíveis publicamente	Dados de fontes não confiáveis
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de ações
	Inexistência de um plano de continuidade	Falha de equipamento
	Inexistência de política de uso de correspondência eletrônica (*e-mail*)	Erro durante o uso
	Inexistência de procedimentos para a instalação de *software* em sistemas operacionais	Erro durante o uso
	Ausência de registros nos arquivos de auditoria (*logs*) de administradores e operadores	Erro durante o uso
	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso

REFERÊNCIA

NBR ISO/IEC 17799 – Código de Prática para a Gestão de Segurança da Informação.

NBR ISO/IEC 27001 - Sistema de Gestão de Segurança da Informação.

NBR ISO/IEC 27005 – Gestão de Riscos de Segurança da Informação.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**, Rio de Janeiro: Editora Ciência Moderna Ltda., 2003.

Guia Oficial para Formação de Gestores em Segurança da Informação – Security Officer

KUROSE, J.F.;ROSS, K.W. **Redes de computadores e a internet**, São Pulo: Editora Pearson Addison Wesley, 2006.

NAKAMURA, Emilio Tissato, GEUS, Paulo Lício. **Segurança de redes: em ambientes cooperativos**, São Paulo: Editora Futura, 2003.