UNIVERSIDADE FEEVALE

LUIZ HENRIQUE LISBOA

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo
2020

LUIZ HENRIQUE LISBOA

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

Orientador: Vandersilvio da Silva

Novo Hamburgo
2020

RESUMO

Dia após dia surgem novas vulnerabilidades no nosso meio, causando grandes prejuízos para as empresas e muitas vezes esses problemas podem ser amenizados, dificultados e muitos deles até mesmo evitados. Muitas empresas não estão preparadas para lidar com os riscos de segurança da informação.

Com isso este estudo tem como objeto explicar e demonstrar de forma teórica e prática a gestão de riscos relacionados à segurança da informação e sua aplicabilidade, tendo como fatores a identificação, análise, avaliação e sequencialmente o tratamento destes riscos.

Serão apresentadas diretrizes da norma ISO 27005, que define processos de gestão de riscos visando auxiliar profissionais do ramo e gestores de organizações para a importância deste controle. Ao se falar em gestão de risco automaticamente tratamos de cenários cujas consequências afetam a confidencialidade, integridade e disponibilidade.

Palavras-chave: Gestão de risco. Gestão de informação. Norma ISO/IEC. Segurança da Informação. CID.

SUMÁRIO

MOTIVAÇÃO 5
OBJETIVOS 8
METODOLOGIA 9
CRONOGRAMA 10
BIBLIOGRAFIA 11

MOTIVAÇÃO

Este trabalho tem como propósito instigar, disseminar e motivar gestores de empresas, profissionais de TI a terem uma visão mais crítica sobre os problemas voltados para a gestão de riscos, deixando-as assim mais suscetíveis às ameaças.

Diante da evolução tecnológica que vivemos a cada dia, as organizações precisam se proteger de inúmeros fatores relacionados à segurança da informação, dentro deste contexto amplo, temos a gestão de riscos que fornece diretrizes para o processo.

Gerenciamento de risco se baseia em determinar, identificar, analisa, avaliar, tratar os riscos e aceitar os que não foram ou não puderam ser tratados, assim, deixando o ambiente menos vulnerável possível e aceitável.

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade.

Segundo a cartilha da Cert.br (2006), um sistema é dito seguro se atende a três critérios básicos: confidencialidade, integridade e disponibilidade.

Segundo Santos (2008), a gestão de riscos é implementada para aumentar a eficiência operacional, reduzindo assim, perdas como fraudes, falhas, sinistros e acidentes, conduzindo a empresa a uma melhoria nos seus processos. Com base em uma análise mais detalhada e focada na área de Tecnologia da Informação.

A dependência que as organizações têm da infraestrutura de TI junto com a crescente facilidade de acesso à tecnologia elevaram a importância das informações, um ativo intangível importante para a tomada de decisões nas organizações. (ALBUQUERQUE JUNIOR, et al. 2014).

AMARAL (2001, p. 3) alerta para que esse novo ambiente computacional no qual os computadores estão ligados em rede tornou-se extremamente complexo, heterógenos e distribuído, dificultando o gerenciamento de questões relativas à segurança da informação nos mesmos.

A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (SÊMOLA, 2001, p. 18).

MOREIRA (2001, p. 3) comenta que “a informação vem sendo considerada como um dos principais ativos para as empresas, e, desta forma, a segurança da informação vem se

tornando uma real necessidade no dia-a-dia das organizações para proteger seus segredos de negócios ou suas estratégias comerciais, sendo considerada hoje fator de sobrevivência e competitividade para as corporações modernas".

Para Schneier (2001), "as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados." O crime no ciberespaço inclui tudo o que se pode esperar do mundo físico: roubo, extorsão, vandalismo, voyeurismo, exploração, jogos de trapaças, fraude etc.

Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Segundo Thomas A. Wadlow, "A segurança deverá ser proporcional ao valor do que se está protegendo". Ou seja, a implantação do sistema de segurança da informação tem de apresentar um custo benefício que torne a tentativa de ataque tão cara que desestimule o atacante, ao mesmo tempo em que ela é mais barata do que o valor da informação protegida.

MOREIRA (2001, p. 4) destaca que agentes ameaçadores aos ambientes computacionais estão em constante evolução, seja em número ou em forma, e que novos vírus surgem em um curto espaço de tempo, trazendo riscos às informações das empresas. Ataques à rede interna das empresas podem quebrar o sigilo de informações confidenciais, e ter as mesmas divulgadas imediatamente na internet ou para concorrentes.

Pesquisas mostram que 40% do acesso à Internet nas empresas não estão relacionados aos negócios, o que resulta em perda de produtividade e abertura para a entrada de spywares e vírus (CADERNO DIGITAL, 2008).

À medida que os avanços nos desenvolvimentos de soluções apontam para um cenário mais exigente, a tendência pela busca de alternativas e otimizações nas técnicas de Segurança da Informação também aumenta. Isto ocorre devido à exposição natural de todo e qualquer "organismo tecnológico" à carga diária de ataques e intrusões (MALERBA, 2010).

Diante deste cenário a gestão de risco em tecnologia da informação se torna cada vez mais indispensável para as empresas, precisando se adequar e tentando evitar qualquer um destes problemas que podem afetá-los. Criando mecanismos visando evitar, dificultar ou até mesmo impossibilitar que haja alguma falha na organização.

Baseado nisso, entende-se que há uma grande importância no desenvolvimento de processos de educação e conscientização relacionados à Segurança da Informação. Contudo,

sabe-se que existe uma carência no que diz respeito a métodos eficazes para instruir pessoas que trabalham em ambientes corporativos e lidam com dados sensíveis.

O principal intuito desta pesquisa é auxiliar gestão de riscos em segurança da informação, bem como trazer uma visão diferente para gestores de organizações a darem mais importância para este assunto. Trazendo um agrupamento que proporciona formas de se proteger e manter os três pilares básicos sobre segurança intactos o máximo possível.

OBJETIVOS

Demonstrar de forma prática os benefícios da Gestão de Riscos em Segurança da Informação.

Objetivos específicos:

- Explicar o que é Gestão de Riscos em Segurança da Informação;
- Demonstrar a importância da Gestão de Riscos;
- Mapear pontos importantes para controles;
- Demonstrar formas de aplicar correções;
- Fazer um estudo de pesquisa baseado em uma empresa;
- Trazer uma abordagem prática de como funciona este gerenciamento.

METODOLOGIA

A elaboração deste estudo se baseia em trazer uma abordagem teórica e prática sobre o tema.

A busca de pesquisa será realizada principalmente com base na ISO/IEC 27005:2011 que tem como princípio estabelecer diretrizes para o processo de gestão de riscos de segurança da informação.

Serão realizadas pesquisas bibliográficas e em sites com exemplos de aplicabilidades, além de pesquisas e análises em trabalhos anteriores buscando unir estratégias a fim de criar uma forma explicativa de como podemos atuar para minimizando os riscos ao máximo.

Serão identificação as principais causas de insucessos na gestão de risco.

Estudos serão elaborados sobre como aplicar a gestão de riscos nas organizações, definindo estratégias.

Será aplicada a gestão de riscos em uma organização de acordo com as estratégias definidas anteriormente, acompanhando o processo e trazendo um comparativo de antes e depois da sua aplicação.

CRONOGRAMA

Trabalho de Conclusão I

Etapa	**Meses**			
	Ago	**Set**	**Out**	**Nov**
Estudo teórico sobre o tema escolhido	X	X		
Elaboração do anteprojeto	X	X		
Estudo sobre técnicas de gestão de risco		X	X	
Escrita do TC I			X	
Revisão e melhorias do TC I			X	X
Entrega do TC I				X

Trabalho de Conclusão II

Etapa	**Meses**			
	Mar	**Abri**	**Mai**	**Jun**
Análise inicial de caso de estudo	X			
Levantamento de dados e estrutura		X		
Elaboração de plano de ação		X	X	
Executar plano de ação		X	X	
Análise de dados após execução do plano de ação			X	X
Elaboração do TC2	X	X	X	X
Revisão e melhorias do TC2			X	X
Entrega do TC2				X

BIBLIOGRAFIA

ALBUQUERQUE JUNIOR, Antonio Eduardo de; SANTOS, Ernani Marques dos; ALBUQUERQUE, Elaine Santos de. Segurança da Informação em um instituto de pesquisa: uma análise utilizando a norma ISO/IEC 27002: 2005. 2014.

LAUREANO, Marcos AP; MORAES, Paulo Eduardo Sobreira. Segurança como estratégia de gestão da informação. **Revista Economia & Tecnologia**, v. 8, n. 3, p. 38-44, 2005.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. Brasport, 2012.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Saraiva Educação SA, 2017.

FREITAS, Eduardo Antônio Mello; AMOUZOU, Koffi Djima. Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação. V13, 2009.

GABBAY, Max Simon. **Fatores influenciadores da implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte**. 2006. Dissertação de Mestrado. Universidade Federal do Rio Grande do Norte

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v. 4, n. 3, p. 375-397, 2007.

ALEXANDRIA, João Carlos Soares de. **Gestão de Segurança da Informação-uma proposta para potencializar a efetividade da Segurança da Informação em ambiente de pesquisa científica**. 2009. Tese de Doutorado. Universidade de São Paulo.

LIMA, Adriano. **Gestão da segurança e infraestrutura de tecnologia da informação**. Senac, 2018.

SÊMOLA, M. Gestão da Segurança da Informação: visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003 - 17a reimpressão.

Santos, R. **O Bê-a-Bá da Gestão de Risco e Governança.** 2008.