Capítulo 3

Gestão de riscos de segurança da informação

Neste capítulo apresentamos as regras fundamentais da gestão de riscos de segurança da informação. Nele vamos abordar por que essas regras são importantes, o que aconteceria num possível incidente dentro de uma área de TI que não tenha nenhuma norma para agir nesta possível ocorrência e os danos, às vezes irrecuperáveis, que poderão causar numa organização que não possua nenhuma gestão de riscos.

Enfatizamos a importância da norma ISO/IEC 27005, que identifica os riscos, seus tratamentos e monitoramento desde a sua ocorrência até a sua total resolução e normalização na área de TI.

1 Fundamentos de gestão de riscos

O cenário competitivo atual apresenta empresas em constante preocupação para com a segurança de seus dados. Gerir esses dados é estratégia fundamental para o sucesso nos negócios. Uma empresa que trata bem seus dados consegue fortalecer a sua imagem perante o mercado, sob os aspectos de confiabilidade e integridade.

Mas o que é um risco? Trata-se da incerteza sobre o alcance de um determinado objetivo e está relacionado com a possibilidade de ocorrência de algo diferente do esperado, podendo ser positivo ou negativo. O risco de segurança é o efeito da incerteza quanto ao atendimento dos princípios de CID (confidencialidade, integridade e disponibilidade) (AGUILERA-FERNANDES, 2017).

Promover a gestão de riscos é, portanto, tarefa essencial do profissional de tecnologia da informação nas organizações.

2 Norma NBR ISO/IEC 27005

As normas internacionais possuem papel importante no processo de norteamento das ações da gestão de riscos das organizações, pois apresentam conceitos e práticas padronizadas. Uma delas é a NBR ISO/IEC 27005, que faz parte da série de normas ISO/IEC 27000, considerada em todo o mundo como referência para a gestão da segurança da informação.

A NBR em estudo tem foco na tecnologia da informação, técnicas de segurança e gestão de riscos da segurança da informação. A ISO/IEC 27005 define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização (LUND; SOLHAUG; STØLEN, 2010).

Segundo Sampaio (2014), a norma ISO/IEC 27005 convém para que a gestão de riscos de segurança da informação possa contribuir para:

- Identificação de riscos.
- Análise/avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência.
- Comunicação e entendimento da probabilidade e das consequências destes riscos.
- Estabelecimento da ordem prioritária para tratamento do risco.
- Priorização das ações para reduzir a ocorrência dos riscos.
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas, além de serem mantidas informadas sobre a situação da gestão de riscos.
- Eficácia do monitoramento do tratamento do risco.
- Monitoramento e análise crítica regular de riscos e do processo de gestão dos mesmos.
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos.
- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.

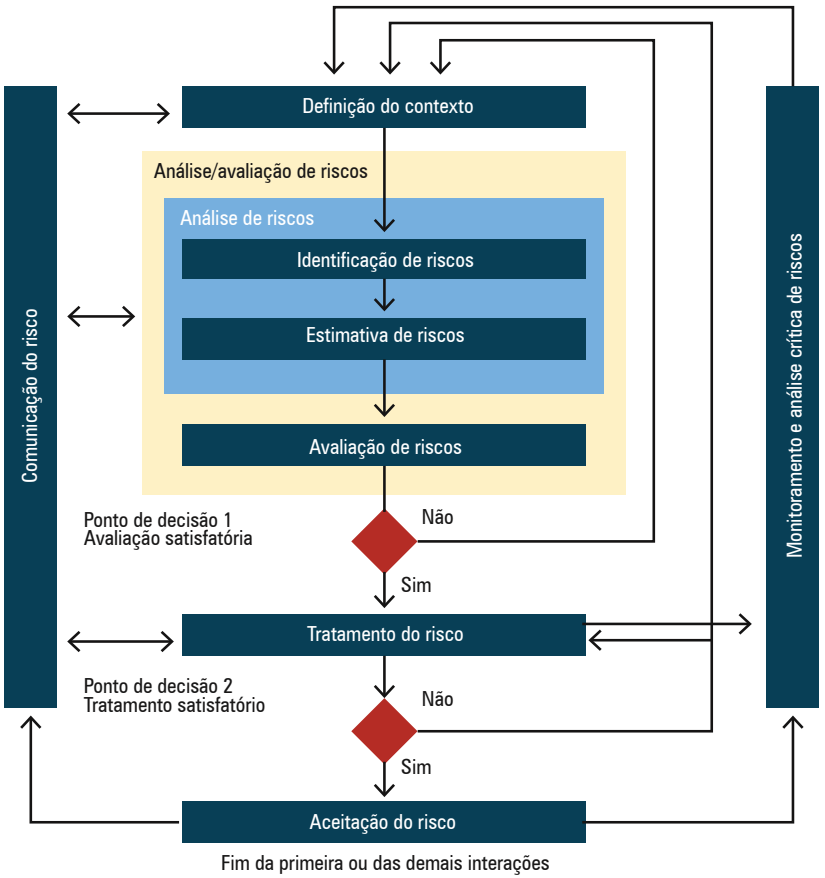
3 Processo da gestão de riscos de segurança da informação

Segundo a NBR ISO/IEC 27005, o processo da gestão de riscos se divide em diretrizes descritas a seguir:

- Definição do contexto: é essencial descrever os processos, determinando os critérios gerais de aceitação de riscos pela organização.
- Identificação de riscos: faz-se necessário identificar as ocorrências que possam ter impacto nos negócios da empresa, identificando suas vulnerabilidades e as ameaças que podem causar danos aos ativos.
- Estimativa de riscos: analisar as probabilidades do impacto de um risco, numa visão qualitativa e/ou quantitativa e suas consequências.
- Avaliação de riscos: avaliar uma comparação entre o nível estimado de um risco e o nível aceitável estabelecido pela empresa, como contextualiza a figura 1 a seguir, no ponto de decisão 1.
- Tratamento do risco: como apresentado no ponto de decisão 2, ainda na figura 1 a seguir, a organização deve implementar controles para evitar ou diminuir os riscos, designando os responsáveis por cada ação.
- Aceitação do risco: realizar formalmente o registro dos planos de tratamentos de riscos já aprovados pela empresa.
- Comunicação do risco: elaborar planos de comunicação dos riscos para assegurar que todos tenham consciência sobre esses riscos e os controles que devem ser adotados pela empresa.
- Monitoramento e análise crítica de riscos: avaliar constantemente possíveis mudanças do contexto, adequando os processos de segurança à realidade presente.

Na figura 1 a seguir ilustramos o processo completo:

Figura 1 – Processo de gestão de riscos de segurança da informação



Fonte: adaptado de ABNT (2019, p. 5).

4 Identificação de ativos, ameaças, controles existentes e vulnerabilidades e consequências

Os ativos de uma organização representam todos os itens existentes na mesma, nos quais informações são criadas, processadas, armazenadas e compartilhadas.

Os ativos das instituições constituem-se também do capital intelectual, e esse tipo de capital é geralmente chamado de capital intangível (OLIVEIRA, 2017), que pode ser entendido como algo que não pode ser tocado ou visto fisicamente, porém, no caso do ativo intangível, seria um bem que a empresa possui, como licenças, direitos autorais e carteira de clientes.

Para um bom gerenciamento dos riscos de segurança da informação, é imprescindível que sejam analisados os ativos de informação (como dados de funcionários, clientes e histórico de vendas) e os ativos físicos (como equipamentos, funcionários, rede de comunicação) para, assim, se identificar a fonte (por exemplo, um ataque ou um evento acontece), a ação (o método de como esse ataque ou evento aconteceu) e consequência de uma ameaça, que é a violação resultante do ataque ou evento ao sistema de informação da empresa.

De acordo com Oliveira (2017), a análise de risco é um processo que:

- Promove o levantamento de informações em relação aos riscos que existem dentro de uma empresa, sejam eles físicos ou lógicos.
- Identifica os recursos críticos que podem afetar a organização.
- Faz o mapeamento das vulnerabilidades e ameaças existentes.
- Elabora um cálculo do nível de risco que está associado a cada um em relação à vulnerabilidade e à ameaça que podem ocasionar impactos nos negócios.

5 Avaliação das consequências e probabilidades

Com a análise dos ativos e das ameaças bem rastreados, agora é a hora de avaliar as consequências e elaborar as probabilidades dos eventos que ocorreram. Segundo a 27001 Academy, podemos classificar as análises como simples e complexas.

Na análise de risco simples você

> analisa as consequências e probabilidade diretamente. Uma vez que você tenha identificado os riscos, você simplesmente tem que usar escalas para analisar separadamente as consequências e probabilidade de cada risco. Por exemplo, você pode usar a escala de 0 a 4, onde 0 seria muito baixo, 1 baixo, 2 médio, e assim por diante, ou a escala de 1 a 10, ou Baixo-Médio-Alto, ou qualquer outra escala. Quanto maior a escala, mais precisos serão os resultados que você terá, mas também mais tempo você gastará para realizar a análise (KOSUTIC, 2015).

Exemplo (KOSUTIC, 2015):

- Ativo: notebook.
- Ameaça: roubo.
- Vulnerabilidade: empregados não sabem como proteger seus dispositivos móveis.
- Consequências: 3 (em uma escala de 0 a 4).
- Probabilidade: 4 (em uma escala de 0 a 4).

Na análise de risco detalhada, em vez de analisar dois elementos (consequência e probabilidade), analisamos três elementos: valor do ativo, ameaça e vulnerabilidade.

Exemplo (KOSUTIC, 2015):

- Ativo: notebook.
- Ameaça: roubo.
- Vulnerabilidade: empregados não sabem como proteger seus dispositivos móveis.
- Valor do ativo: 3 (em uma escala de 0 a 4).
- Valor da ameaça: 2 (em uma escala de 0 a 2).
- Valor da vulnerabilidade: 2 (em uma escala de 0 a 2).

6 Mensuração do nível de riscos

Para desenvolver uma análise confiável do nível de riscos, é imprescindível que se elabore um levantamento dos recursos críticos da empresa, que são todos aqueles existentes na empresa, mapeamento de todas as vulnerabilidades da empresa (com pessoal, sistemas e local), avaliando os impactos que resultam de uma possível exploração dessas vulnerabilidades e também mapeando as possíveis ameaças que podem ocorrer e os seus consequentes danos.

Segundo Caruso e Steffen (2006, p. 72 apud OLIVEIRA, 2017), podemos classificar os graus de impactos da seguinte forma:

- Alto risco: a empresa como um todo ou boa parte dela tem de interromper suas atividades essenciais, colocando em risco sua sobrevivência.
- Médio risco: a empresa sofre sérias dificuldades em suas atividades, com prejuízos significativos, porém, que não chegam a afetar a sobrevivência da empresa como um todo.
- Baixo risco: as atividades da empresa não são afetadas de forma contundente pela ocorrência.

7 Critérios de avaliação

Os critérios de avaliação de riscos são baseados no escopo e limites definidos pela empresa, e é gerada uma lista de riscos já avaliados, ordenados por prioridades de acordo com parâmetros definidos, como no exemplo a seguir:

NA PRÁTICA

Em caso de queda de energia e desligamento de computadores da empresa, tem-se preestabelecido que a equipe de TI deve realizar a instalação e manutenção de nobreaks, que têm como principal função fornecer energia sem interrupção aos equipamentos, mesmo que a rede elétrica esteja desligada, devido às suas baterias internas. Assim, os(as) usuários(as) poderão salvar seus arquivos e não perder tempo de trabalho.

8 Como definir prioridades e ordenar os riscos

As prioridades da gestão de riscos são definidas de acordo com o grau de criticidade que o problema apresenta. Cada evento de risco deve ter suas prioridades, dependendo do grau de criticidade identificado. Por exemplo: um possível incêndio nas dependências da organização onde se localiza o computador central (servidor) é um evento de altíssima criticidade. Neste caso, a organização deverá ter uma norma de procedimento que deve ser seguida rigorosamente para evitar o máximo de interrupção em seus processos.

Com a avaliação dos níveis de riscos (alto, médio e baixo), já elaboradas e mencionadas, pode-se definir as prioridades e a ordenação dos riscos potenciais que a empresa deve enfrentar.

9 Processo de tratamento, redução e retenção dos riscos

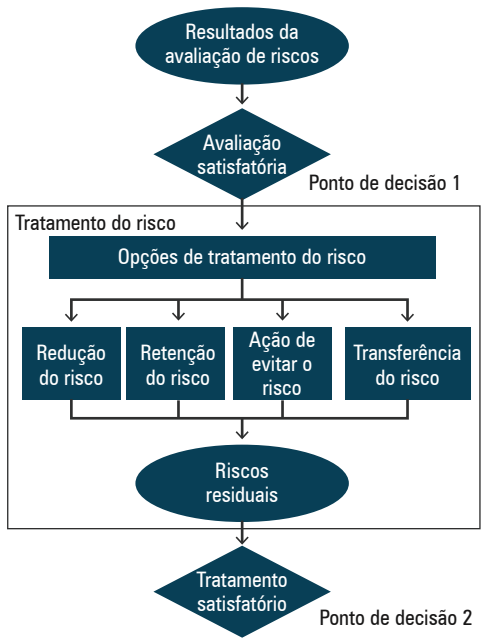
O processo de tratamento dos riscos é o que será usado para modificar o risco. Ele identifica a probabilidade, a consequência, e deve mitigar, prevenir ou até mesmo eliminar totalmente o risco.

Assim, a redução dos riscos é o tratamento que deve ser adotado para identificar as vulnerabilidades existentes na organização, como: falhas no sistema, acessos indevidos por hackers, acidentes que possam causar interrupção nos processos e o que pode ser feito para que, quando ocorrer algum problema, o dano causado seja o menor possível.

A retenção dos riscos é uma forma d a organização assumir as consequências do risco porque a probabilidade é pequena ou porque os danos são pequenos ou porque o custo para sua total mitigação é maior do que o custo de sua consequência.

Na figura 2 a seguir, apresentamos o gráfico que demonstra a avaliação do risco, quais opções de tratamento poderão ser adotadas, e, após sua avaliação, se há mais algum risco que ainda apresenta algum grau de criticidade.

Figura 2 – A atividade de tratamento de risco



Fonte: adaptado de ABNT (2019, p. 21).

10 Ações para evitar, transferir e aceitar o risco

Entre as ações que ajudam a evitar os riscos estão:

- Criar formulários para serem preenchidos no momento da notificação de um incidente ajuda na agilidade do processo.
- Ter claramente quais procedimentos devem ser seguidos para as providências em caso de um incidente deixará a equipe de trabalho mais segura em suas ações.
- Elaborar um processo disciplinar formal, para proteção da empresa contra possíveis ataques de usuários internos, com possíveis advertências ou até demissões.
- Possuir mecanismos de acompanhamento para acompanhar todos os procedimentos descritos acima e outros que sejam específicos da organização.

Segundo Sampaio (2014), a decisão de aceitar os riscos deve ser realizada e formalmente registrada, juntamente com a responsabilidade pela decisão. Como entrada recebe-se a aceitação do risco, plano de tratamento do risco e a análise/avaliação do risco residual sujeito à decisão dos gestores da organização relativa à aceitação do mesmo. Como saída é gerada uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.

11 Processo de comunicação e monitoramento dos riscos

Uma das características mais importantes do profissional de tecnologia da informação é a capacidade de transmissão de informação aos

seus pares. Quando se tem um incidente na empresa, deve-se comunicar aos profissionais da equipe de TI e aos demais gestores da organização o que foi previamente acordado, para não gerar alarde em toda a empresa. Dependendo do incidente, deve-se registrar o mesmo em órgãos competentes, como uma delegacia de polícia no caso de roubos.

De acordo com Sampaio (2014), o processo de comunicação e monitoramento dos riscos é uma importante atividade do processo de gerenciamento de riscos. Ele garante que todos os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de se manter uma visão geral dos riscos.

12 Análise crítica e melhoria do processo

Uma análise crítica torna-se necessária ao final do processo, após possuir todas as informações sobre os riscos, para avaliar, junto com a equipe de trabalho e de gestão da empresa, os aprendizados e novos alinhamentos para a melhoria constante dos procedimentos.

Essa análise e melhoria deverão prever e identificar, o mais rápido possível, eventuais mudanças no contexto atual da empresa e manter uma visão focada na gestão dos riscos.

Para isso, as empresas podem adotar o famoso método PDCA (Plan, Do, Check and Act) para estruturar os processos de segurança da informação, sendo eles, conforme quadro 1 a seguir:

Quadro 1 – Processos de Segurança da Informação e Gestão de Riscos

PROCESSOS DO SGSI	PROCESSO DE GESTÃO DE RISCOS DE SI
Planejar	• Definição do contexto • Análise/avaliação de riscos • Definição do plano de tratamento do risco • Aceitação do risco
Executar	• Implementação do plano de tratamento do risco
Verificar	• Monitoramento contínuo e análise crítica de riscos
Agir	• Manter e melhorar o processo de gestão de riscos de segurança da informação

Fonte: adaptado de ABNT (2019, passim).

Considerações finais

Neste capítulo apresentamos a norma ISO/IEC 27005, que trata da importância da gestão de riscos da segurança da informação e explora detalhadamente a vertical de atividades que toda a área de TI deve seguir para não ocorrer um colapso de segurança.

Aprendemos o que é identificação de ativos, avaliação, mensuração dos níveis de riscos e todos os critérios de avaliação necessários e suas consequências.

Aprendemos também como definir as prioridades, os processos de tratamento, redução e retenção dos riscos, bem como quais são as ações para evitá-los. Abordamos a importância dos processos de comunicação e monitoramento dos riscos, itens que a organização deve adotar. Por fim, vimos que a análise crítica e a melhoria de processos deve ser contínua e dinâmica.

Não se limite apenas aos assuntos abordados neste capítulo. Há milhares de exemplos sobre todos esses temas e que corroboram a nossa

preocupação em levar a sério tais questões, cabendo a você explorá-los o mais detalhadamente possível.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27005**: 2010. Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2019. 66 p. (ABNT/CB-201)

AGUILERA-FERNANDES, Edson. **Padrões, normas e políticas de segurança da informação**. São Paulo: Editora Senac São Paulo, 2017. (Série Universitária).

OLIVEIRA, Roberto Carlos Queiroz. **Tópicos de Segurança da Informação**. São Paulo: Editora Senac São Paulo, 2017. (Série Universitária).

LUND, M. S.; SOLHAUG, B.; STØLEN, K. Evolution in relation to risk and trust management. **IEEE Xplore**, 2010, p. 49-55. Disponível em: https://ieeexplore.ieee.org/document/5472891. Acesso em: 16 jul. 2021.

KOSUTIC, DEJAN. Como avaliar consequências probabilidades na análise de risco da ISO 27001. **Advisera**, 3 jun. 2015. Disponível em: https://advisera.com/27001academy/pt-br/knowledgebase/como-avaliar-consequencias-e-probabilidade-na-analise-de-risco-da-iso-27001/. Acesso em: 16 jul. 2021.