SEGURANÇA DA INFORMAÇÃO

Prof. Luis Gonzaga de Paulo

TEMA 1 – SEGURANÇA DA INFORMAÇÃO E GESTÃO DO RISCO

O risco é um fator inerente à atividade humana e os negócios. Com base nessa premissa, é necessário considerar o risco ao tratarmos de qualquer aspecto da segurança da informação, especialmente das informações sensíveis ao elevado nível de complexidade e à interdependência dos processos e dos sistemas. Somando isso à velocidade e o alcance da TIC, temos como resultado um mínimo intervalo de tempo entre uma falha, um erro ou um incidente de segurança da informação e seu impacto subsequente no ambiente dos negócios. A alta exposição das pessoas e das organizações, aliada aos fatores expostos, potencializa os efeitos negativos desses incidentes, ao mesmo tempo em que eleva o grau de severidade e a percepção de risco.

1.1 Definição de risco

Os riscos decorrem da incerteza inerente à tomada de decisões, do descuido ou despreparo (imprudência ou imperícia), da abordagem inadequada, de fatores naturais ou planejados, ou mesmo em consequência das atividades humanas. Para manter a qualidade e o nível de seus produtos e serviços, é preciso honrar os compromissos e prazos. As organizações e as pessoas necessitam quantificar e qualificar os riscos aos quais estão expostos. Com a segurança da informação não é diferente, mas gerenciar riscos exige mais do que somente entender, localizar onde está e medir os riscos. É essencial determinar o que fazer com cada risco identificado e atuar preventiva e proativamente contra ele.

Mas, efetivamente: o que é o risco? Risco é geralmente definido como qualquer evento ou condição que pode ter um impacto no resultado de uma atividade. No contexto segurança da informação e da TIC, risco é a probabilidade de que uma ameaça se transforme em um incidente. Reforçando, o risco é a probabilidade – isto é, não é uma certeza – de sofrer uma perda no valor da informação. Essa perda pode resultar em qualquer coisa – desde a redução da qualidade de um produto ou serviço até um aumento de custo, ou prazos perdidos ou uma falha total e completa – decorrente da alteração de características de *confidencialidade, integridade* ou *disponibilidade* da informação.

Como já dissemos, os riscos surgem da incerteza em torno das decisões e dos resultados operacionais. Associamos a ideia de risco ao potencial de perda

de valor, controle, funcionalidade, qualidade ou oportunidade de conclusão de uma atividade. No entanto, os resultados também podem resultar em falha para maximizar o ganho em uma oportunidade. Também podemos dizer que as incertezas na tomada de decisões que levam a esse resultado envolvem elementos de risco.

1.2 Atenuação do risco

Sabendo o que é o risco, necessitamos identificar os riscos e decidir como iremos enfrentá-los. Isso é cada vez mais importante para a TIC em geral e determinadas operações e informações em particular, pois cada vez mais as pessoas e as organizações tornam-se suscetíveis aos incidentes causados por problemas de segurança da informação causados ou relacionados à TIC.

O número e a gravidade desses incidentes especificamente relacionados à TIC e à segurança da informação estão aumentando com o tempo porque:

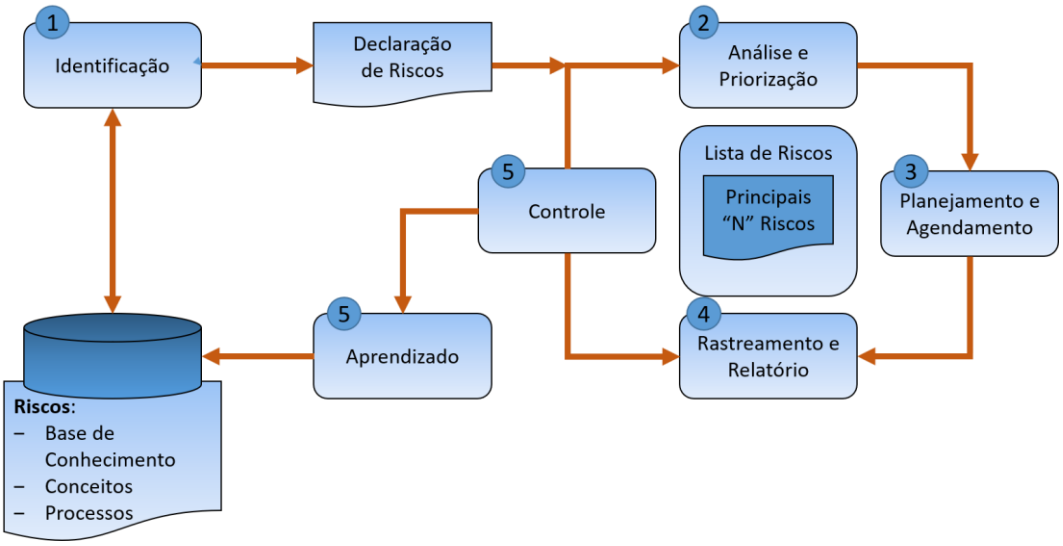
- As atividades das pessoas, as operações e os processos de negócios são cada vez mais dependentes da TIC, portanto é mais provável que falhas dela oriunda afetem os negócios, e esse impacto tem cada vez mais probabilidade de ser grave;
- O ambiente de TIC é cada vez mais complexo. Mesmo que o ambiente permaneça imutável, o número de vulnerabilidades aumenta;
- As áreas de TIC controlam cada vez menos a infraestrutura. Assim, gerenciar a possibilidade de falha torna-se muito importante, pois as áreas de TIC têm menor capacidade de reagir após a ocorrência da falha.
- Dada a agilidade dos negócios em um mundo conectado, quando ocorre uma falha de TIC, há menos tempo entre a ocorrência da falha e seu impacto no negócio.
- As falhas da TIC são cada vez mais visíveis fora da organização ou dos ambientes restritos e, portanto, mais pessoas são afetadas negativamente quando ocorre uma falha.

Podemos concluir que a TIC tem cada vez mais potencial para suportar e aprimorar os processos de negócios, porém as falhas em TIC têm mais potencial para interromper as operações de negócios e afetar diretamente a lucratividade e o sucesso de uma organização. Para fazer frente a isso é necessário implementar um consistente processo de gestão de risco.

TEMA 2 – GESTÃO DE RISCOS

A gestão de riscos é uma disciplina que aplica técnicas comprovadas de probabilidade, estatística e *assessment* aos desafios enfrentados pelas organizações e pessoas. Existem muitos modelos, estruturas e processos para gerenciar riscos, e todos abordam o planejamento perante incertezas. Isso é buscado pela aplicação de princípios, conceitos e um processo estruturado e repetível de seis etapas, as quais precisam ser incorporadas às atividades do cotidiano. Estas etapas, mostradas na Figura 1, são detalhadas nos itens a seguir.

Figura 1 – Processo de gestão de riscos



2.1 Identificação dos riscos

A identificação de riscos é o primeiro passo no processo proativo de gerenciamento de riscos. Ele fornece as oportunidades, indicadores e informações que permitem que uma organização levante os principais riscos antes que eles se transformem em incidentes, afetem as atividades e, consequentemente, os negócios.

Essa etapa está diretamente ligada ao termo "classificação" do ITIL (*Information Technology Infrastructure Library* ou Biblioteca de Infraestrutura da Tecnologia da Informação é um *framework* de gestão de serviços da TIC cuja principal finalidade é garantir a entrega dos serviços), identificando, de maneira clara e específica, incidentes, problemas e erros conhecidos por origem, sintomas e causas.

2.2 Análise e priorização dos riscos

A análise de risco tem como base a informação dos riscos gerada na etapa de identificação, convertendo-a em informação de tomada de decisão. Nessa etapa, mais três elementos são adicionados ao registro do risco na lista de riscos principais: probabilidade, impacto e exposição do risco. Esses elementos nos permitem classificar os riscos, o que, por conseguinte, nos permite direcionar de modo mais adequado os esforços de tratamento e adequar o gerenciamento da lista de riscos principais.

2.3 Planejamento e agendamento de ações para o tratamento dos riscos

Planejar e agendar ações de tratamento dos riscos é a etapa de inteligência do processo de gestão de riscos. As atividades de planejamento executadas nessa etapa utilizam a lista de riscos priorizados para produzir planos de ação. O planejamento envolve o desenvolvimento de estratégias e ações detalhadas para cada um dos principais riscos, priorizando as ações de tratamento do risco e criando um plano de gestão de riscos integrado. O agendamento envolve a integração das tarefas necessárias para implementar os planos de ação de tratamento do risco nas atividades diárias, atribuindo-as a indivíduos ou funções e rastreando ativamente seu status.

2.4 Rastreamento e registro dos riscos

Na etapa de rastreamento de riscos, as atividades da TIC reúnem informações sobre possíveis alterações dos riscos. Essas informações suportam as decisões e ações que serão tomadas na etapa de controle de risco.

Para o acompanhamento do risco, a etapa de rastreamento de risco monitora três alterações principais:

- **Alertas** – Se um alerta de risco for ativado, um plano de contingência precisa ser executado;
- **Condição, consequências, probabilidade e impacto do risco** – Se algum destes itens mudar (ou se for considerado impreciso), eles precisam ser reavaliados;
- **Progresso de um plano de mitigação** – Se o plano está atrasado ou não está tendo o efeito desejado, ele precisa ser revisado.

Esta etapa monitora essas alterações em basicamente três períodos de tempo, a saber:

- **Constante** – Muitos riscos podem ser monitorados constantemente ou pelo menos várias vezes ao dia. Por exemplo, ferramentas automatizadas podem monitorar o uso da largura de banda de um servidor da *web* a cada poucos segundos;
- **Periódico** – As partes interessadas de operações de TIC, especialmente as ligadas a serviços, revisam periodicamente a lista dos principais riscos, procurando alterações nos principais elementos. Geralmente isso é feito em reuniões ordinárias;
- **Sob demanda** – Em alguns casos, percebe-se que parte de um risco ou todo o risco mudou. Isso deve ser rastreado e registrado.

O acompanhamento dos riscos produz o relatório de *status* de risco com dois propósitos dois níveis – *interno* e *externo*. Para as operações de TIC (internas), os relatórios regulares de status de risco devem considerar quatro possíveis situações de gerenciamento de riscos para cada risco:

- **Resolução** – Um risco foi devidamente tratado, completando o plano de ação de tratamento do risco;
- **Consistência** – As ações de tratamento do risco são consistentes com o plano de gerenciamento de risco, de modo que as ações do plano de tratamento do risco continuem conforme o planejado;
- **Variância** – Algumas ações de tratamento de risco estão em desacordo com o plano de gerenciamento de risco, então medidas corretivas devem ser definidas e implementadas;
- **Mudança** – A situação mudou significativamente com relação a um ou mais riscos, e isso geralmente envolve a necessidade de reanalisar os riscos ou replanejar as atividades.

2.5 Controle dos riscos

Durante essa etapa, são realizadas as atividades relacionadas a planos de contingência em função dos alertas de riscos. As ações corretivas são executadas com base nas informações de rastreamento de risco. A gestão de riscos dispõe de processos e infraestrutura padrão existentes para:

- Monitorar os planos de ação de tratamento de riscos;
- Correção das variações de planos;
- Responder aos alertas de riscos.

Os resultados e as lições aprendidas da implementação de planos de contingência são então incorporados em um relatório de *status* e resultados do plano de contingência, de modo que a informação se torne parte da base de conhecimento de risco de operações. É importante registrar o máximo possível de informações sobre problemas que ocorrem ou sobre um plano de contingência quando ele é ativado para determinar a eficácia de tal plano ou da estratégia de controle de risco.

Essa etapa pode não parecer necessária, e a distinção entre ela e a etapa de rastreamento pode não ser tão clara. Na prática, a necessidade de agir é frequentemente detectada por uma ferramenta ou por pessoas que não têm a responsabilidade, autoridade ou experiência necessárias para reagir por conta própria. A etapa de controle de risco garante que as pessoas certas ajam no momento certo, realizando as ações corretas.

2.6 Aprendizado com os riscos

Aprender com o risco é a última etapa do processo e acrescenta uma perspectiva estratégica, empresarial ou organizacional às atividades de gestão de riscos. A aprendizagem de risco deve ser uma atividade contínua em todo o processo de gestão de riscos e pode começar a qualquer momento. Concentra-se em três objetivos principais:

- Fornecer *garantia de qualidade* nas atividades de gestão de riscos, para que a TI possa obter *feedback* constante e regular;
- *Gerar conhecimento* e identificar as *melhores práticas*, especialmente em torno da identificação de riscos e estratégias de mitigação bem-sucedidas – isso contribui para a evolução da base de conhecimento de riscos;
- *Melhorar o processo de gestão de riscos*, obtendo o *feedback* da organização.

A gestão de risco é abordada em profundidade pela norma ISO 31000 (*Risk Management – Principles and Guidelines on Implementation*), proposta em 2009 e em processo de revisão no Brasil por um comitê da ABNT. Quanto à gestão de riscos de segurança da informação, os processos são identificados e descritos

nas seções de 7 a 12 da norma 27005:2011 (ABNT, 2011).

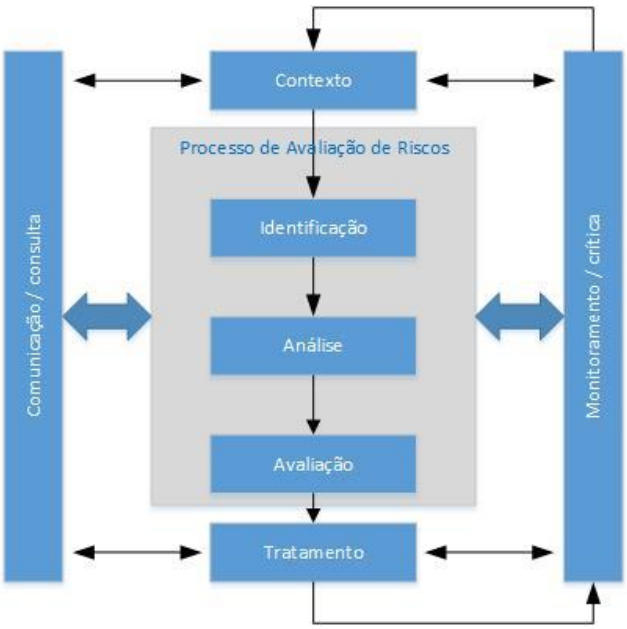
TEMA 3 – OS PROCESSOS DA GESTÃO DE RISCOS

Os processos da gestão de riscos refletem uma abordagem sistemática com o intuito de identificar os requisitos de segurança da informação e prover o atendimento a esses requisitos. No que tange à segurança da informação, os processos de gestão de riscos devem estar alinhados com a gestão de riscos da organização como um todo. A gestão de riscos busca a melhor maneira de tratar os riscos como um todo, de modo efetivo, no momento e no local mais adequado.

Segundo a norma ISO 27005:2011 (ABNT, 2011), a gestão de riscos da segurança da informação contribui significativamente para:

- A identificação dos riscos;
- O processo de avaliação dos riscos em função das consequências aos negócios e da probabilidade de sua ocorrência;
- A comunicação e o entendimento da probabilidade e das consequências desses riscos;
- O estabelecimento da ordem prioritária para o tratamento desses riscos;
- A priorização das ações para reduzir a ocorrência dos riscos;
- O envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e para que elas sejam mantidas informadas sobre a situação da gestão de riscos;
- A eficácia no monitoramento e tratamento dos riscos;
- O monitoramento e a análise crítica periódica dos riscos e do processo de gestão de riscos;
- A coleta de informações de forma a melhorar a gestão de riscos;
- O treinamento de gestores e do pessoal a respeito dos riscos e das ações para mitigá-los. (ABNT, 2011)

Figura 2 – Processos de gestão de riscos



Fonte: ABNT, 2011.

A gestão de riscos é um processo formal de negócios usado para identificar os riscos (que podem ser também *oportunidades*) em uma organização, estimar o impacto potencial desses riscos e fornecer um método para tratar esses impactos, reduzindo as ameaças a um nível aceitável – ou alcançando as oportunidades (Espinha; Sousa, 2007). Como mostrado na Figura 2, contempla as atividades de *identificação, análise, avaliação* e *tratamento*.

3.1 Identificação dos riscos

Raspotnig e Opdahl (2013) analisaram diversas técnicas de identificação de riscos – considerando a segurança dos usuários (*safety*) e a segurança de sistemas e da informação (*security*). A conclusão foi que os métodos e as técnicas voltadas para a segurança do usuário estão em um nível de maturidade bastante avançado, seja em função do emprego há longo tempo – algumas técnicas remontam às décadas de 60 ou anteriores –, seja em função da própria maturidade da indústria que as implementa, usa e aprimora. Nesse aspecto, temos as técnicas de identificação de riscos empregadas pela indústria aeronáutica e de transporte aéreo, e pelos setores militares ligados às defesas dos países, tais como:

> *Functional Hazard Assessment* – FHA ou Avaliação Funcional de Perigos: Originou-se na indústria aeronáutica e, em função da simplicidade e da eficiência, tornou-se conhecida e usada nas demais indústrias (ARP, 1994);
> *Preliminary Hazard Analysis* – PHA: Foi desenvolvida pela área de defesa dos Estados Unidos nos anos 60 (Ericsson, 2005). É empregada para a elicitação de requisitos de segurança de sistemas no projeto inicial ou nas suas especificações;
> *Hazard and Operability* – HAZOP: É empregada pela indústria química desde a década de 70, mas aplicada em diversas indústrias (Raspotnig; Opdahl, 2013). Trata-se de técnica para identificar e analisar perigos e ameaças operacionais em um sistema;
> *Failure Mode and Effect Analysis* – FMEA: Consiste em analisar falhas em potencial de um sistema e avaliar os possíveis efeitos (Raspotnig; Opdahl, 2013). Padronizada pelos militares americanos na década de 40, busca estabelecer a confiabilidade dos sistemas;
> *Fault Tree Analysis* – FTA : É uma técnica mais sofisticada que faz uso de um gráfico em formato de árvore. Baseada na lógica booleana, busca estabelecer a causa raiz do evento analisado. (Raspotnig; Opdahl, 2013)

No que tange especificamente à segurança da informação, Raspotnig e Opdahl (2013) analisaram seis técnicas diferentes, comparando-as com base em critérios específicos. As principais são apresentadas a seguir:

> KAOS – *Knowledge Acquisition in Automated Specification*: é um framework com uma metodologia voltada inicialmente para engenharia de requisitos, baseada em suporte à modelagem e elaboração de

requisitos com foco em metas. Os artefatos de modelagem incluem as metas, os objetos, os agentes, as operações, os requisitos e os obstáculos;
Secure Tropos é uma técnica voltada para todas as fases do desenvolvimento, e enfatiza a abordagem precoce da engenharia de requisitos voltada para a segurança. O ponto principal é um modelo representado graficamente, que é refinado e estendido à medida em que se avança nas fases do desenvolvimento;
Casos de uso impróprio (*Misuse Case*) é uma referência aos casos de uso para criar e relatar os casos de uso impróprio, que expõem o sistema a riscos ou ameaças e o levam a ocorrência de faltas;
Abuse frame ou quadro de uso impróprio é uma técnica derivada dos quadros de problemas de Jackson, que buscam estabelecer os limites do sistema, e que tem por objetivo prover um modelo abstrato das ameaças impostas por usuários maliciosos a estes limites;
Técnica da árvore de ataques (*Attack Tree*) é uma maneira formal e metódica de descrever a segurança dos sistemas baseadas em ataques;
Técnica da árvore de ameaças (*Threat Tree*) é uma técnica analítica cujo objetivo é apoiar a análise de requisitos de segurança e seus desdobramentos em função das ameaças.

3.2 Análise dos riscos

A análise de riscos compreende a identificação de parâmetros para a posterior avaliação dos riscos perante os critérios estabelecidos pela organização para o enfrentamento dos riscos. Os métodos utilizados compreendem a análise qualitativa, a análise quantitativa ou ambas.

Em geral, a análise qualitativa é empregada inicialmente para a apresentação do nível geral de risco da organização e para permitir a identificação dos maiores riscos aos quais a organização está exposta, possibilitando a priorização no tratamento desses riscos. Em seguida, realiza-se a análise quantitativa, mais específica, porém mais complexa e de maior custo, nesses riscos.

A análise qualitativa emprega uma escala de grandeza que se refere à gravidade das consequências dos riscos – isto é, do impacto, dos danos – para o negócio, tal como “muito baixa, baixa, média, alta, muito alta” ou algo semelhante. A cada risco identificado, é então associada uma probabilidade de ocorrência, também baseada em escala semelhante. Cada uma dessas escalas pode ser associada à uma graduação numérica equivalente (escala de Likert), e o produto impacto x probabilidade de ocorrência vai apresentar um valor final, o qual é então utilizado para classificar, em ordem decrescente, os riscos. A Tabela 1 apresenta um modelo simplificado utilizado para uma análise qualitativa.

Tabela 1 – Análise qualitativa.

Descrição do Risco	Severidade (Impacto)	Probabilidade	Classificação
Roubo do notebook do CEO	Muito Alta	Baixa	10
Interrupção de energia por até 01 hora	Média	Média	9
Crash do HD do servidor de rede	Muito Alta	Muito Baixa	5
Interrupção de energia por mais de 01 hora	Alta	Muito Baixa	4
Escala utilizada: Muito Baixa = 1; Baixa = 2; Média = 3; Alta = 4; Muito Alta = 5			

A análise qualitativa tem como principal atrativo a sua simplicidade, razão pela qual geralmente é de fácil entendimento por todos os envolvidos. Além disso, as descrições dos riscos e da escala podem ser adaptadas para diferentes tipos de riscos. Como desvantagem pesa a subjetividade da avaliação e da própria escala. Por isso, seu uso é indicado para uma verificação inicial, que resultará em uma identificação de quais riscos exigirão uma maior atenção e uma análise mais detalhada, ou seja, para a priorização no tratamento dos riscos. Também deve ser considerada nos casos em que essas informações são suficientes para a tomada de decisão, quando os dados são insuficientes para uma análise quantitativa, ou ainda quando a exigência de recursos ou tempo para conseguir os dados é muito elevada.

A análise quantitativa utiliza valores numéricos para ambas as escalas – normalmente o valor financeiro do ativo ou das consequências e uma taxa de ocorrência para a probabilidade – obtendo-se assim uma grandeza em uma unidade conhecida – a moeda corrente, por exemplo – que será utilizada para a quantificação do risco. A Tabela 2 apresenta um exemplo simplificado utilizado para uma análise quantitativa

Tabela 1 – Análise quantitativa

Descrição do Risco	Consequência (Danos ou Perdas)	Probabilidade (Ocorrências por ano)	Impacto no Resultado Anual	Observações
Interrupção de energia por até 01 hora	R$ 25.000,00	6,00	R$ 150.000,00	Seis vezes ao ano
Roubo da base de dados de clientes	R$ 5.000.000,00	0,02	R$ 100.000,00	Uma vez a cada 50 anos
Site de e-commerce fora do ar por até 01 hora	R$ 6.000,00	10,00	R$ 60.000,00	Dez vezes ao ano
Incêndio no data center	R$ 1.000.000,00	0,01	R$ 10.000,00	Uma vez a cada 100 anos

Por utilizar geralmente séries de dados históricos ou estatísticos, a análise

quantitativa é muito mais precisa e também pode ser relacionada diretamente com os interesses da organização e os objetivos da segurança da informação. Entretanto, seu uso é mais complexo e torna-se muito difícil para novos riscos, ativos intangíveis (como valor da marca, confiabilidade do cliente, etc.) ou mesmo quando não há dados confiáveis ou auditáveis, comprometendo assim a precisão dos resultados.

3.3 A avaliação dos riscos

Uma vez identificados e analisados os riscos, devemos avaliá-los para definir qual será o tratamento mais adequado – e possível de ser aplicado. Para isso, é necessário conhecer o nível de risco aceitável, isto é, o perfil de risco da organização. Pode ser que, devido ao negócio, a organização esteja mais habituada a expor-se a riscos, com um perfil mais arrojado, ou não possa correr riscos, com um perfil mais conservador.

A norma ISO 27005:2011 estabelece que devemos considerar, nessa etapa, as propriedades da segurança da informação (a relevância dos critérios) e a importância do processo ou atividade (ABNT, 2011). Também devemos avaliar se tal processo ou atividade deve ser mesmo executado, em função de elevados riscos, e a prioridade do tratamento dos riscos, definida na etapa de análise. Questões contratuais, legais e regulatórias são de grande importância para a avaliação dos riscos.

3.4 Tratamento dos riscos

O planejamento de respostas a riscos é o principal aspecto do tratamento de riscos. Abrange a discussão e a avaliação do registro de riscos, dos perfis de risco e da matriz de controle de causas. Basicamente quatro estratégias são formuladas e documentadas nessa etapa, a saber:

- **Evitar o risco**: a prevenção de riscos requer identificação dos riscos em primeiro lugar. Isso pode ser alcançado através de experiências e do histórico. Analisando aqueles que têm uma tendência maior, o curso da ação pode ser alterado para impedir que o risco se transforme em uma ocorrência.
- **Transferência de risco**: é uma das melhores maneiras para diminuir o impacto do risco. Típico das áreas financeiras, nesse tratamento, um risco

é repassado para um terceiro, de forma que a atividade ou o processo não sofram o dano ou tampouco seja impactada pelas consequências da ocorrência.

- **Mitigação de riscos**: é um processo de controle que busca interromper um risco antes que comece a causar impacto, e assim deixá-lo em um nível aceitável para a organização. Geralmente implica ativar um plano de contingência.
- **Aceitação do risco**: existem certos riscos que são inevitáveis. Essa estratégia é a melhor quando o risco é baixo, porém exige um plano para determinar o grau de exposição e também para fazer pequenos ajustes. Um risco aceitável pode ser considerado passivo, uma vez que nenhuma ação é tomada sobre ele.

TEMA 4 – TRATAMENTO DOS RISCOS

Como resultado do planejamento de resposta ao risco, vários estratégias correspondentes são documentadas. Um registro de risco está pronto e contém todos os detalhes em relação ao momento da ocorrência, prioridade e as pessoas envolvidas no tratamento do risco. Os riscos já foram classificados, e o tratamento dos riscos relevantes são atribuídos aos responsáveis.

É bastante comum – e também recomendável – que o tratamento dos riscos de segurança da informação seja delegado a uma equipe multidisciplinar da organização (CERT – Centro de Estudos, Resposta e Tratamento de Incidentes), especializada na aplicação do plano de resposta ao risco e conhecedora das características da organização, assim como de posse dos recursos e informações necessárias para fazer frente aos riscos.

Como é impossível para qualquer organização conhecer e tratar adequadamente todos os riscos durante todo o tempo, é necessário ter ciência dos riscos residuais e monitorá-los, tanto quanto revisar e atualizar as informações sobre os riscos e fazer a adequação do tratamento, como mostrado na Figura 3.

Figura 3 – Processo de tratamento de riscos

TEMA 5 – GESTÃO DA CONTINUIDADE DOS NEGÓCIOS

Como consequência da inexorabilidade dos riscos e da incapacidade das organizações de evitarem todos os riscos o tempo todo, é necessário que estas estejam preparadas para enfrentar as consequências dos incidentes. Isso é possível por meio da gestão da continuidade dos negócios (GCN), processo que garantirá que as operações da organização prossigam com o máximo possível de normalidade.

A GCN utiliza a análise dos impactos no negócio – BIA – *Business Impact Analisys* – para identificar as operações críticas para o negócio e as relações de dependência com fornecedores, pessoas, outros processos de negócios, serviços e processos de TI, ou seja, tudo o que suporte ou tenha relação com essas operações. A BIA trata dos requisitos para a recuperação dos serviços, designados como:

- Objetivos de tempo de recuperação: o RTO – *Recovery Time Objective* define o limite de tempo para os serviços serem recuperados e retornarem à normalidade operacional;
- Objetivos de pontos para recuperação: o RPO – *Recovery Point Objective* estabelece a máxima perda de informações que a organização aceita em função de um incidente.
- Metas de nível de serviço: o SLO – *Service Level Objectives* são as mínimas condições para cada serviço da organização que permitam a continuidade operacional em situações de emergência, sob a ocorrência de incidentes. Nesses momentos, provavelmente não será possível cumprir as metas e acordos de níveis de serviços operacionais por conta da situação.

A GCN é um processo contínuo que usa o modelo PDCA – *Plan, Do, Control, Act* para estabelecer diversos planejamentos de enfrentamento de incidentes de forma preditiva, preventiva e corretiva, entre os quais:

- PCO – Plano de Continuidade Operacional: tem por finalidade identificar as operações críticas da organização e prover meios para que estas prossigam mesmo perante os incidentes, por mais graves que sejam. Abrange os negócios, áreas e processos;
- PGI – Plano de Gestão de Incidentes: estabelece as responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas, que permitam aprender com os incidentes, quantificar e monitorar esses incidentes. Garante a preservação e a coleta de evidências, seu armazenamento e apresentação em conformidade com a legislação e as normas;
- PRD – Plano de Recuperação de Desastres: tem por finalidade o enfrentamento de desastres, calamidades e tragédias, ou seja, incidentes de grandes proporções que coloquem em risco a sobrevivência da organização. É a preparação para a sobrevivência em cenário de crise. Abrange os ativos, as tecnologias, as pessoas, os sistemas e o ambiente;
- PAC – Plano de Administração de Crises: estabelece o passo a passo das atividades de equipes ligadas à ativação das contingências, antes, durante e depois do incidente. Estabelece também os procedimentos a serem realizados no retorno à normalidade, a estratégia de comunicação – para os meios de comunicação, autoridades e sociedade em geral – do fato

ocorrido. É orientado para a gestão dos processos em estado de contingência;

- PTV – Plano de Testes e Validação: tem por objetivo promover a execução de testes e a validação dos resultados de forma recorrente, de modo a manter prontos e preparados todos os recursos para a ativação dos demais planos, incluindo as pessoas envolvidas.

A GCN possibilita estabelecer condições e recursos para a execução de cada um destes planos, cuidando também de sua simulação e testes recorrentes, e também da sua divulgação e da capacitação de todos os envolvidos, de modo a estarem preparados e prontos para colocar em execução esses planos.

REFERÊNCIAS

ABNT NBR. ISO/IEC 27005: 2011. São Paulo: ABNT, 2011.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

ENGEMANN, K. J.; HENDERSON, D. M. **Business continuity and risk management**: essentials of organizational resilience. EUA: Rothstein Associates, 2011.

ESPINHA, R.; SOUSA, J. Melhorando processos através da análise de risco e conformidade. **Engenharia de Software Magazine**, DevMedia: Rio de Janeiro, Ano 1, 2007, pp 10.

FONTES, E. **Segurança da informação**. 1. ed. São Paulo: Saraiva, 2001.

KIM, D. **Fundamentos de segurança de sistemas de informação**. Rio de Janeiro: LTC, 2014.

KOLBE JR. A. **Sistemas de segurança da informação na era do conhecimento**. Curitiba: InterSaberes, 2017.

RASPOTNIG, C.; OPDAHL, A. Comparing risk identification techniques for safety and security requirements. **The Journal of Systems and Software,** n. 86, p. 1124-1151, 2013.

RIBEIRO, R. A**. Segurança no desenvolvimento de software**. Rio de Janeiro: Campus, 2002.

TURBAN, E.; VOLONINO, L**. Tecnologia da informação para gestão**: em busca de um melhor desempenho estratégico e operacional. 8. ed. São Paulo: Bookman, 2013.