SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
XX SEGeT
INTELIGÊNCIA ARTIFICIAL: Impactos e Desafios
Realização: AEDB | UniDomBosco Centro Universitário Dom Bosco do Rio de Janeiro

Estruturação de Um Plano de Metas e Ações para Segurança Cibernética com o Apoio do NIST Cybersecurity Framework

Dacyr Dante de Oliveira Gatto
dacyr.gatto@uni9.pro.br
UNINOVE

Renato José Sassi
sassi@uni9.pro.br
UNINOVE

Resumo:A ascensão da era digital tem gerado aumento expressivo na produção e uso de dados, trazendo consigo novos desafios para a segurança cibernética e necessidade de gerenciamento de seus riscos. Com o grande volume de informações pessoais, financeiras e corporativas em circulação, a falta de um gerenciamento efetivo de riscos pode ter consequências devastadoras para as organizações, incluindo perdas financeiras, danos à reputação e interrupções operacionais, como ocorrido na empresa foco desta pesquisa. Para lidar com esses riscos, não basta apenas implementar tecnologias avançadas. É essencial adotar uma abordagem estruturada que possibilite a identificação, análise, tratamento e monitoramento contínuo dos riscos cibernéticos. Nesse sentido, o NIST Cybersecurity Framework (NIST CSF), desenvolvido pelo National Institute of Standards and Technology, apresenta-se como uma estratégia amplamente adotada para gerenciamento de riscos cibernéticos. Este artigo tem como objetivo analisar a adoção do NIST CSF no apoio ao gerenciamento de riscos cibernéticos, destacando seu papel na melhoria da resiliência organizacional. Através de pesquisa de campo, foi observada a aplicação do NIST CSF em uma empresa que administra uma rede de shopping centers em São Paulo, e a elaboração de um Plano de Metas e Ações, como parte de seu Plano Diretor de Segurança da Informação. Observou-se na pesquisa de campo executada a estruturação de processos de

segurança cibernética que ao serem adotados ou, quando existentes, melhorados, o direcionamento de ações conscistentes para que a empresa mapeasse os riscos de segurnaça cibernética com o objetivo de evitar novos incidentes cibernéticos. Observou-se também a relevância do NIST CSF na gestão de riscos cibernéticos atuais, enfatizando seu potencial para guiar empresas na busca por robustez em segurança cibernética. O estudo também contribui para a literatura acadêmica ao abordar a interseção entre práticas de gerenciamento de riscos cibernéticos e

Palavras Chave: Seg. Cibernética - Riscos Cibernéticos - NIST CSF - Pl. de Metas e Ações

-

1. INTRODUÇÃO

A era digital emergente, impulsionada por avanços significativos em tecnologias da informação e comunicação, tem levado a um aumento exponencial na produção e uso de dados. No entanto, esta digitalização de massa também tem implicado novas e complexas ameaças à segurança cibernética, tornando o gerenciamento de riscos uma necessidade crítica para todas as organizações (KRUMAY; BERNROIDER; WALSER, 2018).

Os riscos de segurança cibernética são uma das preocupações mais urgentes para as empresas modernas, dada a alta dependência de sistemas de informação e a quantidade crescente de dados pessoais, financeiros e corporativos gerados. A falta de um gerenciamento de riscos eficaz pode resultar em consequências graves, incluindo perdas financeiras, danos à reputação e até mesmo interrupções operacionais. Portanto, é essencial que as organizações invistam em estratégias eficazes de gerenciamento de riscos para garantir a segurança, integridade e disponibilidade de seus ativos de informação (GARBA; BADE, 2021).

Uma estratégia de gerenciamento de riscos cibernéticos eficaz, no entanto, não é apenas sobre a implementação de tecnologias avançadas; também envolve a criação de uma estrutura robusta que permita a identificação, análise, tratamento e monitoramento contínuo dos riscos. Nesse contexto, o *NIST Cybersecurity Framework* oferece uma abordagem holística para gerenciamento de riscos flexível, personalizável e aplicável a uma ampla gama de contextos empresariais. Desenvolvido por uma das organizações líderes em tecnologia e ciência, o *NIST (National Institute of Standards and Technology)*, se destaca como um dos padrões mais utilizados no mundo para gestão de riscos cibernéticos (NIST, 2018, DIMITROV; KALAYANOVA; PETROV, 2021).

O NIST CSF fornece uma estrutura consistente e compreensível que ajuda as organizações a entenderem, gerenciar e reduzir seus riscos cibernéticos, enquanto melhora a resiliência de seus sistemas e processos. Este estudo, portanto, busca analisar como a adoção e implementação do NIST CSF pode melhorar o gerenciamento de riscos cibernéticos e contribuir para a resiliência das organizações. Este artigo procura explorar a importância do gerenciamento de riscos de segurança cibernética e como o NIST CSF pode apoiar empresas nesse processo de gerenciamento, através de uma pesquisa de campo da aplicação deste *framework* em uma empresa administradora de uma rede de *Shopping Centers* em São Paulo.

Este artigo pretende lançar luz sobre a relevância do NIST CSF na prática atual de gerenciamento de riscos cibernéticos, destacando seu potencial para orientar as empresas em seu caminho para a segurança cibernética robusta. Além disso, a pesquisa também pretende contribuir para a literatura acadêmica existente, ampliando o entendimento sobre a interseção entre as práticas de gerenciamento de riscos cibernéticos e o uso de *frameworks* de segurança cibernética, através de uma pesquisa de campo, no qual acompanhou a implementação do NIST CSF em uma empresa que administra uma grande rede de *Shopping Centers*. Esta implementação foi parte do projeto de elaboração do Plano Diretor de Segurança da Informação na referida empresa.

2. PROBLEMA DE PESQUISA E OBJETIVO

O problema de pesquisa deste artigo, é explorar e analisar a situação deficiente de segurança cibernética em uma empresa específica e as consequências que a falha na segurança cibernética teve para o negócio. A empresa sofreu uma violação significativa de dados que resultou em perda financeira substancial e danos à reputação, em momento anterior a esta pesquisa. O artigo mostrou como a empresa implementou formalmente o processo de gerenciamento de riscos cibernéticos em sua estrutura de negócios, tendo como base o NIST

CSF, e os resultados obtidos como parte do projeto de elaboração de um Plano Diretor de Segurança da Informação.

Objetivo deste trabalho foi analisar a aplicação do NIST CSF no processo de gerenciamento de riscos cibernéticos na empresa administradora de uma rede de *Shopping Centers*.

3. FUNDAMENTAÇÃO TEÓRICA

3.1. GERENCIAMENTO DE RISCOS CIBERNÉTICOS

O gerenciamento de riscos cibenéticos é um componente vital para qualquer organização no mundo digital contemporâneo. O processo envolve a identificação, a análise e a avaliação de riscos que podem afetar a integridade, disponibilidade e confidencialidade das informações, bem como a adoção de medidas adequadas para mitigar esses riscos. Este processo não é uma atividade isolada, mas deve ser uma parte integrante da estratégia global de negócios de uma organização, pois está intrinsecamente relacionado à continuidade dos negócios, à conformidade regulatória e à proteção da reputação da empresa (ATOUM; OTOOM; ALI, 2014; DA SILVA; GARCIA, 2019).

Os riscos de segurança cibernética podem surgir de várias fontes, como ataques cibernéticos, falhas de *hardware* ou *software*, erros humanos e desastres naturais. Eles também podem variar em termos de gravidade, desde pequenas interrupções que podem ser facilmente resolvidas até violações de dados massivas que podem resultar em perdas financeiras significativas e danos irreparáveis à reputação. Portanto, as organizações precisam de uma estratégia de gerenciamento de riscos que seja abrangente e adaptável, capaz de responder efetivamente a uma variedade de ameaças em constante mudança (ALEXANDRE; PANGULURI; 2017; DEDEKE, 2017).

A primeira etapa do gerenciamento de riscos cibernéticos é a identificação de riscos, que envolve a detecção de potenciais ameaças aos ativos de uma organização. Isso pode ser feito por meio de várias técnicas, incluindo avaliações de segurança, auditorias e análise de logs. Após a identificação de riscos, eles devem ser analisados e avaliados em termos de sua probabilidade de ocorrência e o impacto potencial que poderiam ter sobre a organização. Isso permite que as organizações priorizem os riscos e aloquem recursos de maneira eficaz (DE FRANCO; JINO, 2016).

De Franco e Jino (2016) ainda explanam que uma vez que os riscos foram identificados e avaliados, eles devem ser tratados por meio de uma combinação de medidas de prevenção, detecção, resposta e recuperação. As medidas de prevenção podem incluir a implementação de controles de segurança, como firewalls e sistemas de detecção de intrusão, bem como a formação de funcionários em práticas seguras de tratamento das informações. As medidas de detecção e resposta envolvem a monitorização contínua dos sistemas de informação para detectar possíveis violações de segurança e responder a elas de maneira rápida e eficaz. Por último, mas não menos importante, as organizações também devem ter planos de recuperação em vigor para se recuperar de violações de segurança e minimizar o impacto sobre as operações comerciais.

Em última análise, o gerenciamento de riscos cibernéticos é uma tarefa contínua que exige uma abordagem proativa e adaptativa. As organizações devem se esforçar para manter-se atualizadas com as últimas tendências e ameaças de segurança, adaptar suas estratégias de gerenciamento de riscos conforme necessário e cultivar uma cultura de segurança que envolva todos os níveis da organização. Com um gerenciamento de riscos cibernéticos eficaz, as organizações podem proteger seus ativos valiosos, garantir a continuidade dos negócios e manter a confiança dos *stakeholders* (SABILLON, 2017; DUTTA; AL-SHAER, 2019).

O NIST CSF pode apoiar o gerenciamento de riscos de segurança cibernética ao fornecer uma estrutura abrangente e adaptável para a identificação, proteção, detecção, resposta e recuperação de ameaças cibernéticas. Com um conjunto de padrões, melhores práticas e diretrizes, ele permite que as organizações avaliem e melhorem suas capacidades de gerenciamento de riscos, identifiquem lacunas na segurança e implementem medidas de controle eficazes (ROY, 2020).

3.2. *NIST CYBERSECURITY FRAMEWORK*

O NIST *Cybersecurity Framework* (NIST CSF), desenvolvido pelo *National Institute of Standards and Technology* dos EUA, é uma estrutura de segurança cibernética que visa ajudar as organizações a gerenciarem e mitigarem riscos cibernéticos. Ele foi projetado para ser flexível e adaptável, permitindo que as organizações o apliquem de acordo com suas necessidades e circunstâncias específicas (NIST, 2018).

A estrutura do NIST CSF baseia-se em três componentes principais: o Núcleo da Estrutura, as Camadas de Implementação e os Perfis de Estrutura, conforme representado na Figura 1.

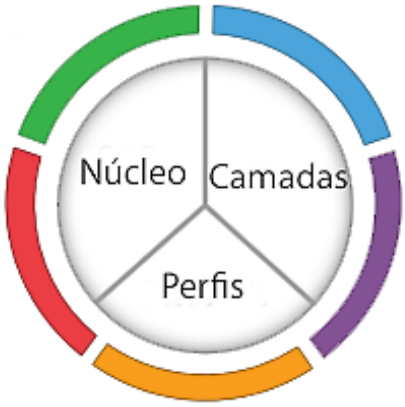

Figura 1: Estrutura do *NIST CSF*
Fonte: *NIST* (2018)

O Núcleo da Estrutura é o coração do NIST CSF e é composto por cinco funções: Identificar, Proteger, Detectar, Responder e Recuperar. Cada uma dessas funções é subdividida em categorias e subcategorias que descrevem os objetivos (categorias) e atividades de segurança (subcategorias) que as organizações devem implementar, conforme demonstrado na Figura 2 (NIST, 2018).

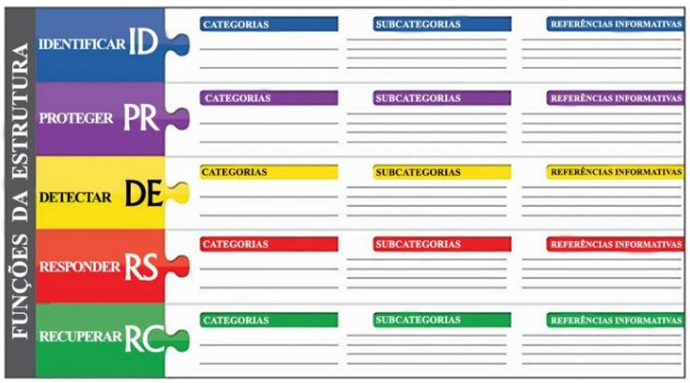

Figura 2: Núcleo da Estrutura Básica do *NIST CSF*
Fonte: *NIST* (2018)

A função "Identificar" envolve o desenvolvimento de uma compreensão organizacional para gerenciar o risco de segurança cibernética aos sistemas, ativos, dados e capacidades. Isso inclui a identificação de ativos de informação, análise de risco e desenvolvimento de uma estratégia de gerenciamento de riscos. A função "Identificar" é dividida em seis categorias: Gestão de Ativos; Ambiente de Negócios; Governança; Avaliação de Riscos; Estratégia de Gerenciamento de Riscos e Gerenciamento de Riscos na Cadeia de Suprimentos (NIST, 2018; ROY; 2020).

A função "Proteger" diz respeito à implementação de salvaguardas apropriadas para garantir a entrega de serviços de infraestrutura crítica. Isso envolve a proteção de ativos de informação por meio de controles de acesso, treinamento de conscientização e proteção de informações, entre outros. A função "Proteger" é dividida em seis categorias: Gerenciamento de Identidade, Autenticação e Controle de Acesso; Conscientização e Treinamento; Segurança de Dados; Processos e Procedimentos de Proteção da Informação; Manutenção e Tecnologia Protetora (NIST, 2018; ROY; 2020).

A função "Detectar" envolve a implementação de atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética. Isso pode incluir monitoramento contínuo e sistemas de detecção de anomalias. A função "Detectar" é dividida em três categorias: Anomalias e Eventos; Monitoramento Contínuo de Segurança eProcessos de Detecção (NIST, 2018; ROY; 2020).

A função "Responder" é sobre o desenvolvimento e implementação de atividades apropriadas para agir em relação a um evento de segurança cibernética detectado. Isso pode envolver planos de resposta a incidentes, comunicação e análise de incidentes. A função "Responder" é dividida em cinco categorias: Planejamento de resposta; Comunicações; Análise; Mitigação e Melhorias (NIST, 2018; ROY; 2020).

E a função "Recuperar" envolve o desenvolvimento e implementação de atividades apropriadas para manter planos de resiliência e restaurar quaisquer serviços que foram prejudicados devido a um evento de segurança cibernética. A função "Recuperar" é dividida em três categorias: Plano de Recuperação; Melhorias; Comunicações (NIST, 2018; ROY; 2020).

As categorias dividem-se em 108 subcategorias que equivalem a atividades a serem executadas para a gestão dos riscos cibernéticos (NIST, 2018).

As Camadas de Implementação apresentam contexto sobre como uma organização lida com o risco de segurança cibernética e os processos envolvidos para gerenciar esse risco. Descrevem o grau em que as práticas de gerenciamento do risco de segurança cibernética de organização evidenciam as características definidas na estrutura. Existem 4 (quatro) camadas de implementação descritas na estrutura de segurança cibernética do NIST CSF, quanto mais alta a camada, mais próximo o programa de gerenciamento de riscos de segurança cibernética da organização está das características definidas na estrutura (AL-TURKISTANI; ALDOBAIAN; LATIF, 2021).

As 4 camadas de implementação são:

- Nível 1: Parcial (Tier 1: Partial);
- Nível 2: Risco informado (Tier 2: Risk Informed);
- Nível 3: Repetível (Tier 3: Repeatable);
- Nível 4: Adaptável (Tier 4: Adaptative);

Durante o processo de seleção de Camada de Implementação, uma organização deve levar em consideração suas práticas atuais de gerenciamento de riscos, o ambiente de

ameaças, requisitos legais e regulamentares, objetivos de negócio, missão e restrições organizacionais.

Os Perfis de Estrutura do NIST CSF ajudam as organizações a alinharem suas necessidades de segurança cibernética com seus requisitos de negócios, tolerância ao risco e recursos. Eles são usados para identificar oportunidades para melhorar a postura de segurança cibernética de uma organização, criando um "perfil atual" que descreve as práticas de segurança cibernética atuais e um "perfil de destino" que descreve o estado desejado de segurança cibernética (VARELA-VACA, *et al*., 2021).

Em resumo, o NIST CSF oferece uma estrutura eficaz e flexível para o gerenciamento de riscos cibernéticos. Com sua abordagem holística e centrada no risco, ele permite que as organizações se protejam contra ameaças cibernéticas, respondam efetivamente a incidentes e mantenham a resiliência de seus sistemas e operações (NIST, 2018).

4. METODOLOGIA

4.1 CARACTERIZAÇÃO METÓDOLÓGICA

Para a elaboração deste artigo foram utilizadas como referência teórica literaturas (artigos de periódicos, congressos e obras) referente a gerenciamento de riscos cibernéticos e NIST CSF, para efeito de contextualização do conteúdo demonstrado. Os artigos de periódicos pesquisados, foram obtidos das bases de conhecimento *Scielo, Science Direct e ResearchGate*, e as obras utilizadas são de autores relacionados ao referencial teórico da pesquisa.

Foi utilizada a metodologia de pesquisa descritiva e exploratória com a finalidade de descrever sistematicamente a situação e o problema encontrado, e investigar as possibilidades encontradas, buscando esclarecer os conceitos teóricos apresentados no referencial. A abordagem da pesquisa foi qualitativa, abordando o estudo da empresa administradora da rede de Shopping Centers, utilizando-se de análise documental para efeito das evidências necessárias para a abordagem do gerenciamento de riscos de segurança da informação, observando-se o ambiente, acompanhando os membros da equipe nas situações investigadas, efetuando anotações a respeito do comportamento observado, assim como seus resultados, através do acompanhamento das atividades entre Maio e Outubro de 2022. Por tratar-se de um processo estratégico da organização, não foi autorizada a divulgação do seu nome, apenas dos resultados obtidos (KUMAR, 2019).

Como procedimento metodológico abordou-se a pesquisa de campo como método de coleta de dados que envolveu a observação direta e o engajamento com as pessoas em seu ambiente natural. O processo de coleta de dados envolveu entrevistas e análise de documentos (GIL, 2019; KUMAR, 2019).

4.2 CARACTERIZAÇÃO DA EMPRESA

A empresa foco do estudo é uma empresa que administra uma grande rede de *Shopping Centers* no estado de São Paulo, e como parte do seu projeto de elaboração de uma Plano Diretor de Segurança da Informação, solicitou a uma empresa de Consultoria de Segurança da Informação a implementação formal do seu processo de gerenciamento de segurança da informação, que serviu de insumo para a elaboração do referido Plano.

Ao iniciar-se a pesquisa na empresa, verificou-se que existia um gerenciamento de riscos corporativos implementado, mas em uma esfera mais ampla na organização, não enfatizando riscos cibernéticos, o que não previu uma violação significativa de dados que resultou em perda financeira substancial e danos à reputação da referida empresa. Diante do

cenário tecnológico atual esta lacuna de gerenciamento de riscos comprometeu toda estrutura de negócios da organização, uma vez que os riscos cibernéticos se tornaram um potencial incidente de segurança cibernética.

4.3 CARACTERIZAÇÃO DO PROBLEMA

Neste contexto a não existência de um processo formal de gerenciamento de riscos cibernéticos na empresa, foco desta pesquisa, deixava a organização exposta a riscos cibernéticos, riscos regulatórios, riscos legais e riscos de imagem, e suas possíveis consequências para a organização, o que se materializou em uma violação de dados.

Um dos principais motivadores para o projeto de elaboração do Plano Diretor de Segurança da Informação, e por consequência da implantação formal do processo de gerenciamento de riscos cibernéticos foi a necessidade de adequação a Lei Geral de Protestação de Dados (LGPD), vigente no Brasil desde 2018, e suas potenciais sanções.

Outro cenário latente que motivou a busca pela formalização do processo de gerenciamento de riscos cibernéticos foi a eminente exposição da empresa a ataques cibernéticos, o que ficou evidenciado com a violação de dados. Segundo fontes que atuam diretamente no combate a ataques cibernéticos, como a empresa BugHunt, houve uma aumento em 8% dos ataques cibernéticos em 2022 em empresas do seguinte de Tecnologia da Informação, Varejo e Finanças (BUGHUNT, 2023).

5. ANÁLISE DE RESULTADOS

A primeira atividade realizada baseou-se na identificação do cenário de riscos cibernéticos que a empresa se encontrava, compilando informações oriundas de entrevistas realizadas como gestores da empresa. Para esta atividade utilizou-se a ferramenta de Análise SWOT. A Análise SWOT, representada pela Matriz SWOT compilou as informações obtidas através das entrevistas com as áreas de Gestão (Nível Tático) e COMEX (Nível Estratégico) da referida empresa.

Obteve-se o documento a seguir como resultado a aplicação da Análise SWOT, representado na Figura 3.

	Forças	Fraquezas
Fatores Internos	Conscientização enraizada da importância da segurança da informação em todas as áreas	Comunicação das ações de Segurança carece de ser praticada
	COMEX tem visão mais ampla dos processos chaves de segurança da informação em execução	Gestores de área tem menor percepção das práticas de segurança nos processos chaves
	Comitê de TI formalizado	Iniciativas de segurança da informação em sua maioria são embrionárias ou se são executadas não são formalizadas
	Adequações de privacidade estabelecidas ou encaminhadas	Processo de identificação, avaliação e tratamento de riscos precisa de melhorias
	Processos de Negócios são em sua maioria mapeados	Processo orçamentário para segurança da informação precisa de melhorias
		Políticas parcialmente estabelecidas, ou não comunicadas
		Processo de auditoria não contemplam toda organização
		Parte dos controles técnicos precisam de formalização de implementação

	Oportunidades	Ameaças
Fatores Externos	Existe uma percepção positiva em relação a evidências das ações estratégicas executadas na organização em todas as áreas.	Riscos externos referentes a ameaças cibernéticas não são tratados em sua totalidade
		Riscos de TI não são tratados em sua totalidade

Figura 3: Matriz SWOT resultado da Análise SWOT
Fonte: Autor (2022)

Pôde-se verificar através da Análise SWOT que existia uma compreensão dos riscos cibernéticos no nível estratégico, porém não havia o reflexo desta compreensão no nível tático da empresa. Estratégias de negócios estavam mapeadas, assim como a visão da importância da área de Tecnologia da Informação, porém apesar de existir uma visão estratégica definida, observou-se não haver alinhamento no que diz respeito a segurança cibernética.

A não evidenciação de um processo do gerenciamento de riscos de segurança cibernética formal mostrou-se latente, refletindo também em riscos em tecnologia da informação, o que não suportava a visão estratégica apresentada na análise SWOT.

O que foi identificado como Forças e Oportunidades era ofuscado pelas Fraquezas e Ameaças, corroborando a necessidade de uma estruturação formal do processo de gerenciamento de riscos cibernéticos.

A partir do resultado da Análise SWOT iniciou-se então uma avaliação do status inicial da segurança cibernética, utilizando-se como base o núcleo da estrutura do NIST CSF. Definiu-se então o perfil atual de segurança cibernética da empresa e o nível de implementação em que os aspectos de cibersegurança, se existentes, estavam implementados

Estabeleceu-se o Nível de Implementação para as 108 subcategorias, ou atividades a serem executadas de segurança cibernética, segundo o NIST CSF.

Com a visão atual da segurança cibernética mapeada executou-se a análise dos riscos de segurança cibernética, tendo como o resultado o Mapa de Riscos de Segurança Cibernética demonstrado na Figura 4.

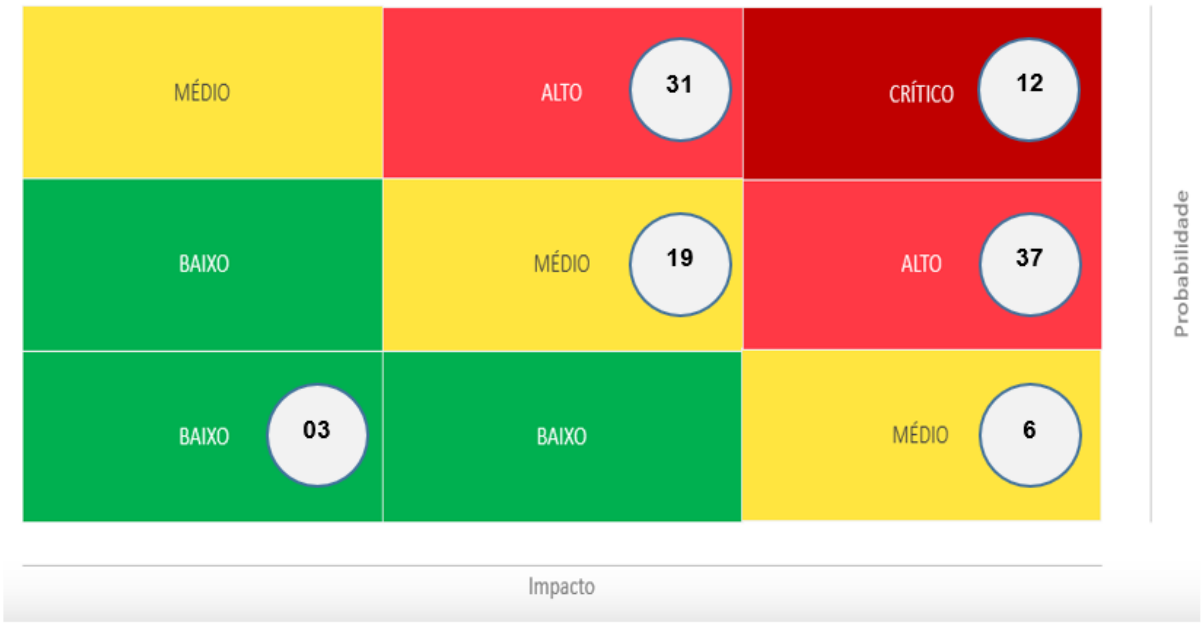

Figura 4: Mapa de Riscos de Segurança Cibernética
Fonte: Autor (2022)

Desta forma identificou-se riscos classificados em níveis de criticidade como resumido na Tabela 1 a seguir.

Tabela 1: Níveis de Criticidade e Totais de Riscos

Nível de Risco	Totalizador
Risco Nível Crítico	**12**
Risco Nível Alto	**68**
Risco Nível Médio	**25**
Risco Nível Baixo	**03**

Fonte: Autor (2022)

Como passo seguinte executou-se a avaliação de riscos cibernéticos. Avaliou-se os controles implementados segundo as 108 subcategorias do NIST CSF, atribuindo-se os

seguintes status de implementação em relação aos níveis de risco, conforme demonstrado na Tabela 2.

Tabela 2: Status de Implementação

Status de Implementação	Descrição do Status
Não se Aplica	**O controle não se aplica ao serviço do fornecedor ou às operações comerciais. (Forneça explicação)**
Não Implementado	**O controle não está em vigor.**
Executado Ad-Hoc	**O controle não existe, mas é praticado reativamente com base em cenários. O objetivo de praticar o controle é atingir um objetivo específico sem um processo passo a passo para alcançá-lo.**
Implementado Parcialmente	**O controle está implementado e executado com base em políticas, padrões e processos documentados e definidos.**
Totalmente Implementado	**O controle é definido por políticas e processos baseados em padrões internacionais ajustados às necessidades, experiências e capacidades da empresa dentro de um Sistema de Gestão da Segurança da Informação formalizado sujeito à Melhoria Contínua e Gestão da Qualidade.**

Fonte: Autor (2022)

Com a avaliação de riscos cibernéticos finalizada apresentou-se o seguinte Plano de Metas e Ações, atribuídos a cada uma das 108 subcategorias do NIST CSF, representado na Tabela 3 a seguir.

Tabela 3: Plano de Metas e Ações por Subcategoria.

Subcategoria	Controle Implementado	Nível de Risco	Metas e Ações
ID.AM-1: Dispositivos físicos e sistemas dentro da organização são inventariados	Executado Ad-Hoc	Alto	Estabelecer procedimento formal para inventariar dispositivos físicos e sua periodicidade
ID.AM-2: Plataformas de software e aplicativos dentro da organização são inventariados	Executado Ad-Hoc	Alto	Estabelecer procedimento formal para inventariar plataforma de software e aplicativos e sua periodicidade
ID.AM-3: A comunicação organizacional e os fluxos de dados são mapeados	Executado Ad-Hoc	Alto	Estabelecer processo formal de comunicação organizacional, assim como mapear o fluxo de dados nestas comunicações
ID.AM-4: Sistemas de informação externos são catalogados	Executado Ad-Hoc	Alto	Estabelecer processo de catalogação de sistemas da informação externos utilizados pela organização
ID.AM-5: Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em sua classificação, criticidade e valor de negócios	Implementado Parcialmente	Médio	Formalizar processo de classificação dos recursos (ativos), referente a sua criticidade e valor de negócios
ID.AM-6: São estabelecidas funções e responsabilidades de cibersegurança para toda a força de trabalho e partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros)	Executado Ad-Hoc	Crítico	Estabelecer processo de atribuição de funções e responsabilidades de cibersegurança para todos colaboradores e terceiros, baseando-se no grau de criticidade de cada um em relação as operações
ID.BE-1: O papel da organização na cadeia de suprimentos é identificado e comunicado	Implementado Parcialmente	Médio	Formalizar processo de identificação da organização junto a sua cadeia de suprimentos, assim como o processo de comunicação entre as partes
ID.BE-2: O lugar da organização em infraestrutura crítica e seu setor industrial é identificado e comunicado	Executado Ad-Hoc	Alto	Estabelecer processo de identificação e validação da infraestrutura crítica para operacionalização dos negócios da organização
ID.BE-3: Prioridades para a missão organizacional, objetivos e atividades são estabelecidas e comunicadas	Executado Ad-Hoc	Alto	Identificar formalmente e alinhar a missão, valores, objetivos e atividades assim como sua comunicação dentro da organização
ID.BE-4: São estabelecidas dependências e funções críticas para a prestação de serviços críticos	Executado Ad-Hoc	Alto	Estabelecer processo de identificação das funções críticas para operação da organização, assim como os serviços críticos prestados
ID.BE-5: Os requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	Executado Ad-Hoc	Alto	Estabelecer processo de continuidade operacional em caso de interrupção de serviços críticos
ID.GV-1: Política organizacional de segurança cibernética é estabelecida e comunicada	Totalmente Implementado	Baixo	Estabelecer processo de melhoria contínua do processo estabelecido e documentado

ID.GV-2: As funções e responsabilidades de cibersegurança são coordenadas e alinhadas com funções internas e parceiros externos	Implementado Parcialmente	Médio	Formalizar processo de atribuição das funções e responsabilidades de cibersegurança, assim como seu ponto focal
ID.GV-3: Os requisitos legais e regulatórios relativos à segurança cibernética, incluindo obrigações de privacidade e liberdades civis, são compreendidos e gerenciados	Implementado Parcialmente	Médio	Formalizar processo de identificação das bases legais e regulatórias, incluindo as relativas a privacidade de dados pessoais, assim como sua divulgação e conscientização dentro da organização
ID.GV-4: Processos de governança e gerenciamento de riscos abordam riscos de cibersegurança	Implementado Parcialmente	Médio	Formalizar processo de governança e gerenciamento de riscos referentes a cibersegurança, e sua periodicidade de acompanhamento e revisão
ID.RA-1: As vulnerabilidades patrimoniais são identificadas e documentadas	Implementado Parcialmente	Médio	Formalizar processo de identificação das vulnerabilidades organizacionais/operacionais, assim como sua documentação
ID.RA-2: A inteligência de ameaças cibernéticas é recebida a partir de fóruns e fontes de compartilhamento de informações	Executado Ad-Hoc	Alto	Estabelecer processo de comunicação com contatos especializados em segurança da informação, relativo a obtenção de inteligência de ameaças
ID.RA-3: Ameaças, internas e externas, são identificadas e documentadas	Implementado Parcialmente	Alto	Formalizar processo de identificação de ameaças internas e externas, assim como sua documentação
ID.RA-4: Potenciais impactos e probabilidades nos negócios são identificados	Implementado Parcialmente	Alto	Formalizar processo de identificação de impactos nos negócios relativos a probabilidade de ameaças explorarem vulnerabilidades, assim como sua documentação
ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos	Implementado Parcialmente	Alto	Formalizar processo de identificação, avaliação e tratamento de riscos, assim como sua documentação
ID.RA-6: As respostas de risco são identificadas e priorizadas	Implementado Parcialmente	Alto	Formalizar processo de resposta a riscos, assim como sua documentação
ID.RM-1: Os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados por partes interessadas organizacionais	Implementado Parcialmente	Alto	Formalizar processo de gestão de riscos com envolvimento de todas as partes interessadas
ID.RM-2: A tolerância ao risco organizacional é determinada e expressa claramente	Executado Ad-Hoc	Alto	Estabelecer o nível de tolerância a riscos organizacionais, assim como sua documentação
ID.RM-3: A determinação da organização sobre tolerância ao risco é informada por seu papel na infraestrutura crítica e na análise de risco específica do setor	Executado Ad-Hoc	Alto	Estabelecer processo de comunicação de riscos organizacionais, assim como seu impacto as infraestruturas críticas. Convém que cada setor tenha sua documentação
ID.SC-1: Os processos de gerenciamento de risco da cadeia de suprimentos cibernéticas são identificados, estabelecidos, avaliados, gerenciados e acordados por partes interessadas organizacionais	Implementado Parcialmente	Alto	Formalizar processo de gestão de riscos vinculados a prestadores de serviços, assim como a formalização dos Acordos de Nível de Serviços e seu gerenciamento
ID.SC-2: Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados por meio de um processo de avaliação de risco da cadeia de suprimentos cibernéticos	Executado Ad-Hoc	Alto	Estabelecer processo de gestão de riscos relativo ao fornecimento de sistemas Informatizados por parceiros
ID.SC-3: Contratos com fornecedores e parceiros terceirizados são usados para implementar medidas adequadas projetadas para atender aos objetivos do programa de cibersegurança de uma organização e do Plano de Gerenciamento de Riscos da Cadeia de Suprimentos Cibernéticos.	Implementado Parcialmente	Alto	Formalizar processo de adequação em relação as medidas de gestão de riscos de fornecedores alinhadas ao processo interno de gestão de riscos da organização
ID.SC-4: Fornecedores e parceiros terceirizados são avaliados rotineiramente usando auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais.	Executado Ad-Hoc	Alto	Estabelecer processo de auditoria aos prestadores de serviços, assim como sua periodicidade
ID.SC-5: O planejamento e os testes de resposta e recuperação são realizados com fornecedores e provedores terceirizados	Executado Ad-Hoc	Alto	Estabelecer processo de continuidade operacional relativo aos fornecedores

PR.AC-1: Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	Implementado Parcialmente	Médio	Formalizar processo de gerenciamento de credenciais em relação ao uso de dispositivos, acessos de usuários e execução de processos
PR.AC-2: O acesso físico aos ativos é gerenciado e protegido	Implementado Parcialmente	Alto	Formalização de processo de acesso físico a ativos da organização
PR.AC-3: O acesso remoto é gerenciado	Implementado Parcialmente	Alto	Formalização de processo de acesso remoto a ativos da organização
PR.AC-4: São gerenciadas permissões de acesso e autorizações, incorporando os princípios de menor privilégio e separação de deveres	Implementado Parcialmente	Médio	Formalização de processo de aplicabilidade "Need To Know", e segregação de funções em relação as permissões de acesso.
PR.AC-5: A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	Implementado Parcialmente	Médio	Formalização de processo de integridade de redes, assim como sua documentação técnica
PR.AC-6: Identidades são provadas e vinculadas a credenciais e afirmadas nas interações	Implementado Parcialmente	Médio	Formalização de processo de validação de autenticidade de acesso e vinculação a suas credenciais de acesso
PR.AC-7: Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifatorial) proporcional ao risco da transação (por exemplo, riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais)	Implementado Parcialmente	Médio	Formalização de processo de autenticação de acesso aos ativos, assim como documentação técnica do método utilizado
PR.AT-1: Todos os usuários são informados e treinados	Implementado Parcialmente	Alto	Formalizar processo de treinamento de cibersegurança de colaboradores
PR.AT-2: Usuários privilegiados entendem suas funções e responsabilidades	Implementado Parcialmente	Alto	Formalizar processo de atribuição de responsabilidade a usuários privilegiados, assim como seu monitoramento
PR.AT-3: Partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) entendem seus papéis e responsabilidades	Implementado Parcialmente	Alto	Formalizar processo de atribuição de papeis e responsabilidade a fornecedores.
PR.AT-4: Executivos seniores entendem seus papéis e responsabilidades	Implementado Parcialmente	Alto	Formalizar processo de atribuição de papeis e responsabilidade aos executivos seniores (COMEX)
PR.AT-5: Pessoal físico e de cibersegurança entende seus papéis e responsabilidades	Implementado Parcialmente	Alto	Formalizar processo de atribuição de papeis e responsabilidade aos colaboradores tanto que usam como os que não usam recursos computacionais
PR.DS-1: Dados em repouso são protegidos	Implementado Parcialmente	Médio	Formalizar processo de manutenção de segurança de dados em repouso
PR.DS-2: Dados em trânsito são protegidos	Implementado Parcialmente	Médio	Formalizar processo de manutenção de segurança de dados em trânsito
PR.DS-3: Os ativos são formalmente gerenciados durante a remoção, transferências e disposição	Implementado Parcialmente	Médio	Formalizar processo de gerenciamento de ativos referente a transferência física dos mesmos
PR.DS-4: Capacidade adequada para garantir que a disponibilidade seja mantida	Implementado Parcialmente	Médio	Formalizar processo de gerenciamento de capacidade, tecnologias que suportam disponibilidade, assim como sua documentação técnica
PR.DS-5: Proteções contra vazamentos de dados são implementadas	Implementado Parcialmente	Médio	Formalizar processo de "Data Loss Prevention", assim como as tecnologias de proteção e sua documentação técnica
PR.DS-6: Mecanismos de verificação de integridade são usados para verificar software, firmware e integridade das informações	Implementado Parcialmente	Alto	Formalizar processo de verificação de integridade dos ativos de informação, assim como sua periodicidade.
PR.DS-7: Os ambientes de desenvolvimento e teste são separados do ambiente de produção	Executado Ad-Hoc	Baixo	Estabelecer processo de segmentação de servidores
PR.DS-8: Mecanismos de verificação de integridade são usados para verificar a integridade do hardware	Totalmente Implementado	Baixo	Documentar o processo
PR.IP-1: Uma configuração de linha de base de tecnologia da informação/sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	Executado Ad-Hoc	Médio	Estabelecer "baseline" de tecnologia implementada, relativo a definição do mínimo necessário a ser mantido em cibersegurança

PR.IP-2: Um ciclo de vida de desenvolvimento de sistema para gerenciar sistemas é implementado	Executado Ad-Hoc	Alto	Estabelecer processo de esteira de desenvolvimento seguro de software
PR.IP-3: Os processos de controle de alteração de configuração estão em vigor	Implementado Parcialmente	Alto	Formalizar processo de gerenciamento de configuração dos ativos de informação
PR.IP-4: Backups de informações são realizados, mantidos e testados	Implementado Parcialmente	Crítico	Formalizar processo de backup, assim como seus testes e armazenamento
PR.IP-5: Políticas e regulamentos sobre o ambiente operacional físico para ativos organizacionais são cumpridos	Implementado Parcialmente	Alto	Formalizar processo de verificação do cumprimento das normas e políticas internas
PR.IP-6: Dados são destruídos de acordo com a política	Executado Ad-Hoc	Crítico	Estabelecer processo de descarte seguro das informações decorrentes da finalização do seu ciclo de vida
PR.IP-7: Os processos de proteção são melhorados	Implementado Parcialmente	Alto	Estabelecer processo de análise crítica e melhoria contínua dos processos de cibersegurança
PR.IP-8: A eficácia das tecnologias de proteção é compartilhada	Implementado Parcialmente	Médio	Formalizar processo de compartilhamento de conhecimento referente ao uso das tecnologias de cibersegurança
PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e gerenciados	Executado Ad-Hoc	Crítico	Estabelecer formalmente Planos de Resposta a Incidentes e Planos de Recuperação de Desastres
PR.IP-10: Planos de resposta e recuperação são testados	Executado Ad-Hoc	Crítico	Estabelecer periodicamente testes dos Planos de Resposta a Incidentes e Planos de Recuperação de Desastres
PR.IP-11: A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desprovisionamento, triagem de pessoal)	Implementado Parcialmente	Alto	Formalizar processo, junto a área de recursos humanos de seleção de perfis, baseados também em controles de segurança da informação
PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	Executado Ad-Hoc	Alto	Estabelecer plano de gerenciamento de vulnerabilidades, assim como sua implementação e respectiva política.
PR.MA-1: Manutenção e reparação de ativos organizacionais são realizadas e registradas, com ferramentas aprovadas e controladas	Implementado Parcialmente	Alto	Formalizar processo de manutenção dos ativos de informação, segundo políticas internas estabelecidas
PR.MA-2: A manutenção remota dos ativos organizacionais é aprovada, registrada e realizada de forma a impedir o acesso não autorizado	Implementado Parcialmente	Alto	Formalizar processo de manutenção dos ativos de informação, de maneira remota, quando aplicável, segundo políticas internas estabelecidas
PR.PT-1: Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política.	Não Implementado	Crítico	Desenhar e Estabelecer processo de auditoria formal dentro da organização, assim como sua documentação e registros. Estabelecer periodicidade para execução
PR.PT-2: A mídia removível é protegida e seu uso restrito de acordo com a política	Implementado Parcialmente	Alto	Formalizar processo de uso de mídia removível
PR.PT-3: O princípio da menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais.	Executado Ad-Hoc	Alto	Estabelecer processo de "Need-To-Know" ao gerenciamento de configuração de sistemas
PR.PT-4: Redes de comunicação e controle são protegidas	Implementado Parcialmente	Alto	Formalizar processo de gerenciamento de redes de comunicação de forma segura
PR.PT-5: Mecanismos (por exemplo, failsafe, balanceamento de carga, hot swap) são implementados para alcançar requisitos de resiliência em situações normais e adversas	Implementado Parcialmente	Alto	Formalizar processo e documentar tecnologia utilizada para efeito de redundância e manutenção da disponibilidade dos ativos de informação
DE.AE-1: Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	Implementado Parcialmente	Alto	Formalizar processo de identificação de baseline relativos aso dados e fluxos de redes permitidos por categoria de usuário e sistemas
DE.AE-2: Eventos detectados são analisados para entender alvos e métodos de ataque	Implementado Parcialmente	Alto	Formalizar processo de detecção, análise e categorização de eventos em ambiente cibernético
DE.AE-3: Os dados do evento são coletados e correlacionados a partir de múltiplas fontes e sensores	Implementado Parcialmente	Médio	Formalizar processo de elaboração de base de conhecimento de detecção, análise e categorização de eventos em ambiente cibernético
DE.AE-4: Impacto dos eventos é determinado	Implementado Parcialmente	Alto	Formalizar processo de identificação e análise dos impactos referente a eventos em ambiente cibernético

DE.AE-5: Limiares de alerta de incidentes são estabelecidos	Implementado Parcialmente	Alto	Formalizar processo de identificação de categorização de um evento quando este deve ser interpretado como incidente
DE.CM-1: A rede é monitorada para detectar potenciais eventos de cibersegurança	Implementado Parcialmente	Crítico	Formalizar processo de identificação de eventos de cibersegurança em redes de comunicação, assim como as tecnologias empregadas
DE.CM-2: O ambiente físico é monitorado para detectar potenciais eventos de cibersegurança	Implementado Parcialmente	Alto	Formalizar processo de identificação de eventos de cibersegurança em ambientes físicos, assim como as tecnologias empregadas
DE.CM-3: A atividade do pessoal é monitorada para detectar possíveis eventos de cibersegurança	Implementado Parcialmente	Alto	Formalizar processo de identificação de eventos de cibersegurança no decorrer das atividades do pessoal, assim como as tecnologias empregadas
DE.CM-4: Código malicioso é detectado	Implementado Parcialmente	Crítico	Formalizar processo de identificação de códigos maliciosos, assim como as tecnologias empregadas
DE.CM-5: Código móvel não autorizado é detectado	Implementado Parcialmente	Crítico	Formalizar processo de identificação de código móvel não autorizado, assim como as tecnologias empregadas
DE.CM-6: A atividade do provedor de serviços externos é monitorada para detectar possíveis eventos de cibersegurança	Implementado Parcialmente	Alto	Formalizar processo de identificação de eventos de cibersegurança junto a provedores de serviços
DE.CM-7: O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	Implementado Parcialmente	Alto	Formalizar processo de monitoramento de pessoal, conexões, dispostos e software, relativo a uso de recursos não autorizados
DE.CM-8: Exames de vulnerabilidade são realizados	Implementado Parcialmente	Alto	Formalizar processo de gerenciamento de vulnerabilizas, assim como as tecnologias empregadas
DE.DP-1: Funções e responsabilidades para detecção são bem definidas para garantir a prestação de contas	Implementado Parcialmente	Alto	Formalizar processo de identificação de funções e responsabilidade no que refere a prestação de contas e responsabilizações
DE.DP-2: As atividades de detecção cumprem todos os requisitos aplicáveis	Totalmente Implementado	Alto	Formalizar processo de detecção de eventos relativo a itens mandatórios por normas ou regulações. O uso de Playbooks evidencia a existência de processos de detecção e tratamento
DE.DP-3: Os processos de detecção são testados	Executado Ad-Hoc	Alto	Estabelecer processo de testes periódicos de detecção de eventos relativo a itens mandatórios por normas ou regulações
DE.DP-4: Informações de detecção de eventos são comunicadas	Parcialmente Implementado	Alto	Formalizar processo de comunicação de detecção de eventos relativo a itens mandatórios por normas ou regulações
DE.DP-5: Os processos de detecção são continuamente melhorados	Parcialmente Implementado	Médio	Formalizar processo de melhoria contínua de detecção de eventos relativo a itens mandatórios por normas ou regulações
RS.RP-1: Plano de resposta é executado durante ou após um incidente	Executado Ad-Hoc	Crítico	Estabelecer plano de resposta a incidente que contemple ações reativas e corretivas
RS.CO-1: O pessoal conhece seus papéis e ordem de operações quando uma resposta é necessária	Executado Ad-Hoc	Alto	Estabelecer processo de validação de responsabilidades referente a resposta a incidentes
RS.CO-2: Os incidentes são relatados consistentes com critérios estabelecidos	Executado Ad-Hoc	Alto	Estabelecer processo de relato e comunicação referente a resposta a incidentes
RS.CO-3: As informações são compartilhadas consistentes com planos de resposta	Executado Ad-Hoc	Médio	Estabelecer validação do relato e comunicação referente a resposta a incidentes
RS.CO-4: Coordenação com stakeholders ocorre consistente com planos de resposta	Executado Ad-Hoc	Alto	Estabelecer processo validação junto as partes interessadas sobre relato e comunicação referente a resposta a incidentes
RS.CO-5: O compartilhamento voluntário de informações ocorre com as partes interessadas externas para obter uma consciência situacional de segurança cibernética mais ampla	Não Implementado	Alto	Desenhar e estabelecer processo de comunicação junto a contatos especiais externos para contemplar uma visão mais ampla da segurança cibernética em outros cenários
RS.AN-1: Notificações de sistemas de detecção são investigadas	Totalmente Implementado	Alto	Formalizar processo de melhoria contínua do processo estabelecido e documentado.
RS.AN-2: O impacto do incidente é entendido	Totalmente Implementado	Alto	Formalizar processo de melhoria contínua do processo estabelecido e documentado.
RS.AN-3: Perícia é realizada	Totalmente Implementado	Médio	Formalizar processo de melhoria contínua do processo estabelecido e documentado.

RS.AN-4: Incidentes são categorizados consistentes com planos de resposta	Totalmente Implementado	Alto	Formalizar processo de melhoria contínua do processo estabelecido e documentado.
RS.AN-5: São estabelecidos processos para receber, analisar e responder às vulnerabilidades divulgadas à organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança)	Totalmente Implementado	Alto	Formalizar processo de melhoria contínua do processo estabelecido e documentado.
RS.MI-1: Incidentes estão contidos	Implementado Parcialmente	Alto	Formalizar processo de contenção de incidentes cibernéticos, assim como as tecnologias empregadas
RS.MI-2: Incidentes são mitigados	Implementado Parcialmente	Crítico	Formalizar processo de mitigação de incidentes cibernéticos, assim como as tecnologias empregadas
RS.MI-3: Vulnerabilidades recém-identificadas são atenuadas ou documentadas como riscos aceitos	Implementado Parcialmente	Alto	Formalizar processo de categorização de vulnerabilidades residuais, assim como seu tratamento. A Matriz de Riscos apoia na formalização
RS.IM-1: Planos de resposta incorporam lições aprendidas	Executado Ad-Hoc	Alto	Estabelecer processo de registro de lições aprendidas post mortem (após ocorrência do incidente)
RS.IM-2: As estratégias de resposta são atualizadas	Executado Ad-Hoc	Médio	Estabelecer processo de revisão de estratégias de resposta a incidentes post mortem (após ocorrência do incidente)
RC.RP-1: Plano de recuperação é executado durante ou após um incidente de segurança cibernética	Executado Ad-Hoc	Alto	Estabelecer plano de recuperação pós incidente cibernético
RC.IM-1: Planos de recuperação incorporam lições aprendidas	Executado Ad-Hoc	Médio	Estabelecer atualização dos plano de recuperação com lições aprendidas
RC.IM-2: Estratégias de recuperação são atualizadas	Executado Ad-Hoc	Alto	Estabelecer processo de revisão de estratégias de recuperação
RC.CO-3: As atividades de recuperação são comunicadas a partes interessadas internas e externas, bem como equipes executivas e de gestão	Implementado Parcialmente	Alto	Estabelecer processo de comunicação de recuperação com partes externas a organização, quando aplicável

Fonte: Autor (2022)

Com a documentação inicial formalizada da execução do processo de gestão de riscos cibernéticos, a empresa pode estabelecer ações para tratar os riscos identificados adequando esta ações aos fatores organizacionais como orçamento, recursos humanos e tecnológicos para a execução das atividades necessárias de tratamento dos riscos cibernéticos.

Desta forma a empresa iniciou ações estruturadas para a formalização de processos e adoção de tecnologias aderentes aos riscos cibernéticos, agora mapeados, tendo como base a estrututra do NIST CSF.

6. CONCLUSÃO

Para que os objetivos do processo de gestão de riscos cibernéticos possam ser alcançados, convém que as atividades sejam prioritariamente discutidas e estrategicamente alinhadas com todas as partes interessadas, e assim definidas as estratégias para sua condução e execução, no que diz respeito ao Plano de Metas e Ações, definição de orçamento, apoio em relação a recursos humanos e tecnológicos.

Outros aspectos relevantes a serem considerados que foram orientados a empresa para a correta execução do Plano de Metas e Ações:

- Definir recursos dedicados para gestão e execução dos Plano de Metas e Ações;
- Participação contínua do Corpo Diretivo da empresa (Deliberações);
- Dedicação das áreas de negócio na execução dos Plano, que envolvem participação das respecticas áreas;
- Aprovação do investimento para endereçamento das ações estratégicas, táticas e operacionais da empresa.

Os resultados do Plano de Metas e Ações devem ser monitorados e avaliados para que se valide a sua correta execução dentro de prazos e orçamentos propostos e acordados entre as partes interessadas. Desta forma orientou-se que a empresa deveria manter ações de nível estratégico para que as ações táticas e operacionais oriundas do Plano de Metas e Ações fossem executadas a obter-se a melhorias das atividades de segurnaça cibernética esperadas do Plano.

Como parte do Plano de Metas e Ações proposto, um processo de auditoria interna foi estabelecido e passou a ser executado periodicamente para validar que os processos, políticas internas e requisitos legais, assim que estabelecidos sejam cumpridos.

Orientou-se que seja estabelecido um acompanhamento semestral da execução do Plano Diretor de Segurnaça da Informação, assim que concluído, analisando-se os indicadores e métricas de execução estabelecidos e alinhados entre as partes interessadas da empresa, assim como possível reavaliação de prioridades.

Orientou-se que seja estabelecido um plano orçamentário compatível com as necessidades apontadas e aderentes ao Plano de Metas e Ações, para que se possa melhorar continuamente as bases de segurnaça cibernética já estabelecidas e iniciar implantação daquelas que são executadas, mas ainda não são formalizadas, assim como aquelas que não são executadas e são necessárias de acordo com a avaliação do status de implementação de segurnaça cibernética.

A gestão da capacidade de segurnaça cibernética é responsável por assegurar que a segurança cibernética esteja alinhada a capacidade da Infraestrutura de TI, atendendo as demandas do negócio da organização, permitindo sua expansão de modo arquitetado e aderentes as expectativas estratégicas da organização da empresa.

Desta forma, após as devidas orientações, a empresa foco do estudo deste artigo, pode identificar todas as lacunas de segurança cibernética a serem consideradas, que contribuíram para a violação de dados ocorrida, assim como pode receber direcionamento de ações através de uma Plano de Metas e Ações e assim estabelecer de maneira formal o processo de gerenciamento de riscos cibernéticos, alinhados com os objetivos estratégicos da empresa, tendo como base o NIST CSF.

7. REFERÊNCIAS

ALEXANDER, R. D.; PANGULURI, S. Cybersecurity terminology and frameworks. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level, p. 19-47, 2017. DOI: https://doi.org/10.1007/978-3-319-32824-9_2.

AL-TURKISTANI, H. F.; ALDOBAIAN, S.; LATIF, R. Enterprise architecture frameworks assessment: Capabilities, cyber security and resiliency review. 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA). IEEE, p. 79-84, 2021. DOI: 10.1109/CAIDA51941.2021.9425343.

ATOUM, I.; OTOOM, A.; ALI, A. A holistic cyber security implementation framework. Information Management & Computer Security, v. 22, n. 3, p. 251-264, 2014. DOI: 10.1108/IMCS-02-2013-0014.

BUGHUNT. Quais são os principais desafios da proteção de dados cibernéticos no Brasil?. Disponível em: https://blog.bughunt.com.br/desafios-protecao-de-dados-ciberneticos-no-brasil/. Acessado em: 15/07/2023

DA SILVA, C.; GARCIA, V. Uma Modelagem de Risco Centrada em Comportamentos para o Desenvolvimento Seguro de Serviços no Ecossistema Web. Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. SBC, p. 351-364, 2019. DOI: 10.5753/sbseg.2019.13983.

DE FRANCO R., F.; JINO, M. Arquitetura Conceitual Para Avaliação De Segurança De Sistemas Web. Conferências Ibero-Americanas WWW/Internet e Computação Aplicada. p. 393-397, 2016.

DEDEKE, A. Cybersecurity framework adoption: using capability levels for implementation tiers and profiles. IEEE Security & Privacy, v. 15, n. 5, p. 47-54, 2017. DOI: 10.1109/MSP.2017.3681063.

DIMITROV, V.; KALOYANOVA, K.; PETROV, M. Adapted SANS Cybersecurity Policies for *NIST Cybersecurity Framework*. Proceedings of the Information Systems and Grid Technologies. p.293-301. 2021.

DUTTA, A.; AL-SHAER, E. "What","Where", And "Why" Cybersecurity Controls To Enforce For Optimal Risk Mitigation. 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, p. 160-168, 2019.

GARBA, A. A.; BADE, A. M. An investigation on recent cyber security frameworks as guidelines for organizations adoption. International Journal of Innovative Science and Research Technology, v. 6, n. 2, p. 103-110, 2021.

GIL, A. C. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2019.

KRUMAY, B.; BERNROIDER, E. W. N.; WALSER, R. Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23. Springer International Publishing, p. 369-384, 2018. DOI: 10.1007/978-3-030-03638-6_23.

KUMAR, R. Research methodology: a step-by-step guide for beginners. 5. ed. Thousand Oaks: SAGE, 2019.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1. Gaithersburg, MD, 2018. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 13/09/2022

ROY, P. P. A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA). IEEE, p. 1-3, 2020. DOI: 10.1109/NCETSTEA48365.2020.9119914.

SABILLON, R. *et al.* A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). 2017 International Conference on Information Systems and Computer Science (INCISCOS). IEEE, p. 253-259, 2017. DOI: 10.1109/INCISCOS.2017.20.

VARELA-VACA, Á. J. *et al.* CARMEN: A framework for the verification and diagnosis of the specification of security requirements in cyber-physical systems. Computers in Industry, v. 132, p. 103524, 2021. DOI: 10.1016/j.compind.2021.103524.