ESTUDO SOBRE A ISO/IEC 27005– GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Adrian Gustavo Miranda dos Santos
Caio Federico Esquivel Lovera Arze
Jorge Lucas da Silva Maciel
Lucas Toterol Rodrigues
Marcelo Ribeiro Karpovicz

RESUMO

Este artigo tem como principal objetivo estudar a norma internacional ISO/IEC 27005, que oferece diretrizes específicas para a gestão de riscos de segurança da informação. O artigo estuda as principais características de uma gestão de riscos eficaz e eficiente, comunicando seu valor, propósito e intenção no ambiente organizacional. As diretrizes da norma são exploradas, e abordando o contexto, plano de comunicação, papéis e responsabilidades, além da aplicação de matrizes de riscos e mapas de riscos, que são extremamente importantes no que tange a tomada de decisão da organização. Um dos objetivos do artigo, é comunicar o valor da gestão de riscos eficiente, assegurando a segurança e continuidade da organização.

Palavras-chave: ISO/IEC 27005, Gestão de Riscos, Segurança da Informação, Avaliação de Riscos, Tratamento de Riscos.

INTRODUÇÃO

Com o avanço tecnológico, a proteção de informações confidenciais passa a ser essencial. Nesse cenário, a gestão de riscos é indispensável, e a norma internacional ISO/IEC 27005 se mostra como um poderoso guia prático de identificação, avaliação, tratamento e monitoramento de riscos, apoiando a implementação e operação de um Sistema de Gestão de Segurança da Informação (SGSI), conforme a ISSO/IEC 27001 [1]. Segundo ŠENOVSKÝ, a norma fornece os fundamentos e estruturas conceituais necessárias [5]. Ferreira destaca a edição 2023 da norma, reforçando a ênfase em processos cíclicos e adaptáveis [2]. Já Konzen et al. [4] demonstram sua aplicação prática, enquanto a IT Governance [3] fornece uma visão de mercado e compliance.

O propósito da ISO/IEC 27005 é auxiliar as organizações a estabelecer, implementar, manter e melhorar continuamente um processo de gestão de riscos de segurança da informação [1]. ŠENOVSKÝ afirma que envolve a compreensão do cenário de ameaças, a identificação de vulnerabilidades e a avaliação do impacto potencial em caso de um incidente de segurança [5].

POR QUE É IMPORTANTE APLICAR ESSA NORMA?

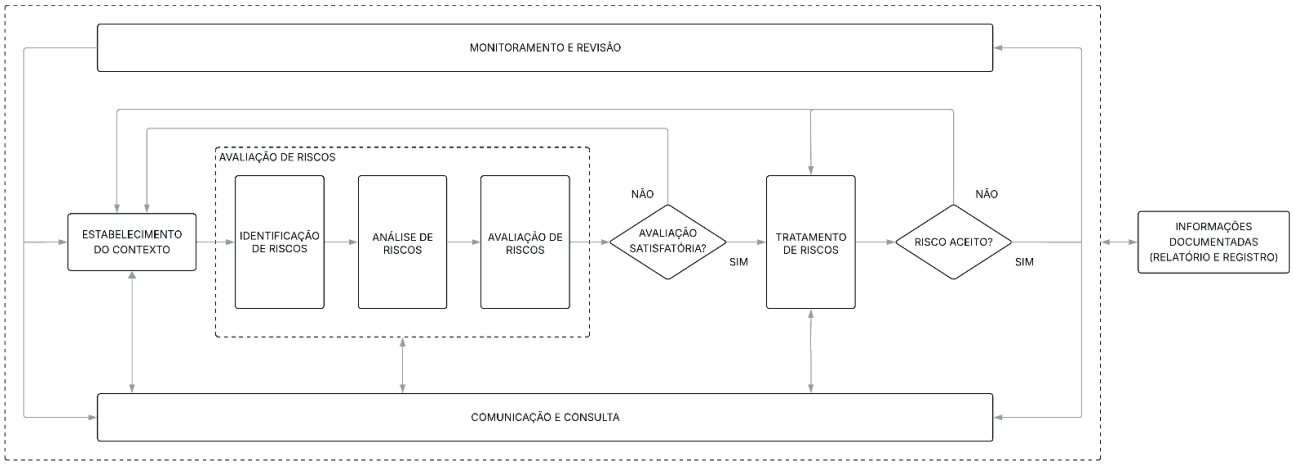
ŠENOVSKÝ diz que ameaças e riscos cibernéticos, são brechas para pessoas mal-intencionadas ganharem acesso ou comprometer o sistema, o que causa uma interrupção das

atividades de uma organização, violação dos conceitos de confidencialidade, integridade e disponibilidade, danos à reputação da empresa e perdas financeiras [5]. KONZEN et al, afirma que no cenário atual, a ISO/IEC 27005 se destaca como um padrão que orienta as organizações, oferecendo diretrizes para aprimorar a gestão de riscos de cibersegurança [4].

PROCESSO DE GESTÃO DE RISCOS

De acordo com IT Governance, a ISO/IEC 27005 não especifique um processo ou metodologia específica de gerenciamento de riscos, ela implica um processo contínuo de gerenciamento de riscos de informações com base em alguns componentes principais: estabelecimento do contexto; avaliação de riscos; tratamento de riscos; aceitação de riscos; informações documentadas; monitoramento de riscos e plano de comunicação [5]. Ferreira afirma que esse processo que o processo de gestão de riscos, funciona de maneira iterativa, e reafirma o que IT Governance afirma sobre os componentes da gestão de riscos [2]. A seguir, uma figura contendo o processo descrito acima:

Figura 1: Processo de gerenciamento de riscos.



Fonte: Autor; FERREIRA,S.

PLANO DE CONTEXTO

O primeiro passo a se fazer, para uma gestão de riscos eficaz, é a definição do contexto em que a organização opera. De acordo com ŠENOVSKÝ, este plano deve conter os fatores internos, como cultura, estrutura e políticas, e fatores externos, como legislação, partes interessadas e ameaças emergentes [5]. Ferreira reforça que essa etapa permite alinhar o escopo do SGSI aos objetivos estratégicos da organização [2]. Konzen et al. exemplificam essa definição em ambientes corporativos reais, destacando como uma compreensão sólida do contexto contribui para uma análise de riscos mais precisa [4].

PLANO DE COMUNICAÇÃO

A comunicação eficaz é fundamental para o processo de gerenciamento de riscos de segurança da informação. Segundo IT Governance, uma comunicação garante que os responsáveis pela implementação do gerenciamento de riscos entendam a base sobre a qual as decisões são tomadas e porque certas ações são necessárias [3]. Ferreira complementa indicando que o plano de comunicação deve abranger tanto situações rotineiras quanto emergenciais [2]. ŠENOVSKÝ acrescenta que o compartilhamento contínuo de informações fortalece a transparência e a colaboração na mitigação de riscos [5].

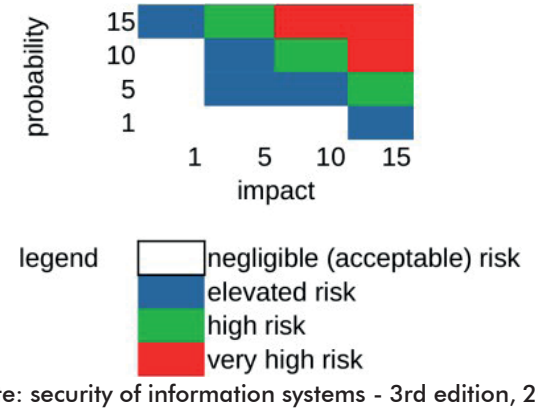
PAPÉIS E RESPONSABILIDADES

Uma clara definição de responsabilidades é essencial para gestão de riscos. Essa etapa visa decidir quem faz o que dentro da organização. ŠENOVSKÝ propõe a utilização da matriz RACI (Responsible, Accountable, Consulted, Informed), a fim de evitar duplicidade de informações ou ausência de ações [5]. Ferreira destaca a importância de envolver diferentes níveis hierárquicos, desde a alta gestão até equipes operacionais [2]. Konzen et al. mostram que a definição clara de papéis contribui para a execução coerente de cada etapa do processo de gestão de riscos [4].

MATRIZ DE RISCOS

A matriz de riscos é uma ferramenta visual que auxilia na avaliação, tomada de decisão e priorização dos riscos de segurança da informação. Ela geralmente cruza a probabilidade de ocorrência de um evento adverso com o impacto potencial que esse evento teria na organização. ŠENOVSKÝ apresenta diferentes modelos de matrizes, reforçando seu valor como instrumento visual de apoio à decisão [5]. Segundo IT Governance, o uso de matrizes qualitativas permite categorizar riscos com clareza e comunicar sua criticidade de forma acessível [2]. Exemplo na imagem abaixo:

Figura 2: Matriz de riscos

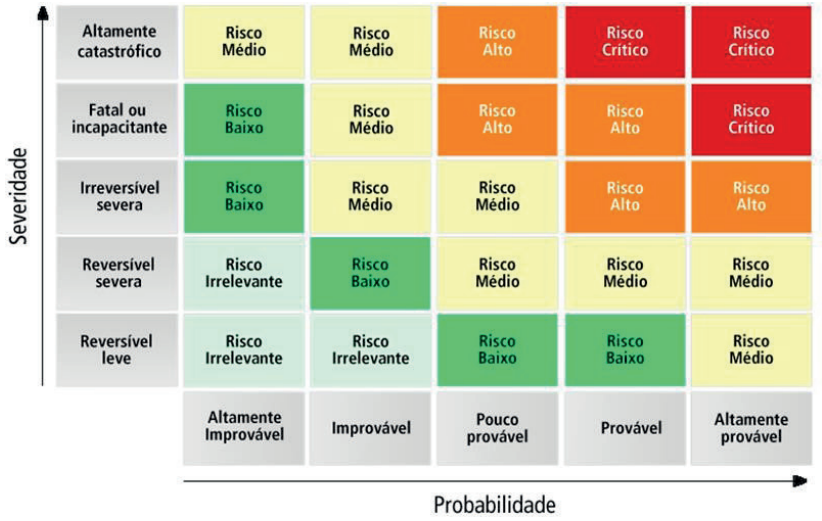


Fonte: security of information systems - 3rd edition, 2021, p.66

MAPA DE RISCOS

Mapa de riscos, também conhecido como heat map, é uma representação gráfica da matriz de riscos, frequentemente utilizando cores para indicar a criticidade dos riscos. Konzen et al. afirmam que essa abordagem facilita a visualização do perfil geral de riscos de uma organização [4]. Ferreira observa que mapas de riscos auxiliam no acompanhamento contínuo e na revisão periódica da matriz, especialmente em ambientes dinâmicos [2]. Exemplo na imagem abaixo:

Figura 3: Matriz de riscos qualitativa (heat map)



Fonte: FERREIRA, S.

CONSDERAÇÕES FINAIS

ISO/IEC 27005 oferece uma estrutura robusta para a gestão de riscos da segurança da informação, sendo fundamental para proteger os ativos valiosos das organizações. Ao combinar conceitos fundamentais teóricos, como os apresentados por ŠENOVSKÝ [1], com aplicações práticas e atualizações normativas discutidas por Ferreira [2], Konzen et al. [3] e IT Governance [4], o artigo demonstra como a abordagem estruturada da norma promove decisões mais seguras, alinhadas aos objetivos organizacionais.

REFERÊNCIAS

[1] ABNT NBR ISO/IEC 27005:2023. Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2023.

[2] FERREIRA, S. Universo Segurança da Informação: NBR ISO/IEC 27005:2023. Disponível em: https://www.estrategiaconcursos.com.br/blog/seguranca-informacao- iso-27005-2023/. Acesso em: 4 jun. 2025.

[3] IT GOVERNANCE. ISO 27005 | IT Governance UK. Disponível em: https://www.itgovernance.co.uk/iso27005. Acesso em: 4 jun. 2025.

[4] KONZEN, Marcos Paulo. Gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005 usando padrões de segurança. 2013. Disponível em: https://repositorio.ufsm.br/handle/1/8276. Acesso em: 4 jun. 2025.

[5] ŠENOVSKÝ, P. Security of Information Systems - 3rd Edition. Ostrava, 2021.Disponível em: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/bis_3ed.pdf. Acesso em: 1 de jun. de 2025.