GESTÃO DE SEGURANÇA DA INFORMAÇÃO

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

Olá!

Nesta aula você irá compreender a Gestão de Riscos em Segurança da Informação:

1. Os conceitos básicos.

2. Como estabelecer o contexto do risco.

3. As etapas da gestão de risco.

4. A Análise e avaliação do risco.

5. O Tratamento dos riscos.

6. A Aceitação e comunicação do risco.

7. O monitoramento e revisão dos riscos.

8. Os Riscos, medidas de segurança e o ciclo de segurança.

Risco

Segundo o Guia de orientação para Gerenciamento de Riscos Corporativos do IBGC, o risco é inerente a qualquer atividade, na vida pessoal, profissional ou nas organizações e pode envolver perdas e oportunidades.Instituto Brasileiro de Governança Corporativa.

Segundo a norma ABNT NBR ISO 31000:2009- Gestão de Risco, Princípios e Diretrizes, as organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tomam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de “risco”.

Ainda segundo a norma, todas as atividades de uma organização envolvem risco. As organizações devem gerenciar o risco, identificando-o, analisando-o, e em seguida, avaliando se o risco deve ser modificado pelo tratamento do risco a fim de atender a seus critérios de risco.

Ao longo de todo esse processo, elas comunicam e consultam as partes interessadas e monitoram e analisam criticamente o risco e os controles que o modificam, a fim de assegurar que nenhum tratamento de risco adicional seja requerido.”

Como estabelecer o contexto do risco

Segundo Beal, os termos e definições do ISO guide 73, dizem respeito a todo e qualquer tipo de situação (ou evento) que constitui oportunidade de favorecer ou prejudicar o sucesso de um empreendimento. Como ele está estruturado de uma forma genérica e básico para o entendimento comum a organizações de diversos países, é necessário algumas adaptações para atender às necessidades dentro de um domínio específico.

Por exemplo, para as empresas do ramo do comércio/indústria, o risco é visto como a exposição às perdas baseada nas freqüências estimadas e custo de concorrência. Já em um organização da área de saúde, segundo a resolução CNS 196/96, o risco é visto como a possibilidade de danos à dimensão física, psíquica, moral, intelectual, social, cultural.

Diante de tantos cenários diferentes de aplicação da gestão de risco, é importante promover ajustes na terminologia adotada, alterando-a e expandindo-a na medida do necessário para tratar a questão dentro do escopo que está sendo estudada.

Alguns termos e definições:

Ativo: Tudo aquilo que tenha valor e que necessita de algum tipo de proteção ou cuidado.

Escopo: Conjunto de ativos que será coberto pelo processo de gestão de risco.

Parte envolvida: Indivíduos, grupos ou organizações que são afetados diretamente por um determinado risco.

Ameaça: Tudo aquilo que tem potencial de causar algum tipo de dano aos ativos. Podem ser: Ambiental ou humana.

Incidente: Quando uma ameaça se concretiza.

Vulnerabilidades: Criam situações que podem ser exploradas por uma ameaça, acarretando prejuízo.

Análise de vulnerabilidades: Processo de identificar as proteções existentes e ausentes, identificar falhas nas existentes e levantar dados que possam prever a efetividade desse conjunto de proteções.

Avaliação das vulnerabilidades: quando esses dados são combinados com uma lista de possíveis ameaças, gerando dados que indiquem a real probabilidade de uma ameaça se concretizar explorando as vulnerabilidades existentes.

Risco

Probabilidade de uma ameaça explorar uma (ou várias) vulnerabilidades causando prejuízos. Os riscos estão sempre associados à ocorrência de algum incidente.

Sua escala é dada por dois fatores:

- Probabilidade de ocorrência da ameaça medida através da combinação da sua freqüência com a avaliação das vulnerabilidades;
- Conseqüências trazidas pela ocorrência do incidente (impacto);

Ameaça é um elemento do risco ao qual se pode associar uma probabilidade de manifestação, cujo valor compõe o cálculo da estimativa do risco. Em muitos casos, a probabilidade associada a uma ameaça é calculada com base na frequência de ocorrência ; em outros, quando dados de frequência não estão disponíveis, a probabilidade pode ser estimada com base no grau de confiança atribuído a ocorrência.

As medidas de proteção também chamada de controles, servem para elimar ou reduzir o risco, reduzindo a probabilidade de concretização de uma ameaça, as vulnerabilidades que podem ser exploradas por essa ameaça ou os impactos advindos de incidentes que venham a se concretizar.

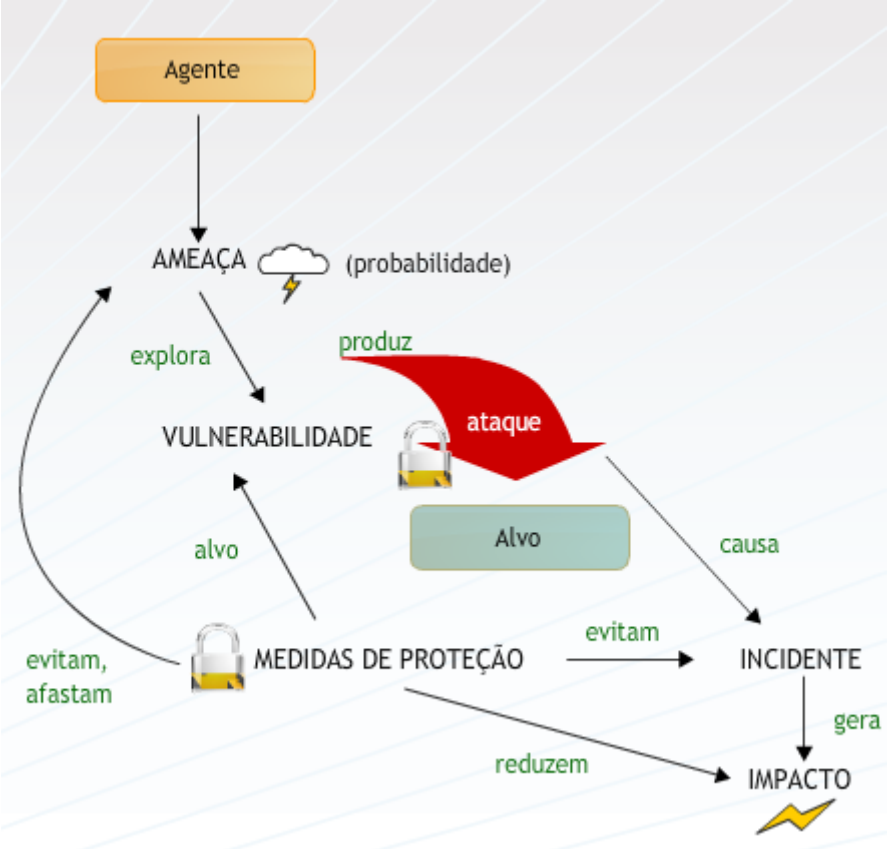
forma como um risco é visto por uma parte envolvida. Pode variar em virtude de critérios, valores, interesses e prioridades.

Você sabia?

Os risco não podem ser completamente eliminados e a porção do risco existente após todas as medidas de tratamento terem sido tomadas é chamada de risco residual.

Fique ligado

Nem sempre o risco percebido é o risco verdadeiro.



Gestão de risco

Uma das premissas básicas da segurança é o fato de que não existe segurança total ou completa. O que torna algo seguro ou não, está muito mais ligado à gerência de uma série de fatores do que à compra ou implementação de uma solução de software ou hardware definitiva. No âmbito da segurança da informação, a gestão de riscos é utilizada com o intuito de prevenir incidentes e melhorar o nível de segurança das informações sob o escopo do Sistema de Gestão de Segurança da Informação (SGSI), sendo um dos componentes mais importantes. É por meio deste processo que os riscos são identificados e tratados de forma sistemática e contínua.

Entender os riscos associados com o negócio e a gestão da informação.

Melhorar a efetividade das decisões para controlar riscos nos processos internos e externos e suas interações.

Melhorar a eficácia no controle de riscos

Manter a reputação e imagem da organização.

Melhorar a eficácia do cumprimento com os requisitos legais e regulatórios

Minimizar as possibilidades de furto de informação e maximizar a proteção de dados.

É essencial determinar o propósito da gestão de riscos a ser implementada na organização, pois ele afeta o processo em geral e a definição do contexto em particular. Esse propósito pode ser:

- Suporte a um Sistema de Gestão de Segurança da Informação (SGSI);
- Conformidade legal e a evidência da realização dos procedimentos corretos;
- Preparação de um plano de continuidade de negócios;
- Preparação de um plano de resposta a incidentes;
- Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

Você sabia?

Segundo a norma AS/NZS 4360 (**primeira norma do mundo sobre Gestão de Riscos: AS/NZS 43:602004**), podemos definir a gestão de risco como:

“Cultura, estruturas e processos voltados ao reconhecimento de oportunidades potenciais concomitantemente ao gerenciamento de seus efeitos adversos.”

E segundo a norma NBR ISO 27002:

“Conjunto de práticas, procedimentos e elementos de suporte que utilizamos para gerenciar o risco”.

Primeira norma do mundo sobre Gestão de Riscos: AS/NZS 4360:2004

Etapas da Gestão de Risco

A gestão de riscos contempla uma série de atividades relacionadas à forma como uma organização lida com o risco e utiliza o ciclo do PDCA (o ciclo PDCA, ciclo de Shewhart ou ciclo de Deming, é um ciclo de desenvolvimento que tem foco na melhoria contínua. Fonde: Wikipedia), que nos permite entender a gestão do Risco como um processo contínuo:

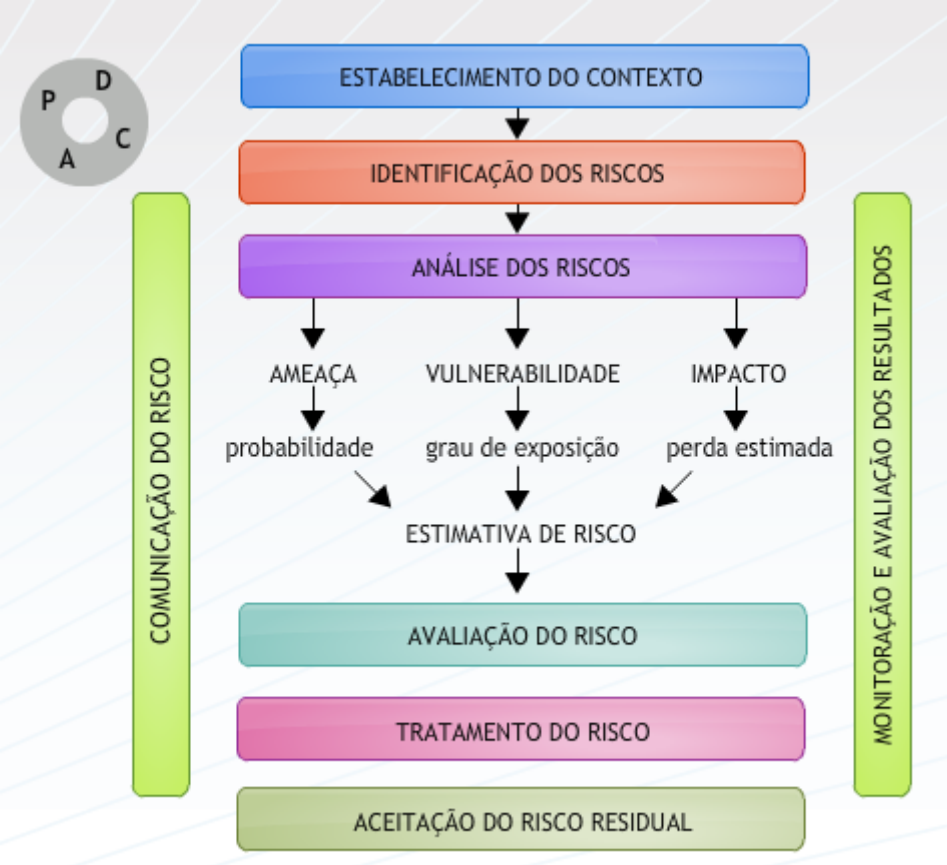
Saiba mais

Clique aqui e saiba mais sobre as Estapas de Gestão de Risco

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/doc01_aula06_gsi.pdf

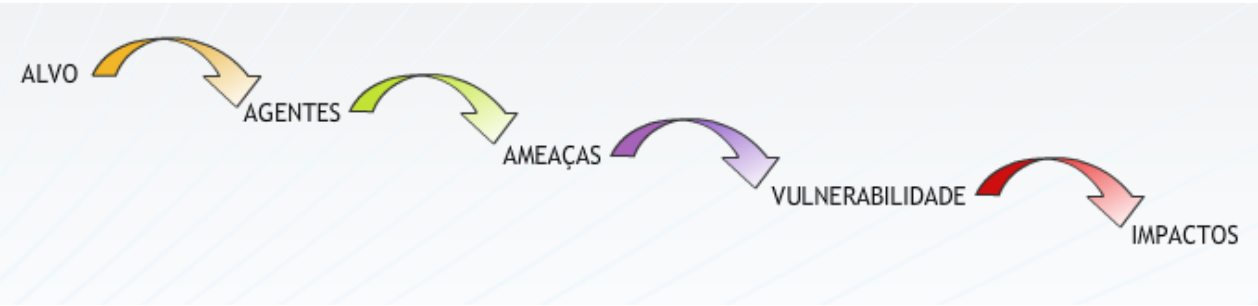
Etapas da Gestão de Risco

Uma forma mais detalhada e que facilita a análise do processo de gestão de risco é apresentada a seguir, cobrindo todo o ciclo de vida do risco, desde a sua identificação até a sua comunicação às partes envolvidas:



Análise e avaliação dos riscos

Cobre todo o processo de identificação das ameaças e estimativa de risco. Inicia-se com a identificação dos riscos e seus elementos, já estudados anteriormente:



A decomposição do risco (na figura anterior) e seus componentes e a posterior avaliação da "características mesuráveis" desses componentes levam a uma estimativa do valor do risco, que pode depois ser comparado com uma referência para que sua relevância seja determinada, possibilitando a tomada de decisão quanto a aceitá-lo ou tratá-lo.

Análise e avaliação dos riscos:

Existem várias metodologias desenvolvidas para a realização de análise e avaliação do risco, que costumam ser classificadas como:

Método Quantitativo:

A métrica é feita através de uma metodologia na qual tentamos quantificar em termos numéricos os componentes associados ao risco. O risco é representando em termos de possíveis perdas financeiras.

Os métodos quantitativos costuma ser vistos com cautela pelos estudiosos devido à dificuldade de obtenção de resultados representativos e pela sua complexidade.

Método Qualitativo:

Em vez de usarmos valores numéricos para estimar os componentes do risco, trabalhamos com menções mais subjetivas como alto, médio e baixo. O que torna o processo mais rápido. Os resultados dependem muito do conhecimento do profissional que atribuiu notas aos componentes do risco que foram levantados. Vários métodos de avaliação qualitativa do risco utilizam questionários e matrizes de risco como a apresentada abaixo:

Gravidade do impacto	Probabilidade de ocorrência do incidente					
	F Impossível	E Improvável	D Remota	C Ocasional	B Provável	A Frequente
I Catástrofe			///////	XXXXXX	XXXXXX	XXXXXX
II Alta				///////	XXXXXX	XXXXXX
III Média					///////	///////
IV Baixa						

XXXXXX: Imperativo reduzir os riscos /////// : Medidas de proteção adicionais requeridas

Em branco: As medidas básicas de proteção adotadas pela organização são consideradas suficientes para manter os riscos em níveis aceitáveis.

Tratamento dos riscos

Fase em que selecionamos e implementamos medidas de forma a reduzir os riscos que foram previamente identificados. Existem várias classificações disponíveis para as medidas de proteção. Segundo Beal, uma classificação possível é:

Medidas preventivas

Controles que reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente/ativo; sistema, reduzindo assim a probabilidade de um ataque e/ou sua capacidade de gerar efeitos adversos na organização.

Medidas corretivas ou reativas

Reduzem o impacto de um ataque/incidente. São medidas tomadas durante ou após a ocorrência do evento.

Métodos detectivos

Expõem ataques/incidentes e disparam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita.

Aceitação do risco

Ocorre quando o custo de proteção contra um determinado risco não vale a pena. Aceitar um risco é uma das maneiras de tratá-lo.

Comunicação do risco

Divulgação de informações sobre os riscos que foram identificados, tenham eles sido tratados ou não, a todas as partes envolvidas que precisem ter conhecimento a respeito deles. Uma das melhores formas de se comunicar os riscos de maneira genérica, com o intuito de notificar os colaboradores a respeito deles, é desenvolver e manter campanha de conscientização de segurança.

A gestão do risco precisa ser desenvolvida de forma permanente e iterativa, para que mudanças nos sistemas e na forma como são usados, no perfil dos usuários, no ambiente, na tecnologia, nas ameaças, nas vulnerabilidades e em outras variáveis pertinentes não tornem obsoletos os requisitos de segurança estabelecidos. Esta etapa consiste na verificação contínua, supervisão, observação crítica ou determinação da situação visando identificar alteração no nível de desempenho requerido ou esperado dos riscos.

Riscos, medidas de segurança e o ciclo de segurança

Segundo Sêmola, para um melhor entendimento da amplitude e complexidade da segurança, é comum estudarmos os desafios em camadas ou fases para tornar mais claro o entendimento de cada uma delas. Estas fases são chamadas de barreiras e foram divididas em seis. Cada uma delas tem uma participação importante no objetivo maior de reduzir os riscos, e por isso, deve ser dimensionada adequadamente para proporcionar a mais perfeita integração e interação:

Barreira1: Desencorajar

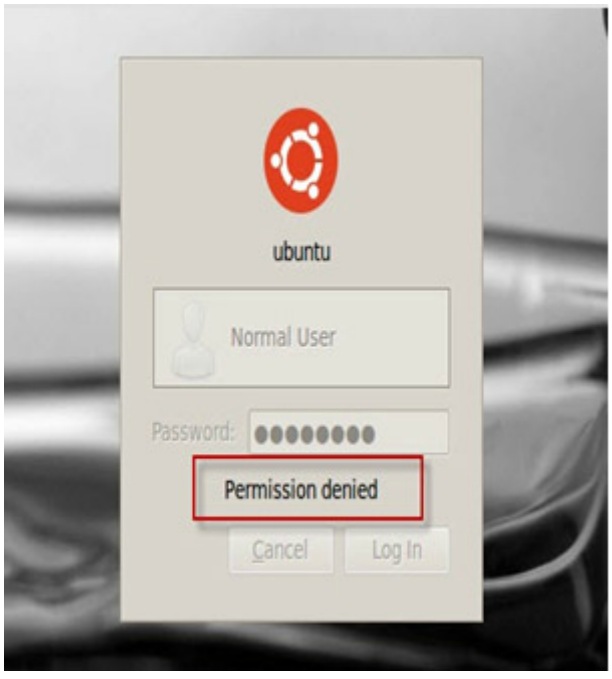
Esta é a primeira das cinco barreiras de segurança e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou podem perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou humanos. A simples presença de uma câmara de vídeo, mesmo falsa, de um aviso de existência de alarmes, já são efetivos nesta fase.

Barreira 02: Dificultar

O papel desta barreira é complementar à anterior através da adoção efetiva dos controles que irão dificultar o acesso indevido. Podemos citar os dispositivos de autenticação para acesso físico, por exemplo.

Barreira 03: Discriminar

Aqui o importante é se cercar de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e banco de dados.



Barreira 04: Detectar

Esta barreira deve munir a solução de segurança de dispositivos que sinalizem , alertem e instrumentem os gestores da segurança na detecção de situações de risco. Seja uma tentativa de invasão ou por uma possível contaminação por vírus, por exemplo.

Barreira 05: Deter

Esta barreira representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, são bons exemplos.

Barreira 06: Diagnosticar

Apesar de representar a última barreira no diagrama, esta fase tem um sentido especial de representar a continuidade do processo de gestão de segurança da informação. Cria o elo de ligação com a primeira barreira, criando um movimento cíclico e contínuo. Devido a estes fatores é a barreira de maior importância. Deve ser conduzida por atividades de análise de risco que consideram tanto os aspectos tecnológicos quanto os físicos e humanos.

Equação do risco

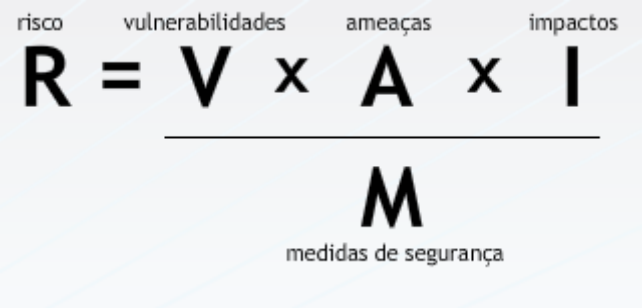
Cada negócio, independente de seu segmento de mercado possui dezenas ou centenas de variáveis que se relacionam direta e indiretamente com a definição de seu nível de risco.

O risco é a probabilidade de que agentes, que são as ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impacto nos negócios.

Estes impactos são limitados por medidas de segurança que protegem os ativos, impedindo que as ameaças explorem as vulnerabilidades, diminuindo , assim o risco.

Por melhor que estejam protegidos os ativos, novas tecnologias, mudanças organizacionais e novos processos podem criar vulnerabilidades ou identificar e chamar a tenção para as já existentes. Além disso, novas ameaças podem surgir e aumentar significativamente a possibilidade de impactos no negócio.

É fundamental que todos tenhamos a consciência de não existe segurança total, e por isso, devemos estar bem estruturado para suportar mudanças nas variáveis da equação, reagindo com velocidade e ajustando o risco novamente aos padrões pré-especificados como ideal para o negócio e lembrando que sempre será necessário avaliar o nível de segurança apropriado para cada momento vivido pela empresa.



O que vem na próxima aula

Tema: Segurança da Informação Segundo a NBR ISO/IEC 27002 (antiga ISO 17799)

•Assunto 1: Conceitos de segurança da informação

•Assunto 2: Normas de segurança da Informação

•Assunto 3: Gestão de Riscos segundo a NBR 27001

•Assunto 4: Política de segurança

•Assunto 5: Segurança Organizacional

•Assunto 6: Classificação e controle dos ativos

•Assunto 7: Segurança em pessoas

•Assunto 8: Segurança física e do ambiente

•Assunto 9: Gerenciamento das operações e comunicações

•Assunto 10: Controle de Acesso

•Assunto 11: Desenvolvimento e Manutenção de Sistemas

•Assunto 12: Gestão de incidentes de segurança da informação

•Assunto 13: Gestão da Continuidade do Negócio

•Assunto 14:Conformidade

CONCLUSÃO

Nesta aula, você:

- Aprendeu sobre a Gestão de Riscos em Segurança da Informação.
- Estudou os conceitos básicos e como estabelecer o contexto do risco.
- Compreendeu as etapas da gestão de risco (análise, tratamento, aceitação, comunicação, monitoramento e revisão do risco).
- Conhecemos as barreiras de segurança e a equação do risco.