REVISÃO DE MODELOS E NORMAS EM GESTÃO DE RISCOS CIBERNÉTICOS

REVIEW OF MODELS AND STANDARDS IN CYBER RISK MANAGEMENT

Gerson Luiz Camillo [1]
Cássio Aurélio Suski [2]

RESUMO: Este artigo trata da gestão de riscos na cibersegurança, pois a segurança da informação está adquirindo importância nos níveis superiores de decisão das organizações. Atualmente, há diversas propostas de metodologias de análise de risco cibernético por meio de padrões e normas. Além disso, têm sido apresentados artigos com propostas alternativas para suprir deficiências ou para especializar os padrões em gestão de riscos. Este trabalho teve por objetivo apresentar esses modelos e destacar as abordagens adotadas quanto aos métodos usados para analisar, qualificar e quantificar riscos. A metodologia adotada foi de pesquisa bibliográfica em normas e artigos científicos. Os resultados indicam que as normas e trabalhos mais recentes estão dando maior enfoque à análise quantitativa dos riscos, pois os dados podem ser agregados à análise de risco corporativo. As abordagens mais recentes adotam estimativas das incertezas dos riscos usando os dois principais métodos: simulações de Monte Carlo e análise Bayesiana.

Palavras-chave: risco; cibersegurança; gestão.

ABSTRACT: *This article addresses risk management in cybersecurity, as information security is gaining importance at the highest levels of decision-making organizations. Currently, several proposals for cyber risk analysis methodologies exist through standards and norms. Moreover, we presented articles with alternative proposals to fill deficiencies or to standardize risk management. This paper aims to present these models and highlight the approaches adopted regarding the methods used to analyze, qualify, and quantify risks. The methodology adopted was bibliographical research in standards and scientific articles. The findings suggest that the quantitative analysis of risks is garnering more attention in the most recent standards and works, as it is feasible to accumulate data for corporate risk analysis. The latest methods incorporate estimates of risk uncertainties, utilizing two primary techniques: Monte Carlo simulations and Bayesian analysis.*

Keywords: *risk; cybersecurity; management.*

[1] Mestrando em Clima e Ambiente. Instituto Federal de Santa Catarina.
E-mail: gerson.camillo@gmail.com
[2] Doutor em Ciência e Engenharia de Materiais. Instituto Federal de Santa Catarina.
E-mail: cassio.suski@ifsc.edu.br

1 INTRODUÇÃO

A informação e o seu processamento em meios eletrônicos estiveram presentes desde os primórdios do século passado, através dos desenvolvimentos atrelados à Segunda Guerra Mundial (Bombe; 2021, ENIAC; 2021). Nas décadas seguintes, seguiu para o desenvolvimento comercial e científico e, nas décadas de 1970 e 1980, iniciou a popularização por meio da computação pessoal. Se antes a informação estava protegida pela restrição do seu uso, com a comunicação via Internet (Internet; 2021) e a disseminação de sistemas em universidades e pequenas empresas, a segurança dos dados começou a ser um problema. Ataques a redes e por vírus fizeram com que meios de defesa e proteção começassem a ser pesquisados e se tornassem processos e produtos.

A disrupção nos sistemas nos primórdios da Internet significou interrupção da comunicação e/ou do processamento de informações. O impacto das inoperâncias não era “relevante” considerando que os maiores usuários eram o meio acadêmico e científico. Contudo, com a Internet se tornando comercial e a sua administração saindo das mãos do governo americano, empresas começaram a usá-la para os mais diversos fins. Conglomerados foram criados com base em produtos e serviços exclusivamente eletrônicos, como o Google e a Amazon, para citar apenas alguns. Agora, os riscos aos negócios deveriam considerar todas as questões envolvidas em manter as propriedades fundamentais em segurança: a confidencialidade, integridade e disponibilidade. Nesse contexto, está se desenvolvendo o tema de cibersegurança. A norma ISO/IEC 27032 define a segurança cibernética (em inglês, cybersecurity) como a preservação das propriedades de segurança no espaço cibernético. Esse é um “ambiente complexo resultante da interação de pessoas, software e serviços na internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe em qualquer forma física” (ABNT, 2015, p. 5).

As atividades envolvendo o ciberespaço se tornaram críticas para o mundo moderno. O Fórum Econômico Mundial, por meio do seu 16.º relatório de riscos, aponta que falhas na segurança cibernética estão no mesmo quadrante de risco, considerando o nível de impacto e de probabilidade, que crises de escassez de recursos naturais e de meios de subsistência (WEF, 2021). Nesse sentido, a gestão de riscos em computação tem se tornado primordial, tanto no setor privado quanto no público.

O gerenciamento de riscos na segurança da informação é parte vital da gestão de riscos de toda a organização. Conforme explicitado por Joyce, Dobrygowski e der Oord (2021): “Cybersecurity is a strategic business enabler” no seu artigo sobre a importância do gerenciamento de riscos cibernéticos para os negócios. Nesse sentido, normas e publicações especializadas têm sido propostas, por considerarem as

especificidades da área, como os tipos de vulnerabilidades, as ameaças e os ataques. Elas variam em abrangência e detalhamento dos processos, apesar de terem os mesmos objetivos finais. As mais recentes procuram incorporar análises quantitativas e métodos estatísticos.

O objetivo deste artigo foi extrair os princípios gerais das normas para gerenciamento de riscos em cibersegurança e apresentar os desenvolvimentos mais recentes nas metodologias que usam métodos quantitativos.

2 FUNDAMENTAÇÃO TEÓRICA

O gerenciamento de riscos inclui os processos que tratam da realização de identificação, análise, respostas, monitoramento e controle e planejamento do gerenciamento de riscos. Os objetivos da gestão de riscos são aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos na organização.

A Análise e Gestão de Riscos consiste em uma série de passos que ajudam uma equipe a entender e administrar a incerteza. Na verdade, convive-se com a incerteza o tempo todo, em maior ou menor grau, mas não se tem consciência dos riscos. Isso está intimamente relacionado com o conhecimento que se possui sobre um determinado assunto. Esse conhecimento pode ser tanto tácito quanto explícito.

Em outras palavras, o risco é um evento ou condição incerta que, se ocorrer, terá um efeito positivo ou negativo sobre a organização em termos de tempo, custo, qualidade, entre outros fatores. Um risco pode ter uma ou mais causas e, se ele ocorrer, um ou mais impactos.

A finalidade do gerenciamento de risco, segundo Salles Júnior *et al.* (2010), está em antecipar-se aos efeitos que o risco pode causar, por meio da utilização de métodos como identificação, análise, planos de ação, monitoramento e controle, e dessa forma, buscando minimizá-los ou cessá-los.

Segundo Weber e Diehl (2014), o risco está intrinsecamente ligado à incerteza, permitindo a ocorrência de eventos inesperados como resultado. O gerenciamento dos riscos pode ser realizado somente após a sua identificação e, a partir disso, permite a elaboração de estratégias de mitigação que minimizem os impactos negativos.

Nesse sentido, o gerenciamento de riscos não só contribui para a estabilidade operacional, mas também para a sustentabilidade de longo prazo das organizações, ao reduzir a vulnerabilidade a eventos adversos e promover uma cultura de proatividade e resiliência. A gestão de risco compõe uma série de entendimentos relacionados à administração do fato de que o risco aconteça ou que já aconteceu (Olson, 2024).

3 PROCEDIMENTOS METODOLÓGICOS

Este trabalho está baseado em uma análise de dados obtida por meio de revisão bibliográfica de normas e artigos que tratem do gerenciamento de risco em cibersegurança. As normas são importantes para contextualizar os padrões usados e nos quais as empresas e organizações se apoiam para gerenciar seus riscos. Essas normas e documentos usados amplamente por empresas e instituições são reconhecidas como padrões de mercado. As normas para segurança compreendem conceituação, sistemas de gerenciamento de segurança da informação, modelos de gestão de riscos e frameworks contendo controles de segurança.

Além dos sistemas normativos e dos padrões de mercado, foram pesquisados artigos científicos relacionando gerenciamento de riscos cibernéticos e os seguintes temas: propostas de novos modelos; aplicações da gestão de riscos em determinadas áreas ou setores, como IoT (Internet of Things), e propostas de abordagens diferentes para análise de riscos.

4 ANÁLISE DOS RESULTADOS

Qualquer organização precisa compreender e medir os riscos envolvidos em projetos ou nas suas operações diárias. Essa necessidade se estende para a segurança das informações, que vem ganhando importância nos níveis mais altos da gerência, de tal forma que a governança da cibersegurança está nos mesmos patamares que fatores ESG (fatores ambientais, sociais e de governança corporativa) (Joyce; Dobrygowski; Der Oord, 2021).

Portanto, gerenciamento de riscos é:

> [...] o processo contínuo de identificação, avaliação e resposta ao risco. Para gerenciar riscos, as organizações devem entender a probabilidade de ocorrência de determinado evento e os possíveis impactos resultantes. Com essas informações, as organizações podem determinar o nível aceitável de risco para atingir seus objetivos organizacionais e podem, assim, apresentá-lo como sua tolerância a riscos. (NIST, 2018, p.4).

O objetivo primário de uma gestão de riscos é reduzi-los a níveis aceitáveis, conforme o apetite de risco da organização (Chapple; Stewart; Gibson, 2021). Além desse foco principal, o gerenciamento de riscos deve servir a dois outros propósitos principais. O primeiro é de servir de suporte às decisões da alta gerência, por meio dos resultados das métricas associadas a cada risco. Em segundo lugar, é o ponto de partida de qualquer processo de implantação de um sistema de gerenciamento de segurança da informação.

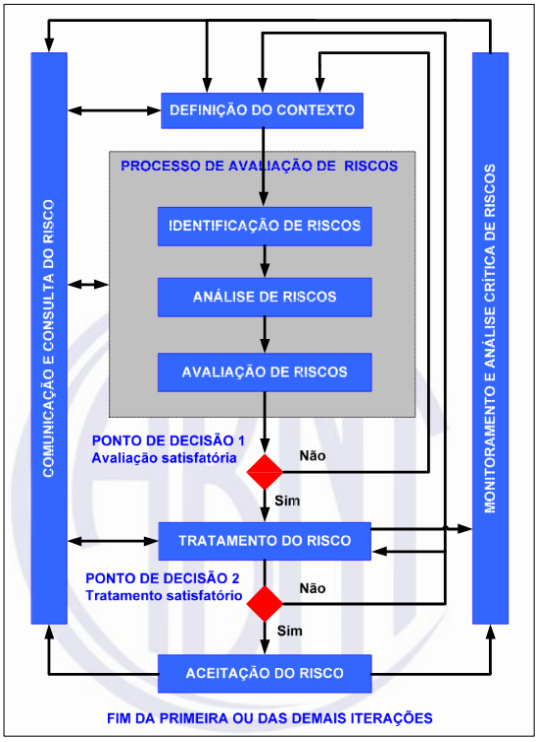
A gestão de riscos é um processo contínuo de identificação, análise e resposta aos riscos conforme fases apresentadas na Figura 1 e concernentes à norma ABNT NBR ISO/IEC 27005:2019 (Gestão de riscos de segurança da informação).

Um aspecto importante do processo de gestão de riscos é o fato de ser um processo cíclico no qual os resultados da última etapa têm um escopo temporal definido, ou seja, os planos de tratamento de riscos devem ser monitorados e revistos periodicamente (ABNT, 2019).

Em termos gerais, o processo inicia pela identificação dos ativos que podem ser tangíveis ou intangíveis e algumas categorias podem ser: pessoas, informação, facilidades, tecnologia e externos. Depois são determinadas as fontes de risco definidas como os elementos que, individualmente ou combinados, têm o potencial para dar origem ao risco. Em cibersegurança, o termo usado é ameaça (no inglês, threat) e podem ser ações ou a falta de ação, além de poderem ser intencionais, ou não intencionais. Algumas ameaças possuem agentes ou atores que agem intencionalmente com o intuito de abusar de vulnerabilidades, que a publicação NIST 800-30 denomina de origens de ameaça adversária e não adversária (Joint, 2012).

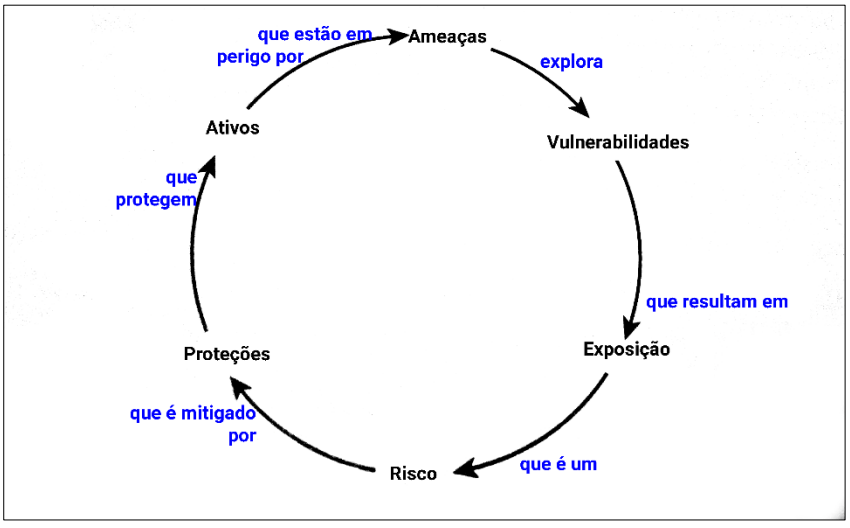
As vulnerabilidades são fraquezas, falhas internas ou falhas de configuração que podem ser exploradas pelas ameaças e cuja exposição configura riscos em segurança. Algumas ameaças podem usar determinados vetores. Um aspecto importante das ameaças é a questão da motivação (que pode ser intencional ou não), pois pode resultar em níveis de riscos mais altos. Essa propriedade das ameaças se incluiu em modelos mais recentes (Stine, 2021; Tucker, 2020). A Figura 2 apresenta os relacionamentos cíclicos dos elementos de risco cibernético.

Figura 1: Ciclo da gestão de riscos em segurança da informação.



Fonte: (ABNT, 2019)

Figura 2: Relacionamentos cíclicos dos elementos de risco cibernético.



Fonte: adaptado de Chapple, Stewart e Gibson (2021).

Evento é a ocorrência ou mudança em um conjunto específico de circunstâncias que pode consistir em várias causas e determinar várias consequências, podendo ser fonte de risco. Um evento implica impacto, o qual é a medida de perda real (custos realizados) quando ameaças exploram vulnerabilidades, ou seja, realização da ameaça (ou do risco). Os impactos podem ser na forma de perda de propriedade, perda da segurança, perdas financeiras ou da reputação e danos à saúde ou até em morte.

Sobre os riscos em cibersegurança, dois tipos merecem um breve comentário. O primeiro são os riscos de conformidade. São aqueles que podem advir do risco de sanções legais ou regulatórias ou, ainda, de perda financeira ou de reputação como resultado da falha no cumprimento da aplicação de leis, acordos, regulamentos, código de conduta e/ou das políticas. Para qualquer entidade brasileira que trate dados pessoais, há um conjunto de regramentos que estão definidos na LGPD (Lei Geral de Proteção de Dados). E as multas podem ser muito onerosas em casos de vazamentos de dados pessoais ou tratamento fora do consentido.

Mas há outras normas e leis, algumas que sujeitam a multas e/ou penalidades. Exemplos: PCI-DSS (Payment Card Industry Data Security Standard) que deve ser adotada por toda instituição que presta serviços bancários/financeiros usando sistemas de pagamento por cartão. O sistema financeiro brasileiro também deve seguir as orientações constantes da Resolução n.º 4.658 do Banco Central, de 26 de abril de 2018, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. A certificação de segurança por meio da norma ABNT NBR ISO/IEC 27001 requer contínuas reavaliações.

A computação avança muito rapidamente e novos riscos ou riscos que tinham probabilidades muito baixas podem se tornar relevantes. Por exemplo, o crime de sequestro de dados (ransomware) com liberação mediante resgate tem atingido todo tipo de indústria, não poupando nem hospitais e educação. Seria um crime provável em setores altamente monetarizados. O autor Nassim N. Taleb convencionou chamar esses eventos de “Cisne Negro”, pois: são extremamente raros; produzem um impacto extremo; e, após a ocorrência, a natureza humana os outorga como evento previsível (e menos aleatório) (Taleb, 2019).

Após definidos os ativos (tangíveis ou intangíveis) e as ameaças potenciais, com os impactos, é necessária a avaliação do risco de cada um. O enfoque e a metodologia variam, conforme o modelo adotado ou os cenários e as particularidades de cada organização.

A análise do par ativo-ameaça pode ser feita por dois enfoques principais (Chapple; Stewart; Gibson, 2021). Algumas metodologias usam o enfoque dos ativos, nos quais são elencadas e pesquisadas na organização as informações e os processos e alguma medida de sensibilidade. Por exemplo, a perda de um notebook pode representar um custo de substituição, mas também dados e informações perdidas e/ou períodos de inoperância de um sistema até sua recuperação total.

O outro enfoque é nas ameaças e nos vetores de ameaças. As metodologias usadas que são denominadas genericamente de análise de ameaças. Dois exemplos: o framework Cyber Kill Chain, desenvolvido pela empresa Lockheed Martin, e se constitui em sete diferentes passos para identificar e prevenir atividades de intrusão. Outro framework é o MITRE ATT&CK, que busca identificar os padrões e comportamentos das ameaças para realizar ataques cibernéticos. É um dos mais recentes modelos de ameaça, criado dentro do MITRE, que é uma organização patrocinada pelo governo americano, além de centros de pesquisas e universidades. Dessa forma, as atividades de análise de riscos, a análise de ameaças e a pontuação de vulnerabilidades (em inglês, vulnerability scoring) são diferentes métodos para a organização conhecer seus riscos cibernéticos (Strom *et al*., 2020).

A análise ou avaliação dos riscos é uma das fases que mais distinguem os modelos. É esta fase que trata de compreender os riscos e suas características, e os níveis deles podem ser determinados basicamente por meio de duas metodologias: a qualitativa e a quantitativa. Elas não são excludentes, podendo ser empregadas juntas, sendo a qualitativa em uma fase anterior da análise (Chapple; Stewart; Gibson, 2021).

A avaliação qualitativa é o processo de forma subjetiva para determinar o impacto de um evento que afeta um projeto, programa ou processo. Envolve normalmente o uso de julgamentos de peritos no assunto e modelos para completar o processo. O resultado mais conhecido é na forma de um “mapa de calor” que usa cores para comunicar nível de risco aos ativos e é baseado num quadrante que possui num sentido a probabilidade de ocorrência e, em outro, o nível de impacto (Hubbard; Seiersen, 2016).

A avaliação quantitativa recorre a processos objetivos para determinar o impacto e usa métricas. Para tanto, precisa de dados históricos e tendências para predizer a probabilidade futura de eventos e dos impactos. O Quadro 1 apresenta um sumário das principais características de ambas as metodologias (Chapple; Stewart; Gibson, 2021).

Quadro 1 – Comparativo das metodologias de análise de riscos qualitativas e quantitativas

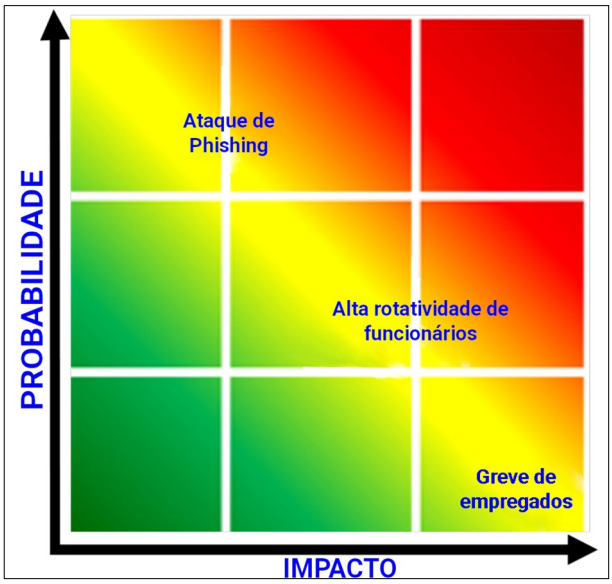
Características	Qualitativo	Quantitativo
Usa funções matemáticas	Não	Sim
Usa análise de custo/benefício	Pode usar	Sim
Requer estimativas	Sim	Alguns
Suporta automação	Não	Sim
Envolve um grande volume de informação	Não	Sim
É objetivo	Pouco	Muito
Depende substancialmente de opinião	Sim	Não
Requer esforço grande e tempo	Em alguns casos	Sim
Oferece resultados úteis e com significado	Sim	Sim

Fonte: adaptado de Chapple, Stewart e Gibson (2021).

Um risco qualitativo poderia ser quantificado como: probabilidade da ameaça contra o impacto. A probabilidade poderia ter os seguintes níveis: improvável (ou baixíssima); raramente (ou baixa); ocasional (ou média); provável (ou alta); frequente (ou altíssima). Algumas normas estabelecem parâmetros para atribuir valores em diferentes escalas. Enquanto isso, o impacto poderia, por exemplo, ser classificado em: insignificante (ou irrelevante); baixo; moderado; crítico (ou alto); catastrófico (ou extremo). O produto da probabilidade de ocorrência pelo impacto constitui uma matriz, que pode ter alocadas cores para indicar o nível de risco, como mostrado num exemplo da Figura 3 (Tucker; 2020).

As análises qualitativas têm a vantagem de possibilitar a compreensão dos riscos para um conjunto muito maior de pessoas (ABNT, 2019), mas não são adequadas para serem integradas à gestão de riscos empresariais. Por isso, muitos autores e normas mais recentes estão procurando incluir metodologias de medidas quantitativas. Pois, como Hubbard e Seiersen (2016, p. X) apontaram em sua obra que os números são a única entrada tanto para engenharia como para inferência estatística. Ainda, os autores fazem a seguinte declaração quanto aos métodos qualitativos: “They are a failure. They do not work” (Hubbard; Seiersen, 2016, p. 14). São apresentadas diversas pesquisas que evidenciam falhas na interpretação que diferentes pessoas têm a respeito de níveis de probabilidade de eventos.

Figura 3: Exemplo de uma matriz de riscos no qual estão definidos três riscos que apesar de possuírem os mesmos níveis, possuem valores de impacto e probabilidade diferentes.



Fonte: alterado de Tucker (2020)

Os métodos quantitativos partem da valoração ou estimativa dos ativos que serão analisados. Algumas das métricas mais comuns são: *Single-Loss Expectancy* (SLE), as quais são o resultado da multiplicação do valor do ativo pelo fator de exposição; *Annualized Loss Expectancy* (ALE), que se obtém do produto da SLE pela probabilidade ou pelo número de vezes que o evento é esperado ocorrer em um ano. Esse último valor corresponde à métrica *Annualized Rate of Occurrence* (ARO), que representa a frequência de um determinado evento em um ano (Conklin *et al.,* 2021).

O problema dos métodos quantitativos é determinar a frequência dos eventos ou a probabilidade da magnitude das perdas. Duas são as soluções: a) usar dados históricos, que podem ou não estar disponíveis, por exemplo, eventos do tipo “Cisne Negro” (Taleb, 2020); b) a outra opção é usar probabilidade para reduzir a incerteza. Um dos métodos mais adotados é a simulação de Monte Carlo, usada para quantificar o nível de confiança (probabilidade de ocorrência) de um evento ou de um resultado de uma decisão. Outra opção, que vários trabalhos recentes vêm fazendo menção, é o uso da decisão Bayesiana, incluindo a proposta dos autores Hubbard e Seiersen (2016).

A fase de tratamento de riscos compreende como a organização responderá aos riscos identificados e selecionados. São quatro principais: aceitar, evitar, transferir ou mitigar. Aceitar um risco é uma decisão na qual se analisam os custos de evitar, transferir ou mitigar em relação à probabilidade de ocorrência e seu potencial impacto. Mas isso não exime que sejam tomadas medidas de monitoramento (Chapple; Stewart; Gibson, 2021).

Evitar um risco pode ser obtido por diversas formas, mas em aspectos gerais é eliminar a causa ou alterar a exposição do sistema às ameaças. A transferência de risco ocorre por meio de acordos legais nos quais terceiros assumem parte ou todo o risco. E, para os casos em que se decide pela mitigação, controles podem ser definidos para endereçar a ameaça ou o agente da ameaça ou mesmo a vulnerabilidade. Os controles são medidas que modificam o risco. A cibersegurança possui diversas normas e padrões que podem auxiliar na definição de controles de segurança. Serão apresentados alguns desses padrões, os quais são os mais conhecidos pelo mercado.

A norma ABNT NBR ISO/IEC 27002 (ABNT, 2013) possui um conjunto de controles de segurança e está relacionada à norma 27001, que determina os requisitos para criar um sistema de gerenciamento de segurança da informação. Elas são bastante conhecidas no mercado, sendo possível obter certificação na 27001 (da mesma forma como a certificação de qualidade ISO 9001). Comparativamente, são mais fáceis de seguir do que algumas normas *National Institute for Standards and Technology* (NIST).

A organização americana de padrões NIST publicou a norma SP 800-53, Revision 5 (*Security and Privacy Controls for Information Systems and Organizations*), a qual é uma revisão (ainda em fase de rascunho), com a inclusão de controles específicos para privacidade. É um framework baseado em controles de segurança de baixo, moderado e alto impacto. Há um apêndice com o mapeamento dos controles dessa norma com os da ISO/IEC 27001. Os controles e respectivos parâmetros da norma 800-53 seguem a mesma linha da ISO/IEC 27002, mas, em contrapartida, são mais amplos e mais detalhados.

O NIST também publicou o framework NIST *Cybersecurity Framework* cuja função é usado para gestão da cibersegurança e, principalmente, para proteção de infraestrutura crítica. O framework é organizado em cinco funções, 22 categorias e 98 subcategorias. As funções são: identificar (ID); proteger (PR); detectar (DE); responder (RS); e recuperar (RC). Um dos melhores e mais fáceis padrões para seguir, estando na versão 1.1 de 2018. Pode ser aplicado a qualquer modelo de gerenciamento de riscos. Esta e outras normas expedidas pelo NIST são de livre acesso. Há uma versão traduzida para o português.

A entidade *Center for Information Security* (CIS) emite recomendações conhecidas como CIS *Controls*, consistindo em um conjunto de ações para proteger diferentes tipos de organizações. Ao todo, são 18 controles de segurança e podem ser adotados em conjunto com outros frameworks específicos. O acesso é livre após um rápido registro e os controles são licenciados sob a Creative *Commons Attribution-Non Commercial-No Derivatives*. Diferentemente das normas

ISO/IEC 27001/2, cuja última versão é de 2013, os controles CIS possuem uma atualização constante, sendo a última versão, a v.8, de agosto de 2020, porém, é menos conhecido e menos adotado.

A entidade *Security Standards Council* (PCI), além de emitir normativas, expediu o documento PCI-DSS (v3.2.1, de maio de 2018), que trata de um padrão para segurança de dados para bancos e financeiras que adotam pagamentos via cartão. Ela é de adoção obrigatória, que além de ser certificada, há revisões periódicas. Essa norma, diferentemente das normas ABNT ISO/IEC 2700x, é de livre acesso.

Nesta seção, serão apresentados os modelos de gestão de riscos cibernéticos mais amplamente adotados e conhecidos pelo mercado. Após uma breve descrição, serão apresentados pontos e informações mais relevantes de cada um. Uma análise detalhada não seria possível, considerando o escopo limitado do presente trabalho. Além dos padrões, serão discutidas as contribuições de alguns artigos selecionados para esta pesquisa.

O primeiro modelo, ou mais precisamente, norma, é a ABNT NBR ISO/IEC 27005:2019 (Gestão de riscos de segurança da informação) (ABNT, 2019), que faz parte do arcabouço de padrões ISO/IEC 2700x. Não é um documento prescritivo, apenas fornece diretrizes gerais para encontrar e analisar riscos, seguindo a linha da norma de Gestão de Riscos ABNT NBR ISO 31000:2018. O documento apresenta tabelas delineando as principais vulnerabilidades e potenciais ameaças. Os níveis de risco foram estabelecidos de forma qualitativa, em uma tabela relacionando valor do ativo, probabilidade da ocorrência da ameaça e facilidade de exploração.

O padrão do NIST, referenciado como Special Publication 800-30, versão de 2012, segue a linha da condução da avaliação de riscos cibernéticos das normas internacionais ISO 31000 e ISO/IEC 27005. Um aspecto importante dessa norma é que as entradas do gerenciamento de riscos são categorizadas em três níveis: organizacional, processo de negócios e ao nível de sistemas de informação. Essa categorização dos riscos em níveis gerenciais permite que o tratamento e a comunicação ocorram de forma mais efetiva. Por exemplo, riscos de alto impacto aos objetivos da organização seriam melhor comunicados à alta gerência para propiciar ações mais efetivas. Riscos tecnológicos que demandam mitigação por controles específicos, são mais adequados aos setores responsáveis por esses ativos.

O risco é qualificado por meio de cinco níveis e obtidos pelo “mapa de calor”, relacionando níveis de impacto e probabilidade de ocorrência. Contém várias tabelas relacionando tipos de ameaças e níveis de intenção. Além dos níveis qualitativos, essas tabelas informam valores semiquantitativos, em duas escalas, uma de zero a dez e outra de zero a cem. Essa norma é prescrita aos órgãos do governo americano e também adotada pelo setor privado.

O órgão de padronização NIST americano está lançando um conjunto de três publicações que compõem a série NISTIR 8286x (*Integrating Cybersecurity and Enterprise Risk Management*), que tratarão de integrar o gerenciamento de risco cibernético (CSRM, em inglês, *Cybersecurity Risk Management*) na gestão de risco empresarial, indicada pela sigla ERM (*Enterprise Risk Management*). A publicação NISTIR 8286A (Stine, 2021a) detalha aspectos gerais da gestão de riscos cibernéticos, como contexto, identificação de probabilidades e impactos, além da forma de apresentação das saídas, por meio de registros, conhecidos como *Cybersecurity Risk Registers* (CSRR).

A publicação informa técnicas para estimativas de probabilidade e de impacto. A probabilidade de eventos pode ser obtida por modelos de ameaças ou pelo conhecimento de eventos passados. No primeiro caso, o framework MITRE ATT&CK (Strom *et al*., 2020) pode fornecer uma valiosa informação sobre as várias ameaças cibernéticas por meio da compreensão do ciclo de vida dos ataques. O documento apresenta uma tabela-exemplo com avaliação mensal, contemplando resultados passados de riscos, limites de tolerância e de apetite, dentre outras informações sobre um ativo em específico. Esse tipo de informação pode auxiliar nas estimativas de probabilidade futuras, apesar da não garantia para probabilidades futuras.

O documento NISTIR 8286A também informa outros métodos para analisar probabilidade e impacto. A primeira é a da estimativa de três pontos, que elenca um cenário otimista, um pessimista e um provável, gerando estimativas quantitativas. A outra técnica elencada é a de análise de árvores de eventos, que é uma espécie de árvore de decisão, com a causa raiz (ameaça) e os resultados finais. A análise qualitativa informa a probabilidade de cada ramo, considerando as probabilidades de sucesso de cada defesa ou controle. São citadas mais duas técnicas quantitativas para análise de riscos: simulação de Monte Carlo e análise Bayesiana. Diferentemente do framework NIST 800-30, em que não há alusão a técnicas quantitativas, as publicações NISTIR 8286x avançam nessa questão, pois buscam inserir a gestão de riscos cibernéticos na gestão de riscos empresarial.

A publicação NISTIR 8286B (*Prioritizing Cybersecurity Risk for Enterprise Risk Management*), lançada em setembro de 2021 (Stine, 2021b), refina as questões da análise do risco. São apontadas as questões para priorização dos riscos, a avaliação e seleção de respostas aos riscos, além de estratégias de comunicação e integração ao ERM.

As normas e padrões anteriores não enfatizavam a questão da análise quantitativa dos riscos cibernéticos, exceto as publicações mais recentes do NIST, que fizeram menção a algumas técnicas. O framework FAIR (*Factor Analysis of Information Risk* - Análise Fatorial de Risco de Informação) já contempla o enfoque

quantitativo da análise de riscos. Usa a simulação de Monte Carlo combinada com técnicas de aproximação estatísticas. O FAIR foi a base escolhida para a metodologia Open FAIR provida pelo OpenGroup por meio dos padrões O-RT (*Risk Taxonomy*) (Opengroup; 2020b) e O-RA (*Risk Analysis*) (Opengroup; 2020a).

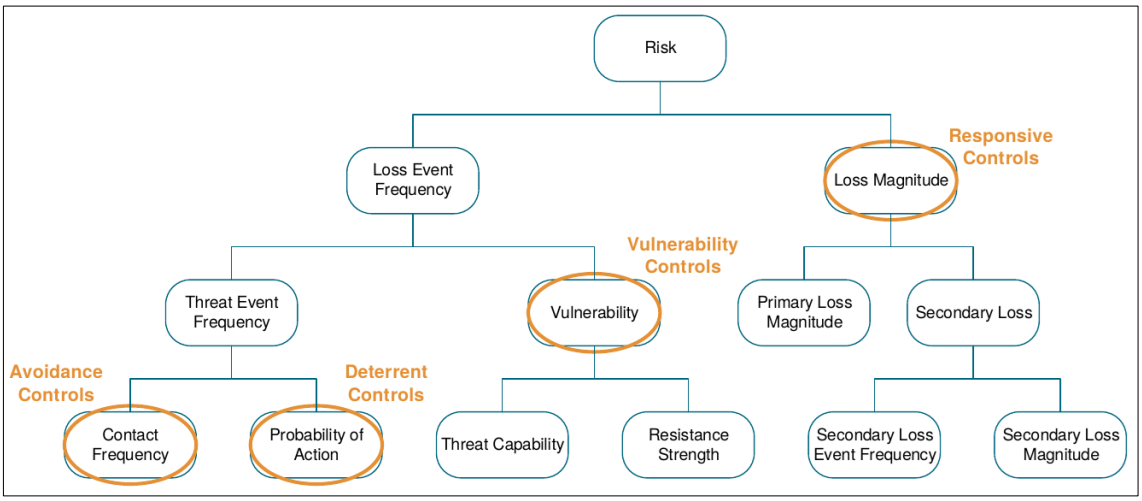
O padrão O-RA faz o processo de análise de riscos em fases e a parte conceitual e a própria linguagem estão baseadas em norma específica, a O-RT, proporcionando um diferencial quando comparado com outras abordagens. As cinco fases compreendem: identificação dos cenários de perda (também o escopo), a avaliação da frequência de eventos de perda, a magnitude das perdas, a derivação e articulação dos riscos e, por fim, a modelagem dos controles de mitigação. O estágio da articulação dos riscos compreende análises quantitativas usando simulações por Monte Carlo e a forma de apresentação dos resultados.

A Figura 4 apresenta os componentes que dão suporte à metodologia de quantificação de riscos, acrescido dos controles de segurança segundo uma categoria própria. A definição e escolha dos controles adequados são executadas na última fase da metodologia. A motivação para incluir controles na norma é que eles representam medidas que podem afetar (diminuir) a frequência ou a magnitude das perdas, ou ambas.

A questão dos controles de segurança é um importante componente do processo geral de gerenciamento de riscos e existem normas e padrões próprios, como a NBR ISO/IEC 27002, a NIST SP 800-53 ou a publicação NIST CSF. No caso da norma O-RA há uma seção que integra as famílias de controles ao framework NIST CSF que trata especificamente das medidas de mitigação via categorização por funções.

Um outro padrão para análise de riscos cibernéticos é o OCTAVE FORTE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation For the Enterprise*) (Tucker, 2020). Esse modelo foi lançado em novembro de 2020, pelo Instituto de Engenharia de Software (SEI) (*Software Engineering Institute*). Essa unidade de pesquisa em computação foi patrocinada pelo governo americano e está vinculada à universidade Carnegie Mellon University.

Figura 4: Componentes da metodologia O-RA com destaque para as categorias de controles definidos na quinta fase.



Fonte: extraído de OpenGroup (2020a).

É constituído em dez passos, iniciando pela estrutura de governança do risco, na qual são definidos o apetite de risco e as políticas de gerenciamento de alto nível dos riscos. Além de descrever o processo OCTAVE FORTE, esse relatório recomenda métodos e fornece um exemplo de política de gerenciamento de risco que as organizações podem consultar ou adaptar ao redigir sua própria política. Os materiais suplementares contêm modelos que as organizações podem usar ao conduzir muitas das atividades do OCTAVE FORTE.

O modelo OCTAVE FORTE, além de ser livremente disponível, contempla o seguinte: a inclusão de planos de resposta e a definição de métricas, tanto para medir a performance dos planos de resposta quanto da efetividade do programa de gestão de riscos. As métricas obtidas deverão vir do monitoramento contínuo do plano. A inclusão dos planos de resposta no documento segue o mesmo princípio adotado pela norma O-RA do OpenGroup.

Os modelos propostos pelas normas e padrões podem apresentar análises quantitativas, como as mais recentes, mas também podem ser omissas nessa questão, como a ABNT NBR ISO/IEC 27005. O trabalho proposto pelos autores Wang, Neil e Fenton (2020) expande o modelo FAIR para acomodar estimativas baseadas em redes Bayesianas. Essa alternativa visava oferecer uma alternativa à questão do conjunto de distribuições dos dados de entrada que, por padrão, são triangulares no esquema FAIR padrão. O problema é que muitos dados não seguem essa distribuição e isso leva a falhas na acurácia das estimativas de perdas dos riscos.

Considerando a evolução temporal dos modelos, eles estão incorporando estratégias quantitativas para os riscos. O objetivo é que o risco cibernético é parte integrante do gerenciamento de risco da empresa na totalidade e as métricas de custo são padrões nesse nível gerencial. Normas mais recentes, como a Open FAIR e a O-RA, e o NISTIR 8286a, incluem análises quantitativas de riscos.

Por outro lado, algumas metodologias ou normas são mais genéricas, definindo diretrizes gerais. Um exemplo é a norma ABNT ISO/IEC 27005, que pode ser apropriada para as organizações que planejam obter certificação ISO/IEC 27001. Algumas abordagens buscam combinar modelos e estratégias (Bakare, 2020).

Os modelos de gerenciamento de riscos em cibersegurança estão seguindo por dois caminhos: o primeiro é especializar-se para determinados setores da computação e, em segundo, são as tentativas de criar um modelo genérico, que possa ser aplicado para qualquer.

5 CONSIDERAÇÕES FINAIS

Foram apresentados os principais modelos e normas em gestão de riscos em segurança da informação. A gestão dos riscos cibernéticos e os tratamentos resultantes são parte dos processos de proteção dos ativos. Mas a postura de segurança compreende mais dois pilares: detecção e resposta. Especificamente, em se tratando de vazamentos (em inglês, breach) de dados, há uma mudança de foco de prevenir para assumir os vazamentos (Diogenes; Ozkaya, 2018). E o motivo é que os vetores de ataques, as motivações e as vulnerabilidades estão em crescente, de forma que o custo para eliminar esses riscos é muito alto ou o processo é tão longo que poderá estar desatualizado na fase de implementação das medidas de mitigação (Gollman, 2011).

Os processos e programas de resposta a incidentes são uma resposta das organizações aos riscos à cibersegurança crescentes. Eles servem tanto para adequação às normas e leis vigentes como um mecanismo rápido para o retorno das operações. Além disso, os processos de investigação e recuperação de desastres servem como fatores de aprendizado.

A gestão de riscos cibernéticos procura qualificar ou quantificar riscos aos ativos de informação em cenários incertos. Dois desses cenários que devem merecer atenção nos processos de análise de riscos são: a presença de sistemas legados (Conklin *et al.,* 2021) e as normas atuais de proteção aos dados pessoais, como a GDPR europeia e a LGPD no Brasil. Essas e outras legislações correlatas demandam multas e penalidades para os riscos de tratamento indevido ou para vazamento de dados pessoais e devem conseguir modificar a postura de risco das organizações (Conklin *et al*., 2021).

REFERÊNCIAS

ABNT. NBR ISO/IEC 27032:2015: **Tecnologia da informação**: Técnicas de segurança: Diretrizes para segurança cibernética. Rio de Janeiro, 2015. 62 p.

ABNT. NBR ISO/IEC 27002:2013: **Tecnologia da informação**: Técnicas de segurança: Código de prática para controles de segurança da informação. 2a. ed. Rio de Janeiro, 2013. 99 p.

ABNT. NBR ISO/IEC 27005:2019: **Tecnologia da informação**: Técnicas de segurança: Gestão de riscos de segurança da informação. 3. ed. Rio de Janeiro, 2019. 66 p.

BAKARE, Adeyinka. **A Methodology for Cyberthreat ranking: Incorporating the NIST Cybersecurity Framework into FAIR Model**. 2020. Tese de Doutorado. University of Cincinnati.

CHAPPLE, Mike; STEWART, James Michael; GIBSON, Darril. CISSP: **Certified Information Systems Security Professional (Official Study Guide).** 9th Edition. US: Sybex. 2021.

CONKLIN, Arthur William. *et al*. **CompTIA Security+:** All-in-One Exam Guide. Sixth Edition. US: McGraw Hill. 2021.

DIOGENES, Yuri; OZKAYA, Erdal. Cybersecurity: Attack and Defense Strategies. Birmingham (UK): Packt Publishing, 2018. ISBN 978-1-78847-529-7.

GIUCA, Olivia *et al*. A Survey of Cybersecurity Risk Management Frameworks. *In*: **International Workshop Soft Computing Applications**. Springer, Cham, 2018. p. 240-272.

GOEL, Rajni; KUMAR, Anupam; HADDOW, James. PRISM: a strategic decision framework for cybersecurity risk assessment. **Information & Computer Security**, 2020.

HUBBARD, Douglas William.; SEIERSEN, Richard. **How to Measure Anything in Cybersecurity Risk**. New Jersey (US): Wiley. 2016.

JOINT TASK FORCE TRANSFORMATION INITIATIVE. NIST SP 800-30: Guide for Conducting Risk Assessments. Rev. 1. Gaithersburg, MD: NIST, 2012.

JOYCE, Sean; DOBRYGOWSKI, Daniel; der OORD, Friso Van. **Principles for Board Governance of Cyber Risk**. Harvard Law School Forum on Corporate Governance. 10 jun. 2021. Disponível em: https://corpgov.law.harvard.edu/2021/06/10/principles-for-board-governance-of-cyber-risk/. Acesso em: 30 ago. 2021.

NIST. **Framework for Improving Critical Infrastructure Cybersecurity**: Cybersecurity Framework Version 1.1. 16 abr. 2018. Disponível em: https://doi.org/10.6028/NIST.CSWP.04162018. Acesso em: 27 ago. 2021.

OLSON, Alexander. Gestão de Riscos. *In*: SMITH, John (org.). **Advanced Risk Management Strategies.** Heidelberg: Springer, 2024. p. 473-478. DOI: https://doi.org/10.1007/978-3-031-55943-3_30.

OPENGROUP. Risk Analysis (O-RA) Standard. Version 2.0, The Open Group Standard (C20A), November 2020. Disponível em: https://publications.opengroup.org/c20a Acesso em: 1º set. 2021.

OPENGROUP. Risk Taxonomy (O-RT) Standard. Version 3.0, The Open Group Standard (C20B), November 2020. Disponível em: https://publications.opengroup.org/standards/open-fair-standards/c20b Acesso em: 1º set. 2021.

SALLES JUNIOR., Carlos Alberto Correa; SOLER, Alonso Mazini; VALLE, José Angelo Santos do. Gerenciamento de riscos em projetos. 2. ed.

STINE, Kevin *et al*. NISTIR 8286A: Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM). 2nd Draft. Gaithersburg:MD(US): NIST (National Institute of Standards and Technology). Jul. 2021. 60 p. Disponível em: https://doi.org/10.6028/NIST.IR.8286A-draft2. Acesso em: 27 ago. 2021

STINE, Kevin et al. NISTIR 8286B: Prioritizing Cybersecurity Risk for Enterprise Risk Management. Draft. Gaithersburg:MD(US): NIST (National Institute of Standards and Technology). Sep. 2021. 42 p. Disponível em: https://doi.org/10.6028/NIST.IR.8286B-draft Acesso em: 18 set. 2021.

STROM, Blake *et al*. MITRE ATT&CK: Design and Philosophy. McLean, VA: MITRE, 2020. Disponível em: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf. Acesso em: 23 set. 2021.

SULOYEVA, Svetlana; GRISHUNIN, Sergei; BUROVA, Ekaterina. Developing a Cybersecurity Risk Analysis System for High-Tech Equipment in Machine Industry. *In*: **Proceedings of the 2019 International SPBPU Scientific Conference on Innovations in Digital Economy**. 2019. p. 1-6.

TALEB, Nassim Nicholas; NEEDHAM, Duncan; WEITZDORFER, Julius. Probability, Risk, and Extremes. **Extremes**, v. 31, p. 46, 2019.

TUCKER, Brett. **Advancing Risk Management Capability Using the OCTAVE FORTE Process. Pittsburgh,** PA: Software Engineering Institute, Carnegie Mellon University, 2020. Disponível em: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=644636. Acesso em: 31 ago. 2021.

WANG, Jiali; NEIL, Martin; FENTON, Norman. **A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model**. Computers & Security, v. 89, p. 101659, 2020.

WANGEN, Gaute Bjørklund. **Cyber Security Risk Assessment Practices: Core Unified Risk Framework.** Tese (Doctoral thesis) - Institutt for informasjonssikkerhet og kommunikasjonsteknologi, NTNU (Norwegian University of Science and Technology), Gjøvik (Noruega), 2017. Disponível em: http://hdl.handle.net/11250/2447264

WEBER, Elson Luciano; Diehl, Carlos Alberto (2014). GESTÃO DE RISCOS OPERACIONAIS: UM ESTUDO BIBLIOGRÁFICO SOBRE FERRAMENTAS DE AUXÍLIO. **Revista De Contabilidade Do Mestrado Em Ciências Contábeis Da UERJ**, 19(3), 41–58. https://doi.org/10.12979/10408

WEF. The Global Risks Report 2021. 16. ed. 19 jan. 2021. Disponível em: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf. Acesso em: 30 ago. 2021.

WIKIPEDIA contributors. Bombe. Wikipedia, The Free Encyclopedia. May 24, 2021, 15:32 UTC. Disponível em: https://en.wikipedia.org/w/index.php?title=Bombe&oldid=1024882980. Accessed August 26, 2021. +

WIKIPEDIA contributors. ENIAC. Wikipedia, The Free Encyclopedia. August 26, 2021, 11:57 UTC. Disponível em: https://en.wikipedia.org/w/index.php?title=ENIAC&oldid=1040746089. Accessed August 26, 2021.

WIKIPEDIA contributors. Internet. Wikipedia, The Free Encyclopedia. August 22, 2021, 14:58 UTC. Disponível em: https://en.wikipedia.org/w/index.php?title=Internet&oldid=1040080585. Accessed August 26, 2021.