NORMA ABNT NBR ISO/IEC 27.005
GESTÃO DE RISCOS DA SEGURANÇA DA INFORMAÇÃO COMO BASE PARA A GESTÃO DE RISCOS CORPORATIVOS

Maurício Roncato Piazza

Resumo

A norma ABNT NBR ISO/IEC 27.005 Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação, tem papel fundamental na GRSI (Gestão de Riscos de Segurança de Informação). Seu passo a passo, fornece condições de geral implementação em uma organização que tem como *core* a Tecnologia da Informação, e até mesmo para um nível departamental relacionado a TI. A visão abrangente desta obra expande sua aplicabilidade para as demais companhias que necessitem de uma implantação de gestão de riscos corporativos, desde que haja uma adaptação em relação à definição de critérios, e consenso geral na organização, seu uso pode ser de extremo sucesso, incluindo mudança de cultura organizacional, tratativa com as pessoas envolvidas e divulgação dos seus conceitos.

Definições e termos utilizados

Riscos de segurança da informação: a possibilidade de uma ameaça explorar vulnerabilidade da segurança da informação.
Identificação de riscos: processo para localizar, listar e caracterizar os riscos.
Mitigação do risco: ações para reduzir a probabilidade de ocorrência do risco.
GRSI: Gestão de Riscos de Segurança de Informação.
SGSI: Sistema de Gestão da Segurança da Informação.

Abstract

The standard ISO / IEC 27005 Information technology - Security techniques - Management of information security risks, has a fundamental role in GRSI (Risk

Management Information Security). Your direction provides general conditions of implementation in an organization that has as its core Information Technology, and even for a departmental level related to IT. A comprehensive overview of this work expands its applicability to other companies requiring a deployment of enterprise risk management, provided there is an adjustment in respect of the definition criteria, and general consensus in the organization, their use can be extremely successful, including changing organizational culture, dealings with the people involved and disclosure of your concepts.

Definitions and terms used

Information security risks: the possibility of a threat exploiting vulnerability of information security.
Risk Identification: Process to find, list and characterize the risks.
Risk Mitigation: actions to reduce the likelihood of the risk occurring.
GRSI: Risk Management of Information Security.
SGSI: Management System of Information Security.

Introdução

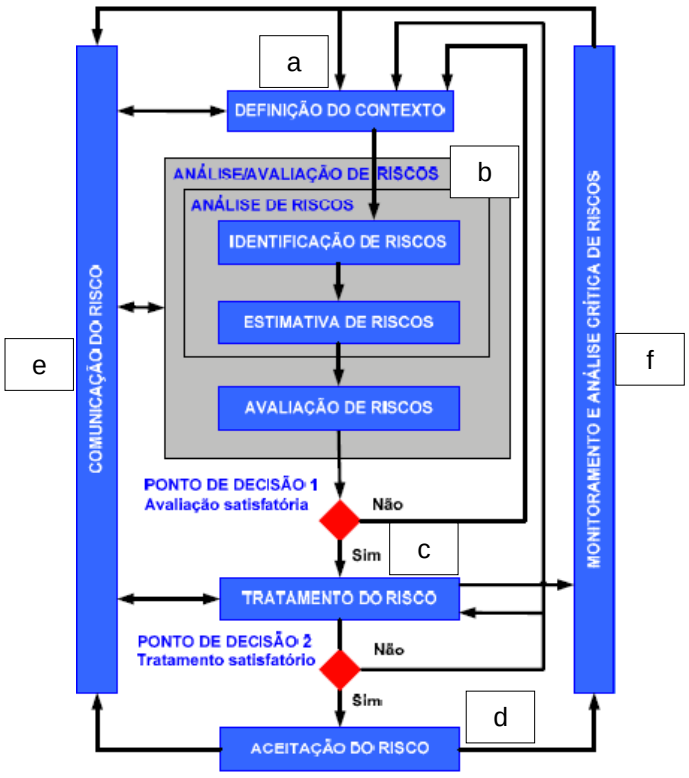
Este artigo tem como premissa introduzir o conceito sobre a norma ABNT NBR ISO/IEC 27.005 Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação, bem como oferecer um juízo crítico de sua aplicabilidade na gestão de riscos corporativos.

Sua abrangência e detalhamento supõe a utilização em diversos ramos de atividade e diferenciadas organizações, onde, apesar de ser uma norma com total relação à segurança da informação, em seu contexto ficam claros os objetivos que tende a alcançar.

Norma ABNT NBR ISO/IEC 27.005

Para um breve entendimento sobre a norma de GRSI (Gestão de Riscos de Segurança de Informação), podem-se identificar diversos fatores que contribuem para a Gestão de Riscos de um modo geral, são conceitos que normalmente podem ser adaptados à estrutura de uma organização com qualquer *core*, ou seja, qualquer que seja o seu negócio.

No Framework da norma ABNT NBR ISO/IEC 27.005, demonstrado a seguir, tem-se um panorama da aplicabilidade de suas etapas e desenvolvimento dentro da GRSI.



O processo de gestão de riscos de segurança da informação no seu framework consiste em:

a) definição do contexto;
b) análise/avaliação de riscos;
c) tratamento do risco;

d) aceitação do risco;
e) comunicação do risco; e
f) monitoramento e análise crítica de riscos.

Definição do contexto

Deve-se levar em consideração a avaliação da estrutura da organização, podendo ser ou não alinhada com a área de gestão de riscos corporativos. Conhecer a organização, seu negócio e estratégias, sua missão, visão e valores são pontos basais para definir a aceitação dos níveis de riscos e dar critérios para as suas tratativas.

Análise e Avaliação de riscos da segurança da informação

Dentre muitas definições o risco é uma condição existente, em uma organização ele sempre está presente acompanhado de fatores, tais fatores influenciam o risco de maneira positiva ou negativa. É importante saber que o risco é uma possibilidade, situação que difere ao perigo, pois, perigo é a origem de uma perda. Portanto, na analise e avaliação de riscos, os fatores e os próprios riscos devem ser tratados para que os perigos não se concretizem.

Para tanto, é fundamental que os riscos sejam identificados, quantificados ou descritos qualitativamente, tendo priorização conforme critérios de avaliação em relevância as definições da organização, através de sua alta gestão. Bem como, conhecer as ameaças e vulnerabilidades da organização, que contribui para uma melhor priorização das ações a serem implementadas em relação à mitigação dos riscos.

Outro fator importante é a identificação dos ativos. Um ativo é algo valoroso para organização, portanto, necessita de proteção. De maneira detalhada os ativos devem ser conhecidos e atestados com as informações suficientes para compor a avaliação de riscos.

Tratamento e aceitação do risco de segurança da informação

O tratamento de riscos consiste em algumas opções que devem ser bastante claras para a organização e sua direção. Podendo ser:

a) Mitigação do risco: Reduzir o risco em níveis menores até deixa-lo aceitável para a organização;

b) Retenção do risco: Trabalhar com o risco existente por ele estar dentro de um nível de criticidade registrado e aceito conforme política da organização;

c) Evitar o risco: Eliminar o risco, normalmente pode ocorrer quando a criticidade deste risco é muito elevada, e o trabalho para mitigação seja muito oneroso em processos e financeiramente, tal condição faz com que a organização elimine o processo, evitando assim o risco por inteiro, deve sempre ser uma decisão estratégica tomada pela alta direção;

d) Transferência do risco: Consiste em transferir o risco para outra entidade ou empresa, como por exemplo, fazer seguro em determinados casos.

A aceitação do risco, consiste em entender e trabalhar com ele independente do seu nível de criticidade, onde o impacto e a probabilidade de ocorrência devem estar registrados, e ser de conhecimento total da alta administração e responsáveis dá área ou processo que possui o risco.

Matriz de vulnerabilidade

Uma matriz sugerida pela ABNT NBR ISO/IEC 27.005, demonstra a relação entre probabilidade de ocorrência de um evento e o impacto estimado para o negócio. A probabilidade de um cenário é dada pela probabilidade de uma ameaça vir a explorar uma vulnerabilidade. A matriz relaciona o impacto ao negócio, relativo ao cenário de incidente. O risco resultante é medido em uma escada de 0 a 8, e pode ser avaliado tendo como base os critérios para a aceitação do risco definidos

pela organização. Essa escala de risco pode também ser convertida em uma classificação simples, mais genérica, do risco, como por exemplo:

• Baixo Risco: 0-2
• Médio Risco: 3-5
• Alto Risco: 6-8

Na Matriz de vulnerabilidade, percebemos as pontuações indicando os níveis mais críticos em relação ao impacto e probabilidade.

	Probabilidade do cenário de incidente	Muito baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito Alta (Freqüente)
Impacto ao Negócio	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Comunicação do risco de segurança da informação

Compartilhar as informações sobre o SGSI, informar os envolvidos sobre os riscos e perigos, gerar um consenso sobre o tratamento dos riscos e as decisões tomadas, enfim, uma comunicação eficaz é muito importante para assegurar um bom entendimento do por que algumas decisões estão sendo tomadas.

Monitoramento e análise crítica dos fatores de risco

Aqui é importante ressaltar que os riscos não são elementos estáticos, os riscos têm características mutáveis. Os fatores de riscos sofrem interferências externas, internas, nos processos, das pessoas e etc. Portanto um risco que não é crítico hoje pode ser amanhã, ou ao contrário, um risco elevado hoje pode deixar de ser assim na próxima avaliação, diante deste cenário um monitoramento constante ajuda a organização a não ser surpreendida em relação ao mapeamento dos riscos.

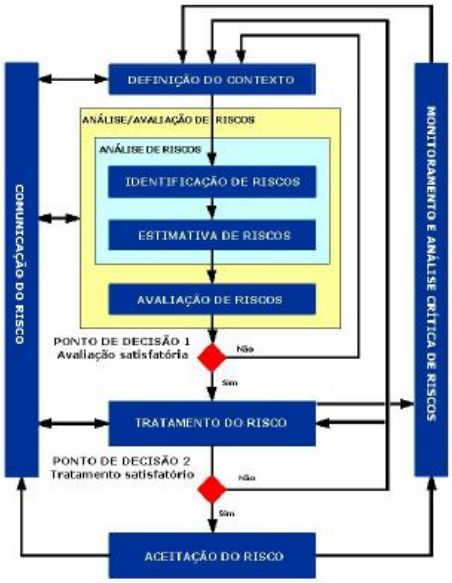
A Norma ABNT NBR ISO/IEC 27.005 para a gestão de Riscos Corporativos

Todo conteúdo da ISO 27.005, abrange e atende os requisitos para a Gestão de Riscos Corporativos, suas premissas e entendimentos, tem norteamento para uma abrangente avaliação, incluindo uma completa estrutura de Gestão de Riscos.

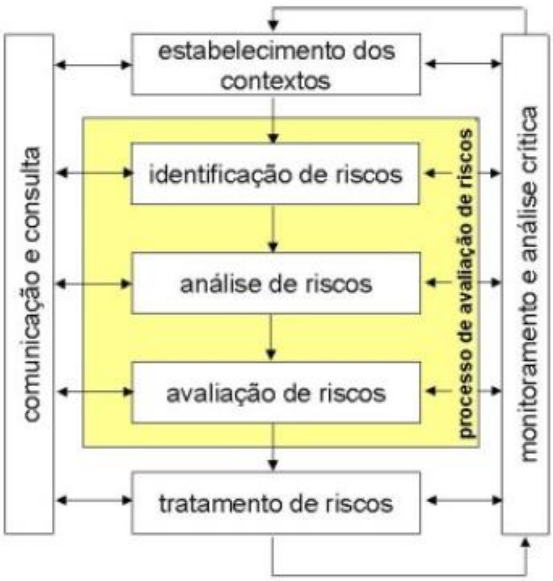
Entre as principais premissas da gestão de riscos corporativos, muitas são citadas com propriedade na ISO 27.005, temos a analise do contexto da organização, a analise dos riscos, a avaliação dos ativos e o tratamento dos riscos mais críticos. Para tanto, é imprescindível o conhecimento da organização e seu negócio, além de procurar informar e demonstrar aos membros da organização os corretos conceitos sobre a matéria de gestão de riscos. Ou seja, a ISO 27.005, também apoia e contribui para garantir a continuidade do negócio e, visa diretamente minimizar os riscos no seu conceito principal, os riscos de segurança da informação, com extensão para os riscos de uma variada gama de negócios em uma organização.

Fazendo uma analogia com a ISO 31.000, que versa diretamente sobre a Gestão de Riscos Corporativos, percebe-se que estas normas estão bem próximas e possuem grande afinidade entre si. Conforme comparativo de visão geral dos processos, nas duas normas fica claro o entendimento em relação as suas equidades. Veja a demonstração abaixo:

ISO 27.005



ISO 31.000



Apesar da gestão de riscos no Brasil, ser uma atividade relativamente recente, ou seja, considerada uma nova variante dentro do processo de uma organização, ela surgiu faz muito tempo, desta forma vem sendo aprimorada de maneira evolutiva no mundo corporativo. Após alguns acontecimentos internacionais como, fraudes em grandes empresas e bancos, ataques terroristas, catástrofes naturais e pandemias, o gerenciamento de risco tomou forma e passou a ser de artigo de primeira utilidade nos países desenvolvidos, sendo utilizado pelos governos, órgãos públicos e privados e grandes organizações. O mesmo ocorreu com a gestão de riscos da segurança da informação, que para garantir a operacionalidade dos recursos de TI, os profissionais desta área se viram obrigados a garantir seus ativos e suas informações sempre à disposição.

O mesmo vem ocorrendo com os administradores e empresários Brasileiros, os exemplos das multinacionais com cultura de gestão de riscos instaladas no nosso território, toda a facilidade de acompanhar o que vem ocorrendo pelo mundo, somados aos agravantes das perdas financeiras, os desperdícios, a violência e os fenômenos naturais, tem causado grande preocupação nas organizações nacionais. O que de certa forma pode direcionar os esforços para a adoção de normas como a ISO 27.005 como base para gestão de riscos, sejam eles relacionados à tecnologia da informação ou para os demais seguimentos dentro de uma organização.

Conclusão

Conclui-se que nitidamente, independente da Norma ISO a ser utilizada, uma solução eficiente em gestão de riscos corporativos envolve conhecimento do negócio, tecnologia, e principalmente, conscientização e aculturamento da organização e dos profissionais envolvidos na gestão de riscos corporativos ou na GRSI.

O fundamento mais importante é que se reconheça o valor do elemento humano nos ambientes relacionados aos processos, uma vez que o ser humano é invariavelmente o elo mais fraco da cadeia, e sobre ele devem incidir os principais cuidados durante as fases de especificação, implementação e gestão dos riscos. Tal

cuidado poderá possibilitar o desenvolvimento de uma cultura de prevenção sistemática dos problemas, valorização dos princípios éticos e de responsabilidade no trabalho, além da própria disseminação da importância do conhecimento sobre o tema gestão de riscos corporativos.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 27005. Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

Sobre o autor

Maurício Roncato Piazza é Contador, Economista e Auditor Chefe da empresa Libbs Farmacêutica Ltda. Responsável pela Auditoria Interna e Ouvidoria, apoia no seu trabalho a gestão de Riscos Corporativos e a área de Compliance da empresa. Tem atuado com sua equipe em relação ao cumprimento dos controles internos, desenvolvimento de politicas e procedimentos e, ainda sugerindo reestruturação de inúmeros departamentos da companhia, também atua no combate a fraudes, desvios de informações e medicamentos. Na contabilidade atuou durante 15 anos na área tributária, desenvolvendo-se em planejamento tributário nos ramos de comércio, indústria e serviços.

Possui profundo conhecimento em implantação de sistemas integrados (SAP, Microsiga, RM e PLACOMP), no que tange as áreas tributárias e de finanças.

Certificado em Negociação de Suprimentos – “Negociando para Ganhar” pela WORKSHOP SEMINÁRIOS PRÁTICOS – Márcio Miranda.

Certificado em *LEAN MANUFACTURING,* pela Ótima Estratégia e Gestão Empresarial.

Certificado PERITO JUDICIAL TRABALHISTA, pela Lex Magister.

Certificado em GCN – Gestão da Continuidade de Negócios pela Brasiliano & Associados FESP/SP.

Atualmente é aluno da Brasiliano & Associados do curso de MBA – Gestão de Riscos Corporativos 11ª turma. Seu *e-mail* para contato é roncato04@gmail.com.