

Gestão/Planejamento Corporativo de Segurança da Informação

Alexandre Marin Tuxen, Jean Cleber Correia, José Mario Souza, Thiago Bueno Nahum

Resumo — As empresas já perceberam que o domínio da tecnologia como aliado para o controle da informação é vital. O controle da informação é um fator de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão. A informação é substrato da inteligência competitiva; deve ser administrada em seus particulares, diferenciada e salvaguardada.

Palavras Chave — Gestão, Implementação de Segurança da Informação, Mecanismos de SI.

I. INTRODUÇÃO

Atualmente as empresas estão integrando todos os elementos da cadeia produtiva, através de conexões híbridas, e compartilhando remotamente informações estratégicas com os clientes internos, que com seus dispositivos móveis acessam a rede e aos dados corporativos.

Tudo isso aparentemente agrega valor e se converte em benefícios, porém, os executivos têm dificuldades em perceber o retorno sobre o investimento em segurança, e as empresas ainda não estão amparadas por um planejamento corporativo de segurança da informação, capaz de minimizar os riscos de vazamentos, invasões, roubos, acessos indevidos, retrabalho, perda de produtividade, perdas financeiras e ainda prejuízos à imagem.

O comprometimento com a segurança deve surgir do mais alto nível da organização, alavancado pelo reconhecimento dos sérios problemas que poderiam resultar da divulgação, modificação ou indisponibilidade da informação. Esse comprometimento tende a ser expresso em uma política formal de segurança, estabelecida no contexto dos objetivos e funções organizacionais.

II. CONCEITOS DO PLANEJAMENTO CORPORATIVO DE SEGURANÇA DA INFORMAÇÃO

As organizações necessitam da informação para tomar decisões em busca de seu objetivo. Isto mostra o quão poderosa é a informação. Sem ela não há estratégias, não há mudanças ou até mesmo não existiria a empresa. Uma consequência natural da importância da informação é a extrema vulnerabilidade a que cada empresa se expõe caso haja perda de dados vitais, como plantas de projetos, planilhas de custos, documentos contábeis, financeiros, etc. Quanto maior for a organização maior será sua dependência da informação (TechNet, 2007).

Devemos tratar a informação como um ativo da empresa com a mesma importância que qualquer outro bem palpável. Por isso, deve ser protegido contra roubo, problemas ambientais, vandalismo, dano acidental ou provocado. Quanto mais interconectada for uma empresa, maior será a complexidade dos sistemas por onde trafegam e são armazenadas as informações e, conseqüentemente, maior será a preocupação com o nível de segurança a ser implantado a fim de garantir a confidencialidade, confiabilidade, disponibilidade e integridade da informação que ela detém. A segurança da informação é o fator crítico de sucesso, elemento que viabiliza aplicações, sendo fundamental para garantir a integridade, confidencialidade e disponibilidade da mesma, quando se manuseia, armazena, transporta e descarta informações. Ela tem como objetivo o conjunto de controles e processos que visam preservar os dados que trafegam ou são armazenados em qualquer meio. As modernas tecnologias de transporte, armazenamento e manipulação dos dados, trouxeram enorme agilidade para as empresas, mas, ao mesmo tempo, trouxeram também novos riscos. Ataques de crackers (black hat hackers), de engenharia social, vírus, worms, negação de serviço, espionagem eletrônica são noticiadas pela imprensa todos os dias. Diante deste cenário, a segurança da informação torna-se imprescindível para as organizações, sejam elas do setor público ou privado (TechNet, 2007).

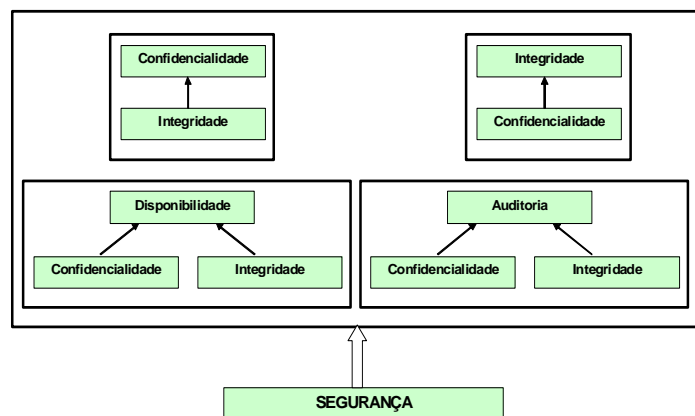


Figura1: Princípios para política de segurança

Com uma política de segurança da informação bem formatada, todos os processos da empresa ficam menos suscetíveis ao extravio de informações por responsáveis internos e externos, além de otimizar todos os processos e diminuir prejuízos por falhas ocasionais. A política de segurança da informação é o ponto de partida para o gerenciamento dos riscos associados aos sistemas de informação ou aos processos da empresa, que conseqüentemente irá diminuir as vulnerabilidades que a empresa apresenta (TechNet, 2007).

III. AS DIFICULDADES PARA IMPLEMENTAR UMA GESTÃO DA SEGURANÇA DE INFORMAÇÃO E SEUS DESAFIOS

Desafios

- Gerenciar riscos operacionais com investimentos alinhados aos objetivos do negocio.
- Manter a organização segura (redes, sistemas, informações), respondendo aos incidentes em tempo hábil.
- Seguir padrões de boas praticas e cuidados exigidos pelo mercado (fornecedores, parceiros e clientes).
- Atender as exigências legais e regulamentares (conformidade), alinhadas com as estratégias da organização.

Como superar estes desafios

Todas essas dificuldades estão atreladas ao mercado, ou seja não conseguimos viver sem elas, portando nao existe uma receita de bolo, mas alguns pontos importantes podem ser trabalhados com o objetivo de ajudar neste desafio, como, por exemplo:

- Conscientizar a alta direção
- Saber quando, onde e no que investir
- Dar suporte as ações de TI, de forma a proteger o negocio da organização
- Atender aos requisitos socioeconômicos e culturais.
- Possuir profissionais qualificados (avanço de TI)
- Evitar priorização de outras atividades
- Quebrar o paradigma de que SI é um processo burocrático e adiável, principalmente em relação aos usuários finais.

Sucesso na Implantação da GSI

Alguns itens são pontos-chaves para aumentar a probabilidade de sucesso na implantação de um GSI.

- Estabelecer linguagem comum entre a direção, o corpo executivo e as gerencias.
- Organizar e planejar a segurança alinhada a estratégia da organização
- Estabelecer política aderente aos requisitos legais, conforme os riscos identificados
- Implantar processos com nível de maturidade coerente com a necessidade de gerencias riscos e segurança da informação.
- Estruturar controles (frameworks) de segurança aderentes a política, aos objetivos do negocio e aos requisitos legais e regulatórios
- Monitorar a eficácia e o progresso de segurança da informação por meio de indicadores dos processos (métricas).

IV. UM MODELO DE IMPLANTAÇÃO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Conforme (Stoneburner, 2001), o modelo de segurança é descrito na próxima figura que mostra os serviços preliminares e os elementos usados para suportar e executar a segurança da tecnologia de informação, junto com seus

relacionamentos preliminares. O modelo classifica também os serviços de acordo com sua finalidade preliminar como segue:

1. Suporte – Serviços genéricos para a maioria das atividades na segurança da informação.
2. Prevenção – Estes serviços focalizam em impedir que ocorra uma falha na segurança.
3. Detecção e Recuperação – Focalizam na detecção e recuperação no caso de uma falha na segurança.

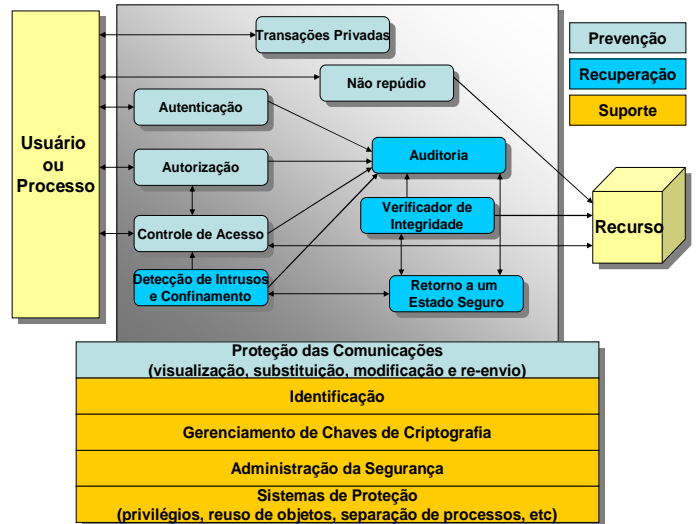


Figura 2: Modelo para implantação de GSI

Definição dos Serviços ou Mecanismos

Os serviços de suporte são, por sua natureza, persuasivos e inter-relacionados com muitos outros serviços:

1. Identificação – Para que sejam executados outros serviços, é necessário que os assuntos e objetos sejam identificados. Este serviço fornece a capacidade para identificar usuários, processos e recursos.
2. Gerenciamento de Chaves de Criptografia – As chaves de criptografia devem ser seguramente gerenciadas, para prover funções criptográficas implementadas em outros serviços.
3. Administração da Segurança – As diversas camadas de segurança precisam de administradores para instalações específicas e controles do ambiente operacional.
4. Sistemas de Proteção – Representam a qualidade das implementações de segurança adotadas. São à base de confiança do sistema de segurança.

Os serviços de prevenção visam impedir que ocorram quebras na segurança:

1. Proteção das Comunicações – Em sistemas distribuídos, os objetivos de segurança somente são obtidos se os sistemas de comunicação são altamente confiáveis. A proteção das comunicações garante os serviços de integridade, disponibilidade e confidencialidade das informações em trânsito.
2. Autenticação – Este serviço provém os meios para verificar a identidade de um sujeito ou objeto.
3. Autorização – Especifica e habilita o gerenciamento das ações que podem ser realizadas dentro de um sistema.
4. Controle de Acesso – Verificar as permissões que um determinado sujeito ou objeto têm sobre o sistema.

5. Não repúdio – Este serviço é executado tipicamente no ponto da transmissão ou da recepção, pois o objetivo é assegurar de que os remetentes não possam negar de ter emitido a informação e os receptores não podem negar a de ter recebido-as.
6. Transação Privada – Protege contra a perda da privacidade no que diz respeito às transações que estão sendo executadas por um indivíduo.

Como nenhum conjunto de medidas de prevenção é perfeito, é necessário que falhas de segurança sejam identificadas e possam ser tomadas ações para reduzir seu impacto:

1. Auditoria – A auditoria é importante para a segurança, pois é através dela que será possível detectar e recuperar as informações após a realização de algum ato indesejado.
2. Detecção de Intrusão e Confinamento – A detecção de situações inseguras é essencial para respostas oportunas. Se uma falha de segurança não for detectada, não será possível iniciar os procedimentos de resposta e confinamento de forma eficaz.
3. Verificador de Integridade – Essencial para identificar uma potencial corrupção da informação ou sistema.
4. Retorno a um estado seguro – Capacidade do sistema retornar (rollback) a um estado salvo caso tenha havido uma falha de segurança.

O modelo conforme os princípios da segurança

A implementação da disponibilidade e da integridade são obtidas através do controle e identificação das pessoas e alterações não autorizadas, e a capacidade do sistema ser recuperado.

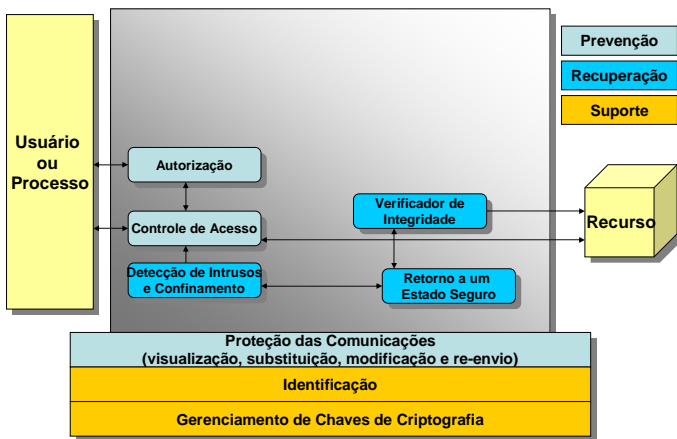
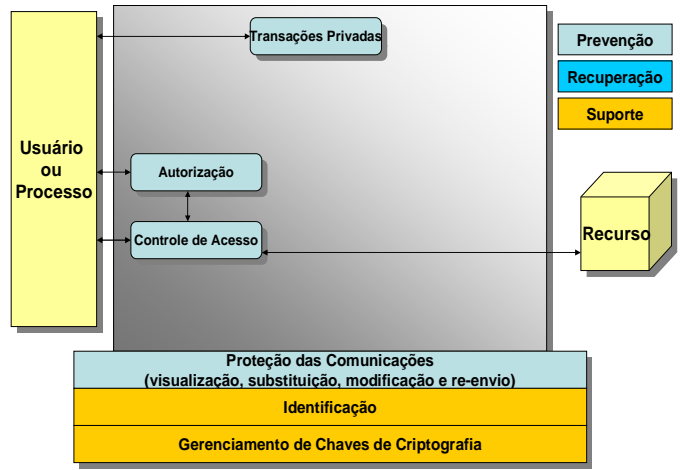
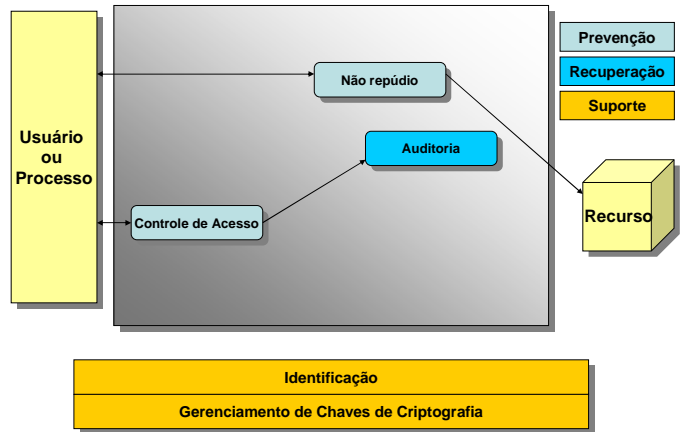


Figura 3: Implementação da disponibilidade e integridade

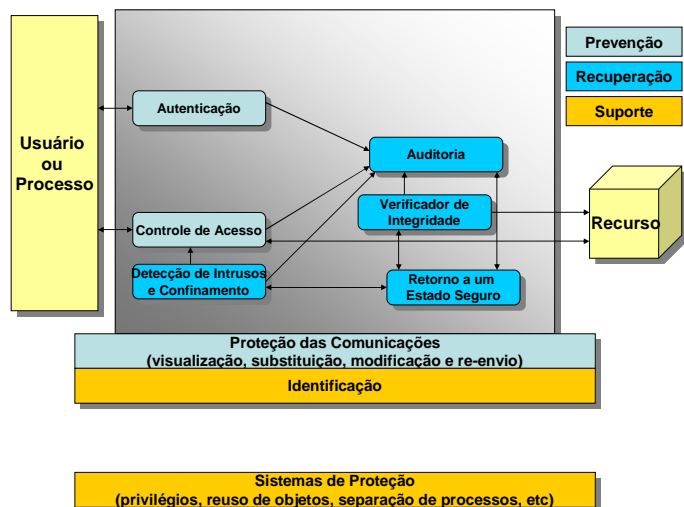
A confidencialidade é obtida através da proteção das comunicações, do controle de acesso e do uso eficaz dos mecanismos de privacidade (de forma a manter a confidencialidade).



A **auditoria** do sistema é necessária para manter a rastreabilidade das ações e o não-repúdio das transações efetuadas no sistema.



E finalmente, é possível obter a garantia (qualidade) segurança de um sistema de informação, se alguns dos serviços citados forem implementados. Esta garantia é dependente da forma e dos objetivos do sistema.



V GESTÃO DO RISCO

Gestão de Risco

O risco não é um novo problema ou uma nova terminologia; os seres humanos sempre tiveram de enfrentar (ou encarar) os riscos no seu meio ambiente, embora seu significado tenha mudado, como tem mudado a sociedade e o próprio meio onde vive. No passado, a grande preocupação estava centrada nos desastres naturais (geológicos e climatológicos) na forma de inundações, secas, terremotos e tempestades.

Após a revolução industrial, os riscos naturais foram substituídos por aqueles gerados pelo próprio homem; nos Estados Unidos, os acidentes originados dos perigos tecnológicos, representam de 15 a 20% da mortalidade humana e tem ultrapassado significativamente daqueles naturais, em termos do impacto perante a sociedade, custo e importância (Leveson et al, 1997).

Uma das ferramentas mais poderosas na gestão de riscos é o conhecimento. Na era do conhecimento, onde a informação é considerada um dos principais patrimônios de grande parte das organizações, esta deve ser tratada como tal, sendo protegida nos seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade, seguindo a linha adotada pelo Governo Federal. Neste contexto, a gestão de risco indica os caminhos e as informações que devem ser protegidas.

Conceitos Básicos

1 Risco

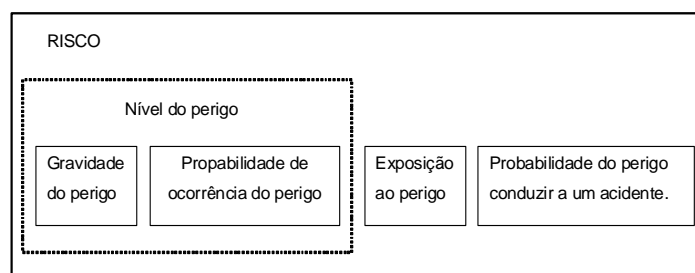
- Uma expectativa de perda expressada como a probabilidade de que uma ameaça em particular poderá explorar uma vulnerabilidade com um possível prejuízo;
- Risco pode se definido como uma medida da incerteza associada aos retornos esperados de investimentos (Duarte Júnior, 2004);
- Subentende-se por risco, o nível do perigo combinado com: (1) a probabilidade de o perigo levar a um acidente e, (2) a exposição ou duração ao perigo (algumas vezes denominado de latente); algumas vezes, o risco é limitado ao relacionamento entre o perigo e o acidente, ou seja, a probabilidade do perigo conduzir a um acidente, mas não da probabilidade do perigo ocorrer (Leveson et al, 1997);
- Conforme (Scoy, 1992), risco não é ruim por definição, o risco é essencial para o progresso e as falhas decorrentes são parte de um processo de aprendizado.

2 Avaliação ou Análise de Risco – Um processo que identifica sistematicamente

recursos valiosos de sistema e ameaças a aqueles recursos, quantifica as exposições de perda (isto é, potencialidade de ocorrer uma perda) baseadas em frequências estimadas e custos de ocorrência, e (opcionalmente) recomenda como alocar recursos às contramedidas no para minimizar a exposição total.

3 Gestão de Riscos – O processo de identificar, de controlar, e os eventos incertos, eliminando ou minimizando os que podem afetar os recursos de sistema.

O perigo tem duas importantes características: a gravidade (algumas vezes denominada de dano) e a probabilidade da ocorrência. A próxima figura ilustra o conceito do risco e o seu relacionamento com o perigo (Leveson et al, 1997).



A gravidade do perigo é definida como o pior acidente possível de ocorrer, resultante do perigo dado pelo ambiente na sua condição menos favorável. A probabilidade de ocorrência do perigo pode ser especificada tanto quantitativamente como qualitativamente; infelizmente, quando o sistema está sendo projetado e os níveis de perigo estejam sendo avaliados e pontuados, para a eliminação dos riscos potenciais, as informações necessárias para a sua avaliação nem sempre estão disponíveis; neste caso, utiliza-se de banco de dados de alguns projetos que estejam disponíveis ou ainda, baseando-se em avaliações puramente qualitativas. A combinação da gravidade somada a probabilidade de ocorrência é freqüentemente denominada de nível do perigo. A exposição ou duração de um perigo é uma componente do risco; desde que um acidente envolve uma coincidência de condições, na qual o perigo é justamente um deles, quanto maior o estado de perigo existir maiores são as chances de que outras condições ocorram, ou seja, a coincidência de condições necessárias para um acidente pode ter estatisticamente, uma baixa probabilidade, mas a probabilidade da coincidência pode dramaticamente ser aumentada, caso o perigo esteja presente por longos períodos de tempo.

Importância da Informação

Para que o processo de classificação possa ser guiado com êxito, não dependendo exclusivamente da avaliação do consultor de segurança, faz-se necessário o envolvimento dos criadores, gestores, curadores e usuários da informação. Estes devem estar habilitados a responder aos seguintes questionamentos.

A. Qual a utilidade da informação ?

Aparentemente simples, a resposta para esta pergunta deve ser consolidada base a uma visão

holística - a informação é parte de um todo muitas vezes indecomponível. A informação que suporta o departamento comercial tem diferente utilidade quando confrontada com as informações provenientes da engenharia. Quando justificar utilidade, lembre sempre dos fins: suporte, operação, estratégia, etc.

B. Qual o valor da informação ?

Existem diferentes métodos para a valoração da informação. São abordagens qualitativas, quantitativas e mistas; algumas compostas de cálculos e fórmulas herméticas - por vezes tão confusas que causam suspeita aos homens de espírito prático. Acredito que tão ou mais eficiente que o aparato analítico informatizado seja a avaliação pessoal do dono da informação. Ele saberá qualificar sua munição: qual o prejuízo caso esta informação seja revelada ou comprometida? Caso haja dificuldade em compor o resultado através de um indicador financeiro preciso, vale também a descrição através de escalas de classificação.

C. Qual a validade da informação ?

Salvo exceções justificadas, toda informação deve possuir um período de validade - manter informações desatualizadas, redundantes ou de integridade duvidosa, quando não por imposição legal, significa espaço em disco, leia-se "custo adicional".

D. Quem é responsável pela manutenção da classificação da informação ?

Em algumas organizações, o criador da informação é responsável pela sua classificação inicial nos quesitos da tríade da segurança - confidencialidade, integridade e disponibilidade. Esta classificação deve ser acompanhada pela definição de grupos, perfis ou usuários individuais com permissão para o acesso.

Na era do conhecimento, onde a informação é considerada um dos principais patrimônios de grande parte das organizações, esta deve ser tratada como tal, sendo protegida nos seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade, seguindo a linha adotada pelo Governo Federal.

Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

De ataques de hackers a epidemias de vírus, sobrecarga de sistemas a utilização indevida por parte dos funcionários, uma variedade de ameaças exige uma abordagem sistemática para identificar, quantificar, tratar e monitorar os riscos a que o negócio está sujeito.

Como analisar riscos sem estudar minuciosamente os processos de negócio que sustentam sua organização? Como classificar o risco destes processos sem antes avaliar as vulnerabilidades dos componentes de tecnologia relacionados a cada processo? Quais são os seus processos críticos? Aqueles que sustentam a área comercial, a área

financeira ou a produção? Você saberia avaliar quantitativamente qual a importância do seu servidor de web? Para cada pergunta, uma mesma resposta: **conhecer para proteger.**

Vale a pena proteger tudo ?

Partindo do pressuposto que segurança da informação requer investimentos, deve ser estimado o valor da informação a ser protegida, de forma que seja maximizado o retorno dos investimentos. É um jogo que não pára. A cada novo investimento as empresas devem tornar os resultados palpáveis, expressando-os em números.

Mas como fazer isso? Uma das técnicas disponíveis no mercado é o ROI, do inglês *Return on Investment*. Entretanto, não existe um modelo unificado para cálculo de ROI, nem o modelo ideal. Esta é uma ferramenta que parte do princípio que a empresa é capaz de mensurar todos os seus ativos e respectivos custos, com base no comportamento histórico.

É preciso conhecimento do negócio para definir o modelo que melhor se adapte a cada situação. Conhecimento do negócio – este é o ponto chave de qualquer Gestão de Riscos.

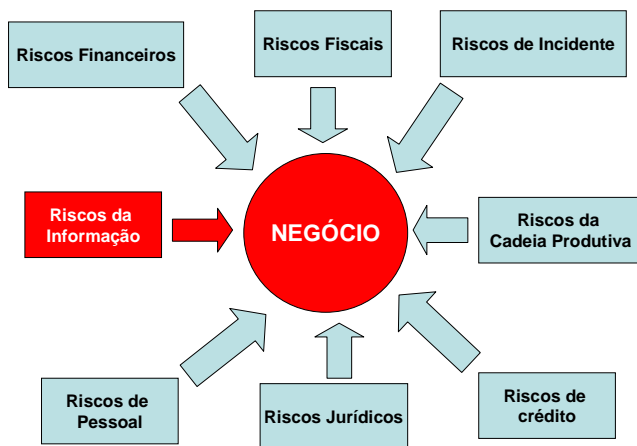
Proteger contra o quê ?

O objetivo da segurança da informação é protegê-la contra riscos. Em linhas gerais, riscos são eventos ou condições que podem ocorrer e, caso realmente ocorram, podem trazer impactos negativos para um determinado ativo (no caso, a informação).

Como pode ser percebida através da leitura da afirmação acima, a incerteza é a questão central do risco. Estamos trabalhando com hipóteses: a probabilidade de ocorrência de uma situação e o grau do dano (severidade) decorrente de sua concretização.

Mas vamos a questões mais práticas: uma vez quantificado o valor de uma informação, devem ser levantados os meios em que esta se encontra, tanto armazenado quanto em trânsito, e delimitado o escopo de atuação. Escopos infinitos caracterizam um dos erros mais comuns cometidos durante uma Gestão de Riscos.

Cabe aqui a ressalva de que nosso objetivo é proteger a informação, não o ativo que a contém. De que adianta investir na proteção de um servidor de rede, por exemplo, que não armazena nenhuma informação crítica ao negócio? Os esforços devem ser concentrados no que realmente é significativo para a empresa.



Mas como proteger uma informação ?

Inicialmente, faz-se necessário uma definição do que seja Gestão de Riscos propriamente dito. Este é um processo que objetiva identificar os riscos ao negócio de uma empresa e, a partir de critérios de priorização, tomar ações que minimizem seus efeitos. É caracterizado, sobretudo, por ter uma abordagem mais estruturada e científica. É dividido em 4 (quatro) etapas básicas:

1. Identificação dos Riscos: Como o próprio nome já diz, nessa etapa são identificados os riscos a que o negócio (o foco sempre deve ser este) está sujeito.

O primeiro passo é a realização de uma Análise de Riscos, que pode ser tanto quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança – quanto qualitativa – baseada em know-how, geralmente realizada por especialistas, que têm profundos conhecimentos sobre o assunto.

Devido a sua agilidade, geralmente as empresas tendem a adotar os modelos qualitativos, que não requer cálculos complexos. Independentemente do método adotado, uma Análise de Riscos deve contemplar algumas atividades, como o levantamento de ativos a serem analisadas, definições de uma lista de ameaças e identificação de vulnerabilidades nos ativos.

2. Quantificação dos Riscos: Nessa etapa é mensurado o impacto que um determinado risco pode causar ao negócio.

Como é praticamente impossível oferecer proteção total contra todas as ameaças existentes, é preciso identificar os ativos e as vulnerabilidades mais críticas, possibilitando a priorização dos esforços e os gastos com segurança.

Uma das ferramentas existentes no mercado é o BIA, do inglês *Business Impact Analysis*. Esta técnica consiste, basicamente, da estimativa de prejuízos financeiros decorrentes da paralisação de um serviço.

Você é capaz de responder quanto sua empresa deixaria de arrecadar caso um sistema estivesse

indisponível durante 2 horas? O objetivo do BIA é responder questões desse tipo.

3. Tratamento dos Riscos: Uma vez que os riscos foram identificados e a organização definiu quais serão tratados, as medidas de segurança devem ser de fato implementadas.

Definições de quais riscos serão tratadas ? Isso mesmo. O ROI e o BIA servem justamente para auxiliar nesta tarefa. Alguns riscos podem ser eliminados, outros reduzidos ou até mesmo aceitos pela empresa, tendo sempre a situação escolhida documentada. Só não é permitido ignorá-los.

Nessa etapa ainda podem ser definidas medidas adicionais de segurança, como os Planos de Continuidade dos Negócios – que visam manter em funcionamento os serviços de missão-crítica, essenciais ao negócio da empresa, em situações emergenciais – e *Response Teams* – que possibilitam a detecção e avaliação dos riscos em tempo real, permitindo que as providências cabíveis sejam tomadas rapidamente.

4. Monitoração dos Riscos: A gestão de Riscos é um processo contínuo, que não termina com a implementação de uma medida de segurança. Através de uma monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes.

Mas como realizar uma monitoração de segurança? O ideal é que este trabalho seja norteado por um modelo de Gestão de Segurança, que defina atribuições, responsabilidades e fluxos de comunicação interdepartamentais. Só que a realidade costuma ser bem diferente... Não são todas as empresas que possuem uma estrutura própria para tratar a segurança de suas informações.

Então a monitoração de riscos pode ocorrer numa forma mais *light*, digamos. Não é necessário todo o formalismo de uma estrutura específica, mas devem ser realizadas algumas atividades importantes, tais como:

1. Elaboração de uma política de segurança, composta por diretrizes, normas, procedimentos e instruções, indicando como deve ser realizado o trabalho.
2. Auditoria de segurança, a fim de assegurar o cumprimento dos padrões definidos e, conseqüentemente, medir a eficácia da estratégia de segurança adotada.

Um efetiva gestão de riscos necessita de alguns requisitos básicos que devem ser de conhecimento de todos os envolvidos nesse assunto. Esse conhecimento, inclusive, é uma outra dificuldade a ser vencida. Normalmente apenas algumas pessoas ficam sabendo do processo de gestão de riscos. O desejável é que todos os envolvidos tenham acesso às informações dessa gestão, considerando, evidentemente, a questão da confidencialidade da informação: acesso parcial, acesso somente de leitura, acesso para atualização, etc... Neste caso o uso de uma ferramenta adequada e

com inteligência para tratar todas as informações geradas é fundamental.

Como requisitos básicos para a de riscos, consideramos que devam existir:

Objetivos de negócio – Antes de qualquer análise de riscos, devem existir os objetivos de negócio relativos à organização ou à área organizacional em estudo. Somente podemos falar em riscos, se existem os objetivos de negócio. Cada objetivo deve ser o mais explícito possível. "Crescer o faturamento em 15% em relação ao ano passado" é muito melhor do que um genérico "aumentar o faturamento". "Garantir um tempo de resposta no ambiente computacional de no máximo três segundos" é muito melhor do que "ter um tempo de resposta que deixe o usuário satisfeito".

Riscos – Para cada objetivo de negócio definido, devem ser identificados os riscos que podem impedir que esse objetivo seja alcançado. Em uma primeira análise pode se fazer uma listagem completa de todos os riscos possíveis e imagináveis. Depois podem ser selecionados os riscos mais significativos para que o trabalho de gestão de risco tenha um custo / benefício adequado.

Ações – Para cada risco selecionado e definido como significativo para o processo de gestão de riscos, devemos identificar ações que possam minimizar a ocorrência desse risco. Essas ações podem já existir ou não.

Na medida em que esses elementos forem sendo identificados em um número crescente, temos a necessidade de avaliar a prioridade e importância de todo esse material. Mas, que parâmetros devemos tomar por base ? Quais as avaliações que devemos fazer ? Para cada um dos elementos sugerimos que sejam analisados:

- 1 Importância para o negócio – Cada objetivo deve ser avaliado sobre a sua importância para o negócio da organização.
- 2 Probabilidade de ocorrência – Os riscos devem ser analisados sob a probabilidade de sua ocorrência. Impacto no negócio – Cada ocorrência de risco traz impactos diferentes para o negócio da organização. Identificar o grau desse impacto será um dado importante para a priorização desse processo.
- 3 Grau de minimização do risco – As ações definidas para minimizar um risco possuem um grau de eficácia. Quanto mais eficazes forem, maior o poder de minimização do risco.
- 4 Esforço a ser gasto – O esforço associado para que a ação possua uma boa eficácia é um parâmetro a ser considerado. Muito esforço em ações que minimizem riscos de pequeno impacto no negócio significa um ponto de atenção.

Para se chegar aos valores desses parâmetros a serem julgadas, as organizações necessita de um processo que expresse verdadeiramente a avaliação das pessoas envolvidas. Este processo pode ser desde um

simples questionário até sessões de trabalho conduzidas por facilitadores e com apoio de softwares de decisão de grupo.

Muitos erros podem ser cometidos nesse processo de gestão de riscos. Uma forma de minimizar esses erros é considerar como fatores críticos de sucesso:

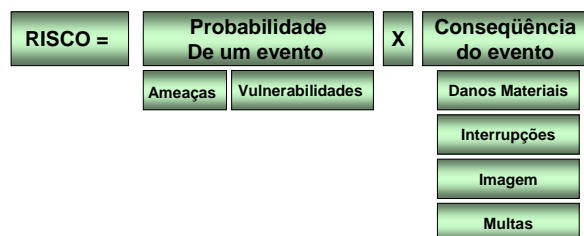
- 1 A definição do escopo da área a ser trabalhada;
- 2 A definição explícita dos objetivos de negócio;
- 3 A existência de uma abordagem metodológica;
- 4 O acesso à informação por todos os envolvidos.

A Análise

A análise de risco consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios.

Através da aplicação deste processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela organização. Proporciona também informações para que se possa identificar o tamanho e o tipo de investimento necessário de forma antecipada aos impactos na Organização causados pela perda ou indisponibilidade dos recursos fundamentais para o negócio. Sem um processo como este não são possíveis identificar a origem das vulnerabilidades, nem visualizar os riscos.

Utiliza-se como métrica as melhores práticas de segurança da informação do mercado, apontadas na norma ISO/IEC 17799. A partir destas informações faz-se possível à elaboração do perfil de risco, que segue a fórmula: (Ameaça) x (Vulnerabilidade) x (Valor do Ativo) = RISCO. Atenção: a ISO/IEC 17799 não ensina a analisar o risco, serve apenas como referência normativa.



A - Por que fazer uma análise de risco ?

Durante o planejamento do futuro da empresa, a Alta Administração deve garantir que todos os cuidados foram tomados para que seus planos se concretizem. A formalização de uma Análise de Risco provê um documento indicador de que este cuidado foi observado. O resultado da Análise de Risco dá à organização o controle sobre seu próprio destino – através do relatório

final, pode-se identificar quais controles devem ser implementados em curto, médio e longo prazo. Há então uma relação de valor; ativos serão protegidos com investimentos adequados ao seu valor e ao seu risco.

B - Quando fazer uma análise de riscos ?

Uma análise de riscos deve ser realizada — sempre — antecedendo um investimento. Antes de a organização iniciar um projeto, um novo processo de negócio, o desenvolvimento de uma ferramenta ou até mesmo uma relação de parceria, deve-se mapear, identificar e assegurar os requisitos do negócio. Em situações onde a organização nunca realizou uma Análise de Risco, recomendamos uma validação de toda a estrutura.

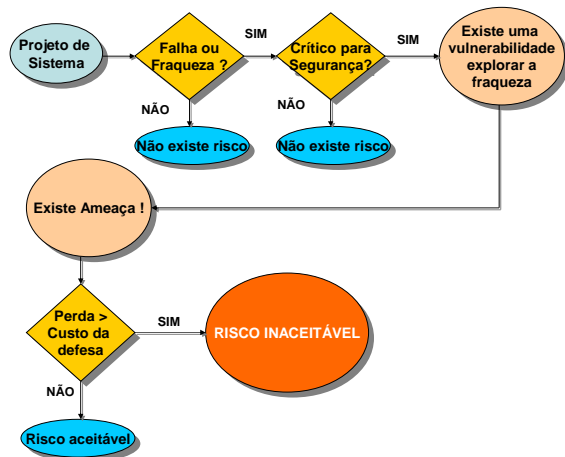
C - Quem deve participar da análise de riscos ?

O processo de análise de riscos deve envolver especialistas em análise de riscos e especialistas no negócio da empresa — esta sinergia possibilita o foco e a qualidade do projeto. Um projeto de Análise de Risco sem o envolvimento da equipe da empresa, muito dificilmente retratará a real situação da operação.

D - Quanto tempo o projeto deve levar ?

A execução do projeto deve ser realizada em tempo mínimo. Em ambientes dinâmicos a tecnologia muda muito rapidamente. Um projeto com mais de um mês — em determinados ambientes —, ao final, pode estar desatualizado e não corresponder ao estado atual da organização.

Conforme (Stoneburner, 2001), a forma para descobrir se existe algum risco em um projeto e se o mesmo é aceitável, é apresentada na próxima figura:



VI. CONCLUSÕES

Mudanças fazem parte de nossas vidas, não temos como fugir desta realidade. Também não é novidade para ninguém que em ambientes de tecnologia, as mudanças têm presença constante, ainda mais com a velocidade que surgem novas soluções ou itens de infraestrutura para suporte à gestão ou oportunizar negócios. Se as mudanças naturais que ocorrem no dia-a-dia das pessoas e organizações já geram complicações, podemos imaginar os impactos quando abordamos as infra-estruturas de tecnologia cada vez mais complexas em nossas empresas. Indisponibilidade ocasionada por alterações de sistemas, ativos de rede, servidores ou processos não modificam somente as rotinas das áreas de tecnologia, também tem impacto significativo na vida dos demais clientes internos e principalmente dos externos.

Este é um dos principais aspectos de segurança da informação que devemos preservar a disponibilidade. Qualquer profissional, do nível mais operacional ao executivo e aqueles diretamente ligados á segurança da informação, jamais poderão esquecer que é responsabilidade de sua área assegurar que um ativo esteja disponível sempre que a organização necessitar, e principalmente quando um processo de negócio depender dele, tendo como propósito a continuidade de negócios. Precisamos minimizar riscos e garantir o menor impacto possível na troca ou modificação em um ativo crítico da nossa infra-estrutura.

Cada vez mais a rotina dos profissionais é caracterizada pela pressão por resultados, redução de custos, otimização de operações e pela transparência, buscando o alinhamento da tecnologia às estratégias da empresa, ficando claro que a eficiência do plano corporativo de segurança da informação e a existência de controles adequados será vital para um processo de mudanças menos doloroso.

VII. REFERÊNCIAS

TECHNET, Microsoft. **Curso Básico de Segurança da Informação**. Microsoft, 2007.

STONEBURNER, Gary. **Underlying Technical Models for Information Technology Security**. NIST Special Publication 800-33, 2001.

