Instanciação do Processo de Gestão de Riscos de Segurança da Informação da ISO 27005 em Organizações Públicas

Vinícius N. Vasconcelos[1], Fernando A. A. Lins[1] , George Valença[1], Maria A. P. F. Losse[2], Ana C. C. M. Morais[2], Edgard T. Sousa[2]

[1]Departamento de Computação
Universidade Federal Rural de Pernambuco (UFRPE) – Recife, PE – Brasil
{viniciusnario,fernandoaires,george.valenca}@ufrpe.br

[2]Tribunal de Contas do Estado de Pernambuco (TCE-PE) - Recife, PE - Brasil
{alice,anacarolina,edgard}@tcepe.tc.br

Resumo. *O aumento dos ataques cibernéticos elevou o interesse por Segurança da Informação. Uma das áreas mais importantes da segurança atualmente é a Gestão de Riscos, onde notadamente se evidencia a identificação de vulnerabilidades e riscos como uma atividade essencial. Neste contexto, a ISO 27005 oferece diretrizes para esse processo, mas há uma lacuna sobre como instanciá-la de forma detalhada e repetível. Este trabalho apresenta uma instanciação prática, baseada em Business Process Management (BPM), deste processo em uma organização pública, detalhando atividades essenciais e também possibilitando a sua replicação por outras organizações interessadas. Os resultados mostram que o uso de BPM facilitou a implantação e ajudou a evidenciar atividades muitas vezes subestimadas, como definição de contexto e aceitação de riscos, aprimorando a gestão de riscos de Segurança da Informação.*

Abstract. *The increase in cyberattacks has heightened interest in Information Security. One of the most important areas of security today is Risk Management, where the identification of vulnerabilities and risks stands out as an essential activity. In this context, ISO 27005 provides guidelines for this process, but there is a gap regarding how to instantiate it in a detailed and repeatable manner. This work presents a practical instantiation of this process in a public organization, based on Business Process Management (BPM), detailing essential activities and enabling its replication by other interested organizations. The results show that the use of BPM facilitated implementation and helped highlight often underestimated activities, such as context definition and risk acceptance, enhancing Information Security risk management.*

1. Introdução

A transformação digital tem provocado mudanças profundas nas organizações públicas e privadas, impulsionando a adoção de tecnologias avançadas como Computação em Nuvem, Inteligência Artificial e Internet das Coisas. Essas inovações não apenas otimizam processos internos e melhoram a eficiência operacional, mas também possibilitam a oferta de serviços mais ágeis e personalizados. No setor público, a digitalização é uma oportunidade para democratizar o acesso a serviços essenciais, promover maior transparência nas operações e estreitar a relação entre governo e sociedade (OECD, 2021).

Entretanto, essa evolução tecnológica também introduz desafios significativos, especialmente no campo da Segurança da Informação. A crescente interconexão de sistemas e a expansão dos ambientes digitais têm exposto governos e organizações públicas a um aumento expressivo de ameaças cibernéticas (Dantas, 2024). Ataques como *ransomware*, violações de dados e *phishing* comprometem informações sensíveis, interrompem serviços essenciais e minam a confiança dos cidadãos nas plataformas digitais governamentais (Dantas, 2024). Diante desse cenário, a Gestão de Riscos de Segurança da Informação surge como uma das possíveis abordagens para defender as organizações contra essas ameaças, garantindo maior resiliência e continuidade operacional.

A Gestão de Riscos é uma atividade fundamental para organizações públicas, uma vez que existe uma ampla gama de ameaças que podem prejudicar o cumprimento da missão e o alcance dos objetivos destas entidades. Entre essas ameaças, destacam-se falhas operacionais, fraudes, corrupção, ataques cibernéticos, mudanças na legislação, instabilidade política, desastres naturais, má gestão de recursos, perda de dados sensíveis, falta de capacitação dos servidores e interrupções nos sistemas de tecnologia da informação. A implementação e melhoria de processos de Gestão de Riscos de Segurança da Informação ajuda a identificar, avaliar e mitigar essas ameaças potenciais. Com um processo de gestão de riscos eficaz, as organizações públicas podem se proteger melhor contra tais riscos. Além disso, a Gestão de Riscos também pode prover suporte à melhoria na tomada de decisão, identificando e avaliando os riscos associados às diferentes ameaças.

Atualmente, um dos padrões mais relevantes neste contexto é a norma ISO/IEC 27005:2022 (ISO, 2022), que propõe um processo para a Gestão de Riscos de Segurança da Informação (SI) em organizações. Este processo pode ser encarado como um guia teórico para dar suporte a esta gestão. Contudo, detalhes específicos da execução das atividades não são suficientemente aprofundados, dificultando a instanciação das mesmas em organizações.

Para preencher essa lacuna, o *Business Process Model* (BPM) surge como uma solução viável, permitindo modelar regras e padrões em processos práticos e visualmente compreensíveis. O BPM possibilita modelar processos organizacionais de forma padronizada, utilizando diagramas que tornam claras as etapas necessárias para alcançar os objetivos propostos (Grefen e Vanderfeesten, 2024). Aplicado à Gestão de Riscos, a metodologia BPM possibilita detalhar cada etapa das práticas recomendadas pela ISO/IEC 27005:2022, facilitando a identificação, análise e tratamento de riscos de forma mais estruturada e automatizada.

Neste contexto, o principal objetivo deste trabalho é a instanciação prática, através de um processo modelado com base no padrão BPM (*Business Process Model*), da abordagem descrita na ISO/IEC 27005:2022. Essa abordagem visa não apenas detalhar o processo de Gestão de Riscos de Segurança da Informação, mas também viabilizar sua execução e automação, promovendo maior clareza e eficiência nos processos internos de Gestão de Riscos de organizações públicas.

Este artigo está organizado da forma que se segue. A Seção 2, Conceitos Básicos, apresenta informações básicas importantes para o entedimento deste trabalho. A Seção

3, Trabalhos Relacionados, discute pesquisas relacionadas que abordam a implementação de processos de Gestão de Riscos. A Seção 4 detalha a abordagem proposta, baseada em BPM, para a implementação da norma ISO/IEC 27005:2022 em organizações públicas. A Seção 5, Resultados, analisa os avanços alcançados com a aplicação da proposta, incluindo os impactos observados. A Seção 6, Conclusões e Trabalhos Futuros, sintetiza os principais achados, reforçando as contribuições da abordagem e descreve possibilidades de pesquisas futuras.

2. Conceitos Básicos

2.1 Gestão de Riscos de Segurança da Informação

A Segurança da Informação é um conjunto de práticas, políticas e controles voltados para proteger dados e sistemas contra acessos não autorizados, modificações indevidas e indisponibilidade. Seu objetivo é melhorar a confidencialidade, dificultando o acesso a informações sensíveis por pessoas não autorizadas; a integridade, assegurando que os dados não sejam alterados indevidamente; e a disponibilidade, garantindo que informações e sistemas estejam acessíveis sempre que necessário. Para alcançar esses objetivos, são adotados mecanismos como controle de acesso e autenticação. Além disso, a conscientização dos usuários é essencial, pois o fator humano desempenha um papel central na manutenção da segurança.

Dentro da Segurança da Informação, a Gestão de Riscos é fundamental para identificar, analisar e tratar ameaças antes que comprometam a operação da organização. Esse processo envolve a avaliação dos ativos de informação, a identificação de vulnerabilidades, a análise dos impactos potenciais e a implementação de controles para mitigar riscos. Esses riscos podem ter diversas origens, como ataques cibernéticos, falhas humanas, exploração de vulnerabilidades tecnológicas e até eventos externos imprevisíveis, como desastres naturais ou crises econômicas.

No contexto da Segurança da Informação, risco é a possibilidade de que uma ameaça explore uma vulnerabilidade, resultando em impactos negativos. Esses impactos podem comprometer a confidencialidade, a integridade ou a disponibilidade das informações, gerando prejuízos financeiros, danos à reputação ou impactos operacionais. A avaliação de riscos considera a probabilidade de ocorrência e a gravidade das consequências, enquanto a mitigação envolve a adoção de medidas preventivas que reduzem vulnerabilidades e aumentam a resiliência dos sistemas.

A Gestão de Riscos não é um processo isolado, mas contínuo, exigindo monitoramento e revisão constantes para adaptação às novas ameaças e ao cenário dinâmico da tecnologia e dos negócios. A adoção de frameworks e normas, como a ISO/IEC 27005:2022 (ISO, 2022), auxilia na estruturação desse processo, garantindo que decisões sejam tomadas com base em critérios bem definidos e alinhados aos objetivos estratégicos da organização.

A ISO/IEC 27005:2022 é uma norma internacional que fornece diretrizes para a Gestão de Riscos em Segurança da Informação. Seu objetivo é estabelecer um modelo sistemático para identificar, avaliar e tratar riscos, permitindo que organizações implementem um processo contínuo de monitoramento e melhoria (ISO, 2022). A norma descreve etapas fundamentais, como a definição do contexto organizacional, a

identificação de ameaças e vulnerabilidades, a análise dos impactos potenciais e a tomada de decisões sobre o tratamento dos riscos. Nesse sentido, metodologias que estruturam e otimizam processos organizacionais podem potencializar a eficácia da Gestão de Riscos de S.I.

2.2 Business Process Management

No contexto da gestão organizacional, o *Business Process Management* (BPM) é uma metodologia voltada a aprimorar a forma como uma empresa executa suas atividades. Essa abordagem envolve a análise, modelagem, execução e monitoramento dos processos de negócio, com o objetivo de torná-los mais eficientes e alinhados aos objetivos estratégicos. Por meio do BPM, organizações podem detectar gargalos operacionais, propor melhorias constantes e aumentar a agilidade na entrega de produtos ou serviços (Grefen e Vanderfeesten, 2024). Além disso, a adoção de boas práticas de BPM permite melhorar a conformidade com normas e regulamentos, reduzindo riscos e trazendo maior transparência para o processo de tomada de decisão. Para tornar essa metodologia ainda mais clara e sistematizada, surge a necessidade de uma linguagem que facilite a visualização dos processos de negócio.

É justamente nesse cenário que ganha destaque o Business Process Model and Notation (BPMN), uma notação padrão para a representação de processos de negócio em formato gráfico (OMG, 2011). Por meio de símbolos como eventos, atividades e gateways, o BPMN permite criar diagramas que ilustram o fluxo de trabalho de maneira acessível a todos os envolvidos, sejam analistas de negócios ou desenvolvedores de software. Essa padronização não apenas facilita a compreensão e a troca de informações entre as áreas, mas também viabiliza a automação de tarefas, pois os diagramas podem ser convertidos em fluxos de trabalho executáveis. Dessa forma, o BPMN reforça a efetividade do BPM, garantindo maior controle das operações e adesão às regras de negócio.

3. Trabalhos Relacionados

A Gestão de Riscos de Segurança da Informação (GRSI) tem sido debatida e aplicada, especialmente em organizações públicas que buscam conformidade com a ISO/IEC 27005. No entanto, sua aplicação prática enfrenta desafios, como a falta de diretrizes detalhadas para instanciação e adaptação da mesma frente a diferentes contextos.

Santos e Filho (2013) propõem um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008. O modelo visa guiar a implementação de um novo sistema ou verificar a conformidade de um sistema existente. Contudo, o estudo se concentra apenas na conformidade normativa, sem aprofundar-se em aspectos práticos da instanciação do processo de Gestão de Riscos, o que dificulta sua aplicação prática em organizações públicas.

Furlan e Pacheco (2021) analisam os desafios da implantação da Gestão de Riscos na Administração Pública com um estudo de caso no Instituto Federal Catarinense. O trabalho dos autores diferencia os conceitos de implantação (fase inicial de estruturação do processo) e implementação (fase operacional), destacando dificuldades como a falta

de entendimento por parte dos servidores e a ausência de indicadores eficazes. No entanto, a pesquisa não propõe um modelo detalhado de instanciação do processo de Gestão de Riscos, o que limita sua aplicabilidade em organizações que buscam uma referência prática e reprodutível.

Silva (2017) propõe diretrizes para a Gestão de Riscos de Segurança da Informação em instituições federais de ensino superior, com base nas normas ISO/IEC 27005:2011 e ISO/IEC 31000:2009. A pesquisa revela que apenas 2% das instituições analisadas aplicam integralmente uma política de Gestão de Riscos, evidenciando a necessidade de modelos acessíveis. O trabalho, entretanto, foca na criação de diretrizes e não na operacionalização dessas diretrizes por meio de um processo detalhado.

Konzen (2013) desenvolve uma metodologia para Gestão de Riscos baseada na norma NBR ISO/IEC 27005:2008 utilizando padrões de segurança para estruturar a análise e avaliação de riscos. A abordagem busca reutilizar soluções testadas para tornar a implementação mais eficaz. Apesar de ser uma contribuição interessante, a pesquisa não aborda a instanciação prática do processo dentro de um contexto organizacional específico.

Balke (2015) propõe uma abordagem colaborativa para a Gestão de Riscos, baseada em argumentação estruturada e jogos de diálogo. A metodologia utiliza um sistema de discussão para aprimorar a qualidade da tomada de decisão no gerenciamento de riscos. Embora promissora, a abordagem é mais voltada para a comunicação entre *stakeholders* do que para a instanciação do processo de Gestão de Riscos em si.

Os trabalhos analisados fornecem contribuições interessantes para a Gestão de Riscos de Segurança da Informação, mas ainda há lacunas importantes na literatura. A maioria das abordagens concentra-se em diretrizes estratégicas, conformidade normativa ou metodologias conceituais, sem apresentar um modelo detalhado de instanciação do processo de Gestão de Riscos que possa ser aplicado diretamente em organizações públicas.

O trabalho proposto neste artigo busca preencher essa lacuna ao propor uma instanciação prática do processo de Gestão de Riscos de Segurança da Informação especificado na ISO/IEC 27005:2022, utilizando a modelagem de processos de negócio (BPM) para estruturar e detalhar cada etapa do processo. Dessa forma, se vislumbra fornecer um modelo replicável e adaptável às necessidades das organizações públicas, possibilitando facilitar a adoção e melhoria da Gestão de Riscos de Segurança da Informação destas organizações.

4. Instanciação do Processo de Gestão de Riscos de S.I.

4.1 Visão Geral

A abordagem proposta visa estruturar a implementação da norma ISO/IEC 27005:2022 em organizações públicas, tendo como estudo de caso o Tribunal de Contas do Estado de Pernambuco (TCE-PE), órgão responsável pela fiscalização contábil, financeira, orçamentária, operacional e patrimonial da administração pública estadual e municipal.

A metodologia adotada foi a pesquisa-ação, com participação ativa dos principais stakeholders na formulação de diagnósticos e soluções. O estudo ocorreu em seis ciclos (mar/2023–jan/2025): (i) diagnóstico participativo, (ii) modelagem BPMN, (iii) validação em workshop, (iv) importação para a Plataforma Channel, (v) execução piloto e (vi) medição de KPIs. Complementarmente, utilizou-se a Abordagem Baseada em Problemas (PBL), tratando aspectos da Gestão de Riscos como problemas reais. A modelagem foi estruturada em diversos subprocessos, como por exemplo identificação, análise, avaliação e tratamento de riscos. O trabalho seguiu uma abordagem participativa e colaborativa, com entrevistas, reuniões e levantamento de práticas existentes.

A Figura 1 apresenta a modelagem geral do Processo de Gestão de Riscos de Segurança da Informação, estruturada conforme as diretrizes da ISO/IEC 27005:2022.

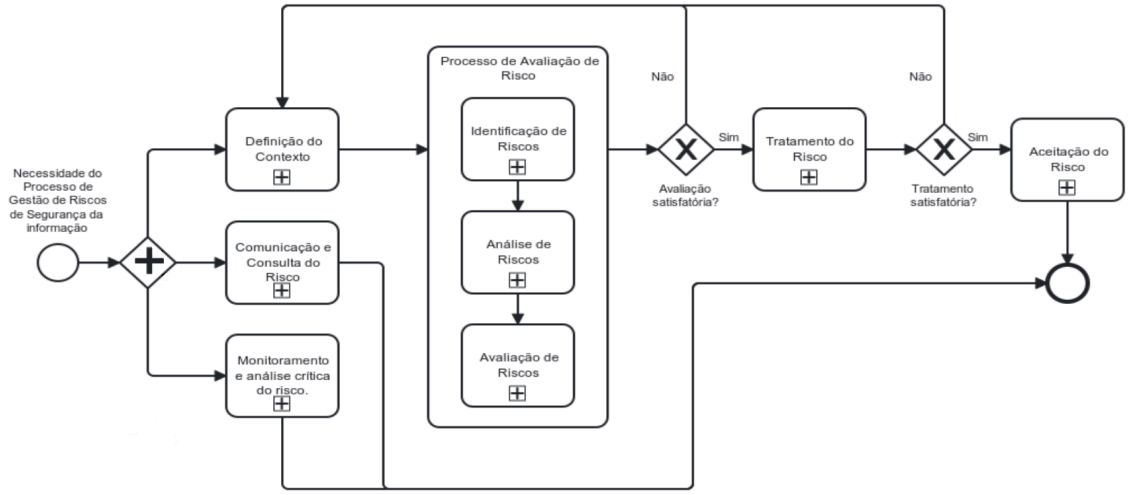

Figura 1. Modelagem do processo geral de Gestão de Riscos de SI proposto pela norma ISO 27005.

O processo geral abordado é composto por diversos subprocessos, cada um contendo internamente duas ou mais atividades. O principal desafio na implementação prática deste processo foi a estruturação e o detalhamento das atividades associadas a cada um dos subprocessos representados na Figura 1. Além disso, foram definidas estruturas condicionais para indicar os diferentes fluxos que o processo pode seguir na prática.

4.2 Modelagem dos subprocessos

A Figura 2 ilustra a modelagem do subprocesso "Definição do Contexto", especificado na Figura 1. Nela, é possível observar não apenas o detalhamento das atividades que devem ser realizadas, mas também a sequência lógica em que devem ocorrer. Esse nível de clareza facilita a compreensão e a replicação do processo por outros interessados.

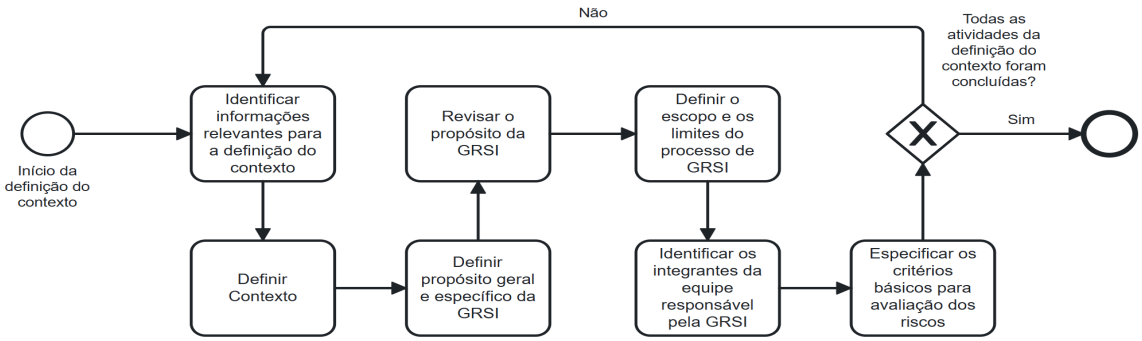

Figura 2. Modelagem do subprocesso de Definição do Contexto.

A definição do contexto se demonstrou essencial para a modelagem da gestão de riscos de S.I, pois estabelece as bases do processo como um todo. Nessa fase, a organização identifica ativos críticos, mapeia *stakeholders*, define limites e critérios de avaliação de riscos, considerando cultura organizacional, maturidade em segurança e regulamentações.

Inicialmente, é necessário mapear o ambiente operacional e os ativos a serem protegidos, como sistemas, dados e infraestrutura, por meio de consultas a *stakeholders* e análise documental. Também se avalia quais são os impactos legais e operacionais que devem ser considerados para o alinhamento estratégico. Também é importante definir as dimensões de impacto e níveis de probabilidade, garantindo uma análise estruturada, considerando disponibilidade, confidencialidade e integridade das informações. Além disso, delimita-se o escopo da gestão de riscos S.I, estabelecendo áreas contempladas e recursos necessários. Questões como inclusão de setores, categorização de ativos e requisitos legais devem ser analisadas.

Com o contexto definido, é possível iniciar a fase de identificação de riscos. Estes riscos são levantados a partir de diferentes fontes, como auditorias, testes de penetração, incidentes reportados e avaliações de vulnerabilidades. A Figura 3 ilustra a modelagem desse subprocesso.

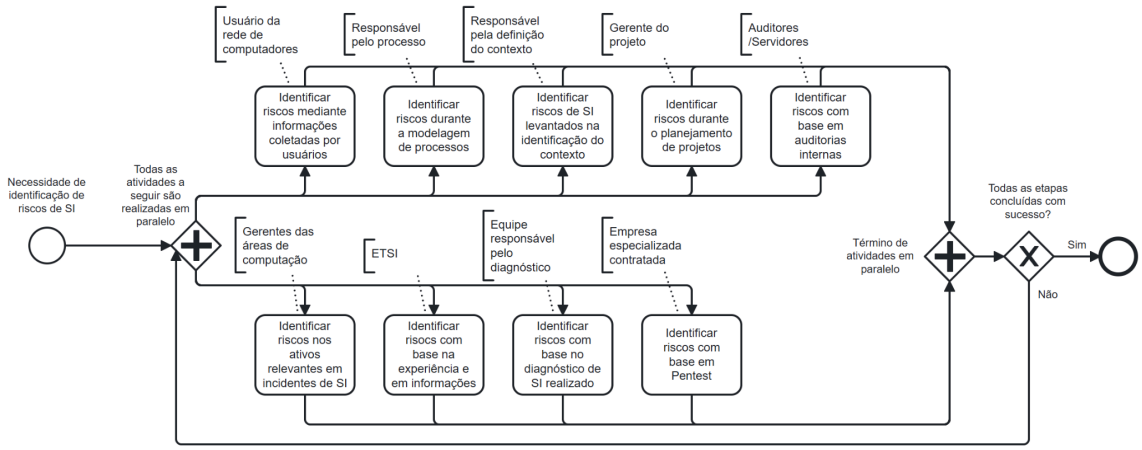

Figura 3. Detalhamento do subprocesso de Identificação de Riscos.

No subprocesso apresentado na Figura 3, observa-se que diversas atividades de identificação de riscos são executadas em paralelo. Esse estágio demanda um esforço considerável da organização, uma vez que múltiplas ações precisam ser conduzidas

simultaneamente para garantir a identificação dos riscos mais relevantes. O sucesso dessa etapa depende da capacidade da organização de consolidar informações estratégicas, permitindo uma visão das ameaças à Segurança da Informação.

Após a identificação de riscos, são conduzidos os subprocessos de análise de riscos e avaliação de riscos, responsáveis pela classificação e priorização das ameaças identificadas. Nesse estágio, os riscos são quantificados com base na probabilidade de ocorrência e no impacto potencial, permitindo determinar seu grau de severidade e estabelecer uma abordagem prática para mitigação.

Para estruturar melhor essa avaliação, foram definidas categorias de impacto que possibilitam uma análise mais detalhada e alinhada ao contexto da organização. As categorias estabelecidas foram pessoas, ativos da informação, imagem institucional e continuidade do negócio.

A categoria “pessoas” avalia o impacto do risco sobre a segurança, integridade e bem-estar dos colaboradores e cidadãos afetados. Já a categoria “ativos da informação” considera a possível perda, vazamento ou comprometimento de dados críticos através dos ativos de informação da organização. A categoria “imagem institucional” refere-se ao impacto sobre a reputação e credibilidade da organização perante o público, fornecedores e órgãos reguladores. Por fim, a categoria “continuidade do negócio” mensura a possibilidade de interrupção das operações e o nível de comprometimento da prestação de serviços essenciais.

Concluída a avaliação dos riscos, inicia-se o subprocesso de tratamento do risco, que tem como objetivo efetivar a implementação de medidas corretivas ou preventivas. A Figura 4 apresenta a modelagem desse subprocesso.

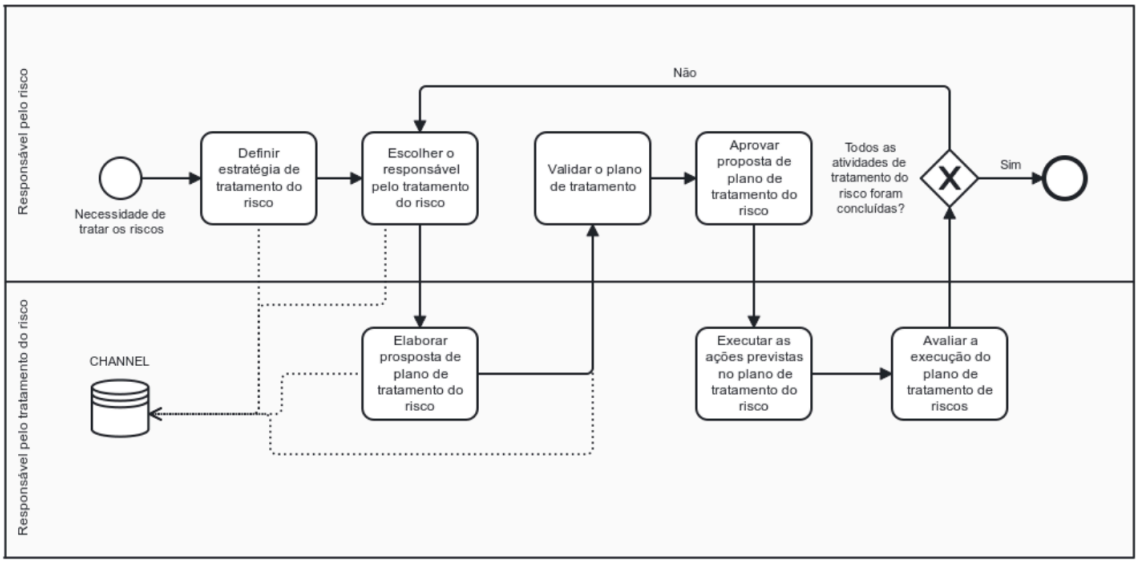

Figura 4. Detalhamento do subprocesso de Tratamento do Risco.

Inicialmente, observa-se a atuação de dois stakeholders principais: o responsável pelo risco e o responsável pelo tratamento do risco. O responsável pelo risco tem a função de identificar e contextualizar o risco dentro da organização, indicar quem será encarregado do tratamento e avaliar a proposta de plano de ação apresentada. Além disso, é sua

responsabilidade garantir que o risco seja devidamente registrado, categorizado e analisado antes da definição das estratégias de mitigação.

Já o responsável pelo tratamento do risco é encarregado de elaborar um plano de ação detalhado, contemplando as medidas necessárias para reduzir a probabilidade de ocorrência ou minimizar os impactos caso o risco se concretize. Além disso, ele deve garantir a implementação das ações propostas, acompanhar a execução de cada etapa e monitorar continuamente a eficácia das medidas adotadas. Esse monitoramento permite ajustes estratégicos caso novos fatores de risco surjam ou a efetividade das ações precise ser revisada.

Após o tratamento do risco, é possível que a probabilidade de ocorrência do mesmo ou o seu impacto tenham sido reduzidos a zero. Contudo, é também possível que reste um risco residual, que não foi totalmente eliminado no tratamento. Para este caso, o subprocesso de aceitação do risco foi modelado[1], e o mesmo busca assegurar que a existência deste risco residual seja avaliada pela organização. A gestão desta organização poderá definir se o risco residual está em um nível aceitável ou não. Caso esteja, o risco é considerado aceito e um documento específico deve ser assinado para formalizar esta decisão. Caso contrário, é possível voltar para atividades anteriores do processo de Gestão de Riscos (ex.: tratamento do risco) e se realizar ações para diminuir ainda mais ou mesmo eliminar o risco residual.

É importante ressaltar que o processo de Gestão de Riscos, proposto na Figura 1, deixa também evidente a importância da comunicação e do monitoramento do risco[1]. A execução da comunicação do risco às partes interessadas busca garantir que todos os stakeholders ligados a aquele risco específico sejam notificados de eventos relevantes (como, por exemplo, proposição de um novo plano de tratamento). Por outro lado, o processo de monitoramento busca garantir que esforços sejam empreendidos na atualização periódica de informações sobre o risco.

Finalmente, em relação à implantação do processo proposto na Figura 1, é também importante ressaltar que o mesmo envolveu a definição do apetite por riscos da organização, alinhando as estratégias de mitigação de riscos com os objetivos organizacionais. Isso incluiu a realização de avaliações periódicas do processo de Gestão de Riscos da instituição, identificando oportunidades de melhoria e propondo ações corretivas.

4.3 Suporte ferramental

Para dar suporte às atividades do processo de Gestão de Riscos proposto, foi adotada uma ferramenta tecnológica com o objetivo de auxiliar de forma estruturada na identificação, análise, avaliação e tratamento dos riscos. Após uma análise das soluções disponíveis no mercado, optou-se pela Plataforma Channel (JExperts, 2024), já utilizada em outros contextos dentro da organização. A escolha eliminou custos adicionais com aquisição e reduziu o tempo de adoção, já que diversos stakeholders já estavam familiarizados com seu uso. O Channel é uma plataforma dedicada à gestão, oferecendo recursos como registro centralizado, atribuição de responsabilidades, monitoramento de ações, geração de relatórios e apoio à tomada de decisão.

[1] Todos os subprocessos modelados estão disponíveis neste link.

5. Resultados

Com a implementação do processo de Gestão de Riscos proposto neste artigo, a definição do contexto da gestão de riscos de segurança da informação foi significativamente aprimorada, proporcionando uma caracterização mais detalhada do ambiente organizacional. Esse refinamento foi essencial para as etapas subsequentes do processo. Antes da modelagem e implantação do novo processo, esse contexto carecia de um detalhamento mais aprofundado, conforme recomendado pela ISO/IEC 27005:2022. A nova abordagem não apenas evidenciou a importância de uma definição clara, mas também destacou a necessidade de explorar aspectos específicos, tornando esse subprocesso fundamental para atividades como a avaliação e a aceitação de riscos.

Além disso, a análise de riscos foi aprimorada com a introdução de critérios mais detalhados para quantificação, considerando tanto a probabilidade de ocorrência quanto o impacto potencial. Anteriormente, essa atividade apresentava desafios para gestores sem formação específica na área. Contudo, com a adoção de diretrizes mais claras, as avaliações tornaram-se mais precisas. O detalhamento do processo estabeleceu parâmetros para avaliação, monitoramento e tratamento dos riscos, permitindo decisões mais embasadas em indicadores concretos.

Outro resultado importante foi a possibilidade de responsabilização dos riscos, garantindo que cada risco fosse atribuído a um gestor específico. Esse responsável passou a acompanhar continuamente o risco e a indicar colaboradores para conduzir ou gerenciar as ações de mitigação. Assim, cada risco passou a contar com uma equipe dedicada, disponível para esclarecimentos ou ajustes no plano de mitigação. A descentralização permitiu ainda que os riscos fossem monitorados diretamente pelas áreas responsáveis, garantindo maior especialização no acompanhamento e no tratamento das vulnerabilidades.

A adoção de uma ferramenta específica para registro e gestão de riscos também trouxe ganhos importantes. Antes, essas atividades eram realizadas manualmente ou por meio de planilhas, dificultando o acompanhamento contínuo e a atualização das informações. A adoção da Plataforma Channel (JExperts 2024) permitiu maior controle e eficiência na administração dos riscos.

A execução do novo processo exigiu mudanças na aceitação de riscos, que foi reformulada para assegurar que essa decisão fosse tomada de maneira estratégica pela gestão organizacional, e não apenas pelo setor de Segurança da Informação ou de Cibersegurança. Essa mudança alinhou o processo à ISO 27005 e reforçou a compreensão de que, em alguns casos, conviver com um risco dentro de níveis aceitáveis pode ser mais vantajoso do que investir recursos excessivos para mitigá-lo.

Outro resultado interessante obtido foi a melhoria na comunicação de riscos. A nova abordagem facilitou o compartilhamento de informações entre a equipe de Segurança da Informação, os gestores de riscos locais e os responsáveis pelos tratamentos, permitindo que desafios como prazos e planos de mitigação fossem gerenciados de forma mais eficiente.

Antes da implementação do processo proposto, a organização havia identificado cerca de 30 riscos. Com o novo processo, esse número passou para mais de 188, abrangendo

áreas como pessoas, ativos da informação, imagem institucional e continuidade do negócio. Os riscos foram mapeados em domínios como LGPD, gestão de incidentes, controle de acesso e segurança operacional. A avaliação dos riscos utilizou critérios de impacto e probabilidade. Já os resultados foram medidos por métricas como tempo médio de tratamento, índice de riscos tratados e frequência de atualizações nos registros. Mais de 76 riscos tiveram seus tratamentos iniciados, evidenciando maior controle e efetividade na gestão.

6. Conclusões e Trabalhos Futuros

A instanciação do processo de Gestão de Riscos de Segurança da Informação baseada na norma ISO/IEC 27005:2022 trouxe avanços interessantes para a organização. A modelagem do processo em BPM permitiu uma estruturação mais clara das atividades, facilitando sua implementação e proporcionando maior transparência na definição de responsabilidades. Além disso, a abordagem adotada melhorou a identificação e análise dos riscos.

Entre os principais benefícios observados, destaca-se o aprimoramento na definição do contexto da gestão de riscos, proporcionando uma visão mais ampla e adaptada às necessidades organizacionais. A análise e avaliação de riscos também se tornaram mais robustas, permitindo que as prioridades fossem estabelecidas de forma objetiva. Além disso, o uso de uma ferramenta de apoio estruturou o registro e monitoramento contínuo dos riscos, tornando o processo mais eficiente e acessível para todos os envolvidos.

Como limitação do trabalho, é importante destacar que este artigo focou em um estudo de caso específico (uma organização pública importante, mas que suas demandas e características podem diferir de outras organizações do mesmo setor e de organizações públicas com foco distinto).

Como trabalho futuro, pretende-se ampliar o uso de métricas e indicadores para monitorar a efetividade das ações implementadas, auxiliando na tomada de decisões estratégicas. O uso de soluções baseadas em inteligência artificial para automatizar a identificação e análise de riscos representa uma oportunidade interessante de continuidade deste trabalho. Por fim, se vislumbra que a adoção de metodologias quantitativas podem complementar as análises qualitativas já utilizadas, proporcionando um embasamento mais sólido para as decisões organizacionais.

Referências

OECD (2021). *The E-Leaders Handbook on the Governance of Digital Government*. OECD Publishing. Disponível em: https://www.oecd.org/en/publications/the-e-leaders-handbook-on-the-governance-of-digital-government_ac7f2531-en.html.

Dantas, D. (2024, julho 24). Incidentes cibernéticos em sistemas do governo dobram no primeiro semestre de 2024. G1. Recuperado em 04 de janeiro de 2025, de https://g1.globo.com/politica/noticia/2024/07/24/incidentes-ciberneticos-em-sistemas-do-governo-dobram-no-primeiro-semestre-de-2024.ghtml

International Organization for Standardization (2022). *ISO/IEC 27005:2022 — Information security risk management*. Recuperado em 04 de janeiro de 2025, de https://www.iso.org/standard/80585.html.

Grefen, P. and Vanderfeesten, I. (Eds.) (2024) *Handbook on Business Process Management and Digital Transformation*, Research Handbooks in Information Systems, Edward Elgar Publishing, ISBN: 978-1-80220-608-1, 450 pp.

Object Management Group (OMG) (2011). Business Process Model and Notation (BPMN), Version 2.0. OMG Specification, formal/2011-01-03. Available at: https://www.omg.org/spec/BPMN/2.0/About-BPMN/

Furlan, L. and Pacheco, A. (2021). "Gestão de risco: Estudo de caso sobre os desafios na implantação e na implementação". *Revista Ibero-Americana de Estratégia*, 20(1), 1–23.

Silva, J. (2017). "Diretrizes Estratégicas de Gestão de Riscos de Segurança da Informação para Instituições Federais de Ensino Superior". *Dissertação de Mestrado*, Universidade Federal de Pernambuco, Brasil. Disponível em: https://repositorio.ufpe.br/handle/123456789/23996 (último acesso: 22 fev. 2024).

Konzen, M. P. (2013). "Gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005 usando padrões de segurança". *Dissertação de Mestrado*, Universidade Federal de Santa Maria. Disponível em: https://repositorio.ufsm.br.

Balke, M. (2015). "Abordagem colaborativa para gerenciamento de riscos de segurança da informação". *Dissertação de Mestrado*, Universidade Federal de Santa Maria. Disponível em: https://repositorio.ufsm.br.

Santos, V. O. and Baldini Filho, R. (2013). "Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008". *Revista Telecomunicações*, 15(1). Disponível em: https://revistatelecom.com.br.

Channel PMO (n.d.). *Channel PMO*. Recuperado em 04 de janeiro de 2025, de https://channelpmo.com.br/.

International Organization for Standardization (2018). ISO 31000:2018 — Risk management — Guidelines. Recuperado em 04 de janeiro de 2025, de https://www.iso.org/standard/65694.htm.