Gestão de Risco em Tecnologia da Informação

Luiz Otávio Botelho Lento

Pós-Graduação

UnisulVirtual
A sua universidade a distância

UNISUL

Créditos

Universidade do Sul de Santa Catarina | Campus UnisulVirtual | Educação Superior a Distância
Avenida dos Lagos, 41 – Cidade Universitária Pedra Branca | Palhoça – SC | 88137-900 | *Fone/fax*: (48) 3279-1242 e 3279-1271 | *E-mail*: cursovirtual@unisul.br | *Site*: www.unisul.br/unisulvirtual

Reitor
Ailton Nazareno Soares

Vice-Reitor
Sebastião Salésio Heerdt

Chefe de Gabinete da Reitoria
Willian Corrêa Máximo

Pró-Reitor de Ensino e Pró-Reitor de Pesquisa, Pós-Graduação e Inovação
Mauri Luiz Heerdt

Pró-Reitora de Administração Acadêmica
Miriam de Fátima Bora Rosa

Pró-Reitor de Desenvolvimento e Inovação Institucional
Valter Alves Schmitz Neto

Diretora do Campus Universitário de Tubarão
Milene Pacheco Kindermann

Diretor do Campus Universitário da Grande Florianópolis
Hércules Nunes de Araújo

Secretária-Geral de Ensino
Solange Antunes de Souza

Diretora do Campus Universitário UnisulVirtual
Jucimara Roesler

Equipe UnisulVirtual

Diretor Adjunto
Moacir Heerdt

Secretaria Executiva e Cerimonial
Jackson Schuelter Wiggers (Coord.)
Marcelo Fraiberg Machado
Tenille Catarina

Assessoria de Assuntos Internacionais
Murilo Matos Mendonça

Assessoria de Relação com Poder Público e Forças Armadas
Adenir Siqueira Viana
Walter Félix Cardoso Junior

Assessoria DAD - Disciplinas a Distância
Patrícia da Silva Meneghel (Coord.)
Carlos Alberto Areias
Cláudia Berh V. da Silva
Conceição Aparecida Kindermann
Luiz Fernando Meneghel
Renata Souza de A. Subtil

Assessoria de Inovação e Qualidade de EAD
Denia Falcão de Bittencourt (Coord.)
Andrea Ouriques Balbinot
Carmen Maria Cipriani Pandini

Assessoria de Tecnologia
Osmar de Oliveira Braz Júnior (Coord.)
Felipe Fernandes
Felipe Jacson de Freitas
Jefferson Amorin Oliveira
Phelipe Luiz Winter da Silva
Priscila da Silva
Rodrigo Battistotti Pimpão
Tamara Bruna Ferreira da Silva

Coordenação Cursos

Coordenadores de UNA
Diva Marília Flemming
Marciel Evangelista Catâneo
Roberto Iunskovski

Auxiliares de Coordenação
Ana Denise Goularte de Souza
Camile Martinelli Silveira
Fabiana Lange Patricio
Tânia Regina Goularte Waltemann

Coordenadores Graduação
Aloísio José Rodrigues
Ana Luísa Mülbert
Ana Paula R.Pacheco
Artur Beck Neto
Bernardino José da Silva
Charles Odair Cesconetto da Silva
Dilsa Mondardo
Diva Marília Flemming
Horácio Dutra Mello
Itamar Pedro Bevilaqua
Jairo Afonso Henkes
Janaína Baeta Neves
Jorge Alexandre Nogared Cardoso
José Carlos da Silva Junior
José Gabriel da Silva
José Humberto Dias de Toledo
Joseane Borges de Miranda
Luiz G. Buchmann Figueiredo
Marciel Evangelista Catâneo
Maria Cristina Schweitzer Veit
Maria da Graça Poyer
Mauro Faccioni Filho
Moacir Fogaça
Nélio Herzmann
Onei Tadeu Dutra
Patrícia Fontanella
Roberto Iunskovski
Rose Clér Estivalete Beche

Vice-Coordenadores Graduação
Adriana Santos Rammê
Bernardino José da Silva
Catia Melissa Silveira Rodrigues
Horácio Dutra Mello
Jardel Mendes Vieira
Joel Irineu Lohn
José Carlos Noronha de Oliveira
José Gabriel da Silva
José Humberto Dias de Toledo
Luciana Manfroi
Rogério Santos da Costa
Rosa Beatriz Madruga Pinheiro
Sergio Sell
Tatiana Lee Marques
Valnei Carlos Denardin
Sâmia Mônica Fortunato (Adjunta)

Coordenadores Pós-Graduação
Aloísio José Rodrigues
Anelise Leal Vieira Cubas
Bernardino José da Silva
Carmen Maria Cipriani Pandini
Daniela Ernani Monteiro Will
Giovani de Paula
Karla Leonora Dayse Nunes
Letícia Cristina Bizarro Barbosa
Luiz Otávio Botelho Lento
Roberto Iunskovski
Rodrigo Nunes Lunardelli
Rogério Santos da Costa
Thiago Coelho Soares
Vera Rejane Niedersberg Schuhmacher

Gerência Administração Acadêmica
Angelita Marçal Flores (Gerente)
Fernanda Farias

Secretaria de Ensino a Distância
Samara Josten Flores (Secretária de Ensino)
Giane dos Passos (Secretária Acadêmica)
Adenir Soares Júnior
Alessandro Alves da Silva
Andréa Luci Mandira
Cristina Mara Schauffert
Djeime Sammer Bortolotti
Douglas Silveira
Evilym Melo Livramento
Fabiano Silva Michels
Fabricio Botelho Espíndola
Felipe Wronski Henrique
Gisele Terezinha Cardoso Ferreira
Indyanara Ramos
Janaina Conceição
Jorge Luiz Vilhar Malaquias
Juliana Broering Martins
Luana Borges da Silva
Luana Tarsila Hellmann
Luíza Koing Zumblick
Maria José Rossetti
Marilene de Fátima Capeleto
Patricia A. Pereira de Carvalho
Paulo Lisboa Cordeiro
Paulo Mauricio Silveira Bubalo
Rosângela Mara Siegel
Simone Torres de Oliveira
Vanessa Pereira Santos Metzker
Vanilda Liordina Heerdt

Gestão Documental
Lamuniê Souza (Coord.)
Clair Maria Cardoso
Daniel Lucas de Medeiros
Jaliza Thizon de Bona
Guilherme Henrique Koerich
Josiane Leal
Marília Locks Fernandes

Gerência Administrativa e Financeira
Renato André Luz (Gerente)
Ana Luise Wehrle
Anderson Zandré Prudêncio
Daniel Contessa Lisboa
Naiara Jeremias da Rocha
Rafael Bourdot Back
Thais Helena Bonetti
Valmir Venício Inácio

Gerência de Ensino, Pesquisa e Extensão
Janaína Baeta Neves (Gerente)
Aracelli Araldi

Elaboração de Projeto
Carolina Hoeller da Silva Boing
Vanderlei Brasil
Francielle Arruda Rampelotte

Reconhecimento de Curso
Maria de Fátima Martins

Extensão
Maria Cristina Veit (Coord.)

Pesquisa
Daniela E. M. Will (Coord. PUIP, PUIC, PIBIC)
Mauro Faccioni Filho (Coord. Nuvem)

Pós-Graduação
Anelise Leal Vieira Cubas (Coord.)

Biblioteca
Salete Cecília e Souza (Coord.)
Paula Sanhudo da Silva
Marília Ignacio de Espíndola
Renan Felipe Cascaes

Gestão Docente e Discente
Enzo de Oliveira Moreira (Coord.)

Capacitação e Assessoria ao Docente
Alessandra de Oliveira (Assessoria)
Adriana Silveira
Alexandre Wagner da Rocha
Elaine Cristiane Surian (Capacitação)
Elizete De Marco
Fabiana Pereira
Iris de Souza Barros
Juliana Cardoso Esmeraldino
Maria Lina Moratelli Prado
Simone Zigunovas

Tutoria e Suporte
Anderson da Silveira (Núcleo Comunicação)
Claudia N. Nascimento (Núcleo Norte-Nordeste)
Maria Eugênia F. Celeghin (Núcleo Pólos)
Andreza Talles Cascais
Daniela Cassol Peres
Débora Cristina Silveira
Ednéia Araujo Alberto (Núcleo Sudeste)
Francine Cardoso da Silva
Janaina Conceição (Núcleo Sul)
Joice de Castro Peres
Karla F. Wisniewski Desengrini
Kelin Buss
Liana Ferreira
Luiz Antônio Pires
Maria Aparecida Teixeira
Mayara de Oliveira Bastos
Michael Mattar
Patrícia de Souza Amorim
Poliana Simao
Schenon Souza Preto

Gerência de Desenho e Desenvolvimento de Materiais Didáticos
Márcia Loch (Gerente)

Desenho Educacional
Cristina Klipp de Oliveira (Coord. Grad./DAD)
Roseli A. Rocha Moterle (Coord. Pós/Ext.)
Aline Cassol Daga
Aline Pimentel
Carmelita Schulze
Daniela Siqueira de Menezes
Delma Cristiane Morari
Eliete de Oliveira Costa
Eloísa Machado Seemann
Flavia Lumi Matuzawa
Geovania Japiassu Martins
Isabel Zoldan da Veiga Rambo
João Marcos de Souza Alves
Leandro Romanó Bamberg
Lygia Pereira
Lis Airê Fogolari
Luiz Henrique Milani Queriquelli
Marcelo Tavares de Souza Campos
Mariana Aparecida dos Santos
Marina Melhado Gomes da Silva
Marina Cabeda Egger Moellwald
Mirian Elizabet Hahmeyer Collares Elpo
Pâmella Rocha Flores da Silva
Rafael da Cunha Lara
Roberta de Fátima Martins
Roseli Aparecida Rocha Moterle
Sabrina Bleicher
Verônica Ribas Cúrcio

Acessibilidade
Vanessa de Andrade Manoel (Coord.)
Letícia Regiane Da Silva Tobal
Mariella Gloria Rodrigues
Vanesa Montagna

Avaliação da aprendizagem
Claudia Gabriela Dreher
Jaqueline Cardozo Polla
Nágila Cristina Hinckel
Sabrina Paula Soares Scaranto
Thayanny Aparecida B. da Conceição

Gerência de Logística
Jeferson Cassiano A. da Costa (Gerente)

Logísitca de Materiais
Carlos Eduardo D. da Silva (Coord.)
Abraao do Nascimento Germano
Bruna Maciel
Fernando Sardão da Silva
Fylippy Margino dos Santos
Guilherme Lentz
Marlon Eliseu Pereira
Pablo Varela da Silveira
Rubens Amorim
Yslann David Melo Cordeiro

Avaliações Presenciais
Graciele M. Lindenmayr (Coord.)
Ana Paula de Andrade
Angelica Cristina Gollo
Cristilaine Medeiros
Daiana Cristina Bortolotti
Delano Pinheiro Gomes
Edson Martins Rosa Junior
Fernando Steimbach
Fernando Oliveira Santos
Lisdeise Nunes Felipe
Marcelo Ramos
Marcio Ventura
Osni Jose Seidler Junior
Thais Bortolotti

Gerência de Marketing
Eliza B. Dallanhol Locks (Gerente)

Relacionamento com o Mercado
Alvaro José Souto

Relacionamento com Polos Presenciais
Alex Fabiano Wehrle (Coord.)
Jeferson Pandolfo
Karine Augusta Zanoni
Marcia Luz de Oliveira
Mayara Pereira Rosa
Luciana Tomadão Borguetti

Assuntos Jurídicos
Bruno Lucion Roso
Sheila Cristina Martins

Marketing Estratégico
Rafael Bavaresco Bongiolo

Portal e Comunicação
Catia Melissa Silveira Rodrigues
Andreia Drewes
Luiz Felipe Buchmann Figueiredo
Rafael Pessi

Gerência de Produção
Arthur Emmanuel F. Silveira (Gerente)
Francini Ferreira Dias

Design Visual
Pedro Paulo Alves Teixeira (Coord.)
Alberto Regis Elias
Alex Sandro Xavier
Anne Cristyne Pereira
Cristiano Neri Gonçalves Ribeiro
Daiana Ferreira Cassanego
Davi Pieper
Diogo Rafael da Silva
Edison Rodrigo Valim
Fernanda Fernandes
Frederico Trilha
Jordana Paula Schulka
Marcelo Neri da Silva
Nelson Rosa
Noemia Souza Mesquita
Oberdan Porto Leal Piantino

Multimídia
Sérgio Giron (Coord.)
Dandara Lemos Reynaldo
Cleber Magri
Fernando Gustav Soares Lima
Josué Lange

Conferência (e-OLA)
Carla Fabiana Feltrin Raimundo (Coord.)
Bruno Augusto Zunino
Gabriel Barbosa

Produção Industrial
Marcelo Bittencourt (Coord.)

Gerência Serviço de Atenção Integral ao Acadêmico
Maria Isabel Aragon (Gerente)
Ana Paula Batista Detóni
André Luiz Portes
Carolina Dias Damasceno
Cleide Inácio Goulart Seeman
Denise Fernandes
Francielle Fernandes
Holdrin Milet Brandão
Jenniffer Camargo
Jessica da Silva Bruchado
Jonatas Collaço de Souza
Juliana Cardoso da Silva
Juliana Elen Tizian
Kamilla Rosa
Mariana Souza
Marilene Fátima Capeleto
Maurício dos Santos Augusto
Maycon de Sousa Candido
Monique Napoli Ribeiro
Priscilla Geovana Pagani
Sabrina Mari Kawano Gonçalves
Scheila Cristina Martins
Taize Muller
Tatiane Crestani Trentin

Universidade do Sul de Santa Catarina

Gestão de Risco em Tecnologia da Informação

Livro Digital

Palhoça
UnisulVirtual
2012

Edição – Livro Digital

Professor Conteudista
Luiz Otávio Botelho Lento

Coordenação de Curso
Vera Rejane Niedersberg Schuhmacher

Design Instrucional
Carmelita Schulze

Projeto Gráfico e Capa
Equipe Design Visual

Diagramação
Daiana Ferreira Cassanego

Revisão
Amaline Boulos Issa Mussi
Diane Dal Mago

ISBN
978-85-7817-495-8

658.4038
L59 Lento, Luiz Otávio Botelho
Gestão de risco em tecnologia da informação : livro digital / Luiz Otávio Botelho Lento ; design instrucional Carmelita Schulze. – 1. ed. – Palhoça : UnisulVirtual, 2012.
136 p. : il. ; 28 cm.

Inclui bibliografia.
ISBN 978-85-7817-495-8

1. Tecnologia da informação. 2. Administração de risco. I. Schulze, Carmelita. II. Título.

Ficha catalográfica elaborada pela Biblioteca Universitária da Unisul

Luiz Otávio Botelho Lento

Gestão de Risco em Tecnologia da Informação

Livro Digital

Designer instrucional
Carmelita Schulze

Palhoça
UnisulVirtual
2012

Sumário

Apresentação

Caro/a estudante,

O livro digital desta disciplina foi organizado didaticamente, de modo a oferecer a você, em um único arquivo pdf, elementos essenciais para o desenvolvimento dos seus estudos.

Constituem o livro digital:

- Palavras do professor (texto de abertura);
- Plano de estudo (com ementa, objetivos e conteúdo programático da disciplina);
- Objetivos, Introdução, Síntese e Saiba mais de cada unidade;
- Leituras de autoria do professor conteudista;
- Atividades de autoaprendizagem e gabaritos;
- Enunciados das atividades colaborativas;
- Para concluir estudos (texto de encerramento);
- Minicurrículo do professor conteudista; e
- Referências.

Lembramos, no entanto, que o livro digital não constitui a totalidade do material didático da disciplina. Dessa forma, integram o conjunto de materiais de estudo: webaulas, objetos multimídia, leituras complementares (selecionadas pelo professor conteudista) e atividades de avaliação (obrigatórias e complementares), que você acessa pelo Espaço UnisulVirtual de Aprendizagem.

Tais materiais didáticos foram construídos especialmente para este curso, levando em consideração as necessidades da sua formação e aperfeiçoamento profissional.

Atenciosamente,

Equipe UnisulVirtual

Palavras do professor

A gestão de riscos Tecnologia da Informação (TI) é um processo contínuo e árduo para qualquer organização, pois a necessidade de estar sempre alinhada ao negócio, dar mais qualidade de serviço aos produtos entregue ao cliente e prover retorno sobre o investimento (ROI - Return on Investment) são atividades, às vezes, simples, mas que necessitam de uma preocupação eterna. A necessidade de investimentos não somente de *hardware* e *software*, mas também de *peopleware*, pode ser considerada uma utopia nesse mundo corporativo.

Há alguns anos, a maioria das empresas não dependia da TI para operacionalizar e manter o seu negócio. O mundo corporativo não era tão dinâmico. Com o decorrer dos anos, essa necessidade, ou mesmo dependência, cresceu de forma exponencial. As empresas passaram a ter mais contato com o mundo virtual; a necessidade de agilizar os processos de negócio passa a ser uma necessidade; a integração mundial pela internet é uma realidade, e a concorrência tornou-se um fantasma para o mundo corporativo.

Consequentemente, as empresas passaram a investir mais em TI (tecnologia da informação), passando a fazer parte desse novo mundo virtual, e junto com isso vieram novos problemas. A gestão de riscos de TI passa a ter um papel importante no negócio da empresa. A necessidade de investimentos na área é uma realidade, alavancando novas empresas e novos negócios. Entretanto, uma pergunta sempre é realizada quando se fala em investir em TI: **o que investir e quanto investir?**

A resposta pode estar em dizer que para investir em TI existe a necessidade de saber quais são as necessidades de negócio da empresa, quais riscos ela possui, o que ela considera um risco aceitável e o quanto a empresa quer investir.

Para auxiliar nas respostas a tudo isso, esse livro irá abordar todos esses questionamentos, inclusive como respondê-los ou minimizá-los por meio da implantação do processo de gestão de riscos em uma organização.

Professor Luiz Otávio Botelho Lento, Msc

Plano de estudo

O plano de estudos visa a orientá-lo/a no desenvolvimento da disciplina. Possui elementos que o/a ajudarão a conhecer o contexto da disciplina e a organizar o seu tempo de estudos.

O processo de ensino e aprendizagem na UnisulVirtual leva em conta instrumentos que se articulam e se complementam, portanto a construção de competências se dá sobre a articulação de metodologias e por meio das diversas formas de ação/mediação.

São elementos desse processo:

- o livro digital;
- o Espaço UnisulVirtual de Aprendizagem (EVA);
- as atividades de avaliação (a distância, presenciais e de autoaprendizagem);
- o Sistema Tutorial.

Objetivo geral

Prover ao aluno técnicas e métodos que permitam reconhecer e avaliar riscos no planejamento e execução dos processos de TI de modo a transformar e melhorar a gestão estratégica da organização.

Ementa

Conceituação de risco, identificação de riscos, origem dos riscos, gerência contínua do risco, gerência da equipe de risco e modelos qualitativos para gestão de riscos em Tecnologia da Informação. Gerência de prazos e riscos de cronograma. Metodologias para seleção de fornecedores, atributos do fornecedor e avaliação do grau de atendimento da solução/fornecedor às necessidades funcionais do negócio. Monitoramento e análise crítica dos riscos.

Conteúdo programático/objetivos

A seguir, as unidades que compõem o livro digital desta disciplina e os seus respectivos objetivos. Estes se referem aos resultados que você deverá alcançar ao final de uma etapa de estudo. Os objetivos de cada unidade definem o conjunto de conhecimentos que você deverá possuir para o desenvolvimento de habilidades e competências necessárias a este nível de estudo.

Unidades de estudo: 4

Unidade 1 – Os riscos na tecnologia da informação

Nesta unidade, você compreenderá a importância da governança e gestão de TI para qualquer organização. Acompanhará, portanto, a amplitude e grande importância que esses dois elementos possui para a organização. Nesse sentido, verificará em detalhes o que cabe à Gestão de Riscos de TI e conhecer as etapas do processo de Gestão de Riscos de TI.

Unidade 2 – Gestão de risco e seus frameworks

Esta unidade apresenta um importante instrumento que foi criado para realizar a gestão de riscos. Tal instrumento consiste no Enterprise Risk Management – Integrated Framework (ERM), um framework capaz de ser adotado em qualquer empresa, que possibilita um maior controle interno das empresas em relação à rede de informação dessa empresa, proporcionando um foco mais consistente e amplo sobre a questão de gestão de riscos corporativos. Na sequência, verifica-se o RISK IT Framework, que foi criado com o objetivo de ajudar os gerentes a relatar os riscos de TI. Ao final desse texto, esperamos que você compreenda por que se pode dizer que o RISK IT framework é um conjunto de boas práticas para identificar, governar e gerenciar os riscos de TI.

Unidade 3 – Gestão de riscos de segurança da informação

Nesta unidade, apresentar-se-ão os conceitos e as funcionalidades da gestão de riscos de segurança da informação. Serão discutidos aspectos de como realizar a avaliação de riscos. Posteriormente, como esses riscos podem ser tratados, e, por fim, como manter o monitoramento e manutenção dos riscos existentes em uma organização.

Unidade 4 – A gestão de risco aplicada a uma empresa

Esta unidade visa a apresentar um exemplo de como realizar uma análise/avaliação de risco. O exemplo apresenta uma situação inicial e a sequência de todo o processo a ser realizado, numa organização para se ter a avaliação dos riscos em relação a ela.

O objetivo do exemplo é apresentar a sequência de realização de todo o processo de análise/avaliação de risco.

A implantação do processo de gestão de risco irá seguir as premissas descritas nas unidades anteriores desse livro, de forma que ao fim você possua um exemplo de como executar um processo de gestão de riscos.

Carga horária: 30 horas

Unidade 1

Os riscos na Tecnologia da Informação

Objetivos de aprendizagem

- Compreender a importância da Governança e Gestão de TI para qualquer Organização.
- Conhecer a Gestão de Riscos de TI.
- Conhecer as etapas do processo de Gestão de Riscos de TI.

Introdução

Atualmente, as organizações enfrentam uma revolução global na governança, afetando diretamente suas práticas de gestão de informação. Há uma crescente necessidade de valorizar as informações protegidas e entregues em termos de serviços habilitados.

Na década passada, aconteceram falhas na segurança da informação de alto nível organizacional, por isso as autoridades legais e órgãos reguladores criaram um complexo conjunto de novas leis, políticas, regulamentos e organizações com o objetivo de forçar uma melhoria na governança organizacional, segurança da informação, controles e transparência das atividades das organizações. Além das falhas organizacionais, a automatização dos processos, entrega de produtos e serviços também forçou um maior controle para manter e proteger a informação.

Em paralelo, o crescente volume de ataques à informação explorando as diversas vulnerabilidades das organições também resultou na necessidade de uma abordagem de governança para gestão da informação, protegendo os ativos de informação mais críticos da organização, bem como a sua reputação.

Desta forma, esta unidade apresentará uma visão do que são os riscos de TI para uma organização, a sua importância e como podem ser geridos de modo que não lhe causem impactos.

A Importância da Governança e Gestão de TI na Organização

Luiz Otávio Botelho Lento

Cada vez mais, a alta administração das empresas se conscientiza do impacto positivo da TI no sucesso do seu negócio. Uma TI bem gerenciada, isto é, bem operacionalizada e com o risco contornável, passa a ser uma vantagem competitva em um mercado tão cruel e globalizado. Logo, ao exercer a governança de TI, a alta administração precisa saber se a sua TI atingirá os objetivos estabelecidos; se ela é capaz de aprender e se adaptar às diversas situações de negócio; gerir de forma criteriosa os riscos de seus ativos e reconhecer as oportunidades de negócio e agir sobre as mesmas. (GULDENTOPS, 2003).

Com isso, conclui-se que empresas bem-sucedidas conhecem e compreendem os seus riscos e exploram os benefícios da TI, buscando e encontrando maneiras de alinhar a estratégia de TI com a estratégia da empresa; fornecendo estruturas organizacionais que facilitem a implementação de estratégias e metas; criando relacionamentos mais eficazes entre negócio e TI e, também, com os parceiros externos; e mantendo uma medição do desempenho da TI.

O nível de informatização

O uso de TI nas organizações melhorou significativamente a eficiência dos processos, proporcionando novas demandas aos seus negócios. O uso adequado e correto da TI traz, normalmente, ganhos significativos às organizações, mas a escolha da tecnologia a ser aplicada deve estar em conformidade com as respectivas estratégias de negócio. (LÖBLER, 2010).

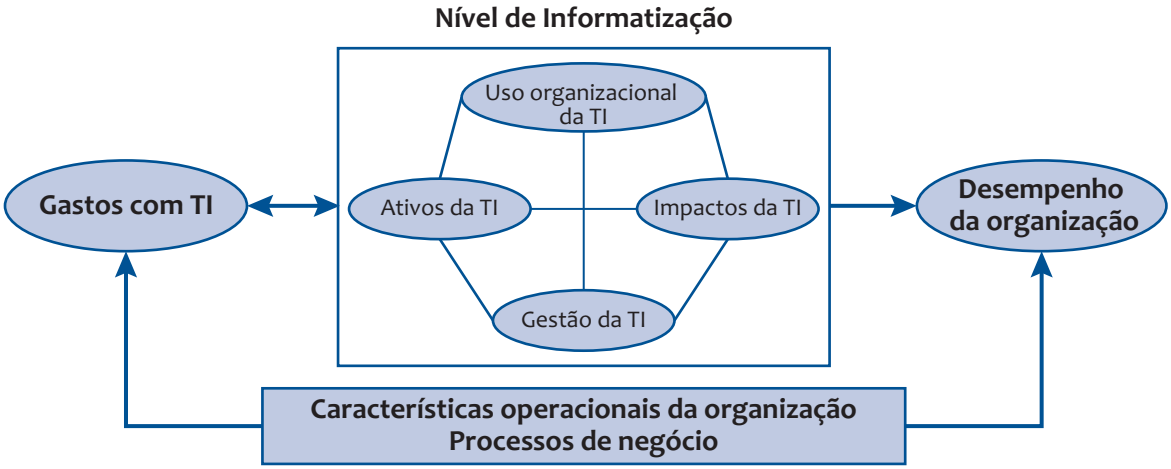
Importante

Todavia vale a pena ressaltar que a adoção de TI nos processos da organização é somente uma das etapas para a gestão correta da informação. Existe a necessidade de um planejamento e avaliação do que será adotado e utilizado, subsidiado por um sistema de gestão e devidamente monitorado, para que os recursos de tecnologia sejam utilizados conforme planejados.

Porém, como saber o quanto a organização está informatizada, isto é, o seu nível de informatização?

Zwicker, Vidal e Ciqueira (2007) descrevem um modelo de nível de informatização, apresentado na figura 1. A ideia é avaliar o grau de informatização de uma organização. Tal avaliação poderá fornecer informações para melhorar o nível de informatização da organização, via a utilização da medição de sua eficácia e eficiência de investimentos.

Figura 1 – Modelo de nível de informatização



Fonte: Zwicker, Vidal e Ciqueira, 2007.

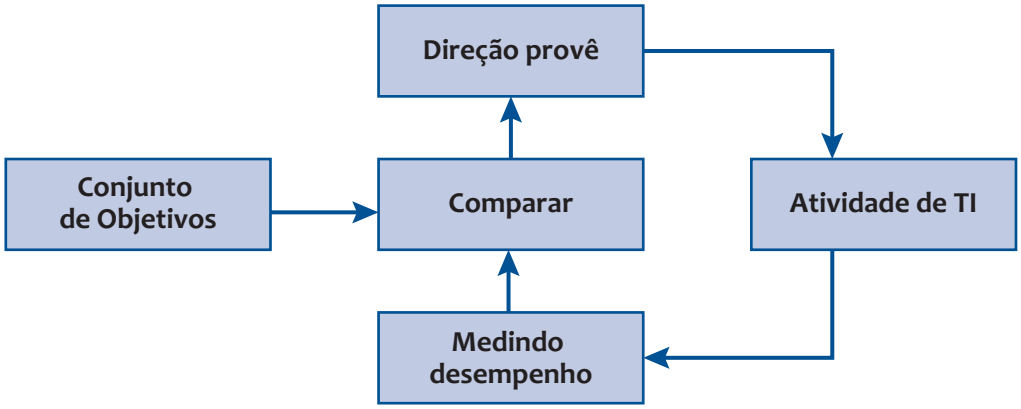
O modelo tem como referência as características operacionais da organização e está relacionado com os processos de negócio da mesma. Com base nesses fatores, verifica-se como a TI está incorporada na organização, analisando se os ativos satisfazem as necessidades da infraestrutura de TI e, também, se são aplicados e gerenciados de forma adequada, minimizando assim o impacto das ameaças à informação nos processos de negócio.

Governança de TI

A Governança de TI faz parte da estrutura de governança da empresa. A integração de ambas é semelhante à necessidade de a TI fazer parte do corpo do negócio da empresa -- diferentemente de apenas constituir um foco isolado para atender a uma determinada demanda. Uma abordagem interessante para justificar essa afirmativa é que, apesar de a evolução da governança ter sido basicamente motivada pela necessidade de transparência dos riscos da empresa e de proteção do valor do acionista, o uso generalizado de tecnologia criou uma dependência crítica em TI, que exige um foco específico em governança da mesma. A figura 2, presente mais adiante, apresenta a integração da TI com os objetivos da Empresa, incluindo sempre uma comparação dos resultados.

A TI passou a ser essencial à gerência das transações, informações e conhecimentos necessários, para iniciar e sustentar as atividades econômicas e sociais das organizações. Na maioria das empresas, a TI se tornou uma parte integrante do negócio e tornou-se fundamental para apoiar, sustentar e fazer crescer os seus negócios. **As empresas bem sucedidas entendem e gerenciam os riscos do seu negócio e as suas limitações da TI.** Como consequência, os conselhos de administração passam a entender a importância estratégica de TI e valorizam uma boa governança de TI.

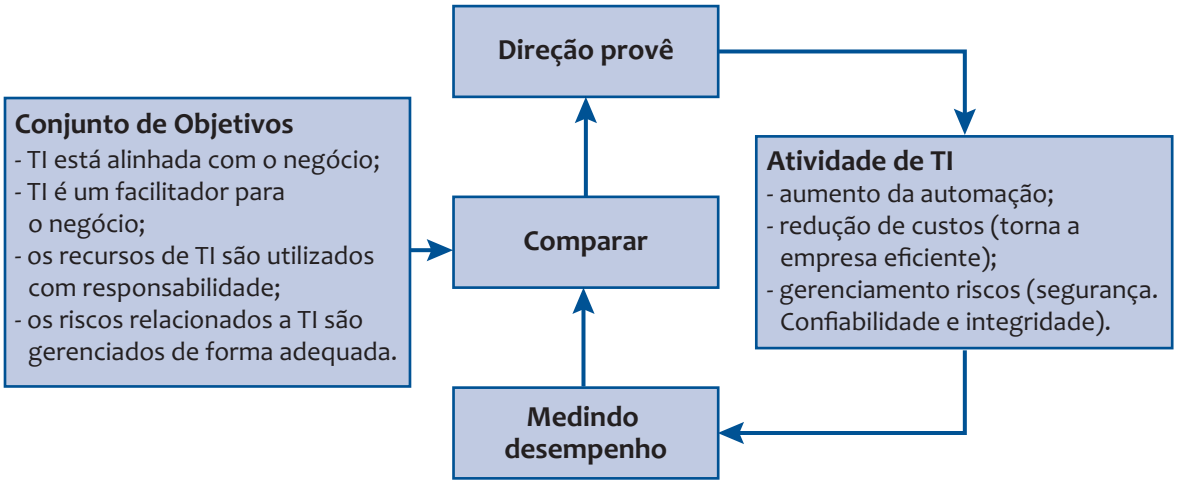
Figura 2 – Interação dos objetivos e das atividades de TI



Fonte: Guldentops, 2003.

Por conseguinte, pode-se concluir que o objetivo global da Governança de TI é compreender os problemas da empresa e a importância estratégica da TI nas respetivas soluções. Isto, por sua vez, ocorre quando a empresa pode manter suas operações e implementar as estratégias necessárias para aumentar as suas atividades no futuro, garantindo assim que as expectativas de TI sejam cumpridas e os riscos de TI sejam mitigados – verificar framework ilustrado na figura 3. Pense que a alta administração espera que a TI agregue valor ao negócio da empresa, proporcionando soluções rápidas e seguras, com alta qualidade de serviços; gerando um retorno de investimento (ROI – *Return on Investiment*); e, obtendo eficiência e ganhos de produtividade e eficácia do negócio.

Figura 3 – Framework de Governança de TI



Fonte: Guldentops, 2003.

Gestão de Riscos de TI

O tema riscos é uma realidade em qualquer Empresa. Possui um conceito bem abrangente, associado, na maioria das vezes, à sua área de finanças. Hoje o conceito de riscos permeia toda a empresa, em todas as áreas de negócio e em todos os seus níveis hierárquicos. Isso pode ser constatado junto com a evolução do mundo corporativo, tanto é assim que a Governança Corporativa assumiu o papel de estabelecer um conjunto de critérios em relação aos riscos dos seus processos, bem como o seu tratamento.

A proximidade da Empresa com a área de TI, aquela dando o suporte para que os processos possam ser executados na área de TI, tornou ainda maior a necessidade de se contar com uma real análise da situação dos riscos que a Empresa corre, para que se possa decidir qual risco é aceitável para a mesma.

Importante

Para se ter conhecimentos dos riscos e saber como tratá-los, existe a necessidade de se implantar um **processo de gestão de riscos**, que consiste em um processo responsável por identificar todos os riscos a que a Empresa está exposta, determinar o seu nível de criticidade, estabelecer um plano para tratá-los e dar ciência às partes interessadas desse processo.

Entretanto não existe uma só metodologia de gestão de risco que atenda plenamente todas as áreas de TI com as suas respectivas funcionalidades. Atualmente, há disponíveis no mercado algumas metodologias, ferramentas e modelos de gestão de risco, sendo que cada uma busca atender uma ou mais necessidades da área de TI. Dentre essas, pode-se destacar a NIST 800-30, ENISA, FAIR, MEHARI, CRAAM, COSO ERM, OCTAVE e IT Risk Framework, da ISACA.

Aqui se apresentarão os conceitos de riscos e gestão de riscos em conjunto com o processo de gestão de risco da NIST 800-30 e o ERM framework e IT Risk framework.

Risco

Devido à amplitude e plenitude da existência de riscos em uma Empresa, defini-los tornou-se uma tarefa interessante, principalmente pela diversidade de definições existentes. Entretanto algumas dessas definições podem ser consideradas como clássicas, pois suprem as necessidades de fundamentar esse conceito.

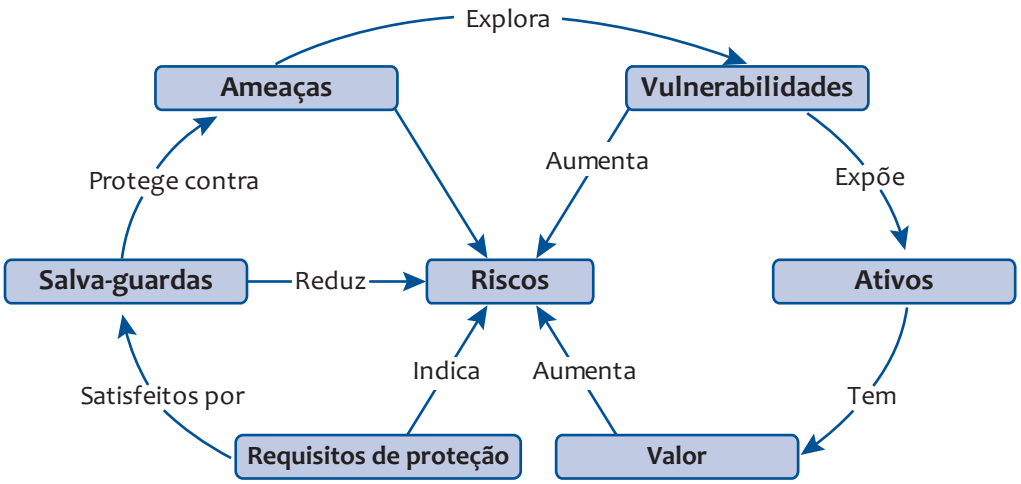
Segundo NIST Stoneburner, Goguen e Feringa (2002), o risco é o impacto negativo de uma ação sobre uma vulnerabilidade, considerando tanto a probabilidade como o impacto dessa ocorrência, isto é, o risco é a função que relaciona a probabilidade de uma determinada ameaça explorar uma vulnerabilidade em potencial e, consequentemente, o impacto resultante desse evento adverso sobre a organização.

A ISO/IEC 27002 (2005) define risco como a possibilidade de um ativo estar sujeito a vulnerabilidades e incidentes (ameaças explorando essas vulnerabilidades), comprometendo a continuidade das atividades de uma organização (impacto).

Outra definição interessante é a apresentada em COSO (2004), onde ele relaciona eventos com riscos e oportunidades. Os eventos podem ter um impacto negativo, positivo, ou ambos. Eventos com um impacto negativo representam riscos que podem impedir a criação de valor ou reduzir o valor existente. Eventos com impacto positivo podem compensar os impactos negativos ou representar oportunidades. As oportunidades são as possibilidades de que um evento irá ocorrer e afetar positivamente a realização dos objetivos, apoiar a criação de valor e de preservação.

Já a ISO/IEC 27005 (2008) define risco como o potencial de uma determinada ameaça explorar vulnerabilidades, proporcionando perdas ou danos a um ativo ou grupo de ativos, de forma direta ou indireta, para a organização. Essa relação é apresentada na figura 4.

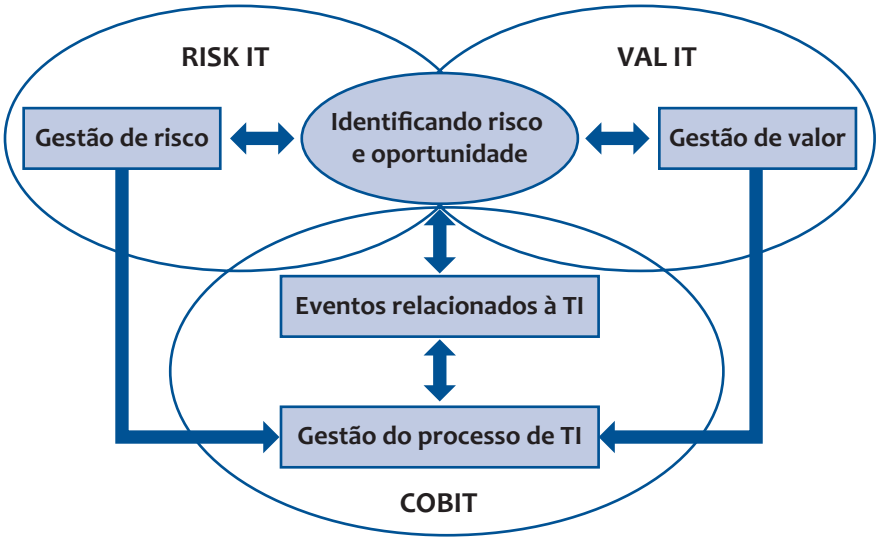
Figura 4 – Riscos



Fonte: ISO 27005, 2008.

Por fim, em conformidade com ISACA (2009), os eventos externos que podem incluir mudanças nas condições de mercado, novos concorrentes, a disponibilidade de novas tecnologias, por exemplo, representam um risco e/ou oportunidade. Quando surgem oportunidades de mudanças na área de TI das empresas, o quadro do VAL IT, em IGTI, 2008, irá descrever melhor a forma de progresso, maximizando o retorno sobre o investimento (ROI – Return on Investiment). O resultado da avaliação da aplicação da TI, provavelmente, terá impacto em alguns dos processos de TI e/ou sobre a contribuição financeira para os processos de TI. Logo, os resultados dos processos de gestão de risco e gestão de valor serão considerados pela gestão de processos, conforme apresentado na figura 5.

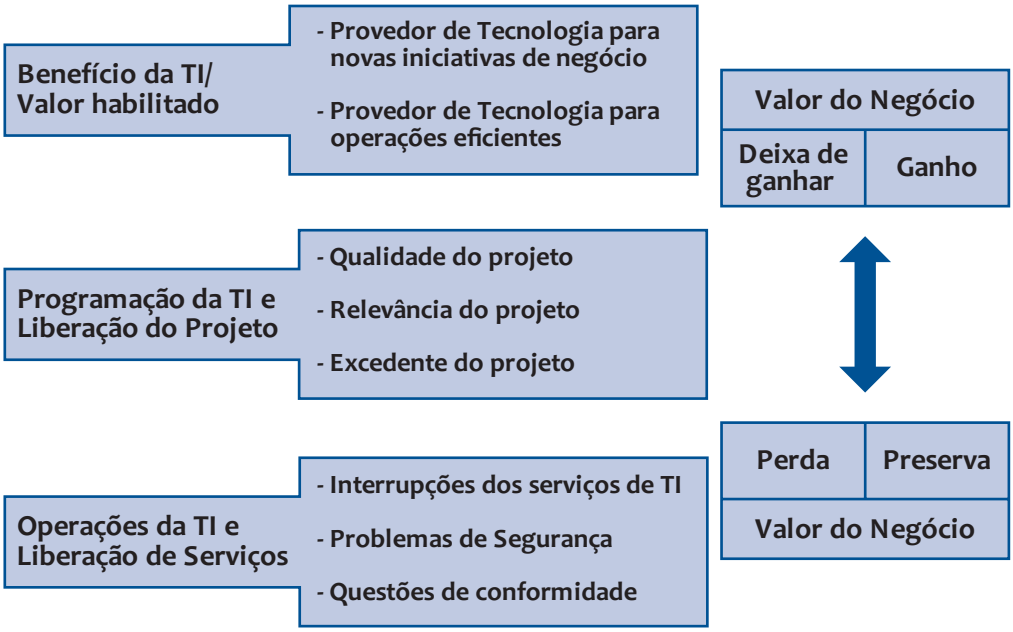
Figura 5 – Posicionamento entre COBIT, VAL IT e Risk IT



Fonte: ISACA, 2009.

Trabalhar com TI tem os seus riscos, isto porque as empresas agregam valor aos seus processos de negócio com a aplicação dos recursos da TI. Em ICASA (2009), o risco do negócio está associado ao uso, propriedade, operação, participação, que influenciam na adoção da TI em uma empresa. Isto porque são eventos relacionados à TI que podem impactar o negócio, ocorrendo com frequência e magnitude incerta, criando desafios na busca de metas e objetivos estratégicos. Logo, os riscos de TI não estão limitados somente aos ativos de informação mas também a atrasos na liberação de projetos, arquitetura obsoleta de TI, problemas na liberação de serviços de TI, entre outros, conforme visualizado na figura 6. (ICASA, 2009).

Figura 6 – Categorias dos riscos de TI



Fonte: ISACA, 2009.

Conceitos de Gestão de Riscos

A crescente importância da TI para os processos de negócio de uma Empresa trouxe, em paralelo, um aumento de problemas de segurança. **A necessidade das empresas em conhecer os riscos dos seus processos de negócio passou a constituir um fator estratégico para o sucesso dos seus negócios.** O papel de um processo de gestão de riscos em uma empresa é fundamental, pois protege os seus ativos de informação dos riscos relacionados à TI. Contudo, para que esse processo seja mais bem compreendido, alguns componentes devem ser esclarecidos, entre eles o risco.

Importante

Segundo Stoneburner, Goguen e Feringa (2002), a gestão de riscos é o processo de identificação dos riscos, avaliação de risco e tomada de medidas (tratamento do risco) para reduzir o risco a um nível aceitável. O objetivo da gestão de risco é permitir que a organização consiga realizar as suas tarefas, isto é, manter os seus processos de negócio ativos através de uma melhor segurança para os sistemas de TI, responsáveis em armazenar, processar e transmitir as suas informações.

Logo, pode-se dizer que o processo de gestão de riscos permite que os gerentes de TI busquem o equilíbrio entre os custos operacionais e econômicos das medidas de proteção, possibilitando, assim, maiores ganhos para a organização, dando um maior retorno sobre o investimento (ROI).

Nesta linha, também será apresentada a metodologia desenvolvida por Stoneburner, Goguen e Feringa (2002), isto é, o NIST 800-30, do processo de gestão de risco. Outras metodologias serão apresentadas, inclusive o processo de gestão de risco no formato da ISO 27005:2008 e as diretrizes de sua implementação no formato da ISO 31000:2009.

Processos da Gestão de Riscos

O processo de gestão de riscos apresentado a seguir descreve um fluxo de atividades que vai desde o levantamento das informações do sistema computacional da organização, passa pela análise de riscos e, por fim, apresenta como esses riscos podem ser tratados. Essa metodologia, apesar de ter sido inicialmente desenvolvida para a segurança da informação, pode ser aplicada diretamente a todos os processos que fazem da TI o suporte para a sua execução.

Segundo Stoneburner, Goguen e Feringa (2002), a gestão dos riscos é composta, basicamente, por **três processos**:

1. Avaliação dos riscos – esse processo inclui a identificação e avaliação dos riscos, o impacto causado pelos riscos e as recomendações de medidas para a redução de riscos.
2. Mitigação de riscos – esse processo trata a priorização, implementação e manutenção das medidas adequadas de redução do risco, com base no processo de avaliação de risco.

3. Manutenção da avaliação – é discutido o processo de avaliação contínua dos riscos com base em parâmetros necessários a sua execução.

A seguir, encontra-se especificado cada um desses processos.

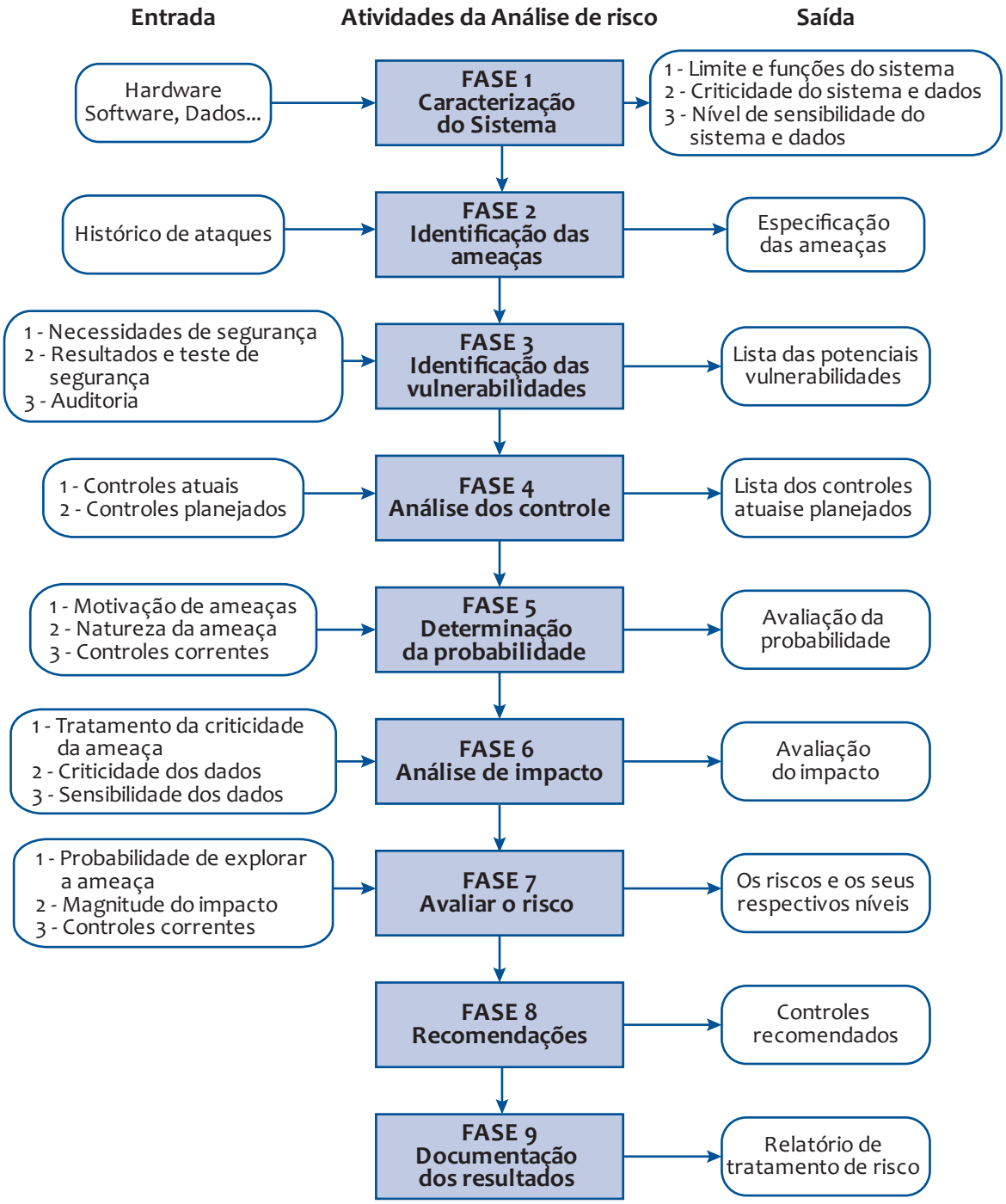
Processo de Avaliação de Riscos

O processo de avaliação de riscos determina a extensão das ameaças em potencial e o risco associado com o sistema computacional da organização, sendo que a saída desse processo é a ajuda para identificar os controles adequados para a redução ou eliminação dos riscos durante o processo de mitigar riscos.

Para determinar a probabilidade de ameaças ao sistema computacional, devem-se analisar também as vulnerabilidades e os respectivos controles por ventura existentes. O impacto se refere ao tamanho do problema que será causado, caso a ameaça se efetive (ataque). Vale a pena ressaltar que o nível de impacto estará diretamente relacionado ao grau de criticidade dos processos de negócio que atinge serviços de TI e ativos.

A NIST 800-30 divide a avaliação de riscos em nove etapas, conforme apresentado na figura 7.

Figura 7 – Processo de avaliação de riscos



Fonte: Stoneburner, Goguen e Feringa, 2002.

Vejamos, agora, cada uma dessas etapas.

1ª Etapa – Caracterização do sistema

Esta etapa tem como objetivo definir o escopo de abrangência da avaliação de riscos, isto é, quais elementos do sistema computacional serão analisados durante o processo. Nesse momento, também são estabelecidos os limites de autorizações quanto à realização de operações no sistema, além de serem providas informações relacionadas ao sistema, como os dispositivos de hardware, software, links, entre outros necessários à caracterização do sistema.

O sucesso desta etapa está baseado nas informações que são coletadas. A combinação de técnicas de coleta de informação é uma estratégia para se alcançar o objetivo final da etapa: possuir a maior quantidade de informações necessárias sobre o sistema computacional, de forma que se tenha a real caracterização do mesmo. Nesse sentido, algumas técnicas podem ser aplicadas, entre elas:

I - Questionário – essa técnica é talvez a mais utilizada pelo universo dos profissionais que trabalham com segurança da informação, principalmente na fase de implantação do processo de gestão de riscos. O questionário foca, normalmente, em questões relativas aos controles operacionais e de gerenciamento. É aplicado a pessoas tanto no nível operacional quanto no gerencial. Pode ser distribuído pessoalmente ou realizado via site. Alguns exemplos de perguntas que podem constar desse tipo de questionário:

a. Quantos são os usuários válidos no sistema?

b. Qual é o negócio ou linhas de negócio da sua organização?

c. Qual é o propósito do seu sistema computacional em relação ao negócio da sua empresa?

II - Análise de documentos – essa estratégia tem como objetivo analisar os documentos referentes ao sistema computacional, políticas (diretrizes, regimentos, etc.), documentos relacionados à segurança da informação (relatórios de avaliação de risco, política de segurança, e outros).

III - Uso de ferramentas de varredura – são métodos proativos que podem ser usados na coleta de informações do sistema (topologia da rede, identificação de serviços executados na rede, etc.).

Encerradas todas as atividades desta etapa, espera-se ter um mapa detalhado das características do sistema computacional bem como definido o escopo de abrangência do trabalho a ser realizado pela gestão de TI.

2ª Etapa – Identificação das Ameaças

Antes de discutir esta etapa, deve-se definir o que vem a ser uma ameaça. Alguns citam que uma ameaça é tudo aquilo que tem potencial para causar danos aos ativos de informação (Ex.: invasão, indisponibilidade de serviços, etc.). Contudo Stoneburner, Goguen e Feringa (2002), na NIST 800-30, definem ameaça como qualquer circunstância ou evento com potencial de explorar (ou agir sobre ela), de forma intencional, ou não, uma vulnerabilidade, de modo a causar danos a um sistema computacional.

Uma ameaça é considerada uma preocupação quando realmente ela puder ser concretizada (ataque), ou quando agir sobre uma vulnerabilidade (queda de energia, por exemplo). Entretanto pode-se afirmar que a origem da ameaça não estará presente quando não existir vulnerabilidade que a ameaça possa explorar. Com isso, para determinar a probabilidade de uma ameaça ocorrer, deve ser levada em consideração a origem da ameaça, as vulnerabilidades em potencial a essa origem e os controles existentes.

Identificação da origem da ameaça

O objetivo desta subetapa é identificar, para uma avaliação, as origens da ameaça em potencial e listar todas aquelas que se aplicam ao sistema computacional. Elas podem ser do tipo natural (incêndio, enchente, tempestades elétricas, etc.), humana (atos intencionais – ataques, negligência, erros, etc.) ou do ambiente (falhas de energia, poluição, etc.).

Entretanto não se pode esquecer que, durante a avaliação das origens das ameaças, independente do tipo, deve sempre ser levado em consideração **o potencial de danos** que elas possam causar ao sistema computacional.

Motivação e ações das ameaças

A motivação e os recursos para a execução de um ataque tornam os humanos uma origem da ameaça em potencial. Depois de mapeada essa motivação, os tipos de ameaças e as ações por elas executadas, tem-se uma visão dos possíveis ataques que a organização poderá vir a sofrer e os danos que os mesmo irão causar.
A tabela 1 apresenta um conjunto de informações coletadas durante a etapa de identificação das ameaças cuja origem da ameaça é humana.

Tabela 1 – Ameaças humanas

Origem da ameaça	Motivação	Ações da ameaça
Hacker, cracker	Desafio Ego Rebeldia	Engenharia social Intrusões no sistema Acessos não autorizados
Crime computacional	Destruição da informação Descoberta ilegal da informação Ganho financeiro Alteração de dados não autorizados	Fraudes Intrusão no sistema Spoofing
Terrorismo	Destruição Exploração Blackmail	Guerra de informações Ataques ao sistema (DDoS) Penetração no sistema
Espionagem industrial	Vantagem competitiva Espionagem econômica	Engenharia social Acessos não autorizados Penetração no sistema Invasão de privacidade

Fonte: Stoneburner, Goguen e Feringa, 2002.

Ao término desta etapa, existirá um documento com a lista das origens das ameaças, A partir dela, será possível explorar as vulnerabilidades do sistema computacional da organização em questão.

3ª Etapa – Identificação das vulnerabilidades

O objetivo desta etapa é desenvolver uma lista com todas as vulnerabilidades do sistema que possam ser exploradas pelas origens das ameaças. Os métodos recomendados para identificar as vulnerabilidades do sistema são a origem da vulnerabilidade, execução de testes de segurança no sistema computacional e desenvolvimento de uma lista de verificação (checklist) com as necessidades de segurança.

Origem das vulnerabilidades

As vulnerabilidades relacionadas ao ambiente computacional podem ser identificadas através das técnicas de coleta de informações (entrevistas, ferramentas de varredura) a serem aplicadas aos técnicos da área de TI. Informações de fornecedores de produtos também são essenciais nessa tarefa, pois indicam falhas,

atualizações e outras medidas que possam minimizar as vulnerabilidades do sistema. Outras fontes de informação de vulnerabilidades podem ser utilizadas, como BID (www.securityfocus.com.br), CAN/CEV (www.mitre.org), entre outras.

Testando a segurança do sistema

Para atender esse item, são utilizados métodos proativos que realizam esses testes, como:

1. Ferramenta de varredura – (nmap,) é aplicada a máquinas (estações de trabalho, servidores, etc.) e/ou a rede de computadores, com o objetivo de verificar, por exemplo, serviços que estão nele sendo executados.
2. Teste de segurança de Análise de Vulnerabilidades – trata-se do procedimento de identificar potenciais vulnerabilidades, normalmente, executadas a partir de ferramentas automatizadas (Nessus, Retina), correlacionando potenciais vulnerabilidades com registros de segurança – BID e CAN/CEV, por exemplo.
3. Teste de invasão (pen teste) – são testes de segurança que buscam ganhar acesso ao sistema (de forma pontual) ou processo que combina vários tipos de teste de segurança como fingerprint, footprint, port scanner, varreduras de vulnerabilidades, etc. Logo, o teste de invasão (pen test) pode ser definido como o processo de identificar, enumerar e buscar explorar vulnerabilidades, utilizando um conjunto de variadas técnicas, dentro de uma metodologia objetiva a qual simula, de forma controlada, a técnica operacional de um invasor.

Desenvolver uma lista de verificação (checklist)

A lista de verificação deverá conter os padrões básicos de segurança que podem ser usados para, de forma sistêmica, avaliar e identificar as vulnerabilidades dos ativos, procedimentos não automatizados, processos e informações transmitidas. Todos estes devem estar relacionados com o sistema computacional nas áreas de gerenciamento, operacional e técnico, conforme apresentado na tabela 2.

Tabela 2 – Critérios de segurança

Área	Critério de Segurança
Gerenciamento	Atribuição de responsabilidades Suporte a continuidade Competência de resposta a incidentes Revisão periódica dos controles de segurança Análise de riscos Treinamento técnico e de segurança Segregação de serviços Plano de segurança
Operacional	Controle de contaminação do ar Controle para garantir a qualidade da energia elétrica Acesso e uso de mídias de dados Distribuição de dados externos Controle de umidade e temperatura Controle de notebooks, laptops
Técnico	Comunicação Criptografia Controle de acesso Identificação e autenticação Detecção de intrusos Auditoria do sistema

Fonte: Stoneburner, Goguen e Feringa, 2002.

Ao final desta etapa, será produzida uma lista de vulnerabilidades que possam ser exploradas pelas origens das ameaças, conforme apresentado na tabela 3.

Tabela 3 – Vulnerabilidades

Vulnerabilidade	Origem da ameaça	Ações da ameaça
O firewall aceita a entrada do tráfego de telnet	Usuários não autorizados	Visualiza os arquivos de dados do sistema como um usuário qualquer.
O fornecedor não fornece mais atualizações do sistema	Usuários não autorizados	Obtenção de acesso não autorizado aos arquivos do sistema
Uso do agente água (uso sprinklers) no data-center para apagar incêndio	Pessoas negligentes, fogo	Sprinklers são acionados dentro do data-center

Fonte: Stoneburner, Goguen e Feringa, 2002.

4ª Etapa – Análise dos Controles

Esta etapa busca analisar os controles de acesso à informação já existentes (implementados) e, também, os planejados para serem implantados. Esses controles têm como objetivo minimizar a probabilidade de as ameaças explorarem as vulnerabilidades do sistema. Por exemplo, a probabilidade de uma vulnerabilidade ser explorada é baixa quando a origem da ameaça que lhe corresponde possui pouco interesse ou pouca capacidade em explorá-la, ou se os controles implantados para impedir tal exploração são eficazes, isto é, podem eliminar ou reduzir a magnitude do dano.

Controles

Os controles de segurança podem fazer uso de aspectos técnicos, ou não. Os controles chamados técnicos (mecanismos de segurança – mecanismos de controle de acesso, mecanismos de identificação e autenticação, mecanismos de criptografia) são aplicados diretamente em hardware ou software. Já os controles que não são técnicos consistem na gestão e controles operacionais, tais como políticas de segurança, procedimentos operacionais e de pessoal, segurança física e segurança ambiental.

Os controles, sejam eles técnicos, ou não, também podem ser divididos em duas categorias:

1. Prevenção – são controles que visam evitar as tentativas de violar a política de segurança. Vale dizer, controles focados no controle de acesso, criptografia e autenticação.
2. Detecção – são controles que têm como objetivo informar quando ocorre alguma violação ou tentativa de violação da política de segurança da informação. São controles focados na detecção de intrusos – por exemplo, as auditorias.

Técnica de Análise de Controle

A lista de verificação de requisitos de segurança, citada anteriormente, é uma das referências para se verificar a aplicação das regras de segurança no sistema computacional.

O resultado desta etapa é uma lista de controles existentes ou previstos, bem como a sua eficiência quanto à redução da probabilidade de uma origem da ameaça ter sucesso na exploração das vulnerabilidades.

Etapa 5 – Determinação da probabilidade

Para determinar o nível da probabilidade de uma vulnerabilidade ser explorada, alguns fatores devem ser levados em consideração:

1. a motivação e capacidade da fonte da ameaça;
2. a natureza da vulnerabilidade; e
3. a existência e eficiência dos atuais controles.

A tabela 4 apresenta um exemplo de 3 níveis de probabilidade com as suas respectivas descrições, onde pode-se determinar a probabilidade da ameaça ter, ou não, sucesso em explorar uma vulnerabilidade.

Tabela 4 – Probabilidade

Nível da Probabilidade	Descrição da probabilidade
Alta	A origem da ameaça está muito motivada e é totalmente capaz, e os controles são ineficientes.
Média	A origem da ameaça está motivada e é capaz, mas os controles podem impedir o ataque.
Baixa	A origem da ameaça não está motivada e não é capaz, ou os controles são eficazes ou, pelo menos, dificultam significativamente o ataque.

Fonte: Stoneburner, Goguen e Feringa, 2002.

Etapa 6 – Análise de impacto

O objetivo desta etapa é determinar o impacto negativo resultante de um ataque bem-sucedido, isto é, o sucesso de uma ameaça explorando uma vulnerabilidade. Entretanto, para que a análise de impacto possa ser realizada, algumas informações são necessárias, obtidas em sua maioria através de documentação existente, tal como o relatório de análise de impacto ou relatório da avaliação de criticidade dos ativos. Outras dessas informações necessárias são:

- A tarefa a ser realizada pelo sistema (os processos realizados pelo sistema de TI).
- O nível de criticidade do sistema e dos dados (a importância de uma organização).
- O nível de sensibilidade dos dados e do sistema.

Uma das tarefas da análise de impacto chama-se BIA (*Business Impact Analysis*). Trata-se de um método que prioriza os níveis de impacto associadamente ao

comprometimento de ativos de informação da organização, com base em uma avaliação qualitativa ou quantitativa da sensibilidade e criticidade desses ativos. A **avaliação da criticidade** de um ativo de informação irá identificar e priorizar os ativos (roteador de borda, sistema corporativo, etc.) que são sensíveis e críticos na execução das tarefas mais críticas da organização. O método BIA é normalmente utilizado para a especificação de Planos de Continuidade de Negócios ou para proteger somente os sistemas e informações mais críticas da organização.

Vale a pena ressaltar que, independentemente do método utilizado para determinar o grau de sensibilidade de um sistema de TI e dos seus dados, os donos do sistema e das informações são os únicos responsáveis em esclarecer o nível de impacto do seu sistema e da informação. Por conseguinte, a abordagem mais adequada na realização da análise de impacto é a técnica de entrevista com o dono do sistema e das informações.

Sendo assim, o impacto negativo de um evento de segurança pode ser descrito em termos de perda ou degradação de qualquer uma das propriedades de segurança (confidencialidade, integridade e disponibilidade), ou, então, pela combinação delas.

Medindo o impacto

Importante

Quando se realiza uma análise de impacto, deve-se levar em consideração as vantagens e desvantagens de se aplicarem avaliações quantitativas ou qualitativas.

Se for realizar uma comparação entre avaliações quantitativas ou qualitativas em termos de segurança da informação, a principal vantagem de uma **avaliação qualitativa** é que ela prioriza os riscos e identifica áreas de melhoria imediata na resolução das vulnerabilidades. Porém a desvantagem é que ela não prevê medidas específicas quantificáveis em relação à magnitude dos impactos, dificultando uma análise custo-benefício da aplicação, ou não, de controles.

No caso de **análise de impacto quantitativa**, a vantagem está em fornecer uma medida da magnitude dos impactos, podendo ser utilizada na avaliação custo-benefício da aplicação, ou não, de controles recomendados. Porém a desvantagem está na dependência da utilização de intervalos numéricos para expressar a medida, o que pode não ficar bem claro no resultado da análise de impacto, forçando uma interpretação de forma qualitativa. Portanto, muitas vezes,

outros fatores devem ser considerados, além dos quantitativos, para determinar a magnitude do impacto.

Assim, é possível dizer que alguns impactos, tangíveis, podem ser medidos de forma quantitativa, com valores de perda da receita, custo da reparação de um sistema, ou o nível de esforço necessário para corrigir problemas causados por um ataque. Contudo impactos como perda de confiança, imagem ou credibilidade não podem ser medidos com valores específicos. A avaliação qualitativa é, então, aplicada, descrevendo-os, em termos de impacto, como de nível alto, médio e baixo, conforme apresentado na tabela 5.

Tabela 5 – Impacto

Nível do Impacto	Descrição do impacto
Alto	O ataque pode resultar em grandes perdas financeiras de ativos ou recursos. Pode causar danos significativos à imagem da organização, impede que ela cumpra as suas tarefas junto aos clientes, ocasiona perda da reputação ou interesse. Pode, ainda, resultar em morte ou ferimentos graves de pessoas.
Médio	O ataque pode resultar em perdas financeiras de ativos ou recursos. Pode causar danos à imagem da organização, impede que ela cumpra as suas tarefas junto aos clientes, ocasiona perda da reputação ou interesse. Pode, ainda, resultar em ferimentos graves de pessoas.
Baixo	O ataque pode resultar em alguma perda de ativos ou recursos. Pode afetar, de forma perceptível, as tarefas da organização e a reputação.

Fonte: Stoneburner, Goguen e Feringa, 2002.

Etapa 7 – Avaliar o risco

Esta etapa tem como objetivo avaliar o nível de risco existente para o sistema de TI. A avaliação de risco de uma ameaça específica para cada uma das vulnerabilidades é calculada com base nos seguintes itens:

1. a probabilidade de uma fonte de ameaça explorar uma vulnerabilidade;
2. o tamanho do impacto, caso um ataque tenha sucesso; e
3. a adequação dos controles de segurança existentes ou planejados para minimizar o risco.

Calcular o Risco

Para que o risco possa ser medido, deve-se criar uma matriz de risco, conforme apresentado na figura 8, presente na sequência, com base em uma escala de risco. A função de cálculo do risco deve ser especificada pelo responsável. A NIST 800-30, Stoneburner, Goguen e Feringa (2002), apresenta um exemplo de função de cálculo de risco.

Função de cálculo de risco: multiplicam-se os valores atribuídos para a probabilidade de ameaças pelo valor do impacto ameaça.

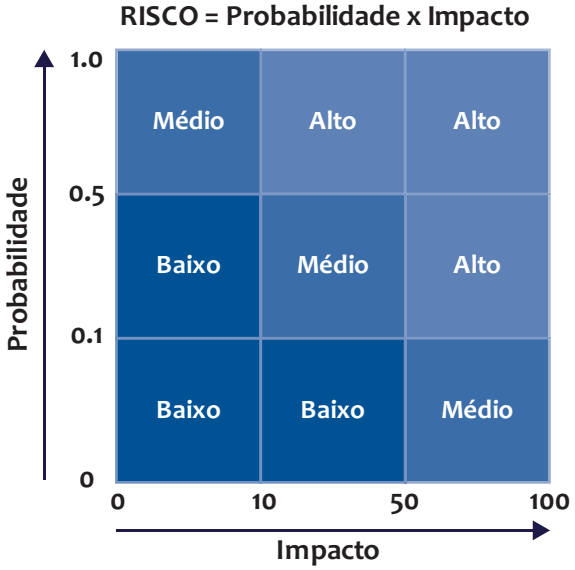
F = Probabilidade × Impacto

A granularidade dos níveis de probabilidade e impacto pode variar em conformidade com a necessidade da organização.

Os valores atribuídos para probabilidade e impacto são:

- O valor atribuído a cada nível de probabilidade é de 1,0 para o alto; de 0,5, para o médio; de 0,1, para o baixo.
- O valor atribuído a cada nível de impacto é de 100 para o alto; 50, para o médio; e de 10, para baixo.

Figura 8 – Matriz de risco



Fonte: Elaboração do autor, 2012

Calculado o risco, com os seus respectivos níveis, segue uma tabela com a descrição de cada nível e as correspondentes ações necessárias.

Tabela 6 – Riscos

Nível do Risco	Descrição e ações
Alto	Se o risco é alto, existe uma grande necessidade de se tomarem medidas corretivas. Deve existir algum plano com medidas corretivas para manter o sistema em funcionamento.
Médio	Se o risco é médio, são necessárias ações corretivas, e um plano deve ser desenvolvido para incorporar essas ações dentro de um período razoável de tempo.
Baixo	Se o risco é baixo, o gerente do sistema deverá determinar se as ações corretivas são ainda necessárias ou decidir aceitar o risco.

Fonte: Stoneburner, Goguen e Feringa, 2002.

Etapa 8 – Recomendações

Esta etapa tem como objetivo prover uma lista com os controles de segurança sugeridos, para que possam minimizar os riscos relacionados à organização até um nível considerado aceitável pela alta direção desta.

Vale a pena lembrar que os controles sugeridos são os frutos do processo de avaliação de risco, e que também levaram em consideração, durante a escolha, os fatores como: eficácia dos controles, por exemplo, a compatibilidade com o sistema; legislação e regulamentação; impacto operacional, por exemplo, o desempenho do sistema; segurança e confiabilidade; por fim, o custo, que também é um fator bastante relevante, pois está relacionado com uma análise custo-benefício.

Etapa 9 – Documentação

Esta etapa tem como objetivo gerar um relatório do processo de avaliação de riscos, descrevendo as ameaças e vulnerabilidades, o cálculo do risco e as recomendações de controles de segurança a serem implementados.

O relatório da avaliação de riscos pode seguir o seguinte sumário:

1 – Introdução

A introdução do documento poderá apresentar o propósito do trabalho – o escopo de abrangência – bem como descrever os componentes do sistema, usuários, entre outros detalhes necessários à realização da avaliação de riscos.

2 – Abordagem da avaliação de riscos

Uma breve descrição de como foi realizada a avaliação de riscos, citando aspectos como: os membros da equipe envolvidos, as técnicas usadas para a coleta de informações e o modo como foi realizada a análise de riscos e a descrição de cada risco.

3 – Caracterização do sistema

Trata-se de uma explanação das características do sistema (hardware, software, links, usuários, etc.). A topologia da rede e o fluxo de entrada e saída de dados são elementos necessários para delinear o esforço da avaliação de riscos.

4 – Declaração de ameaças

Relação de todas as potenciais origens das ameaças.

5 – Resultados da avaliação de risco

Apresentação de uma tabela com os ativos relacionados com suas ameaças e sua probabilidade, vulnerabilidades, impacto, cálculo do risco, controles sugeridos, etc.

6 – Resumo

Resumo com todas as observações pertinentes ao trabalho realizado. Uma sugestão seria a utilização de gráficos relacionando os controles aplicados com os diversos tipos de ameaça.

Minimizar (mitigar) riscos

O processo de mitigar riscos está relacionado à priorização, avaliação e implementação dos controles de segurança recomendados na avaliação de risco.

> **Importante**
>
> Normalmente, a estratégia selecionada no processo de minimizar riscos leva em consideração a seguinte premissa: o controle de segurança a ser implantado deverá ser o mais adequado para reduzir o risco ao nível aceitável, com o menor custo e proporcionando o menor impacto negativo aos recursos e funcionalidades da organização.

O processo de mitigação de riscos pode ser tratado de 6 formas:

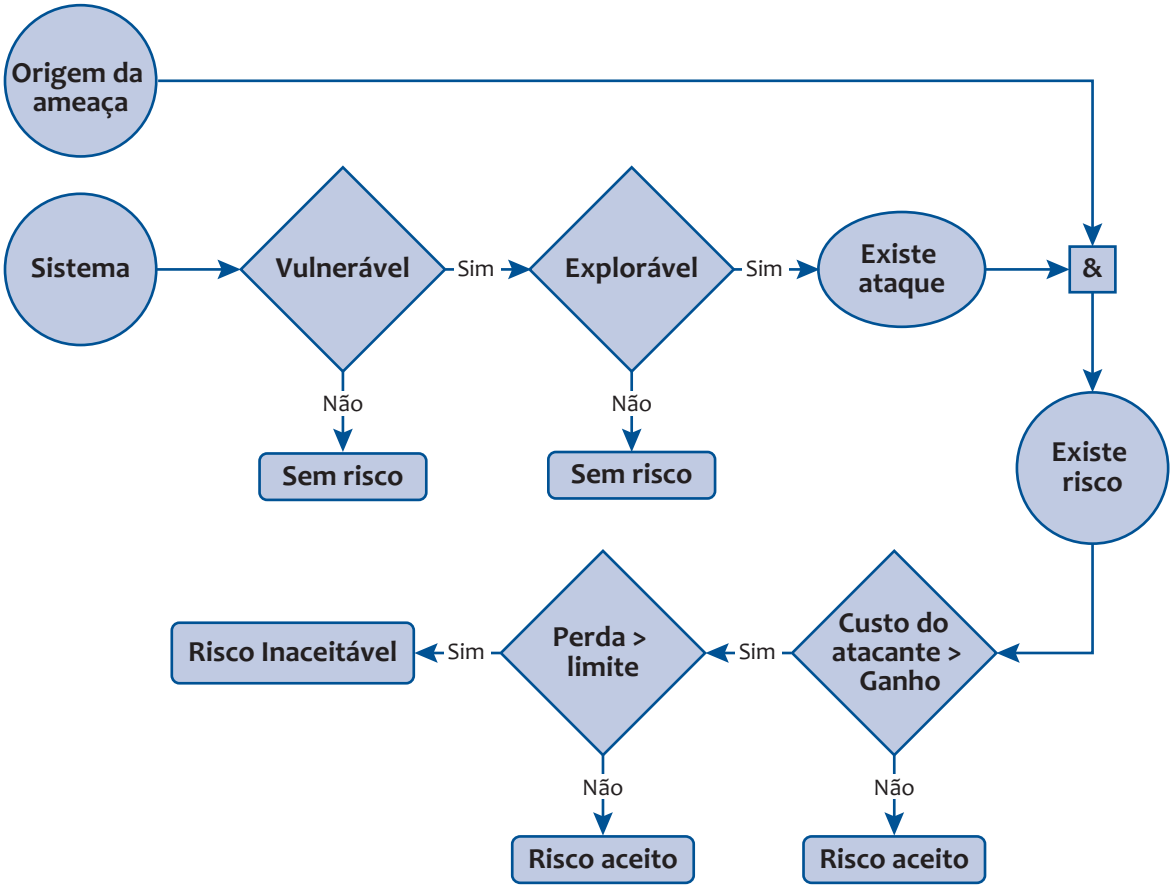
1. Assumir o risco – aceita-se o risco e continua-se a operar o sistema ou implementar controles para trazer o risco a um nível aceitável.
2. Evitar o risco – o risco é evitado, eliminando-se a sua causa ou consequência (evitar a reinicialização do servidor usando Ctrl Alt Del).
3. Limitar o risco – é realizado, implementando controles que reduzam o impacto negativo do ataque (controles de detecção).
4. Planejar riscos – gerencia o risco através do desenvolvimento de um plano de mitigação de risco que priorize, implemente e mantenha os controles de segurança.
5. Pesquisar e reconhecer riscos – visa reduzir o risco de perda do reconhecimento da vulnerabilidade ou falha, e pesquisa controles de segurança para corrigir a vulnerabilidade.
6. Transferir risco – transfere o risco, usando outras opções com o objetivo de compensar a perda (ex.: aquisição de seguro).

A escolha de uma das formas tem que levar em consideração os objetivos e as tarefas da organização. Outra questão a ser pensada é quais riscos serão tratados. Tratar todos é quase que inviável, mas um processo de avaliação, priorizando aqueles que trarão um maior impacto, seria uma estratégia interessante. **Contudo não se esqueça da premissa do controle mais eficiente, mais barato e de menor impacto.**

Definida a forma de tratamento, conhecidos os riscos e os controles recomendados, deve-se definir em quais circunstâncias ou quando serão implantados os controles de segurança.

A figura 9 apresenta uma sequência de atos que são usados durante o processo de decisão – se um risco é aceitável, ou não. Os pontos do fluxograma que possuem a palavra sim são os pontos de acesso para a implementação dos controles.

Figura 9 – Pontos de ação para mitigação de riscos



Fonte: Stoneburner, Goguen e Feringa, 2002.

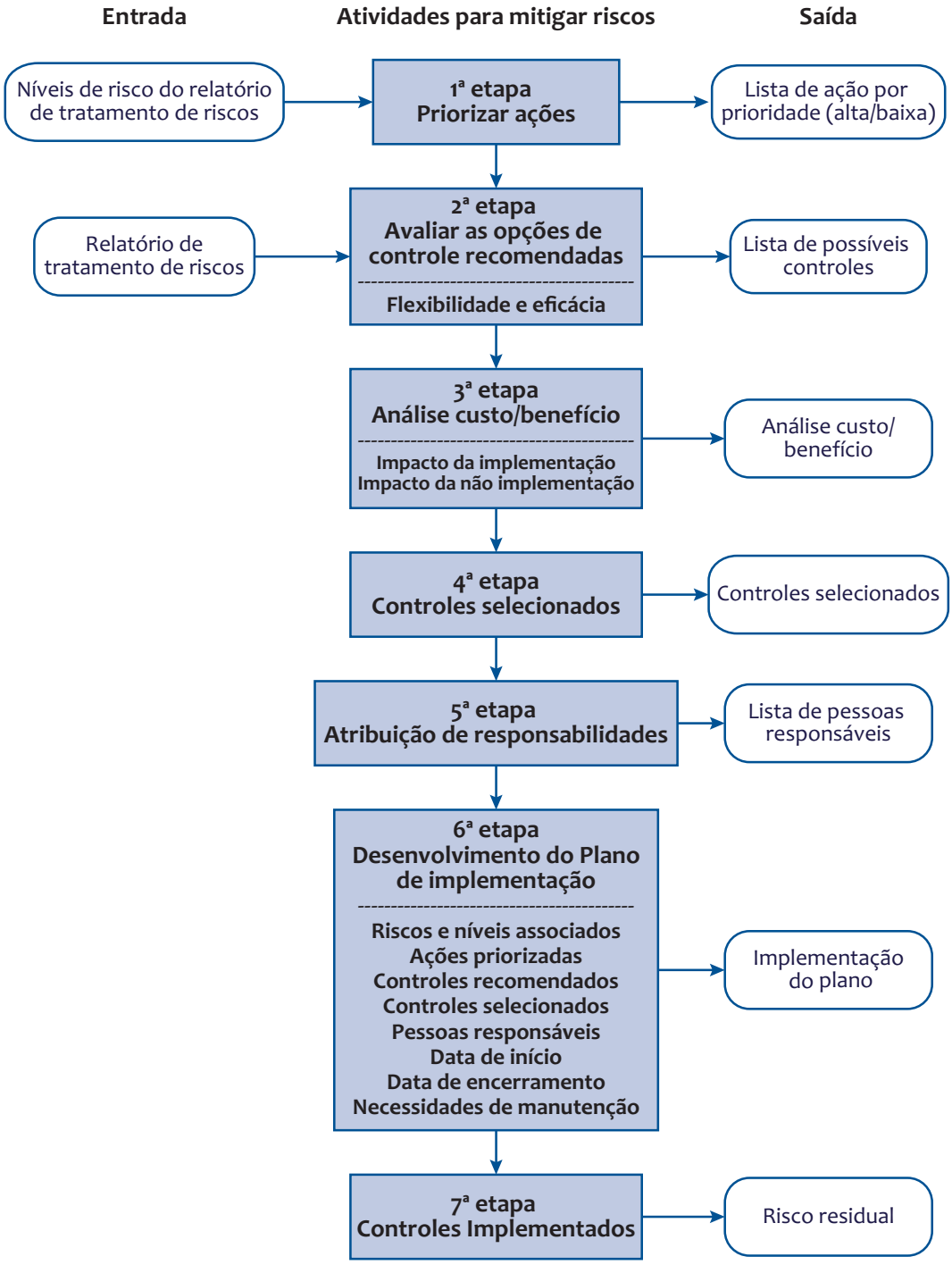
Diante deste fluxograma, temos que, se:

- está vulnerável – implemente técnicas confiáveis para reduzir a probabilidade de uma vulnerabilidade ser explorada;
- explora-se a vulnerabilidade – faça a defesa em profundidade com várias barreiras e use controles administrativos para minimizar o risco ou preveni-lo;
- é maior o custo do atacante que o ganho – faça uso de controles para reduzir a motivação do atacante, aumentando o custo do atacante (usar controles do sistema para limitar acesso do usuário);
- é maior a perda que o limite que se pode perder – aplique mecanismos que minimizem a extensão do ataque, reduzindo assim a perda.

Implementação de controles

Uma vez determinado quando os controles serão implementados, deve-se realizar uma série de ações ordenadas para tal, sempre que necessárias. A seguir, encontram-se as etapas necessárias para implantar os controles.

Figura 10 – Atividades para implementar os controles



Fonte: Stoneburner, Goguen e Feringa, 2002.

Agora, acompanhe a descrição de cada uma dessas etapas.

Etapa 1 – Priorizar ações

As ações são priorizadas com base nos riscos obtidos do relatório de avaliação de risco. A saída é um relatório com as ações a serem realizadas em ordem decrescente.

Etapa 2 – Avaliar as opções de controle recomendadas

São verificadas a compatibilidade e a eficiência do controle sugerido. O objetivo é selecionar o melhor controle à situação.

Etapa 3 – Análise da relação custo/benefício

O objetivo desta etapa é relacionar o custo de cada controle com o benefício da sua implementação, ou não.

Etapa 4 – Seleção de controle

Com base na saída da etapa custo/benefício, os controles que tragam maior benefício ao menor custo devem ser escolhidos.

Etapa 5 – Atribuição de responsabilidade

O objetivo desta etapa é identificar as pessoas com competência para implantar o controle selecionado, gerando um relatório.

Etapa 6 – Desenvolvimento do plano de implementação

O plano de implementação deverá conter os riscos e seus respectivos níveis; controles recomendados; ações priorizadas; os controles selecionados; os recursos necessários para a implementação do controle; lista dos responsáveis; data de início da implementação; e, os requisitos de manutenção.

Etapa 7 – Implementar os controles selecionados

Os controles implementados deverão reduzir o risco, deixando um risco residual.

Análise custo/benefício

A análise custo/benefício pode ser qualitativa ou quantitativa, tendo como objetivo demonstrar que o custo de implementação dos controles pode ser justificado pela redução do nível de risco. Esta análise, quando propõe novos controles ou deseja reforçar os já existentes, engloba os seguintes fatores:

1. O impacto da implementação do controle.
2. O impacto da não implementação do controle.
3. A estimativa dos custos de implementação – hardware, software, custo adicional de políticas e procedimentos; redução da capacidade operacional do sistema com a inclusão de mais segurança; treinamento, manutenção e contratação de pessoal extra para a implementação.
4. Avaliação dos custos de implementação e os benefícios (impacto), com o objetivo de determinar a importância para a organização de implementação dos controles.

Exemplo de análise custo/benefício

Suponha que um sistema crítico de uma empresa, manipulando informações sensíveis entre outros pontos, não possua um módulo de auditoria. A análise custo/benefício irá tentar provar que o módulo de auditoria é vital para o sistema.

Com base nisso, algumas considerações foram feitas nessa tentativa:

1. O impacto com a implantação do recurso de auditoria do sistema – a função de auditoria permitirá que o administrador do sistema monitore as atividades dos seus usuários. Entretanto o desempenho destes sofrerá um impacto negativo, reduzindo a produtividade do usuário. A sua implementação necessitará de recursos adicionais. (Não tangível)
2. O impacto de não implementar o recurso de auditoria – as atividades dos usuário do sistema e as prováveis violações não poderão ser monitoradas e controladas. A segurança não poderá ser maximizada para proteger os dados confidenciais da organização e da missão. (Não tangível)
3. Custo estimado para implantar o módulo de auditoria
    a. custo de desenvolvimento – R$ XXXX
    b. custo de pessoal adicional para executar a auditoria e arquivá-la – R$ XXXX
    c. treinamento – R$ XXXX
    d. geração de relatórios (uso de software) – R$ XXXX

e. manutenção dos dados da auditoria– R$ XXXX

f. custo de manutenção do módulo– R$ XXXX

Total estimado – R$ XXXXXXX

Com base no risco aceitável, o impacto do controle ser incluído, ou não, pode então ser avaliado da seguinte maneira:

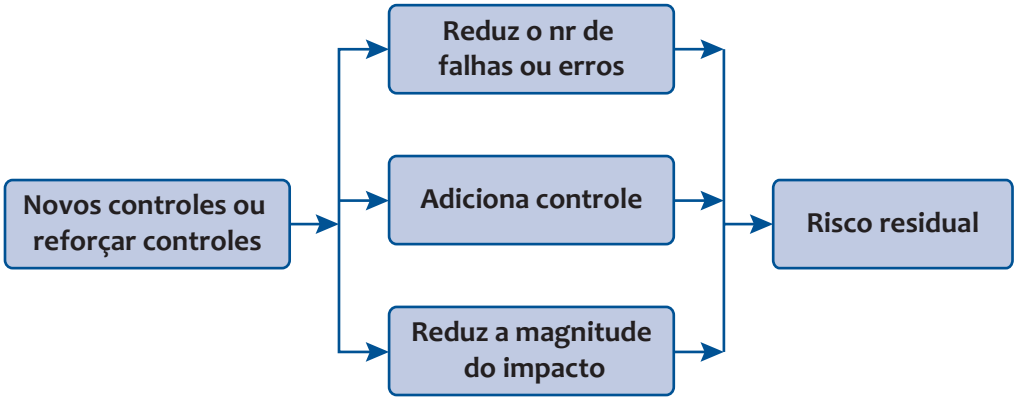
1. Se o controle reduz o risco mais que o necessário, veja se existe uma alternativa mais barata.
2. Se o controle irá custar mais que a redução do risco, busque outra opção.
3. Se o controle não irá reduzir o risco suficientemente, pesquise mais opções.
4. Se o controle oferece uma redução adequada de risco, a um custo adequado, faça uso do mesmo.

Logo, de posse de todas essas informações, a decisão de implementar o controle, ou não, fica a cargo da alta direção da organização.

Risco residual

As organizações podem analisar o quanto o risco foi reduzido após a implementação dos novos controles, levando em consideração os parâmetros de redução da probabilidade da ameaça ou da redução do impacto. Isso porque os controles implementados mitigam o risco pela eliminação de algumas vulnerabilidades do sistema, ou então pela redução da capacidade e motivação da origem da ameaça (tornando o acesso mais difícil ao invasor), ou, ainda, pela redução da amplitude do impacto negativo para a organização. A figura 11 deixa clara a relação entre a implementação de controles e o risco residual.

Figura 11 – Controles implementados e risco residual



Fonte: Stoneburner, Goguen e Feringa, 2002.

Referências

GULDENTOPS, Erik. **Chair do projeto**. 2. ed. Board Briefing on IT Governance – IT Governance Institute, 2003.

ZWICKER, R.; Souza, C. A. de; VIDAL, A. G. da R.; SIQUEIRA, J. de O. **Grau de informatização de empresas**: um modelo estrutural aplicado ao setor industrial do estado de São Paulo. **RAE-eletrônica**, v. 6, n. 2, art. 13, jul./dez. 2007.

STONEBURNER, Gary; GOGUEN, Alice e FERINGA, Alexis. **Risk**- **Management** guide for information technology systems. Ed.: NIST, 2002. NIST SP 800-30.

Atividades de Autoaprendizagem

1) Considerando o conteúdo desta unidade, analise as afirmativas abaixo e insira V para as verdadeiras e F para as falsas.

( ) Um evento pode estar relacionado a um risco. Logo, risco pode ser definido como a possibilidade de um ativo estar sujeito a vulnerabilidades e incidentes.

( ) O risco aumenta em proporção direta ao aumento da probabilidade explorar uma ameaça.

( ) Quanto mais se arrisca em uma empresa, maior é o seu risco de sofrer um evento adverso. Logo, deve-se arriscar, no máximo, até o risco considerado aceitável para a empresa.

( ) O objetivo do processo de riscos é trazer e manter os riscos a um nível considerado aceitável, em conformidade com as necessidades da organização.

Atividade colaborativa

1) Cite e explique, de forma resumida, as etapas do processo de gestão de riscos e os seus objetivos. Publique sua resposta na ferramenta **Exposição**.

Síntese

Nesta unidade, foram apresentados os conceitos de risco e processo de gestão de risco. Foi utilizada como referência a NIST 800-30, o que proporciona uma visão de como o processo de gestão de riscos ocorre em uma organização.

No decorrer do livro foram apresentados frameworks que trabalham com o processo de gestão de risco de TI, os quais proporcionam visões diferentes de como executar essas tarefas. Sendo assim, a escolha pode ser realizada com base no seu conhecimento e/ou no perfil da empresa, mas não se esqueça de ser simples e objetivo/a em suas análises e conclusões. Bom trabalho a todos.

Saiba mais

NIST SP 800-30. **Risk Management** Guide for Information Technology Systems.

ISO 27005 (2008). Gestão de riscos de segurança da informação.

ISACA (2009) The Risk IT Framework. Ed.: ISACA.

STONEBURNER, Gary; GOGUEN, Alice e FERINGA, Alexis (2002). NIST SP 800-30 **Risk - Management** Guide for Information Technology Systems. Ed.: NIST.

ISO/IEC 27005 (2008) Information technology -Security techniques -Information security risk management (draft).

Unidade 2

Gestão de risco e seus frameworks

Objetivos de aprendizagem

- Conhecer o ERM – Eterprise Risk Management Framewok.
- Conhecer o Risk IT Framework e entender as utilidades da aplicação do processo de gestão de risco.

Introdução

A gerência dos riscos em um sistema computacional, associados com a dependência cada vez maior das organizações em tecnologia da informação, é um constante desafio. A pesquisa na busca da execelência da gestão de riscos é um esforço crescente das organizações, pois há necessidade de encontrar maneiras eficientes de entender plenamente os riscos de TI que afectam as suas operações, bem como implementar soluções adequadas para mitigar esses riscos.

Esta unidade irá discutir 2 frameworks que podem ser considerados como base para a realização do processo de gestão de riscos, o ERM (Enterprise Risk Management) e o IT Framework.

O ERM pode ser visto como um framework conceitual, provendo uma estrutura lógica para atender as questões críticas do negócio, como: crescimento, retorno de investimento, consistência e valor agregado, CAS (2003).

O IT Framework provê um framework capaz de controlar e governar os negócios de uma organização, baseado na tecnologia da informação, definindo um conjunto de boas práticas para que as empresas possam identificar, gerir e administrar os riscos de TI, ICASA 2009.

Enterprise Risk Management – Integrated Framework (ERM)

Luiz Otávio Botelho Lento

No decorrer dos anos, as empresas sofreram com escândalos, falhas de investimentos, causando perdas financeiras para si e seus investidores. Com o advento da Lei Sarbanes-Oxley de 2002, as empresas passaram a manter um sistema de controle interno, exigindo gestores qualificados e uma auditoria independente, com o objetivo de atestar a eficácia dos seus sistemas. Com isso, um dos desafios mais críticos para a gerência é determinar qual risco uma organização possui e o quanto ela está disposta a aceitar esses riscos.

Dessa forma, passou a existir a necessidade de se realizar uma gestão de riscos nas empresas, onde estejam bem definidos os seus princípios e conceitos fundamentais, seja utilizada uma linguagem comum entre todos os indivíduos que dela participarem e que existam diretrizes claras sobre o seu processo. Sendo assim, o COSO (Committee of Sponsoring Organizations of the Treadway Commission) criou o Enterprise Risk Management - Integrated Framework, um framework capaz de ser adotado em qualquer empresa, que abrange as características citadas, possibilitando um maior controle interno e proporcionando um foco mais consistente e amplo sobre a questão de gestão de riscos corporativos. Iremos discutir aqui o ERM, apresentando as características desse framework com base na sua publicação, COSO (2004).

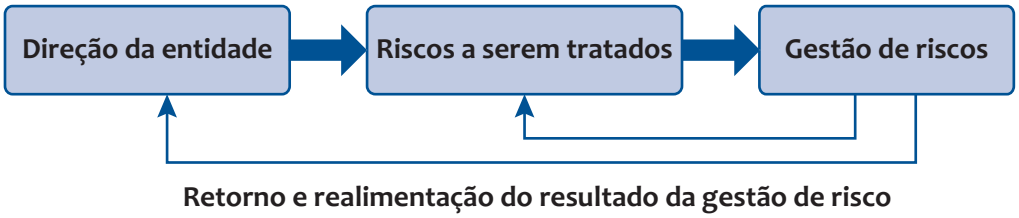
A premissa da existência do ERM é que toda a entidade (empresa, organização, ...) existente é para prover valor para os seus *stakeholders* (investidores, sócios, ...). Isso porque não existe empresa sem lucro, não existe investimento sem lucro. O desafio para o gerente em lidar com a incerteza está em saber até onde arriscar para crescer. Logo, a capacidade de gerir riscos dá à organização uma base para saber até onde se deve arriscar para manter/crescer a sua margem de lucros.

Sendo assim, segundo Coso (2004), o ERM é definido como:

> um processo, efetuado pela diretoria administrativa de uma entidade, gerente e demais componentes necessários a sua execução, aplicado na estratégica da empresa e também na empresa como um todo, desenhado para identificar potenciais eventos que possam afetar a entidade, e gerir os riscos de forma que não passem do nível aceitável, com o objetivo de proporcionar uma razoável garantia em relação à realização dos objetivos da entidade.

Essas ideias são apresentadas na Figura 1.

Figura 1 – Processo do ERM



Fonte: Elaboração do autor, 2012.

Entretanto, CAS (2003) adotou como definição de ERM a disciplina pela qual uma organização acessa, controla, explora e monitora riscos de todas as origens, com o propósito de aumentar os valores a curto e longo prazo para os seus "stakeholders".

A definição do ERM fundamenta atividades como: o fluxo dos processos por meio da entidade; a realização da gestão de riscos por pessoas em todos os níveis da organização; a identificação de potenciais eventos que, caso ocorram, afetarão a entidade; além da possibilidade de gerir os riscos dentro do seu nível aceitável, entre outros. (COSO, 2004)

Uma visão interessante do ERM é o descrito por Thomé (2010). Ela diz que o ERM é caracterizado por práticas de gestão sistemáticas para avaliar e monitorar riscos, e otimizar a forma pela qual o risco é gerenciado, suportado e facilitado pelo framework de gestão de riscos adequado.

Importância do ERM

O ERM possibilita que o gerente trabalhe melhor com a incerteza, o risco associado, e a oportunidade, possibilitando um aumento da capacidade de criar valor, isto é, ele está focado na ação e não somente na análise dos riscos. Por conseguinte, pode-se dizer que o valor de retorno é maximizado quando a administração estabelece a estratégia e os objetivos para atingir um melhor equilíbrio entre crescimento, metas e riscos, possibilitando, assim, uma maior eficiência na utilização dos recursos.
O ERM-framework trabalha com as seguintes características:

- Alinhar o risco aceitável à estratégia, de forma que a administração possa estabelecer os objetivos e o desenvolvimento de mecanismos para gerenciar os riscos relacionados.
- Responder ao risco, tomando decisões na identificação e seleção das alternativas de respostas aos riscos (prevenir, reduzir, transferir e aceitar).
- Reduzir as surpresas e as perdas operacionais, dando às entidades uma maior capacidade para identificar eventos em potencial e estabelecer respostas.

- Identificar e gerir o grande leque de riscos que toda empresa enfrenta nas suas diferentes partes, facilitando uma resposta eficaz aos impactos inter-relacionados e respostas integradas aos múltiplos riscos.
- Aproveitar as oportunidades, considerando uma gama completa de eventos em potencial, capacitando a gerência a identificar e aproveitar as oportunidades de forma proativa.
- Melhorar a implantação do capital, por meio da coleta de informações sobre os riscos, possibilitando o gerenciamento eficaz quanto à avaliação das necessidades de capital, buscando melhorarias à alocação desse capital.

Objetivos do ERM

Os objetivos a serem alcançados por uma entidade devem estar de acordo com a sua missão. Sendo assim, o ERM framework está direcionado aos objetivos de uma entidade e são divididos em 4 categorias:

1. Estratégicos, nos quais são estabelecidas as metas alto nível, alinhadas à missão da organização.
2. Operacionais, os quais buscam utilizar de forma eficiente os seus recursos.
3. Base de informações, proporcionar relatórios confiáveis.
4. Cumprimento das leis e regulamentos.

A divisão em categorias possibilita focar em separado os aspectos do ERM, apesar de elas serem sobrepostas, isto é, um objetivo específico pode pertencer a mais de uma categoria.

Componentes do ERM

O ERM possui 8 componentes que se inter-relacionam:

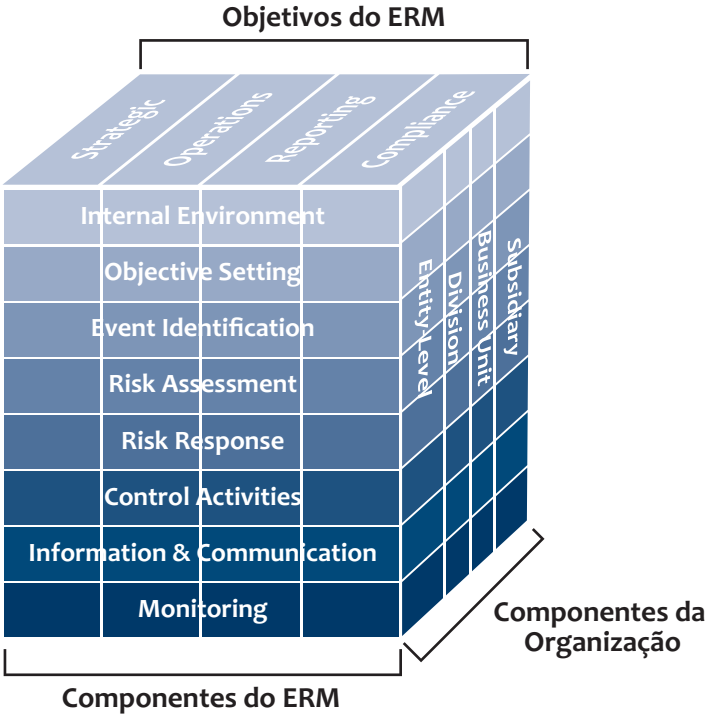
1. **Ambiente interno** – relacionado à organização, define a base de como o risco é visto e dirigido por pessoas de uma entidade, incluindo a filosofia de gestão de risco e a compreensão de risco aceitável, a integridade e os valores éticos, e o ambiente em que os riscos operam.

2. **Fixando os objetivos** – os objetivos devem existir antes do gerenciamento identificar os potenciais eventos que afetam a sua realização. O ERM garante que a gestão de riscos possui um processo para estabelecer objetivos e que esses estão alinhados com a missão da entidade, estando consistentes com o risco aceitável.
3. **Identificação de eventos** – os eventos, sejam internos ou externos, que afetam a realização dos objetivos de uma entidade, devem ser identificados, distinguindo entre riscos e oportunidades. As oportunidades são devolvidas à estratégia de gestão de processos ou definição de objetivos.
4. **Avaliação de riscos** – os riscos são analisados, considerando a sua probabilidade e impacto, para determinar quais deles e como devem ser gerenciados.
5. **Respostas aos riscos** – a gestão de riscos seleciona as respostas aos riscos, evitando, aceitando, reduzindo, ou partilhando os riscos. É desenvolvido um conjunto de ações para alinhar os riscos com a tolerância ao risco da entidade e do risco aceitável.
6. **Atividades de controle** – políticas e procedimentos são estabelecidos e implementados para ajudar a garantir que as respostas aos riscos sejam efetivamente executadas.
7. **Informação e comunicação** – a informação relevante é identificada, capturada e comunicada no formato que as pessoas possam trabalhar as suas responsabilidades.
8. **Monitoramento** – o monitoramento é realizado e as modificações realizadas quando necessárias.

O relacionamento dos objetivos e componentes

Existe uma relação direta entre os objetivos, que são o que uma entidade se esforça para alcançar, e os componentes do ERM, representando o que é necessário para alcançá-los. Esse relacionamento é apresentado em uma matriz tridimensional, sob a forma de um cubo, conforme apresentado na Figura 2.

Figura 2 – Relação entre objetivos e componentes



Fonte: COSO (2004).

Conforme podemos verificar por meio dessa Figura, os relacionamentos entre esses dois grupos de componentes, da Organização e do ERM, demonstram a eficácia e as limitações do ERM, englobando os controles internos, considerando as funções e responsabilidades das pessoas que trabalham na entidade e, por fim, organizando o relatório no que diz respeito à gestão de riscos.

Eficácia

Determinar se a administração de uma entidade de risco da empresa é eficaz, trata-se de um julgamento resultante de uma avaliação dos oito componentes do ERM. Para isso, eles devem estar presentes e funcionando efetivamente, isto é, não podem existir deficiências de materiais para suas realizações e o risco deve estar dentro do aceitável. Quando o gerenciamento de risco da empresa está determinado a ser eficaz em cada uma das quatro categorias de objetivos, o conselho de administração e gestão tem garantia razoável de que entendem até que ponto os objetivos estratégicos e as operações da entidade estão sendo alcançados, que a entidade de informação é confiável e as leis e regulamentos aplicáveis estão sendo cumpridos.

Limitações

Embora o ERM proporcione importantes benefícios, existem limitações: as de julgamento do ser humano em relação à tomada de decisões sobre: como responder ao risco e o estabelecimento de controles; os custos e benefícios relativos; as falhas humanas, como simples erros ou erros, por exemplo.

Engloba os controles internos

O ERM inclui o controle interno, formando um conceito mais robusto e uma ferramenta para a gestão, em que o controle interno é definido e descrito no Internal Control - Integrated Framework [COSO, 2008].

> Saiba mais em Integrated Framework – Guidance on Monitoring Internal Control Systems. Ed.: Committee of Sponsoring Organizations of the Treadway Commission.

Funções e responsabilidades

Todos em uma entidade têm alguma responsabilidade na gestão de riscos corporativos, por exemplo: o diretor executivo é responsável e deve assumir a propriedade, os gerentes apoiam a filosofia do ERM, promovendo o cumprimento do risco aceitável da gestão de riscos dentro de suas esferas de competência. O agente de risco, diretor financeiro, auditor interno, e outros geralmente têm responsabilidades de apoio, e os demais colaboradores da entidade são responsáveis pela execução do gerenciamento de riscos corporativos, de acordo com as diretrizes e protocolos estabelecidos. Existem vários outros papéis e funcionalidades que são criados em conformidade com as necessidades da organização.

Organização do relatório

O relatório proposto pelo ERM pode ser dividido em 2 partes: a primeira parte com um resumo executivo, com a definição do ERM. Nesse resumo, deve-se descrever os princípios e conceitos relacionados com a gestão da segurança da informação, oferecer orientação para todos os níveis de gestão em empresas e outras organizações, para a avaliação e melhoria da eficácia da gestão de riscos corporativos. O sumário executivo proporciona uma visão de alto nível, dirigido a executivos, outros executivos e diretores, por exemplo. A segunda parte do

relatório possui as técnicas de aplicação dessa gestão, proporcionando, portanto, uma visão das técnicas úteis.

Com o entendimento do ERM framework, todas as partes do processo de gestão de riscos estarão em condições de falar a mesma linguagem quanto ao risco dos seus ativos, o que inclui os executivos de negócio; assim, possibilita-se uma tomada de decisão mais adequada às necessidades do negócio.

> Saiba mais em Enterprise Risk Management — Integrated Framework.
> Ed.: Committee of Sponsoring Organizations of the Treadway Commission.

O ERM como um framework conceitual

Uma outra forma de entender o ERM é o proposto em CAS (2003), podendo ser entendido sob a perspectiva de 2 dimensões: a primeira abrangendo os tipos de riscos e a outra abrangendo as etapas do processo de gestão de riscos. O quadro a seguir apresenta essa visão bidimensional.

Quadro 1 – Framework ERM

Framework ERM				
Fases do Processo	**Tipos de Riscos**			
	Perigo	**Financeiro**	**Operacional**	**Estratégico**
Estabelecer o Contexto				
Identificar os riscos				
Análise de riscos				
Integrar riscos				
Avaliar/Priorizar riscos				
Tratar riscos				
Monitorar e revisar				

Fonte: CAS (2003).

As categorias de riscos apresentadas nesse quadro são categorias/tipos de riscos que podem ser observados nas organizações. Com a finalidade de melhor esclarecer esses tipos, são apresentados alguns exemplos a seguir:

I - Perigo – são riscos que podem acontecer ao acaso, levando a prejuízos o negócio da organização.

- Fogo e outro dano de propriedade.
- Tormentas naturais.
- Interrupção do negócio.

II - Financeiro – correspondem aos riscos financeiros que normalmente qualquer organização está exposta. Esses podem inviabilizar, por exemplo, a continuidade da organização.

- Preço do ativo.
- Liquidez (custo operacional, fluxo de caixa, ...).
- Perda de crédito, ou crédito reduzido, ...
- Seguro para os ativos.

III - Operacional – são os riscos relacionados à operacionalidade dos processos de negócio da organização, isto é, tudo aquilo que poderá afetar que esses possam ser executados.

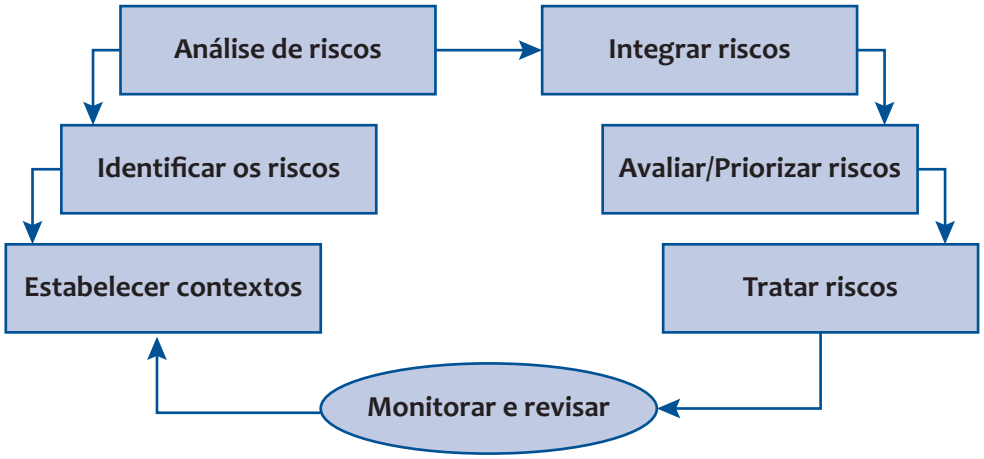
- Operações do negócio (recursos humanos, desenvolvimento de produtos, ...).
- Liderança de equipe.
- Disponibilidade e relevância da tecnologia da informação.

IV - Estratégico – são riscos que, por exemplo, podem afetar a demanda do mercado, reduzindo o volume de negócios da organização.

- Danos na reputação.
- Competição entre concorrentes.
- Inovação tecnológica.
- Disponibilidade de capital.

Segundo CAS (2003), o processo de gestão de riscos é subdivido em etapas, baseado em AS/NZS (2004). Se for analisar e comparar as Figuras 3 e 4, elas apresentam, respectivamente, as fases do ERM e do Risk It Framework, pode-se observar que ambas são compostas por 7 etapas, apesar de a metodologia adotada pela AS/NZS (2004) buscar manter um processo constante de monitoramento do risco, bem como manter informado dos riscos mais críticos encontrados durante o processo. Pode-se dizer que ambas as metodologias apresentam um processo de gestão de riscos dinâmico e flexível, podendo ser adequado às necessidades das organizações.

Figura 3 – Fases do Processo do ERM



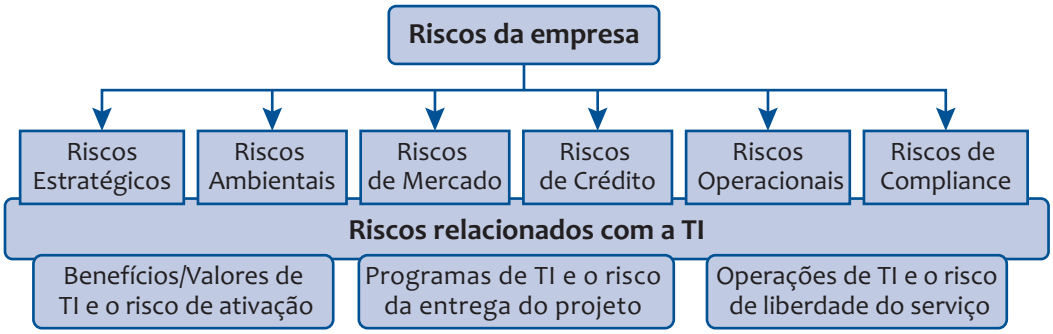
Fonte: CAS (2003).

Risk IT Framework

Apresentaremos aqui o RISK IT Framework, descrito em ICASA (2009), que foi criado com o objetivo de ajudar os gerentes a relatar os riscos de TI. Esse framework está baseado em um conjunto de princípios de gestão relacionados com os processos de negócio. Logo, pode-se dizer que o RISK IT framework é um conjunto de boas práticas para identificar, governar e gerenciar os riscos de TI.

O risco de TI é um componente do risco global da empresa, em que outros riscos como: o risco estratégico, ambiental, de mercado, de crédito, operacional e de compliance, compõem o universo de riscos que uma empresa enfrenta no seu dia a dia, conforme apresesntado na Figura a. Entretanto, os riscos de TI em algumas empresas são relacionados com o risco operacional e estratégico. Esse último, que pode possuir um componente de TI, principalmente quando relacionado a novas iniciativas empresariais. O mesmo se aplica ao risco de crédito, em que os problemas de segurança com a TI podem levar a baixas avaliações de crédito. Logo, o risco de TI não está numa dependência hierárquica com os outros riscos que dizem respeito a uma organização, mas está relacionado aos demais riscos de uma empresa, pois essa depende da TI na realização de suas tarefas.

Figura 4 – Risk IT na hierárquica do risco



Fonte: ICASA 2009.

Trabalhar com TI pode ser considerado um negócio de risco, principalmente se o negócio da empresa estiver associado ao uso, propriedade, operação, participação, influência e adoção de TI. Isso porque os eventos relacionados à TI e às condições em que eles acontecem podem afetar os processos de negócio, criando desafios na busca das metas e objetivos estratégicos. Sendo assim, os riscos de TI podem ser classificados com:

1. Benefícios/Valores de TI e o risco de sua ativação – relacionado às oportunidades de se utilizar a TI com o objetivo de melhorar a eficiência dos processos de negócio ou para novas iniciativas de negócio.
2. Programa de TI e o risco relacionado à entrega do seu projeto – relacionado com a contribuição que a TI dará às melhorias ou novas soluções do negócio, normalmente na forma de programas ou projetos.
3. Operações de TI e o risco de liberação do serviço – relacionados com o desempenho dos sistemas e serviços de TI que possam trazer redução ou destruição do valor da empresa.

Objetivos e benefícios de adotar o Risk IT Framework

O Risk IT Framework explica e possibilita que seus usuários integrem o gerenciamento de riscos de TI no ERM da empresa, possibilitando que a empresa tome decisões de forma consciente quanto ao retorno do risco. Ele também fornece informações sobre a extensão do risco, até se deve arriscar em relação ao risco, isto é, se esse é aceitável para a tomada de decisões da empresa. Por fim, ele dá condições de entender como responder ao risco.

Em resumo, o Risk IT Framework dá à empresa condições de tomar decisões adequadas, tendo consciência do risco que está correndo, isto é, o framework dá à empresa capacidade de entender e gerenciar os riscos de TI considerados significantes. Isso porque o framework provê uma estrutura de processo fim a

fim para gerenciar o risco de TI com sucesso, orientações incluindo ferramentas e técnicas para o entendimento e gerenciamento de forma concreta das operações do negócio. Isso inclui uma lista das potenciais adversidades mais comuns que possam causar impacto à realização dos objetivos do negócio.

Princípios do Risk IT

O Risk IT se baseia em um conjunto de princípios orientadores para a eficaz gestão dos riscos de TI. Os princípios são baseados em princípios comumente aceitos pelo ERM, que têm sido aplicados ao domínio da TI. O modelo de processo do Risk IT foi projetado e estruturado para permitir que as empresas apliquem os princípios na prática e compararem o seu desempenho de TI.

O Risk IT framework está relacionado com o risco do uso de TI nos processos de negócio. Essa conexão com o negócio é fundamentada nos princípios de acordo com os quais o framework foi construído, conforme pode ser visto na Figura 6.

Figura 5 – Princípios do Risk IT

Fonte: ICASA 2009.

Assim, podemos ver que os princípios do Risk It:

a. Conectam-se aos objetivos do negócio:

- O risco de TI é tratado como um risco do negócio.
- O foco do negócio é seu resultado almejado, assim, a TI suporta a execução dos objetivos do negócio e os riscos de TI são expressos como o impacto que eles podem causar à execução desses objetivos.

- Em toda a análise de riscos existe a análise de como os processos de negócio dependem dos recursos de TI.

b. Alinham-se ao gerenciamento do Risk IT com o ERM:

- Os objetivos do negócio e o risco total da empresa estão claramente definidos.
- O processo de decisão da empresa leva em consideração todas as consequências e oportunidades do risco.
- O risco que a empresa quer correr reflete na filosofia de gerenciamento de risco e influencia na sua cultura e no seu estilo operacional.

c. Balancia-se o custo/benefício do Risk IT:

- O risco é priorizado e direcionado de acordo com o quanto se quer arriscar e o que é o risco aceitável.
- Os controles são implementados para um risco e baseados na análise custo/benefício desse.
- Os controles existentes são direcionados para múltiplos riscos ou para os riscos mais críticos.

d. Promovem uma comunicação justa e aberta:

- Informações, claras, objetivas e a tempo sobre o risco de TI são trocadas e servem como base para tomadas de decisão.
- As questões, princípios e gerenciamento de riscos são integrados na empresa.

e. Estabelecem responsabilidades:

- Pessoal chave (ex.: donos do negócio e diretores) estão envolvidos na gestão de risco.
- Existe uma atribuição e aceitação clara da propriedade do risco, incluindo a assunção da responsabilidade, realizando a medida e o gerenciamento integrado do risco.
- As decisões de risco são tomadas por pessoas autorizadas, com o foco na gestão do negócio.

f. Funcionam como parte das atividades diárias:

- Por causa da natureza dinâmica do risco, a gestão de risco é uma atividade interativa e contínua. Toda mudança pode trazer risco e oportunidades, assim, a empresa deve estar preparada para saber quais são esses novos riscos e oportunidades.
- Uma atenção é dispensada para a avaliação de riscos, funções e responsabilidades, ferramentas, técnicas e critérios de riscos. São levados em consideração, principalmente: a identificação dos

principais processos e os seus riscos associados; entendimento dos impactos na execução dos objetivos; e a identificação do fator que indica quando uma atualização da infraestrutura ou componentes dessa são necessários.

- As práticas de gestão de riscos são priorizadas e embutidas nos processos de decisão da empresa.
- As práticas de gestão de riscos são diretas e fáceis de serem usadas, contendo práticas para detectar ameaças e o potencial do risco, bem como preveni-lo e minimizá-lo.

Modelo de processo do Risk IT Framework

O Risk IT framework foi desenvolvido com base nos princípios acima citados e dentro de um modelo de processos. As principais atividades do modelo de processo de gestão de riscos estão relacionadas a um conjunto de processos agrupados em 3 domínios: governança do risco, avaliação e resposta ao risco, conforme apresentado na Figura 6.

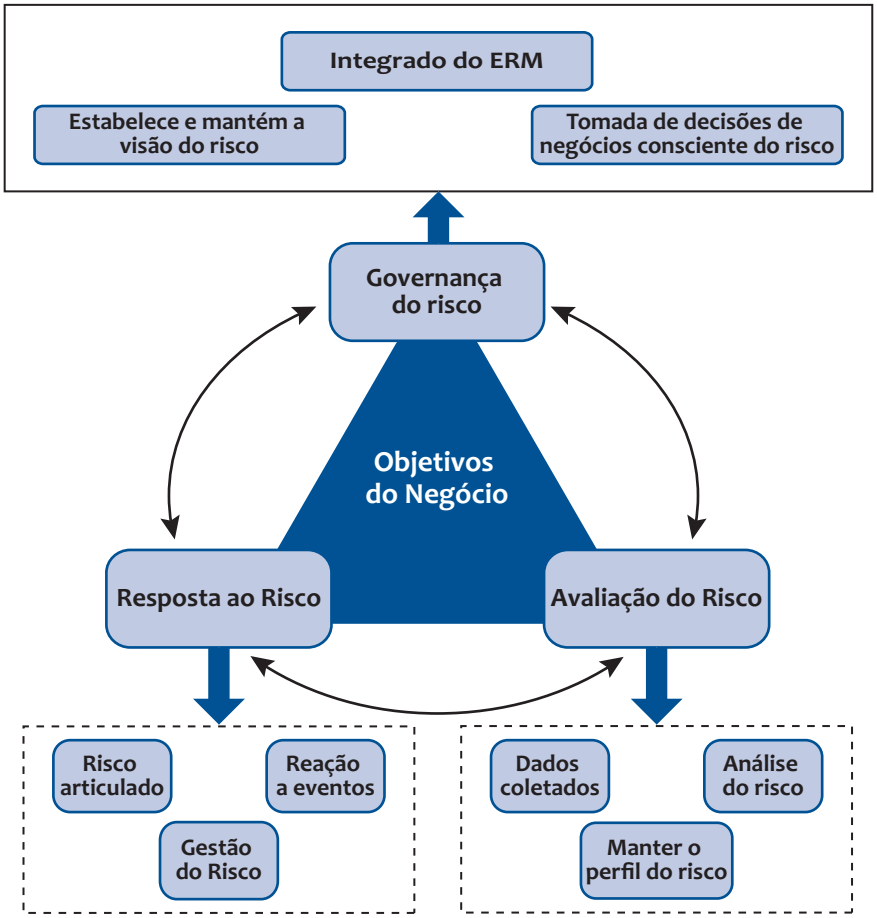
Governança do risco

Garante que as práticas de gestão de risco estejam arraigadas na empresa, melhorando a segurança, via a adequação do risco. Para isso, nessa etapa, são definidos:

1. **O quanto se deseja arriscar e o risco aceitável da empresa** – apesar de os conceitos serem semelhantes, o primeiro consiste no quanto a empresa está disposta a arriscar para alcançar o seu objetivo no negócio. No entanto, o risco aceitável consiste na variação aceitável do risco para se alcançar o objetivo.
2. **As atribuições e responsabilidades para a realização da gestão de riscos** – as atribuições são dadas àqueles que garantem que as atividades sejam concluídas com sucesso. A responsabilidade cabe ao dono dos recursos e ele que tem a autoridade para aprovar a atividade e/ou aceitar o resultado da atividade dentro de um determinado risco.
3. **Conscientização e comunicação do risco** – a consciência do risco é a possibilidade de reconhecer que o risco é parte integrante do negócio. Isso não implica que todos os riscos devam ser evitados ou eliminados, mas que eles sejam compreendidos e conhecidos. A comunicação do risco é parte fundamental nesse processo, que remete à ideia de as pessoas ficarem desconfortáveis ao falar sobre risco.

4. **Cultura do risco** – envolve o comportamento para a tomada de decisão quanto ao risco em relação à política de segurança e quanto aos resultados indesejáveis (negativos).

Figura 6 – Risk IT Framework



Fonte: ICASA 2009.

Avaliação do risco

Essa etapa está relacionada ao impacto do negócio e cenários de risco. Na análise do impacto, a gestão de risco necessita possuir o entendimento mútuo entre a TI e o negócio da empresa quanto ao risco que necessita ser gerenciado, bem como o porquê dessa necessidade.

Todas as partes interessadas (stakeholders) devem ter a capacidade de entender e expressar como os eventos adversos podem afetar o negócio da empresa. Logo, a análise de impacto consiste nas falhas ou eventos relacionados à TI que podem afetar os principais processos e serviços da empresa.

Os **cenários de risco consistem em uma técnica** usada para superar o problema de identificar quais riscos são importantes e relevantes entre todos os existentes. Ela usa como base de sua abordagem o realismo, a introspecção, o engajamento da organização e uma melhor análise e estrutura em relação à complexidade dos riscos de TI.

Importante

Desenvolvidos os cenários de risco, eles são usados durante a análise de risco para verificar a frequência com que o cenário acontece e os impactos estimados nos negócios.

Componentes essenciais de resposta ao risco

1 – Indicadores de risco

Os indicadores de risco são métricas que tem a capacidade de mostrar o quanto a empresa está sujeita ou a probabilidade de estar sujeita a um risco que ultrapasse ao valor que deseja arriscar. Os indicadores são específicos para cada empresa, e sua escolha dependerá de uma série de parâmetros do ambiente interno e externo, tais como o tamanho e a complexidade da empresa, se estão operando em um mercado altamente regulado, e o foco da sua estratégia.

2 – Priorização e definição de resposta ao risco

Com base nesses indicadores, podem ser determinados quais são os riscos mais críticos que devem ser priorizados quanto ao tratamento. Logo, a definição de resposta (tratamento) ao risco tem como objetivo mantê-lo dentro do limite do que se deseja arriscar, isto é, a resposta ao risco necessita ser definida para que o risco residual esteja dentro dos limites do risco aceitável.

3 – Prevenir o risco

Prevenir o risco significa sair da atividade ou das condições que dão origem a ele. Ela se aplica quando não existe uma resposta de risco adequada.

4 – Reduzir o risco

Consiste em uma ação de detectar o risco seguido por outra ação de reduzir a frequência e/ou impacto de um risco.

5 – Compartilhando o risco

Consiste em reduzir a quantidade de ocorrências ou o impacto pela transferência ou compartilhando parte desse risco, normalmente incluem seguros e a terceirização de serviços.

6 – Aceitando o risco

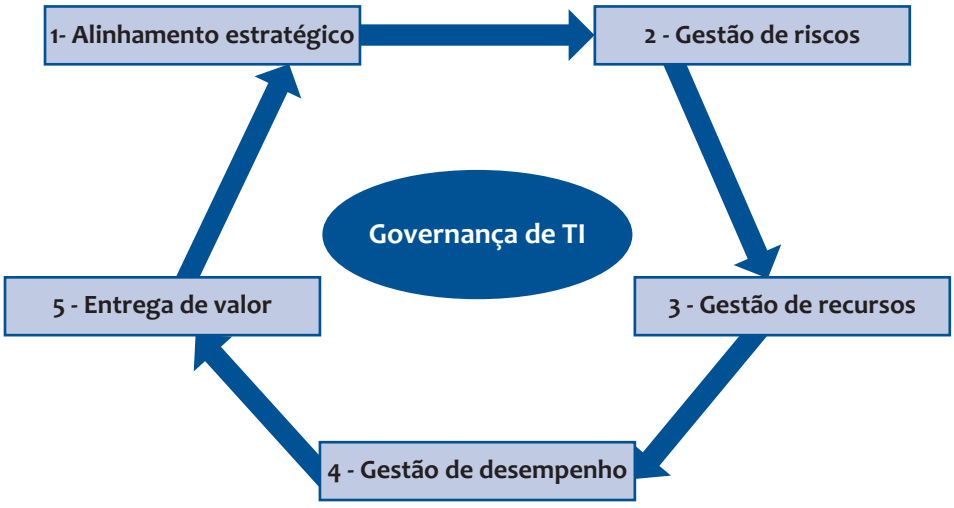
Consiste em aceitar um determinado risco, isto é, a perda é aceitável quando ocorrer.

Saiba mais em:
The Risk IT Framework. Ed.: ISACA.

Utilizar a gestão de riscos a favor da organização

Antes de ver como usar a gestão de riscos a favor da organização, vale a pena ressaltar que a TI deve inicialmente ser parte do seu negócio. A Figura 7 apresenta como o processo de gestão de riscos se encaixa dentro da governança de TI.

Figura 7 – Resultados da Governança de TI



Fonte: Elaborado pelo autor, 2010.

Vamos agora aos significados de cada uma dessas relações da Gestão de TI com a organização. Acompanhe na sequência:

1. **Alinhamento estratégico** – o alinhamento estratégico da segurança da informação com a estratégia do negócio, para dar suporte aos objetivos organizacionais;
2. **Gestão de riscos** – execução de medidas adequadas para gerenciar e mitigar os riscos e reduzir os impactos a um nível aceitável;
3. **Gestão de recursos** – utilizar o conhecimento e a infraestrutura computacional de forma eficaz e eficiente;
4. **Gestão de desempenho** – realizam-se medições e monitoramento, comparando com as métricas estabelecidas, com o intuito de verificar se os objetivos estabelecidos estão sendo alcançados;
5. **Entrega de valor** – alcançado pela otimização dos investimentos realizados no sistema computacional em prol dos objetivos organizacionais.

Analisando a Figura 7, parte-se da premissa que existe o alinhamento estratégico da TI com o negócio. Dessa forma, pode-se saber qual o risco que a organização possui, como tratá-los e gerenciá-los de forma a mantê-los a um nível considerado aceitável (os frameworks discutiram como).

Sendo assim, há condições de fazer o melhor uso dos recursos disponíveis, aplicando-os de forma adequada às necessidades do negócio da organização. Logo, o desempenho poderá estar em acordo com as métricas estabelecidas pela alta direção da organização, retornando todo o investimento realizado (ROI – Return on Investment).

Saiba mais em:
Enterprise Value: Governance of IT Investments - The Val It Framework 2.0 – The IT Governance Institute. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/Documents/ValIT-Framework2.0-Jul-2008.pdf>.

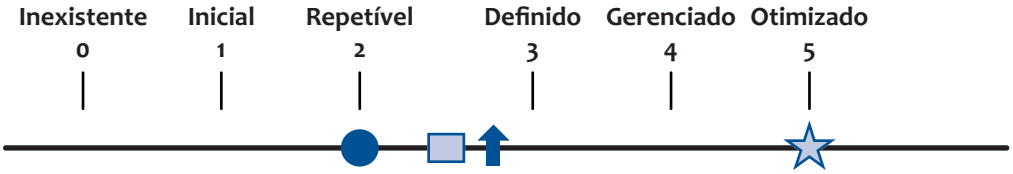
Maturidade da TI

Em virtude da necessidade, pela manutenção da qualidade e segurança das informações e de seus bens, os executivos das empresas buscam otimizar os recursos de TI (ex: aplicativos, hardware, software). Isso significa que para saber qual risco a organização "deseja correr", como, o que e quanto investir, deve-se saber o quanto a sua TI está madura e deverá ficar ainda mais.

Logo, para cumprir todas essas tarefas e alcançar as metas da empresa, os executivos devem entender o nível de arquitetura de TI que possuem e, assim, ter condições de exercer a governança e os controles da informação.

O COBIT apresenta um modelo de maturidade para o gerenciamento e controle dos processos de TI da organização, usando um método de pontuação que varia de 0 a 5, representando as escalas de maturidade, conforme visualizado na Figura 8, bem como uma descrição das características de cada nível.

Figura 8 – Modelo de Maturidade



Status atual da empresa

Padrão internacional para empresas

Normal para a indústria

Meta da empresa

0 - Os processos de controle não são aplicados em nada
1 - Os processos são ad hoc e desorganizados
2 - Os processos seguem um padrão regular
3 - Os processos são documentados e comunicados
4 - Os processos são monitorados e medidos
5 - Melhores prática são seguidas e automatizadas

Fonte: COBIT (2007).

O uso dessa técnica possibilita:

- Apresentar uma visão atual das práticas de segurança da informação adotadas pela empresa;
- Estabelecer metas futuras de desenvolvimento da TI, com base nas escalas do modelo proposto;
- Planejar projetos para alcançar as metas de TI, definindo mudanças necessárias para melhorar o gerenciamento;
- Priorizar projetos de TI, identificando onde é o maior impacto e onde é fácil a sua implementação.

Estabelecida a maturidade da TI da organização, são estabelecidas as suas metas de crescimento. Por exemplo, a empresa encontra-se no nível 2 de maturidade e deseja alcançar o nível 3 nos processos de TI, isto é, possuir todos documentados e cientes pelos seus usuários. A partir desse ponto, pode-se criar projetos para que as metas estabelecidas na alta direção possam ser alcançadas.

Logo, o processo de gestão de risco tem o seu início com, por exemplo:

a. Mapeamento de processos;

b. Pesquisa da cultura de riscos na organização;

c. Identificação e avaliação dos riscos existentes;

d. Avaliação dos controles existentes.

Como resultado do processo de gestão de riscos, pode-se ter:

1. Os riscos principais (estratégicos) mapeados;
2. As oportunidades de melhoria;
3. Os principais controles analisados;
4. Os indicadores de monitoramento.

Valor agregado da gestão de riscos

A gestão de riscos de TI pode agregar vários valores à organização. A forma como ela é aplicada e o seu escopo de abrangência irá trazer, com certeza, benefícios a setores da organização. Enter esses benefícios, poderia citar o **aumento da visibilidade da TI dentro da organização.**

Isso vem ao encontro da necessidade da TI estar alinhada ao negócio da organização. O que, por sua vez, proporciona um maior alcance do sistema computacional, aumentando a sua capilaridade pelos diversos segmentos de negócio. Dessa forma, proporciona-se:

- Razões para uma maior e melhor capacitação técnica da equipe de TI;
- A viabilização de uma avaliação dos riscos existentes - a alta direção terá condições de adequar as estratégias de negócio da organização;
- Por fim, mas não menos importante, a possibilidade de criar uma consciência de gestão de riscos dentro da organização, da qual todos devem fazer parte e que deve ser gerenciada por um Colegiado.

Referências

CAS (2003). Overview of Enterprise Risk Management – Casualty Actuarial Society, Enterprise Risk Management Committee. Maio 2003.

ISACA (2009) The Risk IT Framework. Ed.: ISACA.

COSO (2004). Enterprise Risk Management — Integrated Framework. Ed.: Committee of Sponsoring Organizations of the Treadway Commission.

Thomé, Andréa (2010): Curso sobre Governança e Gestão de Segurança da Informação, agosto de 2010. Ernst & Young.

COSO (2008). Internal Control – Integrated Framework - Guidance on Monitoring Internal Control Systems. Ed.: Committee of Sponsoring Organizations of the Treadway Commission.

Octave (2011). http://www.cert.org/octave/. Obtido em abril de 2011.

ISACA (2011).Risc IT based COBIT. http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx. Obtido em abril de 2011.

AS/NZS (2004).Handbook: Risk Management Guidelines Companion to AS/NZS 4360:2004. Ed: Standards Australia International Ltd.

ITGI (2007): - COBIT 4.1 - COBIT : IT Governance Institute (ITGI).

Atividades de Autoaprendizagem

1) Indique verdadeiro (V) ou falso (F) nos itens abaixo, tendo como base o conteúdo estudado nessa unidade:

( ) O RISK IT Framework foi criado com o objetivo de ajudar os gerentes relatar os riscos de TI, apesar de fazer referência somente aos ativos de TI e não aos processos de negócio.

( ) A premissa da existência do ERM é que toda a entidade (empresa, organização, ...) que existe é para prover valor para os seus *stakeholders* (investidores, sócios, ...).

( ) Um evento pode estar relacionado a um risco. Logo, risco pode ser definido como a possibilidade de um ativo estar sujeito a vulnerabilidades e incidentes.

( ) O risco é diretamente proporcional ao aumento da probabilidade explorar uma ameaça.

( ) Quanto mais se arrisca em uma empresa, maior é o seu risco de sofrer um evento adverso. Logo, deve-se arriscar no máximo até o risco considerável aceitável para a empresa.

Atividade colaborativa

1) Faça uma pesquisa sobre Operationally Critical, Threat, Asset and Vulnerability Evaluation SM – OCTAVE, descrevendo a sua filosofia e as principais características. Faça um breve comparação com CRAMM (CCTA Risk Analysis and Management Method), outra metodologia não abordada nesta unidade. Publique sua resposta na ferramenta Fórum. Verifique as postagens de seus colegas para aprimorar e somar os conhecimentos que você obteve nessa pesquisa. Aproveite também para comentar as postagens desses seus colegas.

2) Por que a análise de Maturidade de TI é importante para o processo de gestão de riscos? Publique sua resposta na ferramenta Exposição.

Síntese

Nesta Unidade, foram apresentados o processo de gestão de risco com base na NIST 800-30, além dos frameworks ERM e Risk IT. Como citado no início da unidade, existem outros métodos e ferramentas, como: ENISA, FAIR, MEHARI, CRAAM e OCTAVE, que podem complementar mais ainda o seu conhecimento. A questão não é conhecer várias metodologias, mas sim saber aplicar a melhor para cada situação. A escolha pode ser realizada com base no seu conhecimento e/ou no perfil da empresa, mas não se esqueça de ser simples e objetivo em suas análises e conclusões.

Saiba mais

Você pode aprofundar seus estudos sobre assuntos abordados nessa unidade em:

NIST SP 800-30 Risk Management Guide for Information Technology Systems.

The Risk IT Framework. Ed.: ISACA.

Integrated Framework - Guidance on Monitoring Internal Control Systems. Ed.: Committee of Sponsoring Organizations of the Treadway Commission.

Enterprise Risk Management — Integrated Framework. Ed.: Committee of Sponsoring.

Organizations of the Treadway Commission.

Unidade 3

Gestão de riscos de segurança da informação

Objetivos de Aprendizagem

- Conceituar o que é gestão de risco de segurança da informação.
- Realizar análises de risco.
- Tratar o risco.
- Realizar a verificação e manutenção constante do tratamento do risco.

Introdução

Armazenar ou disponibilizar informações de forma eficiente, isto é, segura e rápida, é um fator de sucesso para uma empresa. O alinhamento dos processos de negócio com a segurança da informação proporciona qualidade de serviço e retorno de investimento. Trabalhar com Tecnologia da Informação (TI) é sinônimo de risco, no qual a sua gestão é fator crucial para prover valores para a empresa. Assim, esta unidade irá abordar o processo de gestão de riscos de segurança da informação, em conformidade com a ISO 27005, a qual é de 2008.

Fundamentos de gestão de riscos de segurança da informação

Luiz Otávio Botelho Lento

Antes de iniciar a discussão sobre gestão de riscos de segurança da informação, existe a necessidade de se definirem **riscos de segurança da informação**. Segundo a ISO 27005, risco de segurança da informação consiste na possibilidade de uma determinada ameaça explorar vulnerabilidades de um **ativo** ou de um conjunto de ativos, desta maneira prejudicando a organização a que pertencem.

Ativo

Tudo aquilo que é importante para a empresa.

Importante

A gestão de riscos de segurança da informação é um processo dinâmico, interativo e contínuo, composto por medidas que, quando realizadas em sequência, permitem a melhoria contínua dos processos de decisão e da segurança da informação nas empresas.

A gestão de riscos de segurança da informação faz parte do processo de gestão de segurança da informação, contribuindo na implementação e no dia a dia do Sistema de Gestão de Segurança da Informação (SGSI).

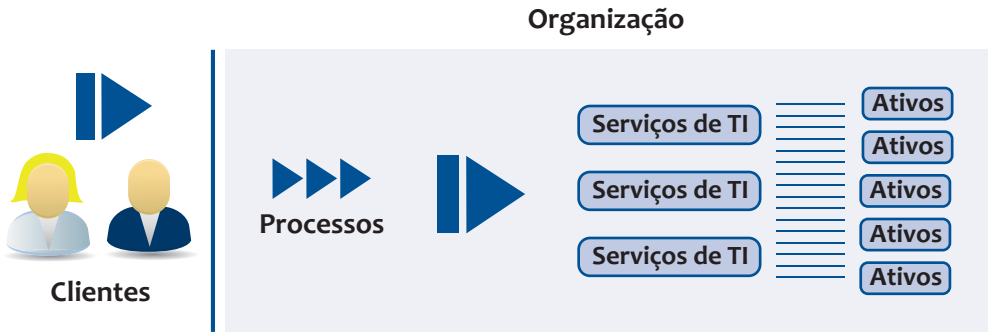
Por ser um processo contínuo, a gestão de riscos de segurança da informação está em constante desenvolvimento. É aplicada à estratégia da organização e à implementação desta. Deve analisar metodicamente todos os riscos inerentes às atividades passadas, presentes e, em especial, futuras de uma organização. Também deve ser integrada na cultura da organização com uma política eficaz, traduzindo a estratégia em objetivos táticos e operacionais, atribuindo responsabilidades na gestão dos riscos a toda organização, como parte integrante da respectiva descrição de funções. Desta forma, o gerenciamento de risco de segurança da informação possibilita que a organização mantenha a sua informação protegida e disponível em tempo hábil, de forma que os seus processos de negócio estejam ativos e a sua missão seja cumprida. Vale a pena ressaltar que um processo de negócio necessita de equipamentos e pessoas para que as informações processadas possam estar disponíveis aos seus clientes, conforme apresentado na figura 1.

Figura 1 – Processo

Fonte: Elaborado pelo autor, 2011.

Para que os processos de negócios possam ser executados, um ou mais serviços de TI devem ser executados. Por conseguinte, um ou mais ativos devem ser executados para garantir a execução desses serviços, conforme apresentado na figura 2. Isto significa que, protegendo os ativos de incidentes de segurança da informação, estará garantindo que os processos de negócio alcancem o seu objetivo.

Figura 2 – Granularidade de uma organização



Fonte: Elaborado pelo autor, 2011.

Desta forma, para prover uma melhor segurança aos componentes do seu sistema computacional (dispositivos de armazenamento, processamento ou transmissão de dados), existe a necessidade de se ter uma noção exata dos riscos que eventualmente ainda existam em seu negócio. (FERMA, 2002 e STONEBURNER, 2002).

Pode-se, então, de acordo com Ferma (2003), afirmar que a gestão de riscos protege e acrescenta valor à organização, pois:

- viabiliza uma estrutura na organização, permitindo que as atividades a serem desenvolvidas sejam executadas adequadamente e controladas;
- possibilita uma melhoria na tomada de decisões, no planejamento e na definição de prioridades, obtida via a interpretação do negócio da organização, dos resultados alcançados através de auditorias e das oportunidades/ameaças que o projeto possa vir a sofrer;

- contribui para uma utilização e distribuição mais eficiente do capital e dos recursos dentro da organização;
- protege e melhora os dispositivos do sistema computacional da organização; e,
- possibilita o desenvolvimento e apoio à base de conhecimentos das pessoas e da organização.

No entanto a gestão de riscos deverá analisar os possíveis eventos de ameaça à segurança da informação e as suas consequências, antes de definir qualquer decisão quanto a reduzir os riscos a um nível aceitável. Para isso, a gestão de riscos deverá (ISO/IEC 27005, 2008):

- identificar os riscos;
- analisar e avaliar os riscos com base nos impactos que irão causar aos processos de negócio e a probabilidade de ocorrerem;
- entender e comunicar a probabilidade e as consequências destes riscos;
- estabelecer a sequência de prioridades para o tratamento do risco;
- assegurar envolvimento das partes interessadas quanto às tomadas de decisão e à situação da gestão de riscos;
- garantir eficácia ao monitoramento do tratamento do risco;
- monitorar e analisar, de forma crítica e regular, os riscos e o seu processo de gestão;
- coletar as informações de forma a melhorar o processo de gestão de riscos;
- treinar a equipe responsável sobre os riscos existentes e as ações para mitigá-los.

Logo, a gestão de riscos de segurança da informação é um processo no qual as organizações analisam os riscos inerentes às suas atividades, com o objetivo de atingir um equilíbrio apropriado entre o reconhecimento de oportunidades e ganhos e a redução de perdas. É um elemento central na gestão da estratégia de qualquer organização.

Uma boa gestão de riscos de segurança da informação consiste na identificação e tratamento dos riscos, acrescentando uma maior sustentabilidade de todas as atividades executadas pela organização.

Processo de gestão de risco

O processo de gestão de riscos é interativo e contínuo, utiliza-se de um método lógico e sistemático para estabelecer o contexto, a análise, avaliação, tratamento, aceitação, comunicação, monitoramento e análise crítica dos riscos associados a qualquer atividade, função ou processo. Tal processo permite que as organizações minimizem suas perdas e maximizem os seus ganhos.

O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo; a uma área específica da organização (por exemplo: um departamento, uma localidade, um serviço); a um sistema de informações; a controles já existentes, planejados; ou, apenas a aspectos particulares de um controle (por exemplo: o plano de continuidade de negócios).

A norma ISO 27005 contém a descrição do processo de gestão de riscos de segurança da informação e das suas atividades. É esta norma que define a gestão de riscos como um processo interativo, composto por medidas que, quando realizadas em sequência, permitem a melhoria contínua nos processos de decisão e facilitam a melhoria contínua do desempenho. Por conseguinte, este processo deve executar um conjunto de tarefas que têm como objetivo identificar as necessidades de segurança de uma organização, proporcionando suporte à criação de um Sistema de Gestão de Informação (SGSI), preparação de um plano de continuidade de negócios ou de um plano de resposta a incidentes.

Importante

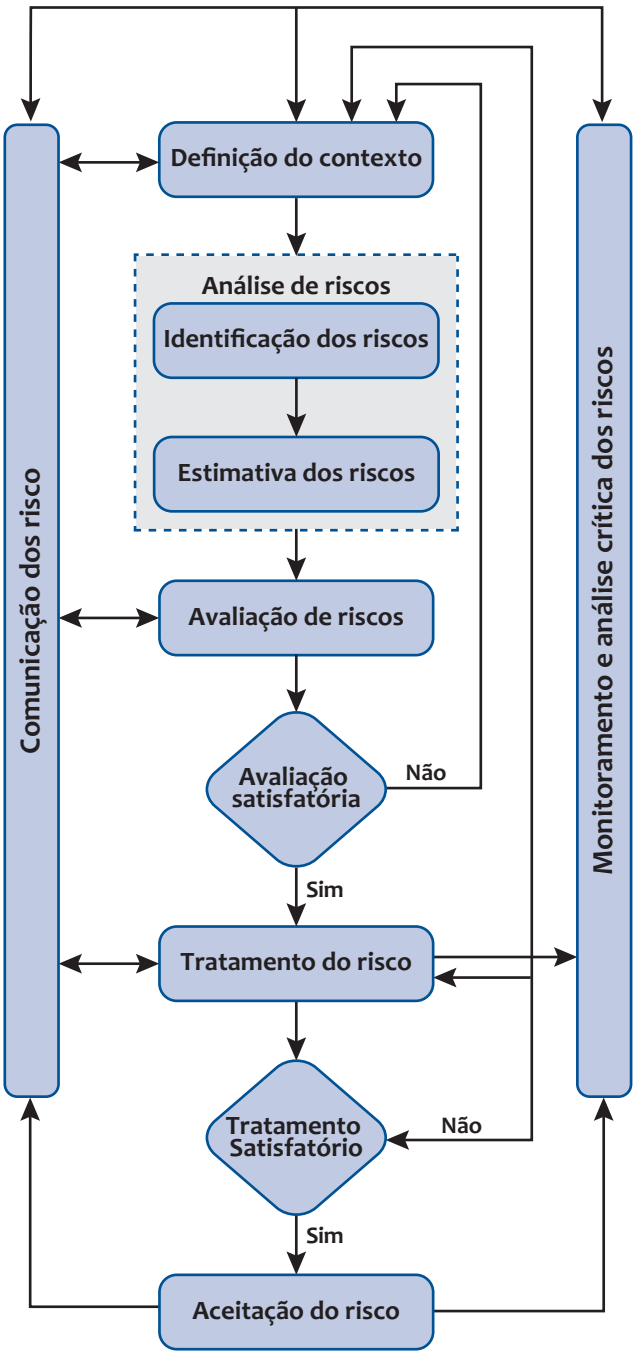
Deste modo, a gestão de riscos busca o equilíbrio adequado entre as oportunidades de ganhos e a minimização de perdas em uma organização, o que a torna uma parte integrante da boa prática de gestão e um elemento essencial da boa governança corporativa.

As etapas do processo de gestão de risco

O processo de gestão de riscos é interativo e contínuo, e se utiliza de um método lógico e sistemático para estabelecer o contexto, a análise, avaliação, tratamento, aceitação, comunicação, monitoramento e análise crítica dos riscos associados a qualquer atividade, função ou processo, permitindo que as organizações minimizem as perdas e maximizem os ganhos. Todas as abordagens e definições desta seção estão baseadas na norma ISO 27005, responsável pela padronização de todo o processo de risco.

A figura a seguir apresenta a relação entre as diversas etapas do processo de gestão de risco.

Figura 3 – Processo de Gestão de risco



Fonte: ISO 27005, 2008.

Conforme mostra-nos tal figura, o processo de gestão de riscos é dividido em 7 etapas. Acompanhe na sequência a definição de cada uma dessas etapas e o que compete à gestão de risco da segurança da informação realizar em cada uma delas.

Etapa 1 – Definição do contexto

Estabelecer o contexto da gestão de risco da segurança da informação consiste em definir os parâmetros básicos sob os quais os riscos sobre a informação devem ser geridos. Isto é, consiste em definir os critérios básicos (critérios de avaliação de riscos, critérios de impacto e critérios de aceitação do risco) a serem adotados pela gestão de riscos de segurança da informação.

Esse contexto define, portanto, o escopo (finalidade – plano de continuidade, SGSI, etc.) da gestão de riscos e os seus limites. Estes últimos, por sua vez, são determinados pelos objetivos estratégicos, políticos e processos de negócio da organização.

Por meio do estabelecimento do escopo dessa gestão de risco, estabelecem-se as responsabilidades apropriadas em relação à operação do processo de gestão de riscos. Estabelece-se quem serão os responsáveis por tal gestão dentro da organização.

A seguir, encontra-se a definição dos critérios básicos que se deve considerar para determinar o escopo da gestão de riscos para segurança da informação, os quais já foram citados aqui anteriormente.

Critérios para a avaliação de riscos

São desenvolvidos para avaliar os riscos de segurança da informação na organização. Consideram o valor estratégico para a organização do processo que trata das suas informações de negócio; a criticidade dos ativos de informação envolvidos; os requisitos legais e regulatórios e as obrigações contratuais; a importância dos negócios, da disponibilidade, da confidencialidade e da integridade; e expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado, a imagem e a reputação.

Os critérios de avaliação de riscos assumirão valores quantitativos: 5 crítico, 4 muito alto, etc.).

Exemplo

Critérios de avaliação do risco

Os níveis e os respectivos valores de risco sobre os ativos de informação variam em conformidade com o cliente.

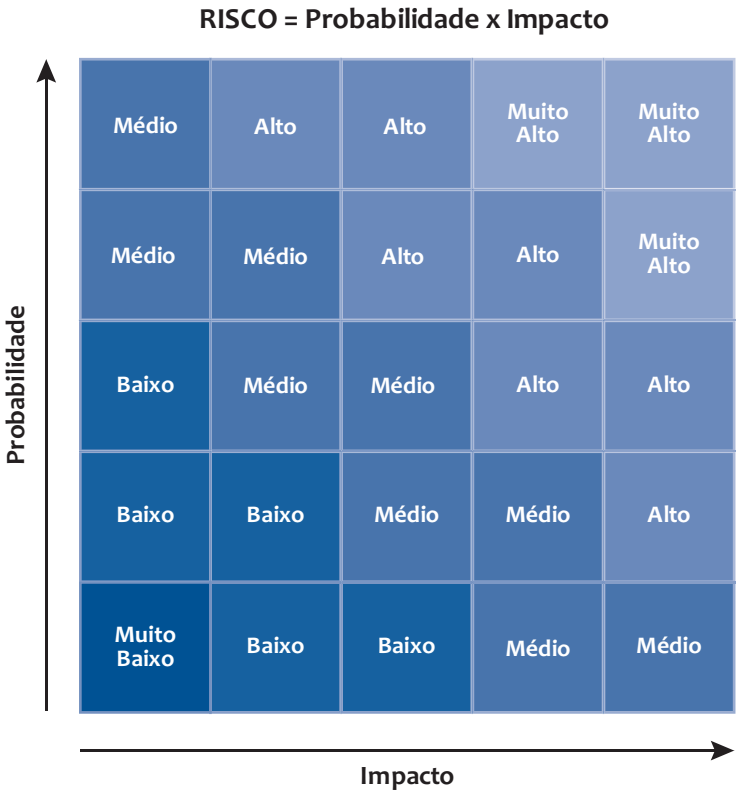
O cálculo do risco está baseado em uma função soma:

$$f_{risco} = \text{probabilidade} + \text{impacto}$$

Aqui foi selecionada uma escala de 1 a 10, dividida em 5 níveis, onde, para cada um desses níveis, atribuem-se valores. Assim, podem ser atribuídos os seguintes valores aos riscos:

Muito baixo – 1, 2
Baixo – 3,4
Médio – 5,6
Alto – 7,8
Muito Alto – 9,10

Figura 4 – Relação Probabilidade X Impacto



Fonte: Elaborado pelo autor, 2011.

Vale a pena ressaltar que outras escalas podem ser criadas, com seus respectivos valores, em conformidade com a função escolhida.

Critérios de impacto

Outros critérios básicos de acordo com os quais deve-se determinar o escopo da gestão de riscos da segurança da informação são os relacionados ao impacto da concretização da ameaça sobre os ativos de informação. São desenvolvidos e especificados em função do montante dos danos ou custos à organização causados por um evento relacionado com a segurança da informação.

Já o nível de danos que a efetividade de uma ameaça à informação pode trazer consigo é determinado através do levantamento dos seguintes itens: o nível de classificação do ativo de informação afetado; as ocorrências de violação da segurança da informação; perda de oportunidades de negócio e de valor financeiro por meio desse ataque; não cumprimento de prazos; danos à reputação e violações de requisitos legais ou contratuais. Os critérios de impacto assumirão valores quantitativos (5 crítico, 4 muito alto, etc.).

Determinação do critério de impacto

Ao se determinar o impacto da concretização de uma ameaça à informação, são levados em consideração os seus malefícios em relação a aspectos estratégicos e operacionais da empresa. Tais malefícios podem, portanto, trazer à empresa: interrupção dos serviços; perda de confiança pelo cliente; interrupção de operação interna; interrupção de operação de terceiros; violação de cláusulas contratuais; perda financeira; perda de clientes; perda de reputação; enfraquecimento da capacidade de negociação; rejeição ao produto; dano material e perda de eficácia.

Segundo a norma ISO 27005:2008, o impacto imediato (operacional) da concretização de uma ameaça a um ativo de informação pode ser direto ou indireto.

Direto:

a. o valor financeiro de reposição do ativo perdido (ou parte dele);

b. o custo de aquisição, configuração e instalação do novo ativo ou do “back-up”;

c. o custo das operações suspensas devido ao incidente até que o serviço prestado pelos ativos afetados seja restaurado;

d. consequências resultantes de violações da segurança da informação.

Indireto:

a. custo de oportunidade (recursos financeiros necessários para repor ou reparar um ativo poderiam estar sendo utilizados para outro fim);

b. o custo das operações interrompidas;

c. mau uso das informações obtidas através da violação da segurança;

d. violação de obrigações estatutárias ou regulatórias;

e. violação dos códigos éticos de conduta.

Assim, o quadro que se segue apresenta um exemplo de níveis desse impacto com os seus respectivos indicadores. Vale a pena ressaltar que vários outros indicadores, em conformidade com o cliente, podem ser estabelecidos aqui.

Quadro 1 – Critério de impacto

Nível de impacto	Aspectos afetados e nível de preocupação da empresa
Muito Alto (5)	O impacto financeiro sobre a organização ultrapassa um determinado valor. O impacto é muito significativo sobre a estratégia (por exemplo, informações sobre projetos) ou sobre as atividades operacionais da organização (acesso ao ambiente computacional). Muita preocupação das partes interessadas.
Alto (4)	O impacto financeiro sobre a organização ultrapassa um determinado valor. O impacto é significativo sobre a estratégia (por exemplo, aspectos financeiros) ou sobre as atividades operacionais da organização (atraso na entrega de serviços, controle de senhas, etc.). Grande preocupação das partes interessadas.
Médio (3)	O impacto financeiro sobre a organização deve estar entre dois valores. O impacto é moderado sobre a estratégia (por exemplo, desvio de produtos) ou atividades operacionais da organização (disponibilidade de informações no ambiente computacional). Preocupação moderada das partes interessadas.
Baixo (2)	O impacto financeiro sobre a organização deve ser inferior a um valor. Impacto baixo sobre a estratégia (por exemplo, demanda retraída de serviços) ou atividades operacionais da organização (contato com terceiros, etc.). Pouca preocupação das partes interessadas.
Muito Baixo (1)	O impacto financeiro sobre a organização deve ser inferior a um valor. Impacto baixo sobre a estratégia ou atividades operacionais da organização. Nenhuma preocupação das partes interessadas.

Fonte: Adaptado de ISO 27005.

Critérios para determinação de probabilidade de ameaças

Esses critérios são desenvolvidos e especificados em função das possíveis ameaças que a organização poderá sofrer. Os critérios de probabilidade de ameaças assumirão valores quantitativos (5 crítico, 4 muito alto, etc.). Esses valores quantitativos são determinados, usando-se como base o quadro anteriormente apresentado aqui.

Importante

A probabilidade é a chance de a ameaça vir a se concretizar.

O critério para determinação da probabilidade de uma ameaça está baseado em indicadores. Abaixo é apresentado um quadro com níveis de probabilidades de uma ameaça, em que se descreve cada nível de ameaça e apresentam-se os seus respectivos indicadores. Estes níveis de probabilidade podem ser alterados, bem como os indicadores, em conformidade com o cliente. Trata-se de um exemplo.

Quadro 2 – Probabilidade de ocorrência de ameaças

Estimativa	Descrição	Indicadores
Muito alta (Muito provável, 5)	Pode ocorrer todos os anos, com possibilidade igual ou superior a 50%.	Já ocorreu algumas vezes dentro de um período de tempo, e tem grande chance de ocorrer várias vezes no próximo período de tempo, com igual extensão. Não existe controle aplicado.
Alta (Provável, 4)	Pode ocorrer todos os anos, com possibilidade superior a 25% e menor que 50%.	Grande chance de ocorrer várias vezes dentro de um período de tempo, no caso, 01 ano. Ocorreu recentemente. O controle não é eficaz ou está inadequadamente aplicado.
Média (Possível, 3)	Pode ocorrer a cada 2 anos, ou com possibilidade inferior a 25%.	Pode ocorrer mais do que uma vez dentro do período de tempo de 2 anos. Pode ser difícil de controlar devido a algumas influências externas. Existe um histórico de ocorrências? Existe controle, aplicado de forma adequada, mostra-se eficaz, mas não se mantém atualizado.
Baixa (Remota, 2)	Não existe a possibilidade de ocorrer dentro de 2 anos, com possibilidade inferior a 5%.	Não ocorreu, mas é possível que ocorra. Existe controle, o mesmo é eficaz, mas pode ser burlado.
Muito Baixa (Muito remota, 1)	Não existe a possibilidade de ocorrer dentro de 4 anos, ou com possibilidade inferior a 2%.	Não ocorreu, e é improvável que ocorra. O controle é plenamente eficaz.

Fonte: Adaptado de ISO 27005.

Critérios para aceitação de riscos

São desenvolvidos e especificados em concordância com as políticas, metas e objetivos da organização, e com os interesses das partes interessadas. Os critérios para a aceitação do risco podem incluir mais de um limite, representando um nível desejável de risco, mas precauções podem ser tomadas por gestores seniores para aceitar riscos acima desse nível, desde que sob circunstâncias definidas. Diferentes critérios para a aceitação do risco podem ser aplicados a diferentes classes de risco, como aqueles que podem resultar em não conformidade com regulamentações ou leis e podem não ser aceitos, e riscos de alto impacto, que poderão ser aceitos, se isto for especificado como um requisito contratual. Estes critérios poderão assumir um valor ou uma série de valores quantitativos.

Ao final desses procedimentos, possuímos a etapa 1 do processo de gestão de risco cumprida. Retome a figura 1 apresentada aqui e você verificará que a próxima etapa nesse processo é a Análise de riscos.

Etapa 2 – Análise de riscos

A análise de riscos consiste no desenvolvimento e entendimento do risco, fornecendo informações necessárias às tomadas de decisões sobre o tratamento, ou não, dos riscos. Tal análise leva em consideração as origens do risco, as suas consequências (impacto) positivas e negativas e as probabilidades de os riscos ocorrerem.

Importante

O risco é analisado através da combinação do seu impacto na organização e a sua probabilidade de ocorrer.

A análise de um risco é dividida em duas atividades: a identificação e a estimativa do risco. Esta identificação tem o propósito de determinar eventos que possam causar uma perda potencial à empresa e deixar claro como, onde e por que tal perda pode acontecer. Já a estimativa de riscos pode adotar uma metodologia qualitativa, quantitativa ou uma combinação de ambas.

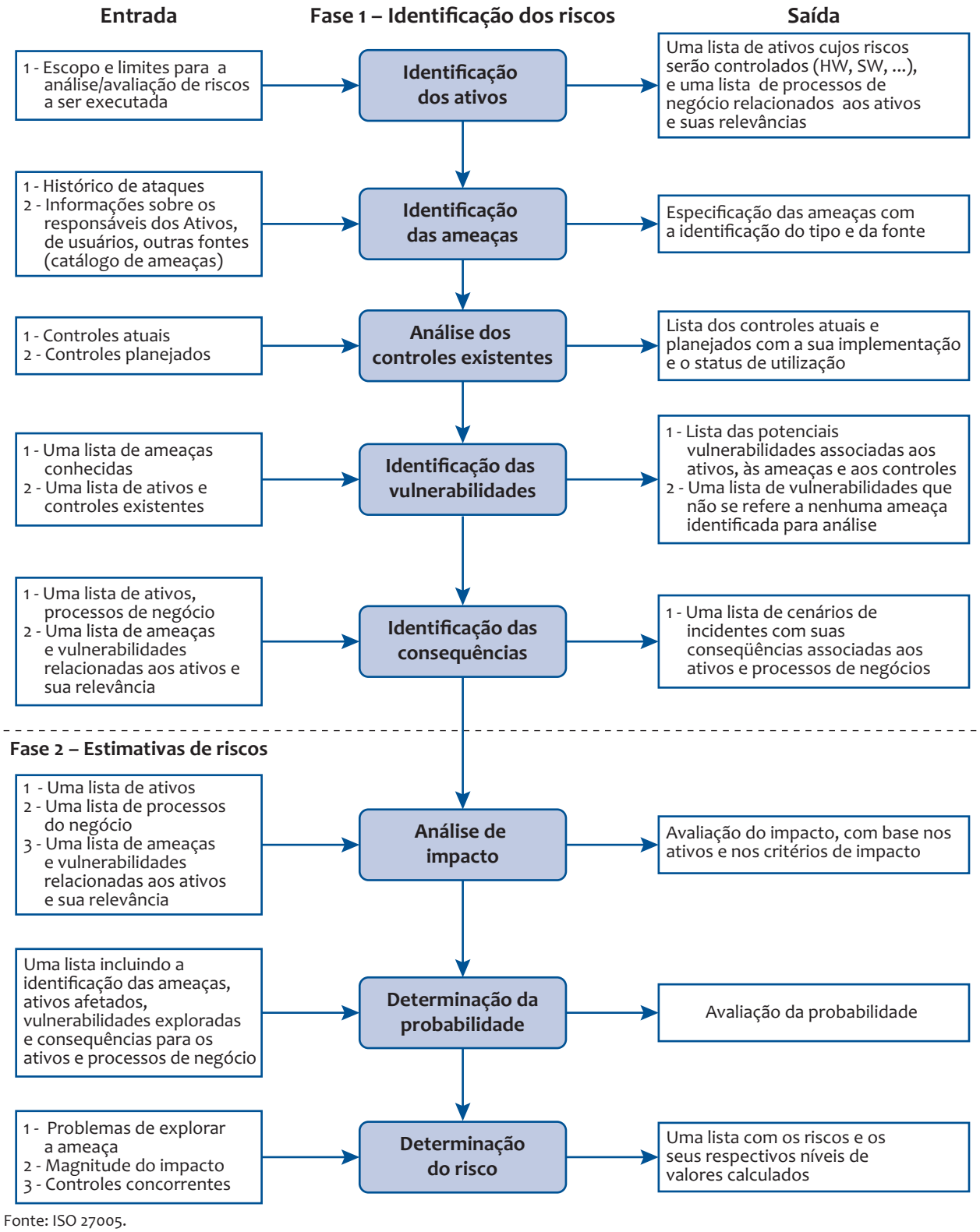
Normalmente, utiliza-se a estimativa qualitativa de risco para obter uma indicação geral do nível de risco e para revelar os grandes riscos. Depois, poderá ser utilizada uma análise quantitativa sobre os grandes riscos detectados pela qualitativa. Vale a pena ressaltar que a forma da análise dessa estimativa deve ser coerente com o critério de avaliação de riscos desenvolvida na etapa de definição do contexto de risco (etapa 1 do processo de gestão de risco, ver figura 1) .

A estimativa qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo: Pequena, Média e Grande) do risco e a probabilidade dessas consequências ocorrerem.
A estimativa quantitativa utiliza uma escala com valores numéricos (e não as escalas descritivas usadas na estimativa qualitativa) tanto para consequências quanto para as probabilidades dos riscos ocorrerem, usando dados de diversas fontes.

A qualidade da análise depende da exatidão e da integralidade dos valores numéricos e da validade dos modelos de cálculo utilizados. A estimativa quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e aos interesses da organização.

A seguir, encontram-se as etapas do processo de análise de riscos.

Figura 5 – Análise de risco



Fonte: ISO 27005.

Conforme mostra essa figura, a análise de risco é realizada por meio de um processo dividido em duas fases, e essas, por sua vez, estão divididas em etapas. Na sequência, essas fases e etapas são abordadas.

Fase I da Análise de risco: Identificação dos riscos

Conforme mostra-nos a última figura, a fase de identificação dos riscos é composta das seguintes etapas: identificação dos riscos; identificação das ameaças; análise dos controles existentes; identificação das vulnerabilidades e identificação das consequências. Na sequência, encontra-se detalhada cada uma dessas etapas.

Identificação dos ativos

Segundo a norma ISO 27005, os ativos são classificados em dois tipos: ativos primários e ativos de suporte e infraestrutura.

1. Ativos primários

   a. Processos e atividades do negócio

      - Processos que não podem ser interrompidos parcial ou totalmente, pois afetarão o negócio da organização.
      - Processos que envolvam procedimentos sigilosos ou tecnologia proprietária.
      - Processos que, se modificados, podem afetar consideravelmente o negócio da organização.
      - Processos necessários para que a organização fique em conformidade com os requisitos contratuais, legais ou regimentais.

   b. Informação

      - Informação vital para o cumprimento das atividades do negócio da organização ou para o desempenho.
      - Informação de caráter pessoal, da forma em que é definida nas leis nacionais com referência à privacidade.
      - Informação estratégica necessária para alcançar os objetivos estratégicos definidos pela alta direção.
      - Informação de alto custo, cuja coleta, armazenamento, processamento e transmissão demandam um longo tempo ou incorrem em um alto custo de aquisição.

2. Ativos de suporte e infraestrutura (sobre os quais os elementos primários do escopo se apoiam): hardware, software, rede, recursos humanos, instalações físicas, etc.

Os ativos primários são compostos pelos principais processos de negócio e as informações mais críticas da organização. Isto limita a análise de riscos a um escopo dos principais componentes do negócio da empresa.

O quadro apresentado na sequência, o qual pode ser elaborado na sua organização por meio de planilha do Excel, serve como sugestão para mapear os ativos da organização. Esse quadro é composto por cinco campos: o ativo primário (processo ou atividade de negócio); a gerência responsável pelo ativo; o setor da gerência que executa o processo; os serviços de TI que são responsáveis pela execução do ativo primário; por fim, todos os ativos de infraestrutura e suporte responsáveis pela execução dos serviços de TI.

Quadro 3 – Exemplo de identificação dos ativos

Ativo Primário	Gerência	Setor	Serviço TI	Ativo de suporte e infraestrutura
Processo de manutenção de sistemas	TI	Suporte	Banco de Dados	Servidor
				Rede Local

Fonte: Elaborado pelo autor, 2011.

Terminada a etapa de Identificação dos ativos, necessário seguirmos para a identificação das ameaças.

Identificação das ameaças

A seguir é apresentado um quadro com as possíveis ameaças sobre a informação, que a organização poderá sofrer. Encontra-se aí um pequeno conjunto do universo amplo de ameaças a que uma organização está exposta.

Quadro 4 – Exemplo de classificação de ameaça por meio de suas origens

Tipo	Ameaças	Origem
Dano físico	1. Fogo	A, I, N*
	2. Água	A, I, N
	3. Poluição	A, I, N
	4. Acidente grave	A, I, N
	5. Destruição de equipamento ou mídia	A, I, N
	6. Poeira, corrosão, congelamento	A, I, N
	7. Falha no fornecimento de energia	A, I
	8. Falha no uninterruptible power supply (UPS)	A, I
	9. Flutuações de energia	A, I
Eventos naturais	10. Fenômeno climático	N
	11. Fenômeno meteorológico	N
	12. Fenômeno sísmico	N
	13. Inundação	N

Tipo	Ameaças	Origem
Paralisação de serviços essenciais	14. Falha do ar condicionado ou do sistema de suprimento de água	A, I
	15. Interrupção do suprimento de energia	A, I, N
	16. Falha do equipamento de telecomunicação (satélite)	A, I
	17. Falha no serviço de comunicação	A, I
Comprometimento da informação	18. Interceptação de sinais de interferência comprometedores	I
	19. Espionagem à distância	I
	20. Escuta não autorizada	I
	21. Furto de mídia ou documentos	I
	22. Furto de equipamentos	I
	23. Recuperação de mídia reciclada ou descartada	I
	24. Divulgação indevida	A, I
	25. Dados de fontes não confiáveis	A, I
	26. Alteração do hardware	I
	27. Alteração do software	A, I
	28. Backup indisponível	A, I
	29. Deterioração das mídias	A, N, I
	30. Validação difícil	A, I
	31. Controle pobre de metodologia de codificação	A, I
	32. Determinação da localização	I
Falhas técnicas	33. Falha de equipamentos de rede/ servidores/estações de trabalho	A
	34. Defeito/degradação de equipamentos de rede / servidores / estações de trabalho	A
	35. Saturação do sistema de informação	A, I
	36. Falha/corrupção de software	A, I
	37. Corrupção de dados	A, I
	38. Corrupção de mídia	A, I
	39. Falha ao gerar backups	A, I
	40. Falha dos dados de segurança	A,I
	41. Desempenho não esperado	A,I
	42. Violação das condições de uso do sistema de informação que possibilitam sua manutenção	A, I
	43. Perda de disponibilidade	A, I
	44. Erros de transmissão	A, I
	45. Negação de serviço	A,I
	46. Degradação do tempo de resposta	A, I
	47. Degradação da disponibilidade	A, I
	48. Capacidade de TI / comunicações inadequadas	A, I
	49. Interrupção de serviço durante a instalação / atualização de equipamentos de trabalho remoto	I
	50. Sobrecarga de tráfego	I, A
	51. Registros inadequados de alterações / modificações	I
	52. Desconhecimento do usuário	A
	53. Cópia não controlada de documentos	A, I
	54. Erro de manutenção	I, A
	55. Erro de construção predial	A, I

*__A__ – acidental; __I__ – intencional; __N__ – natural.

Fonte: Fonte: ISO 27005.

Conforme podemos observar, este quadro é composto por três campos: o campo tipo, que visa estabelecer as classes de ameaças; o campo ameaças, que estabelece um nome para cada uma delas; e o campo origem, que cita se a ameaça é acidental, intencional ou natural.

Seguimos agora para a próxima etapa da fase de identificação dos riscos, que pertence à Análise de riscos.

Análise dos controles existentes

O anexo A da norma ISO 27001, 2005 apresenta uma lista de controles da informação que podem ser aplicados.

O quadro 5, apresentado a seguir, é composto por seis campos, os quais servem para identificar a qualidade dos controles da informação. Neste quadro: o campo 'nome' dá o nome do controle; o campo 'controle' apresenta uma breve descrição do controle; o campo 'aplicado' afirma se o controle é aplicável, ou não, à organização; o campo 'implantado' afirma se o controle está implantado, ou não, na organização, caso ele seja aplicável; o campo 'eficaz' afirma que o controle implantado é, ou não, eficaz dentro da Organização; por fim, o campo 'va,' atribui valores de 0 a 5, conforme os campos – aplicado, implantado e eficaz. Quanto mais baixo o valor obtido no campo "val" mais eficaz é o controle. Como obter os valores desse campo? Através dos outros campos, por meio das seguintes convenções:

Aplicado, implantado e eficaz – **val = 1, 2 ou 3**.

Os valores 1, 2 e 3 são estabelecidos conforme o nível de eficácia do controle. Quanto mais baixo o valor, mais eficaz é o controle.

Aplicado, implantado e não eficaz – **val = 4**.

Aplicado e não implantado – **val = 5**.

Vale a pena ressaltar que os valores podem ser reestruturados junto ao cliente. Também vale a pena ressaltar que foram apresentados cinco controles como exemplo de um universo de mais de 100 controles.

Quadro 5 – Análise dos controles existentes

Nome	Controle	Aplicado		Implantado		Eficaz		Val
		S	N	S	N	S	N	
Documento da política de segurança da informação	Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.	S		S		S		3
Análise crítica da política de segurança da informação	A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.	N		N				5
Comprometi-mento da direção com a segurança da informação	A Direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.	N		N				5
Coordenação da segurança da informação	As atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.	N		N				5
Atribuição de responsabilidades para a segurança da informação	Todas as responsabilidades pela segurança da informação devem estar claramente definidas.	S		S			N	4

Fonte: Elaboração do autor, 2011.

Lembrando: Quanto mais baixo o valor obtido em "Val", mais eficaz é o controle considerado.

Aqui vale a pena ressaltar que esses valores podem ser reestruturados junto ao cliente e que foram apresentados cinco controles como exemplo de um universo de mais de 100 controles.

Agora vamos à penúltima etapa da fase identificação de risco, que pertence à Análise de risco.

Identificação das vulnerabilidades

Nesta fase, são determinadas as vulnerabilidades que podem ser exploradas pelas diversas ameaças que a organização possa vir a sofrer. O quadro 6 apresenta uma classificação dessas vulnerabilidades – física ambiental e infraestrutura – a que está exposta a informação. Essa classificação usa de três campos: o campo 'vulnerabilidade' dá nome a mesma; o campo 'ameaça' cita as possíveis ameaças relacionadas àquela vulnerabilidade; o campo 'controle' apresenta os diversos controles que podem ser aplicados a cada uma das ameaças.

Quadro 6 – Análise dos controles existentes por meio dos tipos de vulnerabilidades a que estão expostas as informações

Vulnerabilidade	Ameaça	Controle
Proteção física inadequada (prédio, sala e CPD)	- Fenômeno climático - Fenômeno meteorológico -Escuta não autorizada - Furto de mídia ou documentos - Furto de equipamentos - Bomba/Terrorismo - Falha no fornecimento de energia	- Política de controle de acesso - Perímetro de segurança física - Controles de entrada física - Instalação e proteção do equipamento - Segurança do cabeamento Incluindo segurança da informação no processo de gestão da continuidade de negócio - Continuidade de negócios e análise/avaliação de risco
Controle de acesso físico inadequado	- Escuta não autorizada - Furto de mídia ou documentos - Furto de equipamentos - Bomba/Terrorismo - Spoofing (fazer-se passar por outro) - Acesso não autorizado ao prédio - Fogo - Falha do ar condicionado ou do sistema de suprimento de água - Falha no fornecimento de energia - Falha no uninterruptible power supply (UPS) - Flutuações de energia - Danos aos links de comunicação	- Política de controle de acesso - Perímetro de segurança física - Controles de entrada física - Instalação e proteção do Equipamento - Segurança do cabeamento - Incluindo segurança da informação no processo de gestão da continuidade de negócio - Continuidade de negócios e análise/avaliação de risco - Acesso do público, áreas de entrega e de carregamento
Rede elétrica instável	- Falha no fornecimento de energia - Flutuações de energia - Falha de equipamento - Defeito/degradação de equipamento - Falha/corrupção de software - Falha de equipamentos de rede/ servidores/estações de trabalho - Corrupção de dados	- Manutenção dos equipamentos - Segurança do cabeamento - Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

Vulnerabilidade	Ameaça	Controle
Ar condicionado	- Falha do ar condicionado ou do sistema de suprimento de água - Corrupção de mídia	- Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação
Desastre natural	- Fenômeno climático - Fenômeno meteorológico - Fogo - Falha do ar condicionado ou do sistema de suprimento de água - Falha no fornecimento de energia - Falha de equipamentos de rede/ servidores/estações de trabalho - Defeito/degradação de equipamentos de rede / servidores / estações de trabalho - Perda de disponibilidade - Degradação do tempo de resposta - Backup indisponível	- Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação - Instalação e proteção do Equipamento

Fonte: Adaptada da ISO 27005 pelo autor, 2011.

Vamos, agora, para a última etapa da fase de Identificação dos riscos.

Identificação das consequências

Nesta etapa, são verificadas as consequências ou prejuízos que a perda das propriedades de segurança da informação (confidencialidade, integridade e disponibilidade) podem trazer para o negócio da organização. Por exemplo, perda da imagem, perda de oportunidades de negócio, entre outras.

Para avaliar estas consequências, deve-se analisar o **cenário de incidente**, que consiste na descrição de como a ameaça explorou uma determinada ameaça durante um incidente de segurança. As consequências, por exemplo, operacionais, provenientes de um cenário de incidente, devem levar em consideração questões como: investigação e tempo de reparo; oportunidade de negócio perdida; custo financeiro para reparar o prejuízo; imagem, reputação e valor de mercado.

Vale a pena ressaltar que o impacto causado pelos cenários de incidentes é determinado com base nos critérios de impacto definidos na fase de definição de contexto, levando em consideração os problemas que ele pode causar em um ou mais ativos.

Valoração dos Ativos

Identificado o ativo, devem-se estabelecer os seus respectivos valores. Para isso deve ser adotada uma escala quantitativa ou qualitativa de valores e critérios para pontuar a importância dos ativos. Dentre os critérios a serem adotados no estabelecimento do valor de um ativo, pode-se destacar o custo original e o custo de sua substituição ou de sua reengenharia. Além desses critérios, também podem ser adotados critérios mais abstratos como seu peso no valor da imagem de uma organização.

Um aspecto importante a ser considerado na valorização dos ativos são os custos decorrentes das perdas das propriedades de segurança (confidencialidade, integridade, disponibilidade, autenticidade e não repúdio). A ISO 27005 apresenta um conjunto de critérios que podem ser utilizados para se estimarem as possíveis consequências resultantes da perda das propriedades de segurança:

- violação da legislação e/ou das regulamentações;
- redução do desempenho do negócio;
- perda de valor de mercado/efeito negativo sobre a imagem e a reputação;
- violação de segurança relacionada a informações pessoais;
- o perigo ocasionado à segurança física das pessoas;
- efeitos negativos relacionados à execução da lei;
- violação de confidencialidade;
- violação da ordem pública;
- perda financeira;
- interrupção de atividades do negócio;
- o perigo ocasionado à segurança ambienta;

Além destes fatores citados, são apresentados mais alguns aspectos que também podem ser levados em consideração na determinação das consequências da exploração dos ativos:

- interrupção dos serviços – incapacidade de prestar os serviços;
- perda da confiança do cliente – perda da credibilidade no sistema interno de informação;
- dano à reputação;
- interrupção de operação interna – descontinuidade dentro da própria organização;

- custo interno adicional;
- interrupção da operação de terceiros – descontinuidade das transações entre a organização e terceiros;
- infração de leis / regulamentações – incapacidade de cumprir obrigações legais;
- violação de cláusulas contratuais – incapacidade de cumprir obrigações contratuais;
- perigo ocasionado à segurança física dos recursos humanos/usuários;
- ataque à vida privada de usuários;
- perda financeira;
- custos financeiros para emergências, reposição e consertos (recursos humanos, equipamentos, etc.).

Importante

Quanto mais relevantes e numerosos os processos de negócio apoiados por um ativo, maior é o seu valor.

Deve-se identificar, também, a dependência de ativos a processos de negócio e a outros ativos, pois esta dependência poderá influenciar os valores dos ativos (garantir a confidencialidade dos dados durante todo o seu ciclo de vida, inclusive durante o seu armazenamento e processamento).

É interessante que, no estabelecimento dos valores dos ativos – onde outros ativos são dependentes dos primeiros desses –, levem-se em consideração os seguintes aspectos:

- se os valores dos ativos dependentes (dados) forem menores ou iguais ao valor do ativo em questão (software), o valor deste último permanece o mesmo;
- se os valores dos ativos dependentes (dados) forem maiores do que o valor do ativo em questão (o software), o valor deste último ativo deve aumentar de acordo com o grau de sua dependência em relação aos outros ativos e os valores destes últimos.

Quadro 7 – Consequências

Cenário de Incidente	Ativo afetado	Consequências	Valor do ativo
Estabilizador inativo	Servidor de POP inativo	Não recebe email	Alto

Fonte: Elaborado pelo autor, 2011.

Fase II da Análise de risco: Estimativa dos riscos

a. Análise de impacto

O impacto está diretamente relacionado com um incidente de segurança da informação. Isto é, relacionado ao quanto a ineficiência do ativo ou parte dele (consequência do incidente de segurança) irá impactar no negócio da organização. **Desta forma, pode-se afirmar que o impacto está atrelado diretamente à medida do sucesso do incidente.** O impacto está relacionado aos aspectos operacionais, impacto imediato, ou às consequências que o negócio da organização irá sofrer no futuro, como perda de sua imagem ou a redução de seu mercado.

A ISO 27005 classifica o impacto imediato como direto ou indireto. O impacto direto está relacionado a aspectos como: o valor financeiro de reposição do ativo perdido (ou parte dele), o custo de aquisição, configuração e instalação do novo ativo ou do "back-up", o custo das operações suspensas devido ao incidente, até que o serviço prestado pelos ativos afetados seja restaurado e, assim, as consequências resultantes de violações da segurança da informação. No entanto o impacto imediato, classificado como indireto, está relacionado ao custo de oportunidade (recursos financeiros necessários para repor ou reparar um ativo poderiam estar sendo utilizados para outro fim); custo das operações interrompidas, mau uso das informações obtidas através da violação da segurança, violação de obrigações estatutárias ou regulatórias e violação dos códigos éticos de conduta.

Na análise de impacto, deve ser levada em consideração a importância do processo de negócio para a Organização, junto com o/os serviço(s) relacionado(s) ao processo e os ativos responsáveis para a execução dos serviços de TI.

O quadro a seguir apresenta um exemplo de como se pode calcular o impacto para cada ativo, levando em consideração o valor do processo, serviço, o valor do ativo para a realização do serviço e, por fim, o impacto deste em relação ao negócio da organização.

Quadro 8 – Cálculo de impacto da agressão a um ativo

Processo/Valor	Serviços TI/Valor	Ativo Infra/Sup	Valor	Impacto
Aquisição – Alto	Serviço de email – Alto	Servidor POP	Alto	Alto

Fonte: Elaborado pelo autor, 2011.

b. Determinação das probabilidades

Identificados os cenários de incidentes, deve-se determinar a probabilidade destes ocorrerem, com base em estimativas quantitativas ou qualitativas. Para tal, são consideradas a frequência da ocorrência das ameaças e a facilidade de se explorarem as vulnerabilidades. Entretanto, para saber esses parâmetros, deve-se ter conhecimento da:

- experiência passada e estatísticas aplicáveis referentes à probabilidade da ameaça;
- as fontes de ameaças intencionais (a motivação, os recursos disponíveis para os atacantes, a percepção da vulnerabilidade e os valores dos ativos para o atacante); e,
- os controles existentes e a eficácia com que eles reduzem as vulnerabilidades.

Contudo, conforme a necessidade de se ter informações mais precisas, os ativos podem ser ou agrupados ou podem ser tratados em separado, relacionados aos seus componentes e os respectivos cenários. O resultado final do valor da probabilidade pode variar em conformidade com a localidade geográfica, a natureza das ameaças a um mesmo tipo de ativo ou em relação à eficácia dos controles existentes.

O quadro abaixo é um exemplo do cálculo de probabilidade, no qual o valor numérico da determinação da probabilidade de uma ameaça pode ser calculado pela média aritmética dos valores para cada ameaça do ativo.

Quadro 9 – Probabilidade da ameaça

Ativo Infra/Sup	Incidente Histórico		Vulnerabilidade	Ameaça	Controle		Prob
	S	N					
Notas fiscais lançadas	5		Controle de recrutamento inadequado	Visão, cópia ou remoção de documentos arquivados	Termos e condições de contratação	5	5
		N	Falta de mecanismos de monitoramento	Manipulação de dados	Registros (log) de administrador e operador	3	3
	5		Arquivos de dados, logs e outros em HDs	Perda de confidencialidade	Reutilização e alienação segura de equipamentos	5	5

Fonte: Elaborado pelo autor, 2011.

c. Estimativa do risco

O cálculo da estimativa do risco é baseado na probabilidade de um cenário ocorrer e o seu impacto sobre o negócio. No quadro a seguir, há uma demonstração de cálculo a ser utilizado para obtenção de tal estimativa. Conforme você pode observar, neste cálculo foi utilizada uma função representada pela soma da probabilidade de cada ameaça sofrida por cada ativo e o seu impacto para o negócio da Organização.

Quadro 10 – Risco = Probabilidade + Impacto

Ativo	Probabilidade Cenário		Impacto	Risco
Notas fiscais lançadas	Visão, cópia ou remoção de documentos arquivados	5	4	9
	Manipulação de dados	3		7
	Perda de confidencialidade	5		9

Fonte: Elaborado pelo autor, 2011.

Depois de verificada a etapa 2 do processo de gestão de risco, Análise de risco, essa última bastante complexa – cheia de subdivisões –, passamos à Avaliação de risco. Essa avaliação é a terceira etapa de um processo de gestão de risco.

Etapa 3 – Avaliação de riscos

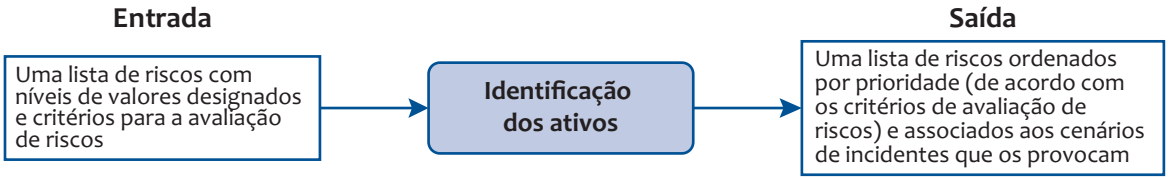
O objetivo da avaliação do risco é tomar decisões baseadas sobre a análise de risco, de modo a determinar quais riscos necessitam de tratamento e quais são as prioridades neste tratamento. Este processo envolve a comparação entre o nível de risco obtido durante a análise de risco e o critério de risco quando o contexto foi considerado.

A ISO 27005 cita que, durante a realização desta etapa, alguns elementos devem ser considerados. Analise.

- Se um critério de risco não for relevante para a organização (por exemplo: a perda da confidencialidade), todos os riscos que provocam esse tipo de impacto podem ser considerados irrelevantes.
- Se o processo tiver sido julgado de baixa importância, os riscos associados devem ser menos considerados do que os riscos que causam impactos em processos ou atividades mais importantes A avaliação de riscos usa o entendimento do risco obtido através da análise de riscos, para a tomada de decisões sobre ações futuras.

Durante a etapa de avaliação de riscos, além dos riscos estimados, convém que requisitos contratuais, legais e regulatórios também sejam considerados.

Figura 6 – Avaliação de risco



Fonte: ISO 27005.

Quadro 11 – Ativos a serem tratados

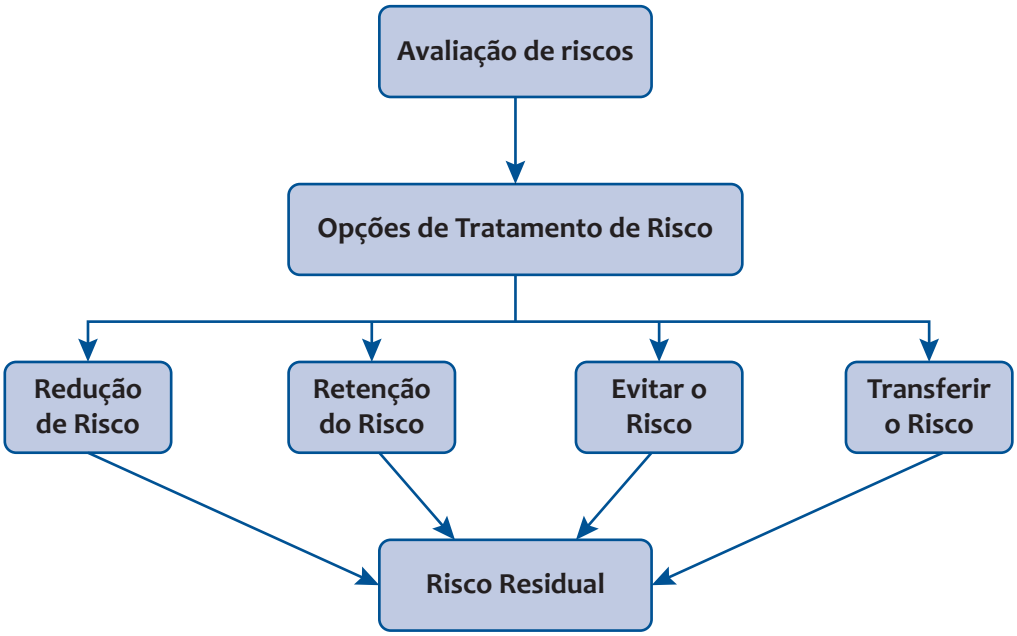
Ativo	Risco	Prioridade	Tratar	
			Sim	Não
Notas fiscais lançadas	Corrupção de dados	1	X	
	Eliminação de dados	2	X	
	Furto de Informação	3	X	
	Visão, cópia ou remoção de documentos arquivados	4	X	
	Perda de confidencialidade	5	X	
	Manipulação de dados	6	X	
	Cópia não controlada de documentos	7	X	
	Deleção de dados de forma negligente	8	X	
Arquivos diversos, planilhas, correspondências, memorandos, contratos, etc.	Visão, cópia ou remoção de documentos arquivados	1	X	
	Manipulação de dados	2	X	
	Eliminação de dados	3	X	
	Furto de Informação	4	X	
	Corrupção de dados	5	X	
	Deleção de dados de forma negligente	6	X	
	Cópia não controlada de documentos	7	X	

Fonte: Elaborado pelo autor, 2011.

Etapa 5 – Tratamento do risco

A fase de tratamento de riscos começa com uma lista de riscos, ordenados entre si por prioridade de tratamento, de acordo com os critérios de avaliação de riscos, e tem como saída o plano de tratamento do risco e dos riscos residuais decorrentes desse tratamento. Este plano, só para lembrar, é sujeitos à decisão de aceitação por parte dos gestores da organização. A figura a seguir apresenta o processo de tratamento de risco com base nos resultados da avaliação de risco, as opções de risco e os seus riscos residuais.

Figura 7 – Tratamento de risco



Fonte: ISO 27005.

As opções de tratamento do risco são selecionadas com base no resultado da análise/avaliação de riscos, no custo esperado para sua implementação (ex: redução de risco com baixo custo) e nos benefícios previstos com sua efetivação. Vale a pena ressaltar que os problemas provenientes do risco devem ser reduzidos ao mínimo possível.

Importante

Redução de risco com baixo custo deve sempre ser realizada.

Vale a pena ressaltar que os problemas provenientes do risco devem ser reduzidos ao mínimo possível.

Todavia, devem-se levar em consideração os riscos improváveis e graves, onde os controles que não são justificáveis do ponto de vista econômico podem precisar ser implementados (por exemplo: controles de continuidade de negócios concebidos para tratar riscos de alto impacto específicos).

As opções para o tratamento do risco **não são mutuamente exclusivas**, pois, às vezes, a organização pode beneficiar-se de uma combinação das opções. Contudo a escolha das opções de tratamento do risco devem considerar como o risco é percebido pelas partes afetadas e as formas mais apropriadas de comunicação com essas partes. As opções de tratamento do risco são redução, retenção, evitar ou transferência do risco.

Redução do risco

Na redução de risco, os controles devem ser os mais apropriados e selecionados para satisfazer os requisitos identificados através da análise/avaliação de riscos e do tratamento dos mesmos. A escolha dos controles deve levar em conta os critérios para a aceitação do risco, assim como requisitos legais, regulatórios e contratuais, bem como os aspectos de custos e prazos para a implementação e os aspectos técnicos, culturais e ambientais.

Restrições técnicas, tais como requisitos de desempenho, capacidade de gerenciamento (requisitos de apoio operacional) e questões de compatibilidade, podem dificultar a utilização de certos controles ou induzir erros humanos, chegando mesmo a anular o controle, a dar uma falsa sensação de segurança ou a tornar o risco ainda maior do que seria se o controle não existisse (por exemplo: exigir senhas complexas sem treinamento adequado leva os usuários a anotar as senhas por escrito).

Retenção do risco

As decisões sobre a retenção do risco são tomadas tendo como base a avaliação de riscos. Caso o nível de risco atenda aos critérios para a aceitação do risco, não existe a necessidade de implementar controles adicionais, podendo assim ocorrer a retenção do risco.

Evitar o risco

Consiste na realização de atividade para que um determinado risco seja evitado. Caso os riscos identificados sejam considerados demasiadamente elevados e quando os custos da implementação de outras opções de tratamento do risco

excederem os benefícios, aborda-se a atividade sobre a qual o risco poderia ocorrer. Sendo assim, pode-se decidir que o risco seja evitado completamente, via a eliminação de uma atividade planejada ou existente ou via as mudanças nas condições em que a operação da atividade ocorre.

Transferência do risco

Um determinado risco é transferido para outra entidade, de modo que possa gerenciá-lo de forma mais eficaz. Vale a pena ressaltar que a transferência do risco pode também criar novos riscos ou modificar riscos existentes e já identificados, tornando talvez necessário um novo tratamento do risco.

Etapa 6 – Aceitação do risco

O processo de aceitação de riscos faz uso do plano de tratamento do risco e a análise/avaliação do risco residual. O processo está sujeito à decisão dos gestores da organização, relativa à aceitação do mesmo, onde se tem como produto uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.

Comunicação do risco de segurança da informação

Todas as informações sobre os riscos obtidas através das atividades de gestão de riscos devem ser trocadas e/ou compartilhadas entre o responsável pelas tomadas de decisão sobre esse assunto e as demais partes interessadas (*stakeholders*). Além disso, deve-se buscar alcançar um consenso sobre como os riscos devem ser gerenciados. As informações a serem trocadas incluem basicamente a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos.

Sendo assim, a atividade da comunicação dos riscos possibilitará o entendimento contínuo do processo de gestão de riscos de segurança da informação da organização e dos resultados obtidos.

Monitoramento e análise crítica de riscos de segurança da informação

Esta atividade tem como objetivo monitorar e analisar todas as informações sobre os riscos obtidas através das atividades de gestão de riscos. Com isto, pretende-se que as eventuais mudanças no contexto da organização sejam identificadas o mais

rápido possível, e manter-se uma visão geral dos riscos. Desta forma, é possível uma análise crítica, e, caso necessário, melhoras na implementação de segurança podem ser implementadas.

Referências

AS/NZS . **Risk management guidelines companion to AS/NZS 4360:2004**. Local: ? Ed: Standards Australia International Ltd, 2004. Handbook.

ISO 31000 (2009). Risk management — Guidelines on principles and implementation of risk management. ISO 31000:2009.

STONEBURNER, Gary; GOGUEN, Alice e FERINGA, Alexis. NIST SP 800-30 **Risk management guide for information technology systems**. Ed.: NIST, 2002.

FERMA. **Norma de gestão de riscos.** Federation of European risk management associations, 2003.

ISO/IEC 27001. Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerenciamento de Segurança da Informação – Necessidades, ISO/IEC. 2005.

ISO/IEC 27002 : Information technology - Security techniques - Code of practice for information security management - Redesignation of ISO/IEC 17799:2005.

ISO/IEC 27005 Information technology -- Security techniques - Information security risk management, 2008.

Atividades de Autoaprendizagem

1) Considerando o conteúdo apresentado nesta unidade, verifique qual a dupla de pergunta e resposta abaixo que está incorreta.

a. ( ) Qual o objetivo de uma Organização realizar a gestão de risco?

Resp.: A gestão de riscos de segurança da informação possibilita que a Organização mantenha a sua informação protegida e disponível em tempo hábil, de forma que os seus processos de negócio estejam inativos para que a sua missão seja cumprida.

b. ( ) Durante a análise de riscos, a fase de análise de impacto é fundamental para o seu sucesso. Descreva quais fatores devem ser levados em consideração durante a fase de análise de impacto.

Resp.: A análise de impacto deve levar em consideração a importância do processo para a Organização, junto com o(s) serviço(s) relacionado(s) ao processo e os ativos responsáveis para a execução dos serviços.

2) Cite todas as etapas do processo de gestão de riscos, informando todos os parâmetros de entrada e saída do processo. Faça um diagrama para facilitar a sua resposta, apresente-a por meio desse diagrama.

Atividade Colaborativa

Como apresentado na unidade, a gestão de riscos de segurança da informação é um processo dinâmico que evolui a cada momento em uma Organização. Um dos seus principais problemas é a questão da comunicação de riscos. Sendo assim, vamos discutir uma estratégia para comunicar os riscos envolvidos no processo de gestão de riscos aos seus Stakeholders. Uma sugestão é analisar a forma como "The Risk IT Framework" publicado pela ISACA usa.

Faça a análise sugerida e em seguida publique seus resultados, por meio da ferramenta Fórum, e discuta com os seus colegas sobre os resultados a que esses chegaram para essa atividade.

Síntese

Nesta unidade, você estudou o que é gestão de riscos de segurança da informação e acompanhou todas as suas etapas. Lembre que a gestão de riscos consiste em um processo contínuo e eterno, onde o monitoramento do risco é constante. Vale a pena ressaltar que a continuidade deste processo leva a realizar a análise de risco em períodos pré-estabelecidos, com o objetivo de ele sempre estar atualizado, por exemplo, de modo a detectar e tratar adequadamente as novas ameaças que o sistema poderá sofrer.

Saiba mais

Para saber mais sobre o assunto estudado, consulte as seguintes publicações:

NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.

ISO/IEC 27005 - Information technology - Security techniques - Information security risk management (draft).

Unidade 4

A Gestão de risco aplicada a uma empresa

Objetivos de aprendizagem

- Conhecer diretivas para a implantação da gestão de risco em uma organização.

Introdução

Esta unidade visa apresentar um exemplo de como realizar uma análise/avaliação de risco. O exemplo apresenta uma situação inicial e a sequência de todo o processo a ser realizado para gerenciar o risco, de modo que não prejudique a organização sobre a qual se dá. É bom esclarecer que o exemplo está em versão reduzida, apresentando apenas alguns serviços, ameaças e vulnerabilidades. É claro que a análise deveria levar em consideração uma maior quantidade de ameaças relacionadas às vulnerabilidades do ambiente onde esse risco encontra-se, mas o objetivo do exemplo é somente apresentar a sequência de realização de todo o processo de análise/avaliação de risco.

Na parte final do exemplo, poderá ser observado que alguns campos do modelo de processo de gestão de risco não foram preenchidos. Estes campos poderão ser complementados por você. Na verdade, o objetivo é dar a você a oportunidade de complementar o aprendizado.

A implantação do processo de gestão de risco irá seguir as premissas descritas nas unidades anteriores deste livro, de forma que, ao fim, você tenha um exemplo de como executar um processo de gestão de riscos.

A unidade apresentará, ainda, no formato de tabelas, um resumo de todas as informações e atividades que irão compor esse processo. As tabelas fornecerão uma base de informações na composição dos diversos relatórios durante todas as etapas de implantação do processo de gestão de risco. Tais tabelas podem vir a formar uma grande planilha, a qual, por sua vez, apresenta os processos de gestão de risco da informação.

Estudo de Caso de segurança da informação na empresa Rebite

Luiz Otávio Botelho Lento

Situação da empresa REBITE

A REBITE é uma instituição que oferece aos seus clientes soluções criativas em Tecnologia da Informação, vale dizer, diferenciais de eficiência e eficácia em seus processos, garantindo a otimização de recursos e aumento de produtividade. Além disso, tem sempre como principal valor a satisfação do cliente e, mais, o relacionamento de longo prazo com ele.

Trata-se de uma empresa que, hoje, provê soluções inovadoras no segmento de administração de ambientes e serviços de TI, Segurança da Informação e *Business Intelligence.* Destaque no mercado desde 1998, tem como um dos seus principais focos, soluções na área de gestão de TI, sendo uma das referências nacionais em Information Technology Infrastructure Library (ITIL).

Proteger o conhecimento e as informações do segmento de negócio da REBITE e de seus colaboradores passou a constituir uma necessidade estratégica e fundamental para o seu sucesso. A necessidade de se ter uma visão dos riscos a que a empresa está suscetível tornou-se uma necessidade para melhor alinhar a TI ao seu negócio. Assim, cabe à empresa assegurar a melhoria de sua capacitação técnica e o melhor gerenciamento de seus recursos para proporcionar um melhor retorno de investimento em relação aos riscos de seus processos de TI.

Para dar conta dessas demandas, a REBITE contratou a empresa de consultoria CGTI Gestão de TI. Assim, a função da CGTI na Rebite é realizar nesta a implantação do processo de gestão de riscos de segurança da informação.

Na sequência, encontram-se os passos dados na relação entre a Rebite e a CGTI Gestão de TI para a gestão dos referidos riscos.

Confecção do projeto

Fase de contratação

O conteúdo do contrato entre a Rebite e a Consultoria CGTI Gestão de TI é considerado **restrito** às partes interessadas ao processo de análise de risco,

com o objetivo de proteger as informações veiculadas. O documento em que se apresenta esse contrato é de uso exclusivo da Empresa REBITE, podendo ser utilizado internamente nesta empresa para avaliação de seus termos, para aprovação, e, posteriormente, o acompanhamento da prestação dos serviços nele descritos. Seu conteúdo não pode ser copiado, total ou parcialmente, sem a prévia autorização por escrito da CGTI Gestão de TI, que, por sua vez, se compromete a manter sob sigilo qualquer informação da Empresa REBITE a ela confiada.

O termo de confidencialidade assinado entre as partes interessadas, Empresa REBITE e CGTI Gestão de TI da Informação, selam o compromisso citado.

Depois de firmado o contrato entre a REBITE e CGTI Gestão de TI da Informação, seguiu-se uma série de etapas, as quais são apresentadas a seguir e já na ordem em que as mesmas foram realizadas.

Etapa 1 – Definição do contexto

Planejamento inicial

Foi realizada uma reunião onde se definiram as expectativas da Empresa REBITE, o escopo, a equipe, o cronograma e os critérios de riscos a serem adotados. Como resultados de tal reunião, foi obtida uma análise dessa organização, verificaram-se as restrições funcionais da Rebite e que o projeto deve atender; o escopo deste projeto, a equipe que deve ser envolvida neste projeto; e, a definição dos critérios básicos de risco a que a Rebite está exposta.

Análise da organização

Na análise da Rebite, constatou-se qual o seu propósito e principal negócio. Afinal, esses dois elementos é que devem ser preservados e fomentados acima de tudo. Logo, precisa-se ter claro o que são eles.

O seu **propósito** é oferecer soluções criativas em Tecnologia da Informação, as quais, portanto, tragam diferenciais de eficiência e eficácia nos processos de seus clientes, garantindo-lhes a otimização de recursos e aumento de produtividade. Em virtude disso, a Rebite tem sempre, como seu principal valor, a satisfação do cliente e o relacionamento de longo prazo com o mesmo.

Já, quanto ao negócio, a REBITE possui dois segmentos de negócio: prover treinamento nas áreas de TI e desenvolver, dar suporte, a soluções de gestão de TI.

Restrições que afetam a REBITE

As restrições funcionais que devem ser respeitadas pela gestão de risco são as seguintes:

1. É necessário que o ambiente virtual da empresa esteja disponível 24 horas, 7 dias na semana e 365 dias ao ano para o aluno, durante o horário comercial.

   Tabela 1 – Tabela de disponibilidade

Disponibilidade Uptime %	Quantidade de Downtime permitido no período de tempo			
	Anual	Mensal	Semanal	Diário
99,99%	0,88 h	4,4 min	1 min	8,7 seg

   Fonte: Elaboração do autor, 2012.

2. Segurança no trato e armazenamento das informações.
3. Alto desempenho do sistema computacional.
4. Gerenciabilidade dos recursos do sistema computacional.
5. Usabilidade adequada dos recursos do sistema computacional:
   - Restrições econômicas – a manutenção dos cursos está ligada à demanda de alunos.
   - Restrições aos recursos humanos – a manutenção de professores e autores capacitados.
   - Restrições relacionadas a métodos – a manutenção do credenciamento dos cursos oferecidos.
   - Restrições orçamentárias – ligadas ao mercado.

Escopo

O processo de gestão de risco (PGR) a ser aplicado na Empresa REBITE visa atender a necessidade de otimizar os seus processos de TI, bem como otimizar o seu uso dos recursos de TI, em conformidade com seu negócio. Entretanto, devido à diversidade de processos de negócio existentes na organização, o PGR foi divido em 2 grupos, de acordo com os aspectos estratégicos do negócio da Empresa.

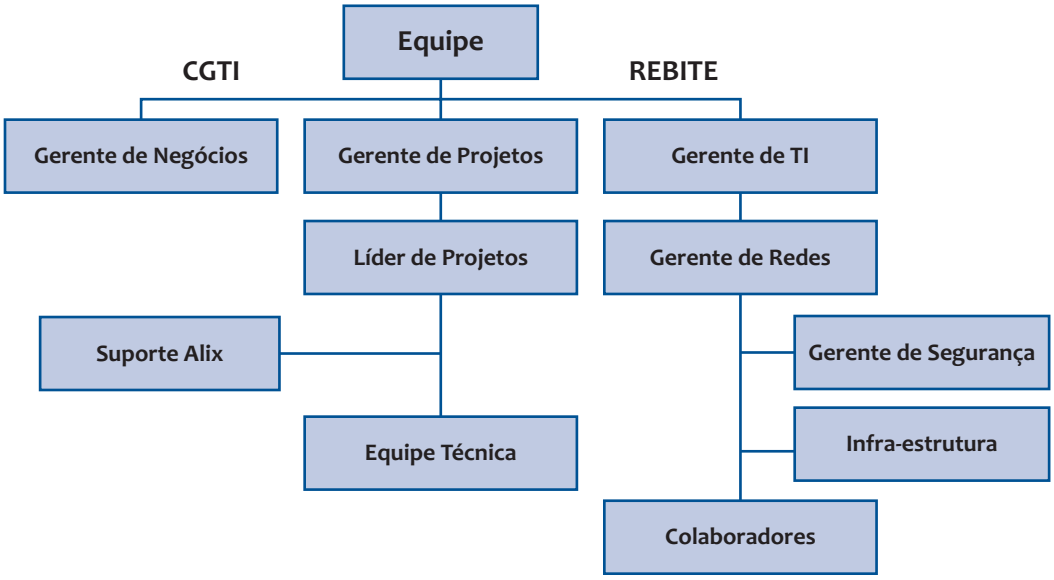
Na fase inicial, foram abordados os processo referentes a compras, contratos e recursos humanos (RH). Posteriormente, em uma segunda etapa, serão tratados os processos de desenvolvimento de soluções, treinamento e atendimento a clientes.

Esse documento irá apresentar os resultados referentes ao primeiro grupo de processos da organização.

Equipe de Projeto

O diagrama que se segue apresenta a estrutura organizacional das equipes das Empresas REBITE e CGTI responsáveis pela implantação do PGR.

Diagrama 1 – Organização entre as equipes da REBITE e da CGTI



Fonte: Elaboração do autor, 2012.

Definição dos critérios básicos de risco

Cabe à Rebite determinar quais tipos de risco ela pode aceitar.

No caso, a empresa aceitou todos os riscos de médio, baixo e muito baixo impacto a seus negócios.

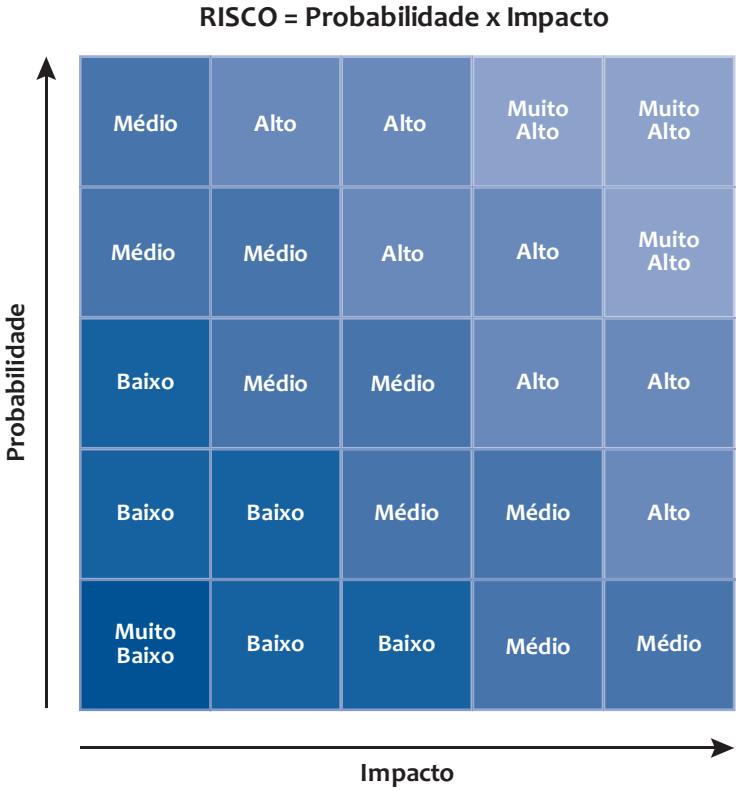
Claro, a empresa precisa saber como classificar um risco para determinar se o aceita, ou não. Para o cálculo do risco, será utilizada uma função soma: **f_{risco} = probabilidade + impacto**.

Foi adotada uma escala de 1 a 10 para representar os 5 níveis de riscos, conforme acordado em reunião com a equipe da contratada. Os valores que foram atribuídos aos riscos são:

Muito Baixo – 1, 2
Baixo – 3, 4
Médio – 5, 6
Alto – 7, 8
Muito Alto – 9,10

A empresa pode construir uma figura com a classificação dos riscos de seus ativos, conforme segue abaixo. Perceba que, quanto mais quadros em vermelho nesta figura, mais ativos da mesma têm impacto muito alto nos negócios da empresa, caso sejam atingidos pelas ameaças às suas informações.

Figura 1 – Cálculo do risco



Fonte: Elaborada pelo autor, 2011.

Critério de impacto e da probabilidade da ameaça

Ao se determinar o impacto, foram levados em consideração os aspectos estratégicos e operacionais, como interrupção dos serviços; perda de confiança pelo cliente; interrupção de operação interna; interrupção de operação de terceiros; violação de cláusulas contratuais; perda financeira; perda de clientes; perda de reputação; enfraquecimento da capacidade de negociação; rejeição ao produto; dano material e perda de eficácia.

A seguir, encontra-se a tabela do que significa cada um dos graus de risco de impacto para a Rebite.

Tabela 2 – Impacto das ameaças

Muito Alto (5)	O impacto financeiro sobre a organização deve ultrapassar 30% do capital bruto da empresa. O impacto é muito significativo, quando os projetos de TI forem acessados de forma indevida e entregues aos concorrentes. As atividades operacionais da empresa foram interrompidas por um período maior ou igual a 6 horas, afetando o prazo de entrega de produtos da empresa, o que acarreta danos significativos à sua imagem. Insatisfação total dos investidores da empresa quanto às consequências do evento de segurança da informação.
Alto (4)	O impacto financeiro sobre a organização deve ultrapassar 20% do capital bruto da empresa, mas é inferior a 30%. O impacto é significativo, quando os projetos de TI forem alterados ou danificados por ameaças intencionais, ou não. As atividades operacionais da empresa foram interrompidas por um período maior ou igual a 3 horas, afetando o prazo de entrega de produtos da empresa, o que acarretou danos à imagem da empresa. Insatisfação parcial dos investidores da empresa quanto às consequências do evento de segurança da informação.
Médio (3)	O impacto financeiro sobre a organização é superior a 10% do capital bruto da empresa, mas não chega a 20%. O projeto de TI teve que ser parcialmente reestruturado e ocorreram pequenos danos à imagem da organização. Preocupação moderada das partes interessadas.
Baixo (2)	O impacto financeiro sobre a organização deve ser inferior a 10% ao capital bruto da empresa. O projeto de TI pode ser recuperado por completo, e não houve danos na imagem da empresa. Os investidores tiveram conhecimento do incidente de segurança da informação, mas não se preocuparam.
Muito Baixo (1)	O impacto financeiro sobre a organização não afeta o capital bruto da empresa. Os projetos de TI e as atividades operacionais não foram afetadas. Investidores não têm conhecimento do incidente de segurança da informação.

Fonte: Elaborada pelo autor, 2012.

A seguir, a tabela com as probabilidades de ocorrências de cada uma das ameaças consideradas para determinar o grau de impacto.

Tabela 3 – Probabilidade de ocorrência de ameaças

Estimativa	Descrição	Indicadores
Muito alta (Muito provável, 5)	O incidente ocorre todos os meses do ano, inclusive com um percentual de 60% de duas ou mais ocorrências. Existe um histórico de ocorrências do incidente que comprova os indicadores.	O incidente de segurança ocorre pelo menos uma vez ao mês. Não existe controle aplicado, ou está desativado.
Alta (Provável, 4)	O incidente ocorre mais de uma vez a cada semestre, com a intensidade superior a 50% ao ano. Existe um histórico de ocorrências do incidente que comprova os indicadores.	O incidente de segurança ocorre a cada 2 ou 3 meses ao ano. O controle aplicado é ineficaz e também desatualizado em relação às ameaças atuais da empresa.
Média (Possível, 3)	Ocorre todo ano, com a intensidade de até 50% de probabilidade de ocorrência ao ano. Existe um histórico de ocorrências do incidente que comprova os indicadores.	Pode ocorrer mais do que uma vez por ano. O incidente pode ser difícil de detectar e controlar devido a algumas influências do negócio da empresa. Existe controle, aplicado de forma adequada, mostra-se eficaz, mas não se mantém atualizado.
Baixa (Remota, 2)	Não existe a possibilidade de ocorrer a cada dois anos ou com possibilidade inferior a 5% ao ano. Não existe histórico do incidente.	Não ocorreu durante o ano, mas é possível que ocorra. Existe controle, o mesmo é eficaz, mas pode ser burlado, caso não seja monitorado.
Muito Baixa (Muito remota, 1)	Não existe a possibilidade de ocorrer a cada quatro anos ou com possibilidade inferior a 2% ao ano. Não existe histórico do incidente.	Não ocorreu durante os últimos três anos, e é improvável que ocorra. O controle é plenamente eficaz, ou o controle não foi aplicado, pela baixa probabilidade de ocorrer a ameaça.

Fonte: Elaborada pelo autor, 2012.

Produto da Etapa 1

Como resultado de todos os passos desta etapa, temos como resultado o **Relatório de Planejamento do Projeto,** o qual deve conter:

a. Declaração de escopo, com a descrição do foco do Projeto, definindo claramente o que será contemplado no Projeto de desenvolvimento e implementação do SGSI na Empresa REBITE através das principais atividades, entregas, premissas e restrições.

b. Apresentação dos papéis e responsabilidades de toda a equipe envolvida no Projeto (da Contratada e na Empresa REBITE).

c. Reunião para apresentação dos produtos da etapa a todos os envolvidos, visando demonstrar os resultados e esclarecer dúvidas.

Etapa 2 – Análise/avaliação de riscos

Para que todo o processo de análise de riscos fosse apresentado de forma simples e sucinta, com o objetivo de tornar o seu entendimento um tanto quanto menos complexo, foram resumidos aqui os ativos a serem analisados, bem como as suas ameaças, controles, vulnerabilidades e consequências. Logo, o objetivo deste exemplo é apresentar uma forma de como pode ser realizada, na prática, uma análise de riscos.

Assim, faz parte como primeiro passo dessa etapa, a identificação do risco.

Identificação dos riscos

As premissas, com base nas quais foi realizada a identificação dos ativos, são as seguintes:

1. Os ativos a serem protegidos foram divididos em três categorias somente: hardware, software e informação. Vale a pena ressaltar que outras categorias como informação, mídias, entre outras, poderiam ser inseridas.
2. Todos os nomes apresentados na tabela a seguir foram fornecidos pelo cliente. Não será levado em consideração, nesse texto, o significado de cada termo utilizado para nomear o ativo.
3. Os serviços selecionados para realizar a análise de riscos foram aqueles considerados os mais críticos para a manutenção do negócio da Empresa REBITE. Os demais serviços não serão considerados nessa análise.
4. Dentre os serviços selecionados, foram escolhidos os serviços que são básicos à execução do seu negócio. Os demais serviços não foram considerados nesta análise.

Tabela 4 – Identificação dos riscos

Ativo Primário	Gerência	Setor	Serviço TI	Ativo de suporte e infraestrutura
Processo de Contratos	Administração	Financeiro	Banco de dados	SGBD
				Servidor BD
			Cadastro clientes	Link
Processo Recursos Humanos	Administrativa	RH	Banco de dados	SGBD
				Servidor BD
			Cadastro pessoal	Sis_Cad_Pes
				Base_dados
Processo Compras	Administrativa	Aquisição	Banco de dados	SGBD
				Servidor BD
			Cadastro fornecedor	Sis_Cad_For
				Base_dados

Fonte: Elaborada pelo autor, 2012.

Na sequência, foi realizada a identificação das ameaças sobre os ativos da empresa. Para identificá-las, levaram-se em consideração algumas ameaças do tipo físico, comprometimento da informação e falhas técnicas. Estas ameaças estão expressas na coluna "Tipo" da nossa próxima tabela.

Tabela 5 – Identificação das ameaças

	Ativo	Tipo	Ameaças
1	**SGBD**	Falhas técnicas	Violação das condições de uso do sistema de informação (1A)
			Falha/corrupção de software (1B)
2	**Servidor BD**	Dano físico	Destruição de equipamento (2A)
			Falha no fornecimento de energia (2B)
3	**Link**	Dano físico	Falha no fornecimento de energia (3A)
4	**Sis_Cad_Pes**	Falhas técnicas	Violação das condições de uso do sistema de informação (4A)
			Falha/corrupção de software (4B)
5	**Base_dados**	Comprometimento da informação	Backup indisponível (5A)
6	**Sis_Cad_For**	Falhas técnicas	Violação das condições de uso do sistema de informação (6A)
			Falha/corrupção de software (6B)

Fonte: Elaborada pelo autor, 2012.

Em seguida, realizou-se a análise dos controles existentes. Foram apresentados somente alguns dos controles encontrados para cada tipo de ameaça. Cada ameaça relacionada a um ativo está identificada com um número e uma letra, conforme a última tabela.

Todos os controles adotados estão de acordo com o Anexo A da norma ISO 27001.

Os valores adotados em relação a esses ativos – números presentes na primeira coluna da última tabela – estão definidos conforme a seguinte escala:

1 – controle instalado e que atende plenamente as necessidades da organização;

2 – controle instalado e que atende as necessidades da organização, mas está desatualizado;

3 – controle instalado e que atende parcialmente as necessidades da organização, mas está desatualizado;

4 – controle instalado, mas que não está atuando, i.é, não atende as necessidades da organização;

5 – não existe controle.

Tabela 6 – Análise dos controles existentes

Ativo	Ameaças	Controle	Implantado		Val
			S	N	
1	1A	Documento da política de segurança da informação		X	5
	1B	Manutenção dos equipamentos		X	5
2	2A	Instalação e proteção do equipamento		X	5
	2B	Utilidades		X	5
3	3A	Utilidades		X	5
4	4A	Rótulos e tratamento da informação		X	5
	4B	Controle de acesso ao código - fonte de programa		X	5
5	5A	Cópias de segurança das informações		X	5
6	6A	Rótulos e tratamento da informação		X	5
	6B	Controle de acesso ao código - fonte de programa		X	5

Fonte: Elaborada pelo autor, 2012.

Feito isso, partiu-se para a identificação das vulnerabilidades. A próxima tabela estabelece uma relação das ameaças apresentadas para cada ativo e auxilia, junto com os controles, no cálculo da probabilidade de a ameaça ser concretizada.

A escala de valor da vulnerabilidade, apresentada na coluna "valor" desta tabela, varia conforme a escala abaixo:

1 – Não existe a vulnerabilidade.

2 – A vulnerabilidade existe, mas difícil de ser descoberta.

3 – A vulnerabilidade existe, o controle é eficaz, mas pode ser descoberta.

4 – A vulnerabilidade existe e, apesar do controle, é facilmente descoberta.

5 – Não existe controle aplicado, está totalmente vulnerável e é facilmente descoberta.

Tabela 7 – Identificação das vulnerabilidades

Ameaças	Vulnerabilidades	Valor
Violação das condições de uso do sistema de informação (1A)	Falta de treinamento no trabalho	5
Falha/corrupção de software (1B)	Aplicação inadequada de regras de desenvolvimento	5
Destruição de equipamento (2A)	Degradação	5
Falha no fornecimento de energia (2B)	Rede elétrica instável	5
Falha no fornecimento de energia (3A)	Rede elétrica instável	5
Violação das condições de uso do sistema de informação (4A)	Uso não controlado/impróprio	5
Falha/corrupção de software (4B)	Aplicação inadequada de regras de desenvolvimento	5
Backup indisponível (5A)	Backup de dados	5
Violação das condições de uso do sistema de informação (6A)	Uso não controlado/impróprio	5
Falha/corrupção de software (6B)	Aplicação inadequada de regras de desenvolvimento	5

Fonte: Elaborada pelo autor, 2012.

Partiu-se, então, para a **identificação das consequências** dos incidentes de segurança da informação. Os resultados dessa identificação também foram dispostos numa tabela, a seguinte:

Tabela 8 – Identificação das consequências dos incidentes

Cenário de Incidente	Ativo afetado	Consequências	Valor do ativo
Prédio da empresa ficou sem energia	SGBD	Não armazena dados	5
Prédio da empresa ficou sem energia	Servidor BD	Não armazena dados	5
Prédio da empresa ficou sem energia	Link	Não existe comunicação fora da empresa	5
Prédio da empresa ficou sem energia	Sis_Cad_Pes	Não cadastra e nem consulta clientes	5
Prédio da empresa ficou sem energia	Base_dados	Não consulta dados de clientes	5
Prédio da empresa ficou sem energia	Sis_Cad_For	Não consulta dados do fornecedor	5

Fonte: Elaborada pelo autor, 2012.

Depois de toda esta identificação do risco, organizada por meio dessas tabelas, pode-se verificar a estimativa do risco.

Estimativa do risco

O primeiro passo para estimar os impactos de um risco é a análise desse impacto.

Os valores atribuídos aos processos e serviços estão em concordância com a tabela de impacto definida na fase de definição do escopo. O valor referente ao ativo de infraestrutura foi obtido da tabela das consequências (ver tabela 8).

O valor do impacto apresentado na coluna final da tabela foi a média aritmética do valor do processo, serviço de TI e o valor do ativo de infraestrutura.

Tabela 9 – Análise de impacto

Processo/Valor	Serviços TI/Valor	Ativo Infra/Sup	Valor	Impacto
Processo de Contratos **5**	Banco de dados **5**	SGBD	5	5
		Servidor BD	5	5
	Cadastro clientes **5**	Link	5	5
Processo Recursos Humanos **5**	Banco de dados **5**	SGBD	5	5
		Servidor BD	5	5
	Cadastro pessoal **5**	Sis_Cad_Pes	5	5
		Base_dados	5	5
Processo Compras **5**	Banco de dados **5**	SGBD	5	5
		Servidor BD	5	5
	Cadastro fornecedor **5**	Sis_Cad_For	5	5
		Base_dados	5	5

Fonte: Elaborada pelo autor, 2012.

Em seguida, deve-se determinar a probabilidade do incidente ocorrer.

Os valores de vulnerabilidade e controle foram obtidos das tabelas **na fase de identificação dos riscos**, a qual foi apresentada aqui anteriormente. O valor de histórico foi obtido em conformidade com os indicadores estabelecidos na etapa 1, definição do escopo, a qual também já foi apresentada aqui.

A probabilidade da ameaça ocorrer, prob, foi calculada por meio da média aritmética dos campos histórico, vulnerabilidade e control. Acompanhe:

Tabela 10 – Probabilidade da ameaça

Ativo	Ameaça	Histórico	Vulnerabilidade	Control	Prob
SGBD	Violação das condições de uso do sistema de informação (1ª)	5	5	5	5
	Falha/corrupção de software (1B)	5	5	5	5
Servidor BD	Destruição de equipamento (2A)	5	5	5	5
	Falha no fornecimento de energia (2B)	5	5	5	5

Ativo	Ameaça	Histórico	Vulnerabilidade	Control	Prob
Link	Falha no fornecimento de energia (3A)	5	5	5	5
Sis_Cad_Pes	Violação das condições de uso do sistema de informação (4A)	5	5	5	5
	Falha/corrupção de software (4B)	5	5	5	5
Base_dados	Backup indisponível (5A)	5	5	5	5
Sis_Cad_For	Violação das condições de uso do sistema de informação (6A)	5	5	5	5
	Falha/corrupção de software (6B)	5	5	5	5

Fonte: Elaborada pelo autor, 2012.

E, para a determinação do risco, construiu-se também uma tabela.

Nela, as colunas "prob" e "impacto" foram obtidas via tabelas anteriores da estimativa de riscos.

O cálculo do risco foi feito pela função: **Risco = Probabilidade + Impacto**

Tabela 11 – Determinação do risco

	Ativo	Prob	Impacto	Risco
1	SGBD	5	5	5
		5	5	5
2	Servidor BD	5	5	5
		5	5	5
3	Link	5	5	5
4	Sis_Cad_Pes	5	5	5
		5	5	5
5	Base_dados	5	5	5
6	Sis_Cad_For	5	5	5
		5	5	5

Fonte: Elaborada pelo autor, 2012.

Avaliação de risco

A avaliação de riscos se baseia na análise de riscos realizada em conjunto com os critérios de riscos determinados na etapa de definição do escopo do projeto.

Todos os riscos que forem alto ou muito alto deverão ser tratados. A prioridade de tratamento deverá estar de acordo com as prioridades estabelecidas pela organização. No caso, essas prioridades resultaram no seguinte:

Tabela 12 – tabela de prioridades de risco a tratar

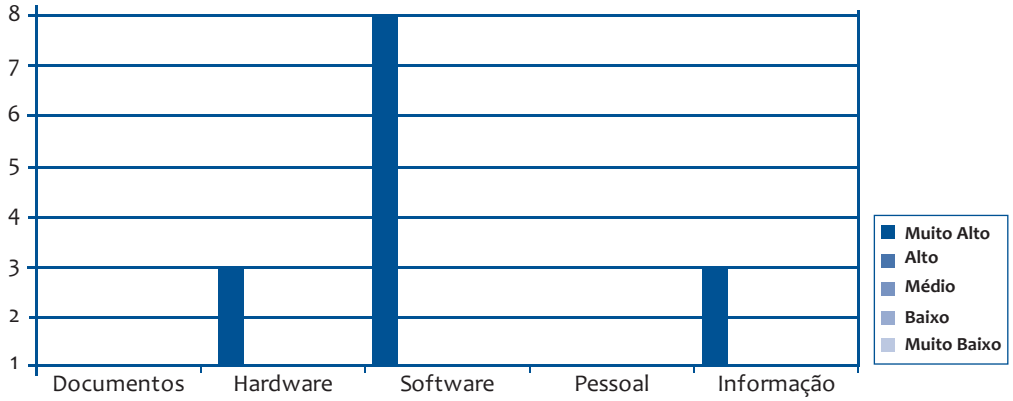
Ativo	Risco por Prioridade	Tratar	
		Sim	Não
SGBD	Violação das condições de uso do sistema de informação (1A)	X	
	Falha/corrupção de software (1B)	X	
Servidor BD	Destruição de equipamento (2A)	X	
	Falha no fornecimento de energia (2B)	X	
Link	Falha no fornecimento de energia (3A)	X	
Sis_Cad_Pes	Violação das condições de uso do sistema de informação (4A)	X	
	Falha/corrupção de software (4B)	X	
Base_dados	Backup indisponível (5 A)	X	
Sis_Cad_For	Violação das condições de uso do sistema de informação (6A)	X	
	Falha/corrupção de software (6B)	X	

Fonte: Elaborada pelo autor, 2012.

Relatório Final da Análise/Avaliação de Riscos

O gráfico 1 apresenta uma visão ampla da situação de risco na organização. Realizando-se uma breve análise, pode-se concluir que a REBITE atualmente possui a maioria de seus componentes com risco alto/muito alto, o que torna a continuidade de seu negócio vulnerável.

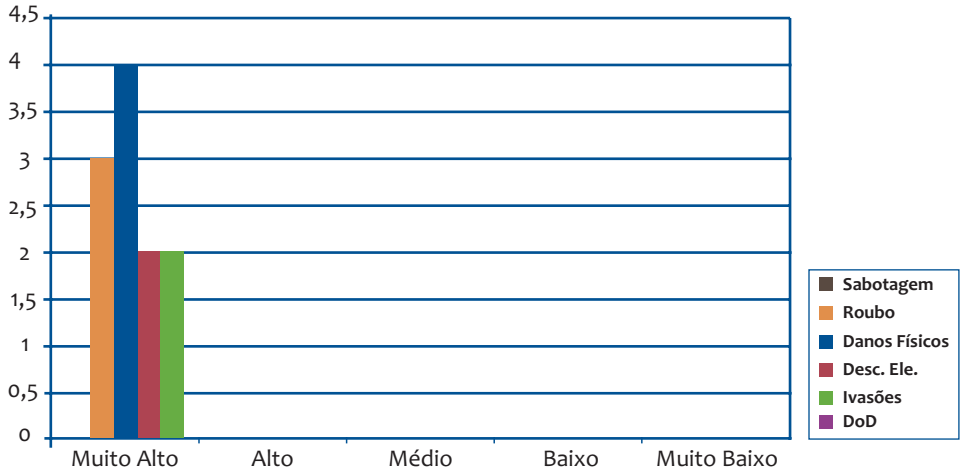
Gráfico 1 – Minimizado da quantidade geral de riscos



Fonte: Elaboração do autor, 2012.

O gráfico 2 apresenta uma visão mais detalhada da quantificação de riscos por categoria. Esta visão demonstra que a organização não possui um controle de acesso físico às suas instalações e nem componentes de proteção físicos adequados às suas necessidades. Vale a pena ressaltar o quanto a REBITE está vulnerável em relação aos seus servidores, em função do perfil de seus componentes (alunos e colaboradores) e das tarefas que lhes são atribuídas.

Gráfico 2 – Minimizado da quantidade riscos por categoria



Fonte: Elaboração do autor, 2012.

Etapa 3 – Tratamento de riscos

No primeiro passo desta etapa, será apresentada a declaração de aplicabilidade (Statement of Applicability – SOA), com os controles necessários, citando aqueles que serão aplicados, ou não, e sua justificativa.

No segundo passo, será apresentada uma tabela com o plano de tratamento dos riscos a serem tratados.

Vamos, então, à descrição dos resultados obtidos em cada um desses passos.

1 – Declaração de aplicabilidade

A declaração de aplicabilidade é uma listagem dos controles aplicados e dos controles não aplicados, isto é, uma listagem com os controles do Anexo A da ISO 27001, podendo ser incluídos controles adicionais.

A seguir, estão apresentadas as listas de alguns controles que fazem parte do SOA.

Tabela 13 – Política de segurança da informação

Controle	Descrição	Aplicado	Justificativa
A.5.1.1	Documento da política de segurança da informação	Sim	Política de Segurança foi aprovada pelo gerente de TI.
A.5.1.2	Revisão da política de segurança da informação	Sim	A política de segurança é analisada criticamente para manutenção em intervalos não superiores a 12 meses.

Fonte: Elaborada pelo autor, 2012.

Tabela 14 – Back-up

Controle	Descrição	Aplicado	Justificativa
A.10.5.1	Back-up de informação	Sim	Para prevenir a perda permanente de informações importantes.

Fonte: Elaborada pelo autor, 2012.

Tabela 15 – Responsabilidades pelos ativos

Controle	Descrição	Aplicado	Justificativa
A.7.1.1	Inventário de ativos	S	Um registro de todos os ativos de informação é mantido no local.
A.7.1.2	Propriedade de ativos	S	Todos os ativos no âmbito deste registro são de propriedade da TI.
A.7.1.3	Uso aceitável dos ativos	S	Uso aceitável dos ativos está previsto nas políticas e procedimentos do sistema.

Fonte: Elaborada pelo autor, 2012.

Tabela 16 – Classificação da informação

Controle	Descrição	Aplicado	Justificativa
A.7.2.1	Diretrizes para a classificação	S	Todos os dados estarão relacionados a aplicação específica.
A.7.2.2	Rótulos e tratamento	N	Não necessário.

Fonte: Elaborada pelo autor, 2012.

Tabela 17 – Segurança de equipamentos

Controle	Descrição	Aplicado	Justificativa
A.9.2.1	Localização e proteção do equipamento	S	Para se proteger contra ameaças ambientais e físicas.
A.9.2.2	Apoio utilitários	S	Equipamento funcionando 24/7/365
A.9.2.3	Segurança do cabeamento	S	Pisos falsos para o cabeamento
A.9.2.4	Manutenção de equipamentos	S	Equipamento necessita de manutenção para garantir alta disponibilidade.
A.9.2.5	Segurança de equipamentos fora das instalações	S	Trabalho de alguns funcionários.
A.9.2.6	Segurança para descarte ou reutilização de equipamentos	S	Todos os dados do cliente tratados de forma eletrônica devem ser descartados de maneira segura.

Fonte: Elaborada pelo autor, 2012.

2 – Plano de tratamento de riscos

O plano de tratamento de riscos foi estruturado em uma tabela composta pelo: controle; os recursos necessários à implantação do controle; o responsável pelo controle; e, a data de início e fim da implantação do controle.

Tabela 18 – Tratamento de riscos

Plano de ação (Control. Selecionados)	Recursos necessários	Responsável	Data início/fim
Documento da política de segurança da informação	Fórum de TI	Gerente de TI	05/2011 a 07/2011
Revisão da política de segurança da informação	Fórum de TI	Gerente de TI	05/2011 a 07/2011
Back-up de informação	Equipe de backup	Gerente de Infraestrutura	05/2011 a 07/2011
Inventário de ativos	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Propriedade de ativos	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Uso aceitável dos ativos	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Diretrizes para a classificação	Equipe de TI	Gerente de TI	05/2011 a 07/2011
Apoio utilitários	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Localização e proteção do equipamento	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Apoio utilitários	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Segurança do cabeamento	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Manutenção de equipamentos	Equipe de Infraestrutura	Gerente de Infraestrutura	05/2011 a 07/2011
Segurança de equipamentos fora das instalações	Token de segurança	Gerente de TI	05/2011 a 07/2011
Segurança para descarte ou reutilização de equipamentos	Local de descarte	Gerente de TI	05/2011 a 07/2011

Fonte: Elaborado pelo autor, 2012.

Referências

GULDENTOPS, Erik. **Chair do projeto**. 2. ed. Board Briefing on IT Governance – IT Governance Institute, 2003.

ZWICKER, R.; Souza, C. A. de; VIDAL, A. G. da R.; SIQUEIRA, J. de O. **Grau de informatização de empresas**: um modelo estrutural aplicado ao setor industrial do estado de São Paulo. **RAE-eletrônica**, v. 6, n. 2, art. 13, jul./dez. 2007.

STONEBURNER, Gary; GOGUEN, Alice e FERINGA, Alexis. **Risk**- **Management** guide for information technology systems. Ed.: NIST, 2002. NIST SP 800-30.

Atividades de Autoaprendizagem

1) Responda verdadeiro (V) ou falso (F), para os itens abaixo:

( ) A confidencialidade do projeto de gestão de riscos é uma necessidade, a fim de m inimizar possíveis vazamentos de informações das vulnerabilidades que uma Empresa possui.

( ) A declaração de aplicabilidade possibilita uma visão ampla de todos os controles que deverão ser implantados, bem como aqueles que não são necessários. Entretanto deve-se justificar todos os controles que não forem aplicados.

( ) É fundamental que a Empresa mantenha uma documentação com todos os ataques sofridos, bem como as estratégias adotadas como proteção. Isso inclusive facilita determinar os possíveis cenários de incidentes que poderão acontecer na empresa.

( ) A etapa de definição do contexto deve ser muito bem estabelecida, pois a mesma é fundamental para o sucesso de todo o projeto de gestão de riscos.

Atividade Colaborativa

1) Durante a implantação do processo de gestão de riscos, na etapa de análise/avaliação de riscos, foram apresentadas algumas ameaças. Conforme a tabela abaixo, informe pelo menos uma ameaça além das citadas na unidade para cada um dos ativos.

2) Nesta unidade, foi apresentada uma tabela de tratamento de riscos. Além disso, foi apresentada outra com o resumo das atividades desenvolvidas durante o processo de gestão de riscos. Sendo assim, vamos criar um formato para o plano de tratamento de riscos, com base nas informações disponibilizadas na unidade. Vamos discutir também uma forma de melhor apresentar esse plano.

Publique sua resposta na ferramenta **Fórum**.

Síntese

Nesta unidade, foi visto um exemplo prático de como é implantado o processo de gestão de riscos de segurança da informação em uma organização. Também foi disponibilizado um resumo de todos os campos que fazem parte do processo de gestão de riscos. A utilização desse resumo possibilitará exercer essa atividade de forma mais clara e precisa.

Vale a pena ressaltar que o exemplo de gestão de risco aplicado nesta unidade teve como objetivos aplicar a metodologia apresentada na unidade anterior e apresentar um formato de todo o processo. As informações apresentadas são fictícias e o relatório apresenta somente detalhes sobre os riscos calculados.

Bom trabalho a todos.

Saiba mais

NIST SP 800-30. **Risk Management** Guide for Information Technology Systems.

ISO 27005 (2008). Gestão de riscos de segurança da informação.

ISACA (2009) The Risk IT Framework. Ed.: ISACA.

STONEBURNER, Gary; GOGUEN, Alice e FERINGA, Alexis (2002). NIST SP 800-30 **Risk - Management** Guide for Information Technology Systems. Ed.: NIST.

ISO/IEC 27005 (2008) Information technology -Security techniques -Information security risk management (draft).

Para concluir os estudos

Ao término desta disciplina, pode-se ter uma base de conhecimento para o estabelecimento do desenvolvimento e da implantação do processo de Gestão de Riscos de TI.

Todo o conteúdo apresentado na disciplina não encerra o assunto, a busca sem fim pelo conhecimento se faz necessária. Além das referências apresentadas, a internet é uma fonte inesgotável de pesquisa sobre o assunto.

As práticas de gestão de riscos de TI quanto ao desenvolvimento e implantação do processo são uma realidade do mercado e cada vez mais aplicadas ao negócio da organização. O processo de gestão de riscos possibilita à empresa chegar a um nível de risco aceitável, bem como mantê-lo nesse patamar. Entretanto, várias questões carecem de estudos mais amplos, amadurecendo as práticas existentes e desenvolvendo novas. A sua capacitação intelectual em gestão de riscos é fundamental para o sucesso do negócio da organização.

Que bons ventos o/a levem a portos seguros nesta nova rota de desenvolvimento de tecnologia voltada a um mercado livre e saudável.

Boa sorte na continuidade de seus estudos.

Professor Luiz Otávio Botelho Lento

Minicurrículo

Luiz Otávio Botelho Lento

Oficial da Marinha da reserva, Mestre em Ciência da Computação pela UNICAMP (Sistemas Distribuídos) e Doutorando na UFSC na Engenharia Elétrica, no Departamento de Automação de Sistemas, com concentração na área de Segurança.

Atuou no governo de Santa Catarina na área de segurança da informação; consultor de treinamento da Aker Security Solutions; Consultor na área de redes e segurança da Empresa Immerson; Gerente de rede e de segurança da Rede Acadêmica do UNICEUB; Professor de disciplinas de rede de computadores e na área de segurança na Graduação do UNICEUB, bem como orientador de projetos finais de curso; Professor de Graduação e Pós-Graduação na área de redes de computadores e segurança na Universidade Católica de Brasília.

Atualmente é Professor de Graduação da UNISUL nos cursos de Tecnologia de Redes de Computadores, Sistemas de Informação, Ciência da Computação e Engenharia Elétrica e Telemática, e Coordenador do Curso de Pós-Graduação de Implantação de Software Livre; Professor do Senai Santa Catarina (CTAI) no curso de Graduação no curso Superior de Tecnologia de Redes de Computadores e Pós-Graduação no Curso de Gestão de Segurança da Informação em Redes de Computadores; Consultor da FIESC (TIC) na área de redes de computadores e segurança; e Consultor de Segurança do CTAI.

Respostas e comentários das atividades de autoaprendizagem e colaborativas

Unidade 1

1) V; V; V; V.

Unidade 2

1) F; V; V; V; V.

Unidade 3

1) a.

Unidade 4

1) V; V; V; V.

Referências

AS/NZS . **Risk management guidelines companion to AS/NZS 4360:2004**. Local: ? Ed: Enterprise Risk Management – Integrated Framework. Ed.: Committee of Sponsoring.

FERMA. **Norma de gestão de riscos.** Federation of European risk management associations, 2003.

Gerenciamento de Segurança da Informação – Necessidades, ISO/IEC. 2005.

GULDENTOPS, Erik. **Chair do projeto**. 2. ed. Board Briefing on IT Governance – IT Governance Institute, 2003.

Information security management - **Redesignation** of ISO/IEC 17799:2005.

Integrated Framework - Guidance on Monitoring Internal Control Systems. Ed.: Committee.

ISACA (2009) **The Risk IT Framework.** Ed.: ISACA.

ISO 27005 (2008). **Gestão de riscos de segurança da informação**.

ISO 31000 (2009). **Risk management** – Guidelines on principles and implementation of risk. ISO 31000:2009.

ISO/IEC 27001. **Tecnologia da Informação** – Técnicas de Segurança – Sistemas de Gerenciamento de Segurança da Informação – Necessidades, ISO/IEC. 2005.

ISO/IEC 27002 : **Information technology - Security techniques -** Code of practice for information security management - Redesignation of ISO/IEC 17799:2005.

ISO/IEC 27005 **Information technology -- Security techniques** - Information security risk management, 2008.

NIST SP 800-30. **Risk Management Guide for Information Technology Systems**.

Integrated Framework - **Guidance on Monitoring Internal Control Systems**. Ed.: Committee of Sponsoring Organizations of the Treadway Commission.

Standards Australia International Ltd, 2004. Handbook.

NIST SP 800-30 **Risk - Management Guide for Information Technology Systems**. Ed.: NIST.

ZWICKER, R.; Souza, C. A. de; VIDAL, A. G. da R.; SIQUEIRA, J. de O. **Grau de informatização de empresas**: um modelo estrutural aplicado ao setor industrial do estado de São Paulo. **RAE-eletrônica**, v. 6, n. 2, art. 13, jul./dez. 2007.