Processo de Identificação de Riscos Cibernéticos em uma Instituição Financeira: Uma Análise baseada no NIST Cybersecurity Framework

Lucilene da Silva Leite
Werley Antonio Mendonça Machado
Edgard Costa Oliveira

UnB, Universidade de Brasília

RESUMO

O presente artigo abordou a segurança cibernética e a importância de implementar controles e padrões para identificação, tratamento e plano de respostas aos riscos cibernéticos. A pesquisa teve como objetivo a apresentação de proposta para a adoção de modelo de identificação de riscos cibernéticos baseado no NIST Cyber Security Framework em uma instituição financeira nacional. O NIST CSF pode ser implementado em conjunto com outros frameworks e normas, tais como o COBIT, a ISO 27001 e a ISO 27032. As suas cinco funções, que vão desde a identificação dos riscos até a recuperação de ambientes que sofreram ataques são muito similares ao processo de gestão de riscos da ISO 31000, já consolidado nas organizações em geral e na instituição financeira alvo da pesquisa. Assim, o modelo proposto pretende trazer melhoria do processo de gestão de incidentes cibernéticos ao passo que atenderá as legislações e normas vigentes.

Palavras-chave: Riscos Cibernéticos; NIST Cyber Security Framework; Gestão de Incidentes Cibernéticos

Cyber Risk Identification Process in a Financial Institution: An Analysis based on the NIST Cybersecurity Framework

Lucilene da Silva Leite
Werley Antonio Mendonça Machado
Edgard Costa Oliveira

UnB, Universidade de Brasília

ABSTRACT

This article addressed cyber security and the importance of implementing controls and standards for cyber risk identification, treatment, and response planning. The research aimed to present a proposal for the adoption of a cyber risk identification model based on the NIST Cyber Security Framework in a Brazilian financial institution. The NIST Cyber Security Framework can be implemented with other frameworks and standards such as COBIT, ISO 27001 and ISO 27032. Its five functions, ranging from risk identification to disaster recovery, are very similar to ISO 31000 - Risk Management Guidelines, consolidated in the organizations in general. Thus, the proposed model aims to improve the cyber incident management process while comply with the current legislations, regulations and standards.

Keywords: Cyber Risks; NIST Cyber Security Framework; Cyber Incident Management

1. INTRODUÇÃO

O Relatório Global de Riscos 2019, publicação do Fórum Econômico Mundial (WEF, World Economic Forum), demonstrou em seus resultados que a tecnologia continua desempenhando um papel importante na formação do panorama de riscos globais. Os riscos cibernéticos estão aumentando, tanto em sua prevalência quanto em seu potencial disruptivo. Ataques contra empresas quase que dobraram em cinco anos, e incidentes que antes seriam considerados excepcionais estão se tornando cada vez mais comuns.

O impacto financeiro de falhas na cibersegurança está crescendo. O mesmo relatório ainda cita exemplos recentes como o ataque WannaCry – que afetou 300 mil computadores em 150 países – e NotPetya, que causou perdas trimestrais de US$ 300 milhões para uma série de empresas afetadas. Outra tendência crescente é o uso de ciberataques para atingir infraestruturas críticas e setores estratégicos, suscitando receios de que, no pior cenário, os atacantes desencadeiem a quebra de sistemas que mantêm as sociedades funcionando.

A Pesquisa Global de Percepção de Riscos (GRPS) mostrou que dois dos cinco maiores riscos estão ligados à cibersegurança. Fraude e roubo maciço de dados foram classificados como o risco global número quatro por probabilidade, num horizonte de 10 anos, e ataques cibernéticos ficou na posição cinco, mantendo o mesmo padrão registrado no ano passado, com os riscos cibernéticos consolidando sua posição ao lado dos riscos ambientais no quadrante de alto risco e alta probabilidade.

Essa nova realidade refletida nos resultados do Relatório do Fórum Econômico Mundial passou a exigir fortes investimentos em processos, ferramentas e capacitação de pessoal para atuar na gestão de riscos e na detecção e resposta à incidentes. Aos órgãos regulamentadores coube a tarefa de definir padrões e estruturas de gerenciamento de riscos cibernéticos e segurança da informação para serem adotados pelas organizações.

No cenário global, o NIST (National Institute of Standards and Technology), órgão do governo americano responsável pelo desenvolvimento de padrões de tecnologia, lançou em 2014, o NIST Cybersecurity Framework, atendendo a Ordem Executiva Presidencial 13636, "Melhorando as técnicas e Infraestrutura de segurança cibernética", que pedia o desenvolvimento de uma estrutura voluntária para ajudar as organizações a melhorar a segurança cibernética, o gerenciamento de riscos e a resiliência de seus sistemas.

O NIST CSF fornece uma estrutura para as empresas e órgãos reguladores adotarem ao criar, orientar, avaliar ou melhorar programas de segurança cibernética, com o intuito de apoiar as organizações públicas e privadas na árdua tarefa de atuar na detecção e respostas a incidentes cibernéticos. Ele pode ser implementado em conjunto com outros frameworks e normas, tais como o COBIT e a ISO 27001, e suas cinco funções, que vão desde a identificação dos riscos até a recuperação de ambientes que sofreram ataque, são muito similares ao processo de gestão de riscos já consolidado pela Norma ISO 31000.

No cenário nacional, o Banco Central do Brasil publicou em 26 de abril de 2018 a Resolução BACEN n° 4.658, 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 serem observados pelas instituições financeiras. A norma determina que as instituições financeiras estabeleçam plano de ação visando a implementação e divulgação de política de segurança cibernética.

Considerando o exposto acima, e as demais regulamentações e normas a respeito dos temas gestão de riscos e segurança cibernética, o objetivo do presente artigo é apresentar proposta para a adoção de modelo de identificação de riscos cibernéticos baseado no NIST CSF em uma instituição financeira nacional. Sendo assim, as seguintes perguntas deverão ser respondidas durante a elaboração de proposta de implantação do modelo de gestão de riscos cibernéticos:

1. Qual é o grau de maturidade em gestão de riscos cibernéticos da instituição antes da implantação do NIST Cyber Security Framework?
2. Como determinar o grau de maturidade em gestão de riscos cibernéticos após o término do primeiro ciclo da implantação do NIST Cyber Security Framework?
3. Como definir os recursos que suportam funções críticas e que, por sua vez, necessitam de proteção?
4. Quais são os riscos identificados como Prioridade 1 e que serão tratados pela função 'Proteger' do NIST Cyber Security Framework?

O NIST Cybersecurity Framework permite lições aprendidas e melhoria do processo de resposta e recuperação de incidentes, que será a cada ciclo mais eficiente. Com a implementação do framework, a

organização terá plenas condições de avaliar suas capacidades atuais e melhorar suas práticas de segurança cibernética por meio da evolução da maturidade em gerenciamento de riscos cibernéticos.

O modelo proposto pretende trazer melhoria do processo de gestão de incidentes cibernéticos ao passo que atenderá as legislações e normas vigentes. Ao final do primeiro ciclo de implementação deverá ser possível realizar a avaliação do grau de maturidade de riscos cibernéticos da instituição para concluir se a adoção do NIST Cybersecurity Framework, aliado à Norma ISO 27032 e ao COBIT, trouxe ganhos significativos para o processo de gerenciamento de riscos cibernéticos da instituição.

2. DESCRIÇÃO

2.1 Contexto Externo

De acordo com o Decreto nº 9.203 da Presidência da República, publicado em 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, a gestão de riscos é o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Retomando o entendimento de que risco é o efeito das incertezas nos objetivos (NBR ISO 31000 - Gestão de Riscos – Princípios e diretrizes, 2018), ainda no Decreto nº 9.203, no Artigo 17, alínea II, é explicado que é importante integrar a gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, visto que esses podem impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional. Ademais, é importante ressaltar que um processo de gestão de riscos bem consolidado pode ajudar no apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

Consonante, a Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, em seu Artigo 1º, informa que os órgãos e entidades do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança.

Do mesmo modo, a Resolução BACEN nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital das instituições financeiras, em seu Artigo 2° informa que as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil devem implementar estrutura de gerenciamento contínuo e integrado de riscos compatíveis com o modelo de negócio, com a natureza das operações e com a complexidade dos produtos, dos serviços, das atividades e dos processos da instituição.

O referido expediente ainda define em seu Artigo 32 o entendimento de risco operacional como a possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas, ou seja, falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI) são compreendidos como riscos operacionais e precisam ser tratados conforme prevê o Artigo 33 da mesma norma:

> *"III - implementação de estrutura de governança de TI consistente com os níveis de apetite por riscos estabelecidos na RAS; IV - sistemas, processos e infraestrutura de TI que: a) assegurem integridade, segurança e disponibilidade dos dados e dos sistemas de informação utilizados; b) sejam robustos e adequados às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse; c) incluam mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais."*

Sob a mesma perspectiva, com foco em segurança, integridade e disponibilidade da informação, a Resolução BACEN n° 4.658, de 26 de abril de 2018, 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 serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Essa resolução prevê que as instituições financeiras devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a

integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Sendo que a política deve ser compatível com o porte, o perfil de risco e o modelo de negócio da instituição, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e a sensibilidade dos dados e das informações sob responsabilidade dela.

Conforme definido no artigo 22º da Resolução BACEN 4.658 de 26.04.2018, as instituições financeiras devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes relevantes tratados no artigo 3º inciso IV desta mesma resolução. Para tanto, foi criada em junho de 2018 uma Subcomissão de Cybersecurity da FEBRABAN que já conta com a participação de 12 instituições do setor, com o objetivo inicial de compartilhamento de informações para combate aos incidentes cibernéticos.

Por meio de plataforma virtual, as instituições fornecerão informações sobre data, horário, tipo de ameaça detectada assim como sistemas afetados e o que fez para resolver o problema identificado, alertando automaticamente os demais parceiros cadastrados. A ferramenta FS-ISAC (Financial Services – Information Sharing Analysis Center) foi a escolhida pelo grupo no último mês de março para ser adotada pelas instituições financeiras participantes ao longo dos próximos meses.

É importante lembrar que no Brasil as atividades operacionais e de normatização da Segurança Cibernética são realizadas pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC). E as ações de defesa são realizadas pelo Centro de Defesa Cibernética (CDCiber), do Exército Brasileiro, vinculado ao Ministério da Defesa (MD). Já o CERT.br é responsável por tratar incidentes de segurança em computadores em redes conectadas à Internet brasileira.

2.2 Contexto Interno

A organização escolhida é uma instituição financeira, sob a forma de empresa pública, integrante do Sistema Financeiro Nacional. Durante o ano de 2017, com a publicação da Resolução BACEN nº 4.557, que dispõe sobre a estrutura de gerenciamento de riscos das instituições financeiras nacionais, a Diretoria de Riscos da organização passou por uma grande reestruturação com o intuito de se adequar à nova norma em vigor.

Em 2018 foi inaugurada a Gerência de Riscos de TI, vinculada à Diretoria de Riscos, e também a Centralizadora de Segurança da Informação, esta última vinculada à Diretoria de Tecnologia da Informação, ambas em atendimento a Resolução BACEN nº 4.557 e também a Resolução BACEN nº 4658, que dispõe sobre a política de segurança cibernética das instituições financeiras nacionais.

A organização já possui Política de Segurança da Informação consolidada, Política de Segurança Cibernética em fase de publicação, norma a respeito do processo de gestão de riscos da segurança da informação baseada na ISO 31000, e norma sobre o tratamento de incidentes cibernéticos em fase de elaboração, contudo, ainda é necessário que os processos e atividades voltados para a gestão de riscos cibernéticos sejam coordenados e padronizados, para se obter melhores resultados com menor custo e esforço.

A implantação de um processo de gestão de riscos cibernéticos coerente e baseado em padrão já consolidado pelo mercado evitará o dispêndio desnecessário de força de trabalho e recursos financeiros para o tratamento dos riscos que não são prioritários ou não reverterão em relevante prejuízo ou ganho financeiro. Com a adoção do modelo proposto, a organização conseguirá identificar os ativos, sistemas e processos que precisam ser protegidos e mapear as probabilidades e impactos decorrentes da existência deles.

2.3 Metodologia

O estudo classifica-se como Pesquisa Aplicada quanto à sua natureza. De acordo com Thiollent (2009), a pesquisa aplicada concentra-se em torno dos problemas específicos nas atividades das organizações e está empenhada na elaboração de diagnósticos, identificação de demandas e busca de soluções.

A pesquisa contará com o auxílio das técnicas de identificação de riscos Lista de Verificação, Análise de Cenário e SWIFT previstas na ISO 31010, e da ferramenta de código aberto e livre THEHIVE (https://thehive-project.org/), plataforma de identificação e resposta a Incidentes de Segurança da Informação. A utilização dessas técnicas e ferramenta será de extrema relevância para o mapeamento, identificação e catalogação dos riscos e posterior plano de respostas.

O modelo de implantação do NIST Cybersecurity Framework será apresentado em sete etapas de modo a termos uma implantação progressiva por meio da criação de perfis atuais e perfis de destino, que irão

evoluindo a cada ciclo. Novos processos, ativos e sistemas serão incorporados ao modelo, agregando assim, por conseguinte, novas categorias e subcategorias a cada ciclo de implementação, de acordo com as prioridades identificadas no processo de gestão de riscos cibernéticos da organização.

3. REFERENCIAL TEÓRICO

3.1 Normas ISO 27000

As normas da família ISO/IEC 27000 convergem para o Sistema de Gestão de Segurança da Informação (SGSI), tendo como as normas mais conhecidas as ISO 27001 e ISO 27002. São relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. As normas da família 27000 que estão mais alinhadas ao presente estudo são as Normas ISO/IEC 27001 e 27032.

A Norma ABNT NBR ISO/IEC 27001:2013 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação (SGSI) dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. O conceito de segurança da informação vai além do quesito informático e tecnológico, apesar de andarem bem próximos. O SGSI é uma forma de segurança para todos os tipos de dados e informações, e possui quatro atributos básicos: confidencialidade, integridade, disponibilidade e autenticidade (ABNT, 2013).

A Norma ABNT NBR ISO/IEC 27032:2015 estabelece diretrizes para melhorar o estado da segurança cibernética de uma organização, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança. Ela aborda a segurança cibernética como a preservação da confidencialidade, integridade e disponibilidade da informação no espaço cibernético e ainda define espaço cibernético como um ambiente complexo resultante da interação de pessoas, software e serviços da Internet por meio de dispositivos tecnológicos e redes conectadas (ABNT, 2015).

3.2 COBIT

De acordo com a própria ISACA, associação internacional que suporta e patrocina o desenvolvimento de metodologias e certificações para o desempenho das atividades de auditoria e controle em sistemas de informação, o COBIT foi lançado pela primeira vez em 1996 e inicialmente projetado como um conjunto de objetivos de controle de TI para ajudar a comunidade de auditoria financeira a navegar melhor pelo crescimento dos ambientes de tecnologia.

Em 1998, a ISACA lançou a versão 2, que expandiu a metodologia para que pudesse ser aplicada fora da comunidade de auditoria. Mais tarde, nos anos 2000, a ISACA desenvolveu a versão 3, que incluiu as técnicas de gerenciamento de TI e de controle de informações encontradas no framework atual. Posteriormente, em 2005, o COBIT 4 foi lançado, seguido pelo COBIT 4.1, em 2007. Essas atualizações incluíram mais informações sobre a governança em torno das tecnologias de informação e comunicação. Em 2012, o COBIT 5 foi lançado e, em 2013, o ISACA lançou um complemento a ele, que incluía mais informações para as empresas sobre gerenciamento de riscos e governança de informações.

Desde a versão 5 o COBIT incorporou a preocupação sobre o gerenciamento de riscos. Realizar a identificação e análise dos riscos da empresa é tão importante, que um dos fatores que podem influenciar a implantação da governança de TI é o perfil de riscos da instituição: analisar o perfil de riscos da empresa em questões relacionadas à tecnologia, ou seja, qual tecnologia está relacionada aos riscos em que a empresa está exposta e identificar quais áreas de risco estão excedendo o apetite a riscos da organização. O COBIT está sendo citado, pois será utilizado em conjunto com o NIST Cybersecurity Framework em sua implementação.

3.3 NIST Cybersecurity Framework (CSF)

O National Institute of Standards and Technology (NIST), órgão do governo americano responsável pelo desenvolvimento de padrões de tecnologia, lançou em abril de 2018 a versão 1.1 do Framework for Improving Critical Infrastructure Cybersecurity. Lançado em 2014, ele é o resultado de 10 meses de discussões

colaborativas com mais de 3.000 profissionais da área de segurança, prevendo o desenvolvimento de um conjunto de padrões, diretrizes e práticas para ajudar as organizações encarregadas de prover os sistemas críticos do país a proteger melhor suas informações e ativos físicos de possíveis ataques cibernéticos.

De acordo com o próprio NIST (2018), o framework compreende uma compilação com base em risco e diretrizes que podem ajudar as organizações a identificar, implementar e melhorar as práticas de segurança cibernética, criando uma linguagem comum para a comunicação interna e externa das questões relacionadas ao assunto. Ele ainda fornece um mecanismo de avaliação que torna possível a organização determinar suas capacidades atuais de segurança cibernética, estipular objetivos individuais para um estado desejado e estabelecer um plano para melhorar e manter seu programa de segurança da informação.

O framework é composto de três partes: O Núcleo do Framework (Core), as Camadas de Implementação (Implementation Tiers) e o Perfil (Profile), conforme segue:

- Núcleo (Core) é um conjunto de atividades de segurança cibernética e referências informativas, organizadas em torno de resultados particulares em setores críticos. O Núcleo apresenta padrões, diretrizes e práticas de maneira que permite a comunicação de atividades e resultados de segurança cibernética em toda a organização, desde o nível executivo até o nível de operações. Ele compreende cinco funções simultâneas e contínuas, que veremos a seguir, nas palavras de Brockman (2019) e na Figura 1 abaixo:

Função 1: Identificar: Qual ativo necessita de proteção? Na medida que você sabe quais dados você tem, é possível identificar ameaças e vulnerabilidades no ambiente. Isso permite que você se concentre em proteger os ativos mais "críticos" ou o que é mais valioso para sua organização.

Função 2: Proteger: Quais medidas de segurança estão disponíveis? Depois de saber o que você precisa proteger, você pode definir medidas para salvaguardar esses dados. Uma abordagem em camadas da segurança é fundamental para proteger a camada de conectividade, a camada de aplicativos e o próprio dispositivo.

Função 3: Detectar: Quais técnicas podem identificar os incidentes? Sempre há mudanças nas circunstâncias, mesmo nos programas de segurança mais maduros. É por isso que você deve monitorar continuamente o ambiente para detectar eventos e possíveis incidentes.

Função 4: Responder: Quais técnicas podem conter os impactos dos incidentes? Tenha um plano de resposta. Como todos sabemos, não é se a empresa sofrer um ataque, mas sim quando o ataque irá acontecer. Ter um plano de resposta formal, testado e conhecido pela organização e seus stakeholders é crucial.

Função 5: Recuperar: Quais técnicas podem restaurar a capacidade? A organização deve se recuperar quando suas operações forem interrompidas por um ataque. Embora nenhuma organização queira passar por isso, esse é o momento de enxergar onde melhorias podem ser feitas.

Figura 1 – Estrutura do Núcleo do Framework

(Fonte: NIST Framework for Improving Critical Infrastructure Cybersecurity versão 1.1)

O Núcleo também possui as categorias e subcategorias, como é possível observar na Figura 1. As categorias são as subdivisões de uma Função em grupos de resultados de segurança cibernética estreitamente vinculado às necessidades e atividades específicas. Exemplos de Categorias incluem “Gerenciamento de ativos”, “Gerenciamento de identidades e controle de acesso” e "Processos de detecção".

As subcategorias dividem ainda mais uma categoria em resultados específicos de técnicas e / ou atividades de gerenciamento. Elas fornecem um conjunto de resultados que, embora não exaustivos, ajudam a suportar o resultado de cada categoria. Exemplos de subcategorias incluem “Sistemas de informação externos são catalogados”, “Dados armazenados são protegidos”, e “Notificações de sistemas de detecção são investigadas.”

- Camadas de Implementação (Implementation Tiers): Descreve como o risco de cibersegurança é gerenciado por uma organização e as características chaves do grau das práticas de gestão de risco. O feedback indica a necessidade do framework permitir flexibilidade para a implementação e traz conceitos de modelos de maturidade. Respondendo aos feedbacks, a camada de implementação do framework propõe refletir como uma organização implementa as funções núcleo (Core) do framework e gerencia o seu risco.

As camadas são progressivas, indo do parcial (Camada 1) para o Adaptativo (Camada 4), e cada camada é construída sobre a camada anterior. As características da camada são definidas no nível organizacional e são aplicadas para o núcleo do framework para determinar como aquela categoria será implementada (NIST CSF, 2018).

Camada 1: A gestão de riscos é feita *ad hoc* com consciência de riscos limitada e sem colaboração de terceiros.
Camada 2: Há processos e programas de gestão de risco em vigor, mas não são integrados em toda a empresa; a colaboração é compreendida, mas a organização carece de capacidades formais.

- Perfil (Profile) é responsável por alinhar os padrões da indústria e das melhores práticas para o Núcleo em um cenário de implementação particular, além de suportar priorização e medição enquanto se integra com as necessidades de negócios. Essa etapa trata da avaliação do perfil da organização por meio do alinhamento de funções, categorias e subcategorias com os requisitos de negócios, tolerância ao risco e os recursos da organização. Permite que as organizações criem um *roadmap* para a redução do risco de segurança cibernética mantendo-se alinhado com os objetivos organizacionais, considerando requisitos legais / regulamentares e melhores práticas da indústria refletindo as prioridades de gestão de riscos. Pode ser usado para descrever o estado atual (perfil atual) e o estado desejado (perfil de destino) de atividades de segurança cibernética (NIST CSF, 2018).

Em suma, o NIST CSF pode ser usado para (a) entender o estado atual da segurança (perfil atual); (b) estabelecer ou melhorar um programa de segurança cibernética; (c) comunicar os requisitos de segurança cibernética aos *stakeholders*; (d) identificar oportunidades para novas normas ou revisões de normas existentes; (e) identificar ferramentas e tecnologias para suportar o processo de gestão de riscos cibernéticos na organização; (f) integrar privacidade e considerações de liberdade civis no programa de segurança.

3.4 Técnicas de Identificação de Riscos (ISO 31010)

Conforme a NBR ISO/IEC 31010 (ABNT, 2012), o processo de avaliação de riscos pode ser conduzido em diferentes graus de detalhe e utilizando um ou muitos métodos que vão do simples ao complexo. Convém que a forma de avaliação e sua saída sejam compatíveis com os critérios de risco, desenvolvidos como parte do estabelecimento do contexto.

Ainda segundo a mesma norma, em termos gerais, convém que as técnicas apropriadas sejam justificáveis e apropriadas à situação ou organização em questão, proporcionem resultados de uma forma que amplie o entendimento da natureza do risco e de como ele pode ser tratado e sejam rastreáveis, repetíveis e verificáveis. Além disso, a escolha das técnicas utilizadas vai depender dos objetivos a serem alcançados pelo projeto ou pela instituição, do grau de maturidade da equipe em gerenciamento de riscos e do tempo e orçamento disponível.

Em relação à identificação de riscos, a ISO 31010 diz que o propósito é identificar o que poderia acontecer, ou que situações poderiam existir, que possam afetar o cumprimento dos objetivos propostos. Abaixo selecionamos as técnicas que iremos utilizar na presente pesquisa, ressaltando que o estudo irá focar na identificação dos riscos cibernéticos, portanto, selecionamos três técnicas que estão mais apropriadas ao contexto:

- Lista de Verificação (CheckList): Técnica onde uma lista de itens (*checklist*) é elaborada para assegurar que os tópicos mais comuns, assim como os mais críticos, sobre o assunto tratado não sejam esquecidos durante a identificação de riscos. Seu uso é recomendado nos casos onde há informação histórica, referências de mercado, e o conhecimento de situações prévias encontra-se largamente disponível.

- Análise de Cenário: Técnica que usa modelos descrevendo possíveis cenários futuros para identificar riscos considerando possíveis resultados, estratégias e ações que levam aos resultados, e possíveis implicações para o negócio. Deve ser considerada em situações em que há múltiplas soluções disponíveis ou os resultados possuem grande variação.

- What If (SWIFT): A técnica envolve equipes multidisciplinares de especialistas e um facilitador que deve liderar a aplicação da técnica. Ela explora elementos de uma atividade prévia de *brainstorming* sendo, entretanto, conduzida em um nível mais elevado de descrição. Ao fazer perguntas como "E se determinado sistema ficar indisponível? " a equipe consegue se unir para encontrar soluções para todos os questionamentos, sempre com base em um consenso entre todos. Imaginar a real possibilidade do problema acontecer faz com que todos se unam para a elaboração de um plano de ação conjunto.

3.5 Ferramenta Computacional: THEHIVE Project

Existem muitas ferramentas no mercado que suportam à gestão de riscos cibernéticos, tais como programas antivírus como os da Avast, McAfee e Symantec, softwares firewalls que já vêm inclusive nativo junto ao sistema operacional Microsoft Windows e outras tantas soluções e tecnologias tanto de hardware como de software que surgem a todo o momento para tentar impedir que as empresas tenham suas preciosas informações violadas. Contudo grandes avanços na segurança cibernética contam com o mesmo núcleo principal: compartilhamento de conhecimento e de informações. Por esse motivo, a ferramenta que foi escolhida como ferramenta de apoio à implementação do processo de identificação de incidentes cibernéticos dos processos, ativos e sistemas da organização é o sistema de código aberto THEHIVE Project.

O THEHIVE Project é uma ferramenta construída por entusiastas de maneira colaborativa, por isso a ideia de colméia (hive em inglês), projetada para tornar a vida mais fácil para Centros de Operação de Segurança (SOCs), para Equipes de Resposta a Incidentes de Segurança da Informação, os famosos CSIRTs (Computer Security Incident Response Team), para os Centro de Pesquisa para Resposta e Tratamento de Incidentes (CERTs) e qualquer profissional de segurança da informação. Trata-se de uma Plataforma de Resposta a Incidentes de Segurança escalável, de código aberto e livre, fortemente integrada com o MISP (Malware Information Sharing Platform), ferramenta similar à FS-ISAC adotada pela Subcomissão de Cybersegurança da FEBRABAN e citada anteriormente neste artigo.

Ao adotar o THEHIVE, vários profissionais podem colaborar em investigações simultaneamente. Por meio de transmissão integrada das informações em tempo real relativas a casos novos ou existentes. Os profissionais podem registrar seu progresso de investigação, anexar elementos de evidência, arquivos ou notas, adicionar tags e importar arquivos compactados protegidos por senha contendo malware ou dados suspeitos sem a necessidade de abri-los. Sendo que os dados já compartilhados no MISP por outros profissionais e organizações podem ser importados para a base da empresa para serem manipulados, analisados e incluídos na identificação e tratamento de riscos cibernéticos da organização.

Resumidamente, a ferramenta THEHIVE Project em conjunto com o MISP, permitirá que a organização se aproprie de base de riscos cibernéticos externos já identificados por outras empresas bem como as informações sobre os tratamentos para detecção da ameaça e para se proteger dela. Da mesma forma, os riscos identificados e detectados pela organização poderão ser compartilhados com as demais organizações e profissionais usuários. O compartilhamento acontece em tempo real, fator fundamental no cenário da segurança cibernética em que os ataques se propagam muito rapidamente.

4. PROPOSTA DE IMPLEMENTAÇÃO DO NIST CSF

O NIST CSF é extenso para ser implementado de uma vez apesar de priorizar apenas atividades essenciais da gestão de segurança da informação. No próprio framework há uma sugestão de passos para uma implantação progressiva por meio da criação de perfis sucessivos, agregando a cada ciclo novas categorias e subcategorias a serem implementadas de acordo com as prioridades identificadas no processo de gestão.

É importante ressaltar que a organização deve usar o CSF como uma parte fundamental de seu processo sistemático de identificar, avaliar e gerenciar o risco de segurança cibernética. O CSF não foi projetado para substituir processos, sendo assim, a proposta é usar o processo atual de gerenciamento de riscos da organização e sobrepô-lo ao framework para determinar as lacunas em sua atual abordagem de risco de segurança cibernética, com a finalidade de desenvolver um plano de melhoria de processo ao passo que mapeia-se os processos e serviços críticos e prioriza-se os esforços e orçamentos para minimizar o impacto sobre eles.

O NIST CSF será usado para comparar as atuais atividades de segurança cibernética da organização com as descritas no framework por meio da criação de um perfil atual. Assim a organização poderá examinar até que ponto eles estão alcançando os resultados descritos nas Categorias e Subcategorias, alinhadas com as cinco funções de alto nível: Identificar, Proteger, Detectar, Responder e Recuperar.

Seguindo essas etapas, a organização poderá eventualmente descobrir que ela já está atingindo os resultados desejados para alguns ativos, sistemas e processos, gerenciando, assim, a segurança cibernética proporcional ao risco conhecido. Nesse sentido, a intenção é que a organização utilize essas informações para desenvolver um plano de ação para fortalecer as práticas existentes de segurança cibernética e reduzir os riscos provenientes dela. Além disso, a organização pode descobrir que está investindo demais em determinados processos para alcançar certos resultados, e pode usar essas informações para redistribuir os recursos em processos que podem trazer mais retorno em termos financeiros e de elevação de segurança.

As etapas a seguir, retiradas do NIST CSF, ilustram como a organização pode usar o CSF para criar um novo programa de segurança cibernética ou melhorar o programa existente. Sabemos que a organização em questão não possui ainda um modelo padronizado de segurança cibernética, portanto, é esperado que tenhamos muitas ações a serem implementadas para evoluir progressivamente o perfil atual rumo ao perfil de destino.

Esses passos devem ser repetidos sempre que necessários, inclusive orientamos a definição de intervalos anuais ou semestrais para a repetição do processo até que a organização atinja um nível de maturidade aceitável. A repetição é fundamental para melhoria continua do processo de gestão da segurança cibernética, bem como eventuais atualizações tanto no contexto externo quanto no contexto interno.

Etapa 1: Definir prioridades e escopo. Identificar os objetivos de negócios e prioridades organizacionais de alto nível – Prioridade Nível 1. Com essa informação, é possível tomar decisões sobre implementações de segurança cibernética e determinar o escopo dos sistemas e ativos que suportam a linha de negócios ou o processo selecionado. A etapa pode ser adaptada para apoiar as diferentes linhas de negócios ou processos dentro de uma organização, que podem ter necessidades de negócios diferentes e tolerância a riscos associados.

Etapa 2: Orientar. Uma vez determinado o escopo do programa de segurança cibernética para a linha de negócios ou processo escolhido, é preciso identificar sistemas e ativos, requisitos regulatórios e abordagens gerais de risco relacionadas. A organização deve consultar fontes de pesquisa para identificar ameaças e vulnerabilidades existentes aplicáveis a esses processos, sistemas e ativos.

Etapa 3: Criar um perfil atual. A organização define um perfil atual indicando quais resultados de Categoria e Subcategoria do Núcleo (Core) do framework estão sendo atualmente alcançados. Se um resultado for parcialmente alcançado, conseguir enxergar essa diferença entre o perfil atual e o perfil desejado ajudará a dar suporte às etapas subsequentes, auxiliando na evolução do processo.

Etapa 4: **Realizar a avaliação de risco**. Essa avaliação pode ser norteada pelo processo de gerenciamento de riscos já implantado na organização ou atividades anteriores de avaliação de riscos do processo. É importante analisar o ambiente operacional para identificar a probabilidade de um incidente relacionado à segurança cibernética e o impacto que esse poderá ter na organização caso

ocorra, por isso o emprego de técnicas de identificação de riscos como as previstas na ISO 31010 são importantes nesta etapa. Deve-se atentar para identificar riscos emergentes e usar informações de ameaças cibernéticas de fontes internas e externas para obter uma melhor compreensão da probabilidade e do impacto dos incidentes.

Etapa 5: Criar o perfil de destino. Deve-se criar um perfil de destino com foco no resultado da avaliação das Categorias e Subcategorias do framework do perfil atual, descrevendo o cenário desejado da segurança cibernética da organização. É possível também, caso seja necessário, incluir nesse perfil de destino, categorias e subcategorias próprias adicionais por ocasião de riscos específicos mapeados na organização. Além disso, necessidades de *stakeholders* externos, como clientes e parceiros de negócios podem influenciar no momento da criação do perfil de destino. Resumidamente, o perfil de destino deve refletir adequadamente critérios dentro do nível de implementação desejado.

Etapa 6: Identifique, analise e elimine as lacunas. Esse é o momento de comparar o perfil atual com o perfil de destino para estabelecer as lacunas – *gaps* - entre os dois. Em seguida, deverá ser criado um plano de ação para endereçar as lacunas – o plano de ação deverá refletir os objetivos do negócio, custos, benefícios e riscos envolvidos no processo de evolução para o perfil de destino. A organização então determina recursos financeiros e humanos necessários para eliminar as lacunas.

Etapa 7: Implementar o plano de ação. A organização determina quais ações devem ser realizadas para eliminar as lacunas encontradas, se existirem, identificadas na etapa anterior e, em seguida, ajusta suas práticas atuais de segurança cibernética a fim de alcançar o perfil de destino. É importante esclarecer que o framework possui as Referências informativas sobre as categorias e subcategorias, mas cabe a organização determinar quais normas, diretrizes e práticas, incluindo aquelas que são específicas do setor, funcionam melhor para as suas necessidades.

As etapas descritas acima serão repetidas conforme necessário para avaliar e melhorar continuamente a segurança cibernética. Por exemplo, a organização pode descobrir que a repetição mais frequente da Etapa 2 melhora a qualidade das avaliações de risco. Além disso, a organização pode monitorar o progresso por meio de atualizações do perfil atual, comparando o perfil atual ao perfil de destino.

Essa proposta abrange a implantação do NIST CSF na empresa objeto da pesquisa, contudo para a implantação do processo de identificação de riscos cibernéticos apenas as etapas de 1 a 3 devem ser cumpridas de acordo com as prioridades organizacionais, ou seja, por meio das técnicas de identificação de riscos, iremos mapear as prioridades organizacionais – Prioridade Nível 1 - e a partir de então iniciar o processo de gestão de incidentes cibernéticos. Conforme as etapas de 1 a 3 forem sendo repetidas, novos processos, ativos e sistemas serão adicionais no escopo e as próximas etapas de 4 a 7 serão cumpridas para os primeiros ativos identificados.

5. ANÁLISSE E DISCUSSÃO DOS RESULTADOS

Após a apresentação da proposta de modelo a ser adotado para a implementação, é necessário respondemos as questões levantadas para a análise e discussão dos resultados:

1. Qual é o grau de maturidade em gestão de riscos cibernéticos da instituição antes da implantação do NIST CSF? Quanto à gestão de riscos cibernéticos, a instituição pode ser classificada na Camada 2 – Camadas de Implementação do NIST CSF – ou seja, há processos e programas de gestão de risco em vigor, mas não integrados em toda a empresa; a colaboração é compreendida, mas a organização carece de capacidades formais. A intenção é que ao longo dos ciclos de implementação do framework a organização consiga evoluir seu grau de maturidade em gestão de riscos para as Camadas 3 e 4.

2. Como determinar o grau de maturidade em gestão de riscos cibernéticos após o término do primeiro ciclo da implantação do NIST CSF? A proposta é usar o processo atual de gerenciamento de riscos da organização e sobrepô-lo ao framework para determinar as lacunas em sua atual abordagem. O CSF será usado para comparar as atuais atividades de segurança cibernética da organização com as descritas no framework por meio da criação de um perfil atual e de um perfil de destino. As etapas de 1 a 7 do modelo

devem ser repetidas sempre que for necessário. Orientamos a definição de intervalos de seis meses para a repetição do processo até que a organização atinja um nível de maturidade aceitável.

3. Como definir os recursos que suportam funções críticas e que, por conseguinte, necessitam de proteção? A intenção é implantar a ferramenta e iniciar processo de catalogação de riscos conforme eles forem sendo identificados. Os processos, sistemas e ativos já existente serão catalogados em níveis de prioridade de modo que a organização consiga iniciar o primeiro ciclo de implementação do modelo proposto nos recursos categorizados como Prioridade 1, e os próximos ciclos de implementação seguirão para a Prioridade 2, 3 e assim sucessivamente. Os incidentes catalogados serão compartilhados com outras instituições, assim como, desde o início será possível utilizar o catálogo de riscos já identificados para trabalhar nas funções reativas – Proteger e Detectar.

4. Quais são os riscos identificados ao final do processo como Prioridade 1 e que serão tratados pela função 'Proteger' do NIST CSF? O modelo proposto ainda será implantado, portanto somente será possível responder essa questão ao final do primeiro ciclo de implementação.

Como visto anteriormente, as Resoluções nº 4557 e nº 4658 do Banco Central do Brasil, trouxeram respectivamente a obrigatoriedade de implantação de estrutura de gestão de riscos e gestão de riscos cibernéticos compatível com a estrutura das instituições financeiras nacionais. E a Febraban (Federação Brasileira de Bancos) já possui uma Subcomissão de Cyber Segurança com a participação das 12 principais instituições financeiras do país.

Essas novas regulamentações trazem à tona a importância de um processo de gestão de riscos cibernéticos bem coordenado para, mais do que atender as legislações vigentes, ser efetivo e coerente com as necessidades do negócio, tanto no poder público quanto na iniciativa privada. Nesse contexto, a escolha de implantação do processo de gestão de riscos cibernéticos com base no NIST Cybersecurity Framework considerou que ele foi projetado para reduzir o risco, ao passo que provê melhoria do gerenciamento do risco de segurança cibernética relacionados aos objetivos organizacionais.

Esclarecemos que o planejamento da presente pesquisa tem foco nas Etapas 1 a 3 de implantação de programa de segurança cibernética proposto pelo NIST CSF, com o objetivo de identificar os incidentes cibernéticos de processos prioritários da organização e servir de base para que a implantação das outras funções do framework aconteçam posteriormente, e que os demais processos, ativos e sistemas da organização também sejam incluídos em novos ciclos de identificação de riscos.

6. CONCLUSÃO

Os ataques cibernéticos fazem parte do cotidiano de toda grande corporação, e nesse sentido, elas vêm utilizando todo o tipo de barreira tecnológica - soluções de hardware e software, processos, modelos, normas e padrões - para se protegerem e evitarem que tais ameaças afetem a integridade, disponibilidade, autenticidade e confidencialidade de suas informações. As instituições financeiras, tão afetadas por esse tipo de crime, vêm atuando ativamente como pioneiras na adoção de padrões e modelos de gestão de riscos cibernéticos para identificarem, recuperarem e se protegerem de novas ameaças.

Como visto, o NIST CSF pode ser implementado em conjunto com outros frameworks e normas, tais como o COBIT, a ISO 27001 e a ISO 27032. As suas cinco funções, que vão desde a identificação dos riscos até a recuperação de ambientes que sofreram ataques são muito similares ao processo de gestão de riscos da ISO 31000, já consolidado nas organizações em geral e na instituição financeira alvo dessa pesquisa.

Com a implantação do NIST CSF, a organização poderá usufruir de um processo de gestão de riscos cibernéticos padronizado, atualizado e em constante desenvolvimento, visto que o framework prevê ciclos contínuos de repetição das etapas do processo com a finalidade de abranger novos processos, sistemas e ativos, incluindo as novas ameaças que surgem constantemente no cenário externo. Assim sendo, não se trata de processo único e que tem começo, meio e fim, e sim de um processo iterativo e constante, corroborando com o aumento gradual do nível de maturidade em gestão de riscos cibernéticos da organização.

Conforme o NIST (2018), as organizações que conseguem implantar adequadamente o framework serão capazes de medir e atribuir valores a seus riscos, juntamente com o custo e os benefícios das medidas tomadas para reduzi-los a níveis aceitáveis. Quanto melhor for a capacidade da organização de mensurar os riscos, custos e benefícios de suas estratégias, mais assertiva, eficaz e valiosa será sua abordagem e seus investimentos em segurança cibernética.

Assim sendo, a pesquisa terá continuidade com o planejamento da implantação das demais etapas e funções propostas pelo NIST CSF, de modo que a organização consiga ao longo das iterações melhorar progressivamente o nível de maturidade de gestão de riscos cibernéticos até chegar ao nível adequado para as suas necessidades de negócio.

7. REFERÊNCIAS

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. Gestão de Riscos – Princípios e diretrizes. NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2018.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. Gestão de riscos: Técnicas para o processo de avaliação de riscos. NBR ISO 31010. Associação Brasileira de Normas Técnicas. 2012.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. NBR ISO 27001. Associação Brasileira de Normas Técnicas. 2013.

[4] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética. NBR ISO 27032. Associação Brasileira de Normas Técnicas. 2015.

[5] AVAST. Novas ferramentas de segurança cibernética reduzem o crime virtual. Publicado em 25/03/2019. Disponível em https://blog.avast.com/pt-br/novas-ferramentas-de-seguranca-cibernetica-reduzem-o-crime-virtual . Acessado em 25/04/2019.

[6] BANCO CENTRAL DO BRASIL. Resolução BACEN n° 4557. Brasília, DF, 23/02/2017. Disponível em : https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50344/Res_4557_v1_O.pdf . Acessado em 23/04/2019.

[7] BANCO CENTRAL DO BRASIL. Resolução BACEN n° 4658. Brasília, DF, 26/04/2018. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf . Acessado em 23/04/2019.

[8] BRASIL. Decreto nº 9.203. Diário Oficial da União, Brasília, DF, seção 1, p.3, 23/11/2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Decreto/D9203.htm . Acessado em 23/04/2019.

[9] BROCKMAN. CARISA. The NIST Cybersecurity Framework (CSF) and What It can do for you. Publicado em AT&T BUSINESS, 19/03/2019. Disponível em: https://www.alienvault.com/blogs/security-essentials/the-nist-cybersecurity-framework-csf-and-what-it-can-do-for-you . Acessado em 24/04/2019.

[10] ISACA. COBIT 2019 Framework: Introduction and Methodology. Disponível em: http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Introduction-and-Methodology.aspx . Acessado em 23/04/2019.

[11] MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. CONTROLADORIA GERAL DA UNIÃO. Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Diário Oficial da União, Brasília, DF, 11/05/2016. Disponível em: https://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf. Acessado em 23/04/2019.

[12] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity. 16/04/2018. Disponível em: https://www.nist.gov/cyberframework/framework. Acessado em 23/04/2019.

[13] THIOLLENT, M. (2009). Metodologia de Pesquisa-ação. São Paulo: Saraiva.

[14] WORLD ECONOMIC FORUM. (2019). The Global Risks Report 2019 - 14th edition. Genebra: World Economic Forum.