ESCOLA SUPERIOR DE GUERRA

NATAN MAIA MORETTE

# FRAMEWORK DE AUTOAVALIAÇÃO PARA MATURIDADE EM DEFESA CONTRA *RANSOMWARE*

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Diego Cardoso Borda Castro

Rio de Janeiro

2024

Documento assinado digitalmente
gov.br
NATAN MAIA MORETTE
Data: 17/01/2025 07:48:03-0300
Verifique em https://validar.iti.gov.br

_____

NATAN MAIA MORETTE

## RESUMO

Os ataques de *ransomware* consolidaram-se como uma das ameaças cibernéticas mais prevalentes e perigosas da última década, apresentando um crescimento exponencial anual. O cenário de ameaças cibernéticas evoluiu significativamente, com os criminosos deixando de focar apenas na interrupção de serviços, como nos ataques de negação de serviço distribuídos (DDoS), que perderam relevância. Atualmente, o objetivo central é o lucro, e, nesse contexto, o *ransomware* destaca-se como a ferramenta ideal devido à sua facilidade de execução e à crescente oferta de serviços criminosos, como o "*Ransomware* como Serviço" (RaaS), que possibilitam a contratação de ataques com simplicidade e rapidez. Diante desse panorama, é essencial identificar as vulnerabilidades nas infraestruturas organizacionais a fim de implementar medidas de proteção mais eficazes. No entanto, o combate ao *ransomware* revela-se complexo, uma vez que envolve múltiplos fatores que podem influenciar a sua ocorrência e propagação. Uma abordagem eficiente e prática para mitigar essa ameaça é a realização de uma autoavaliação abrangente dos diversos aspectos que compõem a defesa contra ataques cibernéticos. Este ensaio tem como objetivo propor a criação de um framework de autoavaliação que auxilie na identificação dos principais vetores de ataque utilizados por *ransomware*, permitindo o fortalecimento das defesas organizacionais e aumentando a resiliência frente a essas ameaças.


**Palavras-chave**: programa de extorsão*; a*rcabouço; autoavaliação.

**ABSTRACT**

*Ransomware attacks have become widely recognized as one of the most prevalent and dangerous cyber threats of the past decade, with exponential growth year after year. The cyber threat landscape has evolved significantly, as criminals have shifted their focus away from service disruption, such as Distributed Denial of Service (DDoS) attacks, which have lost relevance. The primary goal now is profit. In this context, ransomware stands out as the ideal tool due to its ease of execution and the increasing availability of criminal services, such as "Ransomware as a Service" (RaaS), which allow attacks to be initiated with just a few clicks. Given this landscape, it is crucial to identify vulnerabilities within organizational infrastructures in order to implement more effective protection measures. However, combating ransomware is a complex challenge, as it involves a broad range of factors that can influence the occurrence and spread of such attacks. A practical and efficient solution to mitigate this threat is the comprehensive self-assessment of the various aspects that constitute ransomware defense. The aim of this essay is to propose the development of a self-assessment framework that helps identify the main attack vectors utilized by ransomware, thereby enabling organizations to strengthen their defenses and enhance their resilience in the face of this growing threat.*
***Keywords**: ransomware; framework; self-assessment.*

# 1 INTRODUÇÃO

Esta seção tem como objetivo apresentar o contexto, a motivação, a metodologia e os problemas que este estudo pretende abordar, além de detalhar a estrutura do texto.

## 1.1 Motivação e Contexto

Crimes cibernéticos e ataques cibernéticos estão sempre em voga no cenário atual e segundo o relatório *The Global Risks Report 2024 do World Economic Forum* o risco cibernético figura nas primeiras posições de riscos globais até 2034(World Economic Forum, 2024). E se tratando de ataques cibernético nos últimos anos, os ataques de *ransomware* emergiram como uma das maiores ameaças à segurança cibernética global e principalmente a infraestruturas críticas, afetando desde pequenas empresas até grandes corporações e governos. O Brasil figura em diversos relatórios e pesquisas como um dos países que mais são alvos desse tipo de ataque (Associação Brasileira das Empresas de Software, 2023; Trend Micro, 2019). Além disso os custos com esse tipo de ataque têm aumentado cada vez mais e as previsões são que esse tipo de ameaça custará às suas vítimas cerca de US$ 265 bilhões anualmente até 2031, ante US$ 42 bilhões em 2024 e US$ 20 bilhões em 2021 de acordo com a *Cybersecurity* Ventures (Conceal, 2023). Tendo em vista esse cenário é possível entender a gravidade em torno desse tema e a importância dele no cenário cibernético atual.

Os ataques de *Ransomware* se caracterizam principalmente pela capacidade de bloquear o acesso a sistemas e dados cruciais, seguido de uma exigência de pagamento de resgate para restaurar o acesso. Em muitos casos, os dados permanecem comprometidos, mesmo após o pagamento, o que evidencia o caráter devastador dessa modalidade criminosa. Dados recentes indicam que a frequência e a sofisticação desses ataques continuam a crescer exponencialmente a cada ano(Crowe, 2024), impulsionadas por uma economia subterrânea robusta, na qual o *ransomware* é oferecido como serviço.

O conceito de "*Ransomware* como Serviço" (*Ransomware as a Service* - RaaS) exemplifica a profissionalização do cibercrime. Nessa prática, organizações criminosas desenvolvem e mantêm ferramentas de *ransomware*, vendendo-as ou alugando-as, além de oferecer suporte técnico e modelos de divisão de lucros entre atacantes e desenvolvedores(Meland; Bayoumy; Sindre, 2020). O RaaS permite que indivíduos com pouco ou nenhum conhecimento técnico lancem ataques cibernéticos complexos,

tornando o *ransomware* acessível a um público mais amplo. Esse modelo de negócios transformou o *ransomware* em uma indústria lucrativa e em constante crescimento, com prejuízos econômicos globais estimados em bilhões de dólares (Beaman *et al.*, 2021).

A popularidade do *ransomware* como método de extorsão está diretamente ligada à sua simplicidade e eficácia. O ataque geralmente começa com a infecção inicial de um sistema, frequentemente por meio de *phishing* ou exploração de vulnerabilidades de software não corrigidas, resultando no bloqueio dos arquivos da vítima por meio de criptografia. Após isso, uma mensagem de resgate é exibida, exigindo pagamento, frequentemente em criptomoedas, para fornecer a chave de descriptografia. Nos últimos anos, muitos grupos de *r*ansomware passaram a adotar a estratégia de "dupla extorsão", ameaçando divulgar informações sensíveis da vítima caso o resgate não seja pago, aumentando ainda mais a pressão para o pagamento (Mesquita; Prado, 2023)

Esse cenário de constante ameaça impõe uma pressão significativa sobre as organizações para aprimorar suas defesas contra *ransomware*. Contudo, identificar e mitigar todas as vulnerabilidades em uma infraestrutura de TI é uma tarefa desafiadora. As ameaças podem surgir de várias frentes, incluindo falhas de segurança em sistemas desatualizados, falta de treinamentos adequados para funcionários ou deficiências nos processos de backup e recuperação. Diante disso, muitas organizações enfrentam dificuldades para avaliar se suas defesas contra *ransomware* são adequadas.

Nesse contexto, a autoavaliação de maturidade em defesa contra *ransomware* emerge como uma ferramenta essencial para aumentar a resiliência das organizações. Um framework de autoavaliação oferece uma abordagem sistemática para identificar vulnerabilidades e pontos fracos nas defesas cibernéticas, ajudando as empresas a compreenderem seu nível de maturidade em relação à prevenção e mitigação de ataques. Além disso, permite que as organizações adaptem suas estratégias de segurança de acordo com as melhores práticas e lacunas identificadas, promovendo uma defesa mais proativa e robusta. Ademais, existe a possibilidade de o framework ser auditado para que haja maior confiança nas capacidades avaliadas.

A autoavaliação também desempenha um papel crítico na conscientização e no desenvolvimento de uma cultura de segurança dentro das empresas. Ao realizar uma análise detalhada de suas capacidades de defesa, as organizações não apenas se tornam mais preparadas para prevenir ataques, mas também adquirem uma visão mais clara sobre como reagir de maneira eficiente em caso de um incidente. Essa capacidade de resposta é vital, especialmente quando se considera que, em muitos casos, as vítimas

de *ransomware* enfrentam uma corrida contra o tempo para restaurar seus sistemas e minimizar os danos.

Portanto, o desenvolvimento de um framework de autoavaliação de maturidade em defesa contra *ransomware* é uma etapa fundamental para que as organizações possam não apenas medir sua preparação, mas também implementar melhorias contínuas. Este ensaio busca apresentar uma estrutura prática e eficaz para essa autoavaliação, abordando os principais vetores de ataque e destacando as melhores práticas que podem ser adotadas para mitigar os riscos de forma eficaz. Ao fazer isso, esperamos contribuir para a construção de defesas mais fortes e resilientes contra uma das mais desafiadoras ameaças cibernéticas da atualidade.

## 1.2 Objetivo

O presente trabalho propõe o desenvolvimento de um framework de autoavaliação de maturidade em defesa contra *ransomware,* com a finalidade de ajudar organizações não apenas medir sua preparação contra certos ataques, mas também implementar melhorias contínuas. Este ensaio busca apresentar uma estrutura prática e eficaz para essa autoavaliação, abordando os principais vetores de ataque e destacando as melhores práticas que podem ser adotadas para mitigar os riscos de forma eficaz. Ao fazer isso, esperamos contribuir para a construção de defesas mais fortes e resilientes contra uma das mais desafiadoras ameaças cibernéticas da atualidade. Este objetivo geral pode ser decomposto em objetivos específicos:

- Apresentar as etapas necessárias para a construção de um *framework* de autoavaliação de maturidade em defesa contra *ransomware;*
- Definir o *framework* proposto;
- Demonstrar a viabilidade do framework proposto por meio de um estudo de caso simplificado com uma empresa que foi anonimizada por questão de privacidade;

## 1.3 Organização do texto

Este ensaio acadêmico é estruturado em quatro partes. Nesta parte, foi detalhado o cenário, juntamente com a motivação e o problema deste estudo.

A segunda seção fornece a base teórica de alguns tópicos que auxiliam na compreensão deste trabalho, destacando alguns tópicos que podem não ser de conhecimento do leitor.

A seção três detalha a proposta deste ensaio, apresentando a definição do framework, os obstáculos encontrados durante a sua elaboração e a primeira versão dele.

A seção quatro traz um debate final sobre o conteúdo abordado neste estudo, suas contribuições, restrições e possíveis futuras pesquisas.

# 2 REFERENCIAL TEÓRICO

*Ransomware* é uma forma de malware que infecta o usuário criptografando dados sem a permissão do usuário. Ele restringe o acesso legítimo aos dados do usuário e impede o acesso aos dados. O efeito irreversível de um ataque de *ransomware* o torna distinto de outros malwares. Uma vez que a criptografia é alcançada, não há outra maneira de descriptografar os arquivos do usuário, exceto usando a chave de descriptografia (Singh *et al.*, 2023) Essa chave que por sua vez é fornecida pelos criminosos mediante a pagamento de um resgate antes da liberação da chave para descriptografia, pagamento esse que não é aconselhado por muitas organizações como o FBI (Federal Bureau of Investigation, 2024), uma vez que o pagamento financia as atividades criminosas dessas organizações além de que não há garantia que os dados realmente serão descriptografados ou retirados de sites de vendas na *dark web*.

Esse tipo de ataque é caracterizado pelo bloqueio total dos dados da vítima, com a exigência de um resgate, geralmente em criptomoedas, para que o acesso seja restabelecido. Além disso, em muitos casos, os criminosos ameaçam expor publicamente as informações coletadas, ampliando a pressão para que o pagamento seja feito.

Antes de chegar ao ponto de criptografar os dados, o atacante precisa primeiro obter acesso ao ambiente da vítima. Esse acesso pode ser conquistado de diversas maneiras, como explorando vulnerabilidades em ativos, ou por meio de ataques de *phishing*, com o objetivo de obter credenciais que permitam a entrada no ambiente. Essa fase inicial é comumente chamada de Vetor Inicial de Ataque (Freed, 2021).

A partir desse momento, a complexidade de se proteger contra esse tipo de ataque aumenta significativamente. Garantir uma defesa eficaz não é uma tarefa simples, pois existem múltiplas formas de comprometimento, o que exige que os times de segurança atuem de maneira abrangente para mitigar todas as possíveis lacunas de segurança.

## 2.1 Ciclo de vida de um incidente de *ransomware*

O ciclo de vida de um incidente de ransomware compreende etapas distintas, que vão desde a infiltração inicial no ambiente até a execução do ataque e a extorsão da vítima. Essas etapas são marcadas por uma série de ações coordenadas pelos criminosos, com o objetivo de comprometer sistemas, exfiltrar dados e maximizar os danos causados. A seguir, detalharemos cada uma dessas fases, destacando as principais estratégias utilizadas pelos atacantes e os impactos para as organizações vítimas.

### 2.1.1 Acesso inicial

O acesso inicial geralmente ocorre por meio de campanhas de e-mails maliciosos, que contêm *backdoors* e são direcionadas a organizações específicas. Tais campanhas utilizam técnicas de engenharia social e exploram falhas humanas para conseguir capturar credenciais para efetuar o primeiro acesso. Porém em alguns casos vulnerabilidades em sistemas expostos à internet podem ser exploradas para conseguir o acesso inicial (Cyber Security & Infrastructure Security Agency,2024).

### 2.1.2 Consolidação e Preparação

Nesta etapa, o atacante busca aprofundar sua presença na rede da vítima, fazendo movimentação lateral e obtendo privilégios elevados. Esse processo possibilita a ampliação de seu controle sobre o ambiente comprometido, facilitando a execução de ações subsequentes. Essa etapa pode demorar semanas ou meses dependendo da complexidade da rede (Cyber Security & Infrastructure Security Agency,2024).

### 2.1.3 Impacto no Alvo

Quando a fase de movimentação lateral é bem-sucedida, o atacante provavelmente terá acesso a dados privados e tentará exfiltrá-los. Além disso, os dados roubados são analisados para determinar o valor do resgate e verificar se a empresa possui seguro cibernético (Center for Internet Security, 2021).

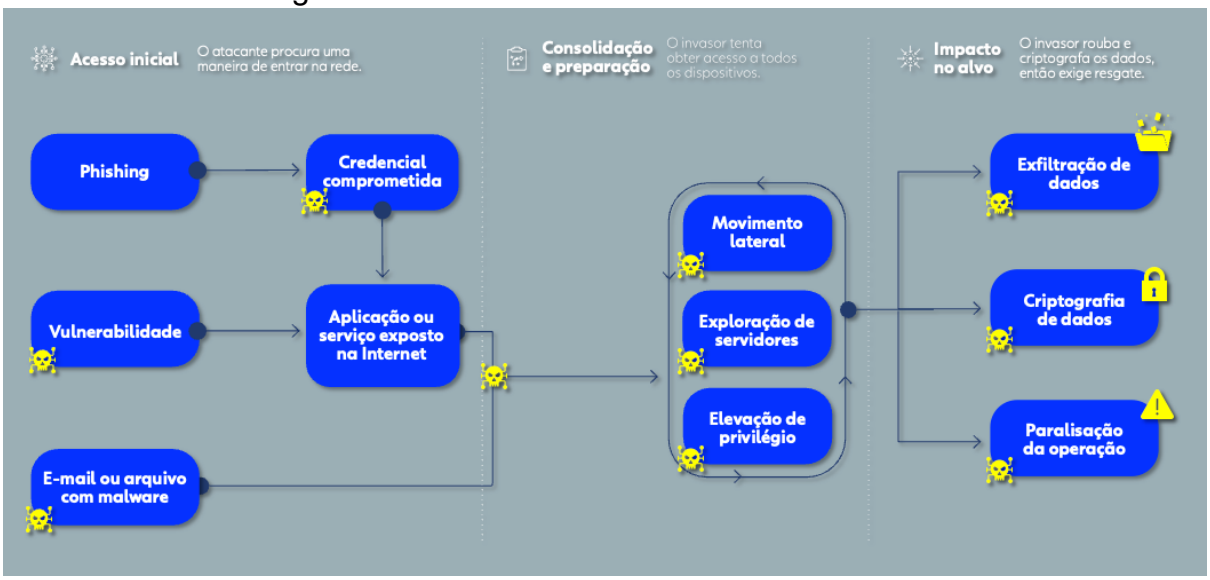
O atacante busca reduzir as chances de a vítima restaurar seus sistemas a partir de backups, interrompendo os processos e sistemas de *backup*, aumentando a dificuldade de recuperação (Kaupe, 2022).

Nessa fase, o atacante implanta o *ransomware*, o que pode causar sérios problemas para a vítima: os arquivos de dados são criptografados e os sistemas de TI tornam-se inutilizáveis, interrompendo as operações (Kosinski, 2024)

Nessa fase, o atacante implanta o *ransomware*, o que pode causar sérios problemas para a vítima: os arquivos de dados são criptografados e os sistemas de TI tornam-se inutilizáveis, interrompendo as operações (Kosinski, data?)

Por fim, o atacante extorque a vítima. Duas formas de extorsão são particularmente prejudiciais: a vítima só recebe a chave de descriptografia após o pagamento do resgate, ou o criminoso ameaça divulgar os dados roubados caso o pagamento não seja realizado.

Figura 1 Ciclo de vida de um Incidente de *Ransomware*



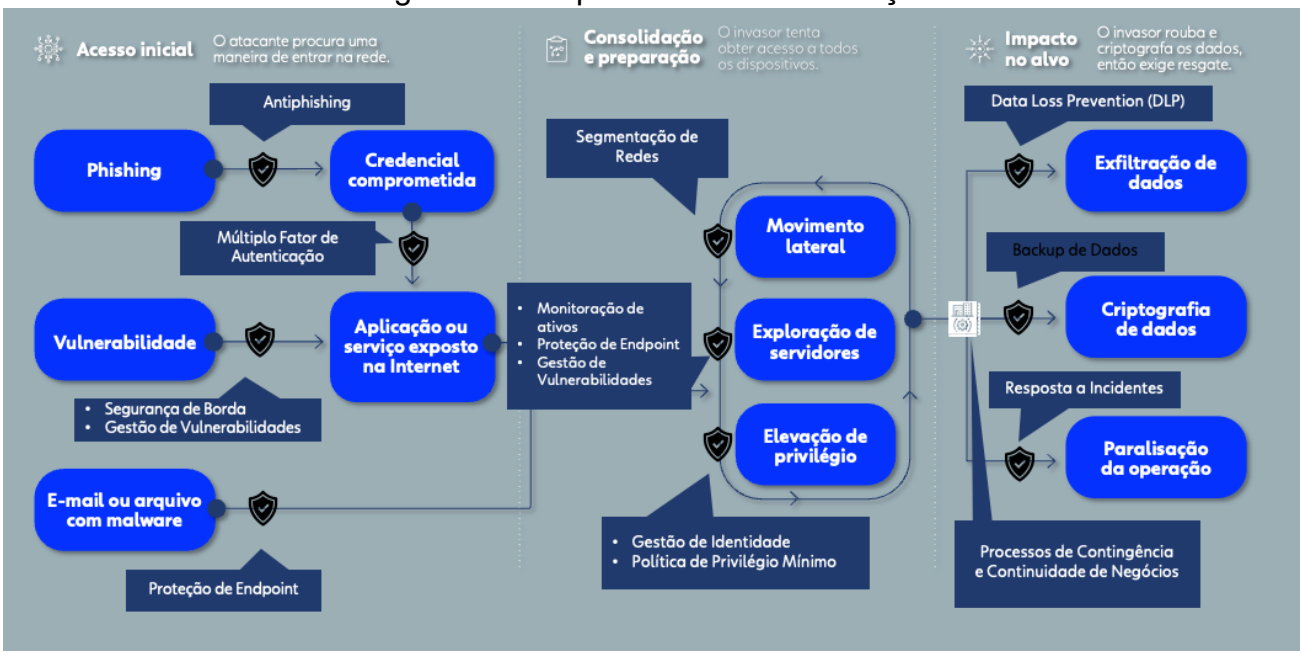

**Fonte:** Cert New Zealand, 2021

## 2.2 Problemas Relativos à Proteção

Devido à complexidade da cadeia de ataques e às múltiplas etapas envolvidas na defesa, é um desafio compreender o nível de proteção contra esse tipo de ataque. Cada etapa demanda soluções de segurança específicas, e por isso é essencial conhecer as vulnerabilidades e os pontos críticos de intervenção. Essa compreensão é fundamental para consolidar uma defesa eficaz contra *ransomware*.

A figura abaixo ilustra as medidas de proteção associadas a cada fase do ataque, destacando algumas das ações necessárias para alcançar uma proteção mais robusta e eficiente contra esse tipo de ameaça.

Figura 2 Boas práticas e recomendações




**Fonte**: Cert Brasil, 2016; Kapoor, *et al,* 2022

# 3 FRAMEWORK PROPOSTO

Um framework é um conjunto de classes que constitui um projeto abstrato para solução de uma família de problemas. Tendo em vista as informações e explicações acerca dos ataques de *ransomware*, o *Framework* de Autoavaliação proposto tem como objetivo ser um guia prático para ser utilizado na autoavaliação de todas as cadeias que estão relacionadas a esse tipo de ataque.

O *Framework* foi dividido em 5 Pilares: Identificar, Proteger, Detectar, Responder e Recuperar. Em cada eixo são descritas atividades que devem ser avaliadas se estão sendo executadas e documentadas para a correta proteção do ambiente. O *Framework* pode ser utilizado em uma corporação inteira para se ter uma visão geral de como está a maturidade de proteção, ou pode ser compartimentalizada em setores diversos como ambientes *Cloud*, *Ompremisses* ou até setores estratégicos dependendo do negócio da empresa como OT, Financeiro, Tecnologia da Informação, Recursos Humanos e entre outros. Compartimentalizando a avaliação será possível verificar a maturidade de forma granular e no fim gerar números para traçar planos de ações e fazer comparativos entre as partes avaliadas.

Outro ponto que precisa ser levado em consideração é que outros frameworks de mercado são complexos e abordam diversos aspectos de Cibersegurança e o aqui temos um Framework focado em ataques *Ransomware*. As atividades do framework estão dispostas com verbos no infinitivo, expressando de forma clara as ações do que precisa ser feito, evitando gerar qualquer tipo de interpretação equivocada em relação a ação a ser executada.

Esse Framework utilizou os seguintes materiais de referência:

- *Tenable White Paper The Ransomware Ecosystem* (Tenable, 2022);
  *National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity* (National Institute of Standards and Technology, 2018);
- *Lifecicle of Ransomware Incident* ( Cert New Zealand, 2021);
- IST *BluePrint For Ransomware Defense* Institute for Security and Technology, 2022);
- NIST *Cybersecurity Framework* (National Institute of Standards and Technology, 2024);
- NIST IR 8374 (Barker *et al.,* 2022);

- MITRE – *Mitigation* (Mitre Att&Ck, 2024);
- CERT.BR – Cartilha *Ransomware* (CERT Brasil, 2016 ).

## 3.1 Identificar

“Identificar” é o primeiro pilar do Framework de Autoavaliação para Maturidade em Defesa contra *Ransomware* e desempenha um papel essencial para garantir uma proteção eficaz. Sem o conhecimento detalhado do ambiente, torna-se inviável estabelecer medidas adequadas de Proteção, Detecção e Recuperação. Assim, esta fase é fundamental para o sucesso dos demais pilares do framework, pois os elementos identificados nessa etapa servem de base para as ações subsequentes.

Para defender uma rede, é indispensável conhecer o que compõe esse ambiente, o que inclui as tecnologias utilizadas e os dados armazenados e/ou transmitidos. No pilar “Identificar” as recomendações que pequenas e são estabelecer e manter inventários de ativos e softwares, de modo a gerenciar eficazmente todos os dispositivos conectados. Além disso, é essencial implementar processos de gerenciamento de dados que descrevam claramente a coleta, uso e armazenamento das informações.

As atividades sob este pilar também abrangem a criação e a manutenção de um inventário de contas, incluindo tanto as contas regulares quanto aquelas com privilégios elevados. A análise do framework (Mitre Att&Ck, 2024),realizada pelo CIS e apresentada no Community Defense Model (CDM) v2.0(Stocchetti, 2021), reforça a importância dessas atividades para a proteção contra incidentes de *ransomware*.

Sem um conhecimento aprofundado dos ativos, softwares e contas da rede empresarial, é difícil responder a incidentes(Neves;Correia, 2016). Dispositivos desconhecidos, por exemplo, podem ser facilmente comprometidos e utilizados por atacantes, o que eleva o risco para a organização. Portanto, compreender o ambiente é essencial para implementar práticas de higiene cibernética e proteger todos os dispositivos de forma eficaz.

A identificação é o primeiro Pilar do framework e possui uma importância fundamental, pois se não conhecemos nosso ambiente não vamos saber o que Proteger, Detectar e Recuperar. Por isso essa etapa é fundamental e os itens que precisam ser verificados serão de extrema importância para os demais pilares do Framework. Em resumo, a Identificação pode ser sintetizada na seguinte premissa: “Conheça seu ambiente”.

Os itens que compõe as atividades desse primeiro pilar são:

- Estabelecer e Manter inventário atualizado de ativos da empresa, identificando os ativos mais críticos da corporação e janelas de manutenção.
- Estabelecer e Manter um Inventário de Software.
- Garantir que somente Software suportados são instalados.
- Estabelecer um Processo de gerenciamento de dados
- Estabelecer e manter um inventário de Contas.

## 3.2 Proteger

O segundo pilar do framework é a “Proteger”, que abrange uma ampla gama de ações e medidas necessárias para resguardar os ativos e dados contra ameaças maliciosas. Após conhecer detalhadamente os componentes de sua rede no pilar anterior, o próximo passo consiste em implementar proteções que atendam à complexidade e capilaridade das redes modernas, que incluem diversos pontos vulneráveis e superfícies de ataque.

“Proteger” é, portanto, o pilar mais extenso, envolvendo diversas práticas e ferramentas essenciais para mitigar riscos e fortalecer a segurança do ambiente. Nesse contexto, é importante considerar todos os pontos críticos da rede para assegurar uma proteção abrangente e eficaz. Cada ação protetiva é fundamental para formar uma camada defensiva robusta contra agentes mal-intencionados que possam comprometer a integridade dos ativos e dos dados.

- Estabelecer e manter um processo de configuração segura;
- Estabelecer e manter um processo de configuração segura para infraestrutura de redes;
- Implementar e configurar um sistema de firewall nos servidores;
- Garantir que não há contas padrão nos sistemas e ativos da empresa;
- Utilizar software para armazenamento e gestão segura de credenciais (ex: contas de serviço);
- Desativar contas não utilizadas;
- Restringir os privilégios administrativos nos servidores;
- Estabelecer um processo de elevação de privilégio (Access Granting Process);
- Estabelecer um processo de revogação de acessos (Access Revoking Process);
- Exigir MFA para aplicações expostas na web;
- Exigir MFA para acesso remoto (Remote Network Access);
- Exigir MFA para acesso administrativo;
- Estabelecer e manter um processo de gestão de vulnerabilidade;
- Estabelecer e manter um processo de remediação;
- Executar o gerenciamento automatizado de patches do sistema operacional;

- Executar o gerenciamento automatizado de patches de aplicativos;
- Estabelecer e manter uma arquitetura de rede segura (segmentação de redes de usuários e servidores por firewalls, microssegmentação de ativos críticos);
- Limitar o tráfego de saída nos firewalls, permitindo apenas portas e serviços necessários, através de gateways e proxies com controle contra ameaças e filtro de conteúdo adequados;
- Garantir que a infraestrutura de rede esteja atualizada;
- Garantir que dispositivos remotos utilizem acessos padronizados e estejam conectados de forma segura à infraestrutura da empresa (VPN para acesso remoto);
- Garantir o uso apenas de navegadores e clientes de e-mail homologados e aprovados;
- Utilizar serviços de Filtro de DNS;
- Implementar e manter um software de anti-*malware* em servidores e estações (principalmente nos ativos mais críticos para a corporação);
- Implementar e manter proteções anti-*malware* no serviço de e-mail (incluindo spam/*phishing*);
- Configurar atualizações automáticas das assinaturas de anti-malware;
- Desabilitar o *autorun* e *autoplay* das mídias removíveis;
- Estabelecer e manter um programa de conscientização;
- Treinar os colaboradores para reconhecer ataques de engenharia social;
- Treinar os colaboradores para reconhecer e reportar incidentes de segurança da informação;

### 3.3 Detectar

O terceiro pilar do framework é “Detectar” que abrangem tanto abordagens preventivas quanto proativas. As equipes devem estar preparadas para identificar sinais de ataque no início da cadeia de eventos ou, caso as medidas de proteção falhem, serem capazes de detectar o ataque após ele ocorrer. Essa capacidade de detecção é essencial para minimizar o tempo de resposta e mitigar possíveis danos. O objetivo é assegurar que, independentemente do ponto em que o ataque seja identificado, as equipes possam responder prontamente para interromper ou reduzir o impacto da ameaça.

- Estabelecer iniciativas de teste de invasão (*PenTest*) em Infraestrutura e no ciclo de vida das aplicações;
- Estabelecer e manter programas de monitoramento de segurança dos ativos/serviços críticos;
- Estabelecer e manter processos de operação de segurança (SOC) 24x7;
- Centralizar e correlacionar alertas de eventos de segurança (SIEM);

### 3.4 Responder

O quarto pilar do framework é “Responder” que abrange ações para lidar com tentativas de ataque ou incidentes que comprometem a integridade do ambiente de uma organização. Embora existam diversas medidas de proteção, é importante reconhecer que, em algumas ocasiões, até as melhores proteções podem não ser suficientes para impedir um adversário determinado, que está disposto a investir tempo e esforço para causar danos a uma empresa (National Institute of Standards and Technology, 2012).

As proteções práticas no pilar “Responder” incluem o relato de incidentes, a definição de contatos essenciais, e o estabelecimento de processos e ferramentas para coleta e armazenamento adequado de logs. A designação de uma pessoa responsável pelo gerenciamento do incidente facilita a coordenação durante a resposta, e essa responsabilidade pode ser compartilhada entre funcionários internos e fornecedores terceirizados.

Outro aspecto vital é a coleta de logs de auditoria antes do incidente, abrangendo logs de sistemas operacionais, aplicações e dispositivos de rede. Durante o incidente, esses logs são fundamentais para a análise e para entender o que ocorreu, possibilitando, assim, aplicar medidas de mitigação para evitar que o ataque se repita. É igualmente importante garantir um armazenamento adequado de logs, já que esses arquivos podem consumir rapidamente o espaço de um sistema e afetar seu desempenho.

Em resumo, o pilar “Responder” assegura que, mesmo diante de uma violação, a empresa tenha os mecanismos e contatos necessários para uma reação coordenada e informada, minimizando os danos e fortalecendo a resiliência contra futuros incidentes.

- Designar uma pessoa para gerenciar o tratamento de incidentes;
- Estabelecer e manter atualizados os canais para reporte de segurança da informação;
- Estabelecer e manter um processo corporativo para reportes de incidentes;
- Estabelecer e manter um processo de gerenciamento de registros (logs) de auditoria;
- Coletar logs de auditoria;
- Garantir um armazenamento adequado para logs de auditoria;

### 3.5 Recuperar

O último pilar do framework é “Recuperar” que é essencial para restaurar dados e sistemas no caso de um ataque bem-sucedido, por mais que todo o framework forneça diversas proteções é sempre importante pensar no pior cenário onde outras salvaguardas falharam e o ataque foi bem sucedido. Uma estratégia crítica para a recuperação eficaz é manter bons backups dos dados essenciais. A adoção de Salvaguardas práticas, como a automação do processo de backup, proteção dos dados e, especialmente, a desconexão regular desses backups da rede, são medidas que garantem a integridade dos dados no caso de um ataque.

Essa última prática é fundamental, pois, mesmo que todas as precauções sejam tomadas para proteger os dados de backup, se eles estiverem diretamente conectados ao sistema ou à rede que foi alvo do ataque, eles também podem ser criptografados. As ações do pilar “Recuperar”, portanto, não é só restaurar a funcionalidade, mas também buscar assegurar que as falhas anteriores não se repitam, reforçando a resiliência contra futuros ataques.

- Estabelecer e manter um processo de recuperação de dados;
- Realizar backups automáticos;
- Proteger os dados de recuperação (principalmente os de ativos críticos);
- Estabelecer e manter uma instância isolada de dados de recuperação;
- Revisar periodicamente os planos de continuidade de negócios da empresa para que estejam preparados para lidar com eventuais impactos causados por ataques hackers em infraestruturas e dados críticos (ex: invasão hacker, infecção e propagação de *ransomware*, etc.);

# 4 CONSIDERAÇÕES FINAIS

A crescente sofisticação dos ataques de *ransomware* exige das organizações uma abordagem cada vez mais robusta e proativa para proteger suas infraestruturas. O framework de autoavaliação proposto neste ensaio surge como uma ferramenta prática e eficiente para auxiliar as organizações a identificarem os pontos frágeis em suas infraestruturas.

Ao longo deste trabalho, foi possível observar como cada pilar do framework: Identificar, Proteger, Detectar, Responder e Recuperar — contribui para uma defesa mais abrangente contra *ransomware*. Esses pilares permitem às organizações não só monitorar e ajustar suas práticas de segurança, mas também fomentar uma cultura de conscientização e resiliência contra ciberataques. O foco na autoavaliação proporciona ainda uma autonomia estratégica, pois facilita a identificação e o enfrentamento das lacunas de segurança, adaptando-se às especificidades de cada organização.

O framework possui dois objetivos principais. O primeiro é auxiliar as equipes técnicas a focarem em lacunas reais de segurança, evitando a perda de tempo com soluções excessivamente complexas e desnecessárias. O segundo objetivo é proporcionar aos gestores uma visão clara dos pontos fracos da empresa em relação a esse tipo de ataque, destacando as áreas que precisam de melhorias para melhorar a maturidade da empresa nesse assunto.

Por fim, o framework apresentado representa um passo importante na direção de defesas mais eficazes e ajustadas às necessidades atuais, em um cenário onde o *ransomware* continua a evoluir. Espera-se que, com a adoção desse modelo, as organizações possam fortalecer suas capacidades de prevenção e resposta, criando ambientes mais seguros e preparados para os desafios de um mundo cada vez mais digital e interconectado.

# REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE. Brasil lidera casos de ransomware nas Américas e é o segundo no ranking mundial. **ABES**, 19 maio 2023. Disponível em: https://abes.com.br/en/brasil-lidera-casos-de-ransomware-nas-americas-e-e-o-segundo-no-ranking-mundial/. Acesso em: 7 out. 2024

BARKER, W.; FISHER, W.; SCARFONE, K.; SOUPPAYA, M. **Ransomware Risk Management**: a cybersecurity framework profile. [*S. l.*]: National Institute of Standards and Technology, 2022. Disponível em: https://csrc.nist.gov/pubs/ir/8374/final. Acesso em: 9 out. 2024.

BEAMAN, C.; BARKWORTH, A.; AKANDE, T. D.; HAKAK, S.; KHAN, M. K. Ransomware: Recent advances, analysis, challenges and future research directions. **Computers & Security**. **Computers & Security**, v. 111, p. 102490, 1 dez. 2021.

CENTER FOR INTERNET SECURITY. **Ransomware:** the data exfiltration and double extortion trends. [*S. l.*]: Center for Internet Security, 2024. Disponível em: https://www.cisecurity.org/blog/ransomware-the-data-exfiltration-and-double-extortion-trends/. Acesso em: 14 out. 2024.

CERT BRASIL. **Você sabe o que é ransomware?** [*S. l.*]: Cert.br, 2024. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 9 out. 2024.

CERT NEW ZEALAND. **Lifecycle of a Ransomware Incident**. [Wellington]: CertNZ, 2021. Disponível em: https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident.pdf. Acesso em: 9 out. 2024.

CONCEAL. **Q2 2023 Who's Who in Ransomware Report**. [*S. l.*]: Conceal, 2023. Disponível em: https://info.conceal.io/hubfs/Website%20Collateral/Reports/Q2%202023%20WHOS%20WHO%20IN%20RANSOMWARE%20REPORT.pdf?_hsenc=p2ANqtz-94qdty9K1gmpyHY5SQ6yg32Q2J5oucWFypR3TjXKaGK9JWY-KppnHwkLv9H2xVJ5aIQR9emdEAAu_m8-BhZFqqCxoVbw&_hsmi=225547762. Acesso em: 7 out. 2024.

CROWE, J. Must-Know Ransomware Statistics, Trends, and Facts. **NinjaOne**, 2024. Disponível em: https://www.ninjaone.com/blog/must-know-ransomware-statistics/. Acesso em: 7 out. 2024.

CYBER SECURITY & INFRASTRUCTURE SECURITY AGENCY. StopRansomware: ransomhub ransomware. **CISA**, 29 Ago. 2024. Disponível em: https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf

FEDERAL BUREAU OF INVESTIGATION. **FBI How Can We Help You - Ransomware**. Washington, DC: FBI, [2021]. Disponível em: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware. Acesso em: 7 out. 2024.

FREED, A. M. What Are the Most Common Attack Vectors for Ransomware? **Cybereason**, [2020?]. Disponível em: https://www.cybereason.com/blog/what-are-the-most-common-attack-vectors-for-ransomware. Acesso em: 14 out. 2024.

INSTITUTE FOR SECURITY AND TECHNOLOGY. **Blueprint for ransomware defense**. [*S. l.*]: IST, 2022. Disponível em: https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf. Acesso em: 9 out. 2024.

KAPOOR, A.; GUPTA, A.; GUPTA, R.; TANWAR, S.; Sharma, G.; Davidson, I. E. Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. **Sustainability**. **Sustainability**, v. 14, n. 1, p. 8, jan. 2022.

KAUPE, J. Backups and Ransomware: theory vs. practice. **ProLion**, Oct. 2022. Disponível em: https://prolion.com/blog/backups-and-ransomware/. Acesso em: 14 out. 2024.

KOSINSKI, M. **O que é ransomware? | IBM**. Disponível em: https://www.ibm.com/br-pt/topics/ransomware. Acesso em: 14 out. 2024.

MELAND, P. H.; BAYOUMY, Y. F. F.; SINDRE, G. The Ransomware-as-a-Service economy within the darknet. **Computers & Security**. **Computers & Security**, v. 92, p. 101762, 1 maio 2020.

MESQUITA, D.; PRADO, F. O ransomware de dupla extorsão no mundo real**. CISO Advisor**. Disponível em: https://www.cisoadvisor.com.br/security-room-posts/o-ransomware-de-dupla-extorsao-no-mundo-real/. Acesso em: 14 out. 2024.

MITRE. Mitigations - Enterprise**. MITRE ATT&CK,** [2024]. Disponível em: https://attack.mitre.org/mitigations/enterprise/. Acesso em: 9 out. 2024.

MITRE ATT&CK. **MITRE ATT&CK Framework**. Disponível em: https://attack.mitre.org/. Acesso em: 9 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Incident Handling Guide (SP 800-61 Rev 2). [*S. l.*: *s. n.*], ago. 2012. Disponível em: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. Acesso em: https://csrc.nist.gov/pubs/sp/800/61/r2/final

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Cybersecurity Framework Profile for Ransomware Risk Management. [*S. l.*: *s. n.*], 26 Feb. 2022. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: https://csrc.nist.gov/pubs/ir/8374/final

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1**. Gaithersburg, MD: NIST, 2018. Disponível em: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Acesso em: 9 out. 2024.

NEVES, P. J. B. das; CORREIA, F. J. R. Resposta a incidentes de segurança da informação: uma abordagem DOTMLPI-I. **Cyberlaw**. **Cyberlaw**, n. 01, jan. 2016.

SINGH, A.; MUSHTAQ, Z.; ABOSAQ, H. A.; MURSAL, S. N. F.; IRFAN, M.; NOWAKOWSKI, G. Enhancing Ransomware Attack Detection Using Transfer Learning and Deep Learning Ensemble Models on Cloud-Encrypted Data. **Electronics**. **Electronics**, v. 12, n. 18, p. 3899, Jan. 2023.

STOCCHETTI, V. **White paper | CIS Community Defense Model 2.0**. Disponível em: https://drive.google.com/file/d/1-dOIvyjzf_WYXzas7CwyUHYshkp6cNiF/view?usp=drive_link. Acesso em: 9 out. 2024.

TENABLE. **A Look Inside the Ransomware Ecosystem**. [*S. l.*]: Tenable, 2022. Disponível em: https://drive.google.com/file/d/1-M1929TkOXSJCdd9tg3WI7Qi_pNBlwas/view?usp=sharing. Acesso em: 9 out. 2024.

TREND MICRO. **Trend Micro alerta: Brasil é o segundo país que mais sofre com ameaças ransomware, atrás apenas dos EUA**. [*S. l.*]: trend Micro, 2019. Disponível em: https://www.trendmicro.com/pt_br/about/newsroom/press-releases/2019/fast-facts-may-2019.html. Acesso em: 7 out. 2024.

WORLD ECONOMIC FORUM. **The Global Risks Report 2024**. [*S. l.*]: WEF, 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 7 out. 2024