JNT FACIT BUSINESS AND TECHNOLOGY JOURNAL
ISSN: 2526-4281 - ANO 2026 - MÊS DE FEVEREIRO
Ed. 71. Vol. 1 - Págs. 385-395
DOI: 10.5281/zenodo.18744107

CAPES

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

QUALIS
A2

ANÁLISE COMPARATIVA DE METODOLOGIAS DE RESPOSTA A INCIDENTES DE SEGURANÇA: UMA REVISÃO DA LITERATURA SOBRE OS FRAMEWORKS NIST, SANS E ISO 27035[1]

COMPARATIVE ANALYSIS OF SECURITY INCIDENT RESPONSE METHODOLOGIES: A LITERATURE REVIEW ON THE NIST, SANS, AND ISO 27035 FRAMEWORKS

Vítor Luís de Jesus dos SANTOS
Faculdade do Leste Mineiro (FACULESTE)
E-mail: vitor.ccb2014@gmail.com
ORCID: http://orcid.org/0009-0006-7528-4775

RESUMO

A presente pesquisa, sob a forma de revisão bibliográfica, realizou uma análise comparativa aprofundada das principais metodologias de resposta a incidentes de segurança cibernética: NIST SP 800-61, SANS Incident Handler's Handbook e ISO/IEC 27035. O objetivo foi identificar e contrastar as abordagens, fases e focos de cada framework. Os resultados demonstraram que, embora todos compartilhem um ciclo de vida similar, o NIST se destaca por sua formalidade e abrangência, o SANS por sua orientação prática e técnica, e a ISO 27035 por sua integração com a governança de segurança da informação. A pesquisa conclui que a escolha da metodologia ideal depende do perfil da organização, e que a combinação dos pontos fortes de cada framework pode resultar em um programa de resposta mais robusto e eficaz.

Palavras-chave: Resposta a incidentes de segurança. Gestão de incidentes. NIST. ISO 27035.

ABSTRACT

This research, in the form of a literature review, conducted an in-depth comparative analysis of the main cybersecurity incident response methodologies: NIST SP 800-61, SANS Incident Handler's Handbook, and ISO/IEC 27035. The objective was to identify and contrast the approaches, phases, and focuses of each framework. The results demonstrated that, although all share a similar lifecycle, NIST stands out for its

[1] COMO CITAR (ABNT): SANTOS, V. L. J. Análise Comparativa de Metodologias de Resposta a Incidentes de Segurança: Uma Revisão da Literatura Sobre os Frameworks Nist, Sans e Iso 27035. **JNT Facit Business and Technology Journal**. Qualis A2. ISSN: 2526-4281, Mês de Fevereiro de 2026 - Ed. 71. VOL. 01. Págs. 385-395 http://revistas.faculdadefacit.edu.br. E-mail: jnt@faculdadefacit.edu.br. Acesso em: ___/___/___.

formality and comprehensiveness, SANS for its practical and technical orientation, and ISO 27035 for its integration with information security governance. The research concludes that the choice of the ideal methodology depends on the organization's profile, and that combining the strengths of each framework can result in a more robust and effective response program.

Keywords: Cybersecurity incident response. Incident management. NIST. ISO 27035.

INTRODUÇÃO

A segurança cibernética tornou-se um dos maiores desafios do século XXI. Com a crescente dependência de sistemas digitais, as organizações enfrentam um cenário de ameaças em constante evolução, onde a complexidade e a frequência dos ataques cibernéticos atingiram níveis sem precedentes. Incidentes de segurança, como *ransomware*, vazamento de dados e interrupções de serviço, não apenas geram prejuízos financeiros significativos, mas também danificam a reputação e a confiança de clientes e parceiros. Em meio a esse ambiente de risco elevado, a capacidade de uma organização de responder de forma rápida, metódica e eficaz a um incidente não é mais uma opção, mas sim um pilar fundamental de sua resiliência e continuidade de negócios.

O desenvolvimento de planos e metodologias de resposta a incidentes (IRP - *Incident Response Plan*) tornou-se uma prática essencial para mitigar os impactos negativos de um evento de segurança. A literatura especializada e as melhores práticas da indústria apontam para a existência de diversos frameworks consolidados que servem como guias para a criação de programas de resposta a incidentes. Dentre os mais renomados, destacam-se o NIST (National Institute of Standards and Technology), o SANS (SysAdmin, Audit, Network and Security) e a ISO/IEC 27035. Embora todos tenham o mesmo objetivo final – guiar a resposta a um incidente – cada um possui uma abordagem, foco e público-alvo distintos.

A presente pesquisa tem como tema a análise comparativa dessas metodologias. Diante do cenário exposto, a pergunta que norteou este estudo foi: Quais são as principais abordagens, etapas, pontos de convergência e divergência entre as metodologias de resposta a incidentes de segurança do NIST, SANS e ISO 27035, e como suas características se aplicam em diferentes contextos organizacionais? A resposta a essa questão é crucial para gestores, analistas de segurança e tomadores de decisão que precisam selecionar ou adaptar um framework que melhor se adeque à realidade de suas respectivas organizações.

O objetivo geral deste trabalho é analisar, comparar e avaliar criticamente os frameworks de resposta a incidentes, identificando suas vantagens, desvantagens e a aplicabilidade de cada um, com base em uma revisão abrangente da literatura disponível. Para alcançar esse objetivo, foram definidos os seguintes objetivos específicos:

1. Descrever detalhadamente as etapas e o fluxo de trabalho dos frameworks NIST, SANS e ISO 27035;
2. Analisar os critérios e as práticas recomendadas por cada metodologia para a gestão de um incidente;
3. Identificar os pontos de sinergia e as principais diferenças entre os frameworks, como a ênfase em processos, tecnologia, governança ou documentação;
4. Sintetizar os resultados da análise para fornecer uma visão clara e consolidada sobre as abordagens mais adequadas para diferentes tipos de organizações.

METODOLOGIA

A pesquisa foi conduzida como uma revisão bibliográfica e exploratória, com o objetivo de compilar, analisar e sintetizar o conhecimento já produzido sobre as metodologias de resposta a incidentes de segurança cibernética. A metodologia de trabalho concentrou-se na coleta sistemática e crítica de informações a partir de fontes primárias e secundárias, garantindo o rigor acadêmico e técnico necessário para uma análise aprofundada.

FASES DA PESQUISA

A pesquisa foi estruturada em três fases principais, detalhadas a seguir:

Fase 1: Coleta e Seleção de Fontes

1.1. Levantamento Bibliográfico Sistemático: Foi realizada uma busca rigorosa e sistemática em bases de dados acadêmicas (IEEE Xplore, ACM Digital Library, Scopus, Google Scholar) e repositórios de segurança cibernética reconhecidos (NIST Publications, SANS Reading Room). Os termos de busca utilizados foram combinados para maximizar a cobertura de materiais relevantes: "NIST SP 800-61", "SANS incident handling", "ISO/IEC 27035", "cyber security incident response", "incident response frameworks comparison" e "gestão de incidentes de

segurança". A busca foi restrita a publicações dos últimos dez anos, a fim de garantir que as informações refletissem as práticas mais atuais.

1.2. Critérios de Inclusão e Exclusão: Foram incluídas na análise publicações que tivessem como foco principal ou secundário a descrição e o funcionamento de pelo menos um dos frameworks NIST, SANS ou ISO 27035, bem como artigos que realizavam a comparação entre eles. Foram excluídas fontes não acadêmicas, como blogs ou fóruns, que não apresentassem o devido rigor técnico e científico. Relatórios de empresas ou materiais de marketing também foram descartados para manter a objetividade do estudo.

Fase 2: Análise e Síntese do Conteúdo

2.1. Análise Crítica dos Materiais: Cada fonte selecionada foi lida e analisada em profundidade. Durante essa fase, as informações pertinentes a cada framework foram extraídas e categorizadas. O foco da análise foi identificar as etapas do ciclo de vida da resposta a incidentes, as ferramentas e tecnologias recomendadas, as funções e responsabilidades das equipes e a ênfase de cada metodologia (seja ela tecnológica, processual, de governança, etc.). A partir dessa leitura, foram criados resumos e anotações para cada documento.

2.2. Consolidação e Sistematização de Dados: As informações extraídas foram organizadas em um modelo analítico que permitiu a comparação direta entre os três frameworks. Foi utilizada uma abordagem descritiva e comparativa para identificar as semelhanças e diferenças em pontos-chave, tais como: (a) número e nome das fases; (b) atividades detalhadas em cada fase; (c) público-alvo (gerencial ou técnico); (d) flexibilidade do framework; e (e) sua relação com outros padrões e normas de segurança.

Fase 3: Elaboração do Artigo

3.1. Estrutura e Redação do Texto: A partir da síntese e organização dos dados, o artigo foi redigido. A estrutura do texto seguiu a norma de trabalhos acadêmicos, com as seções de Introdução, Metodologia, Resultados e Discussões, e Conclusão.

3.2. Tratamento dos Dados: A pesquisa, por ser de natureza qualitativa e bibliográfica, não envolveu tabulação estatística. O tratamento dos dados foi realizado através da análise textual e interpretativa, com as descobertas sendo apresentadas de forma descritiva e comparativa. Todas as afirmações foram devidamente

fundamentadas nas referências consultadas, com a citação e referenciamento de todas as fontes utilizadas ao longo do trabalho.

RESULTADOS E DISCURSÕES

A análise bibliográfica das metodologias de resposta a incidentes de segurança cibernética demonstrou que os frameworks NIST SP 800-61, SANS Incident Handler's Handbook e ISO 27035 representam as abordagens mais influentes na área. Embora todos compartilhem o objetivo de guiar uma resposta eficaz a incidentes, eles diferem significativamente em termos de escopo, público-alvo, nível de detalhe e ênfase. A seguir, detalhamos as características de cada um e, posteriormente, apresentamos uma análise comparativa.

O Framework do NIST (National Institute of Standards and Technology)

O NIST SP 800-61, intitulado "Computer Security Incident Handling Guide", é amplamente reconhecido como um dos guias mais completos e formalizados para a resposta a incidentes. Seu foco é fornecer uma base abrangente para a criação de um programa de resposta a incidentes, abordando tanto aspectos operacionais quanto de gestão. O modelo do NIST divide o processo em quatro fases principais, que se sucedem de forma cíclica e interligada:

1.1. Preparação: Esta fase é considerada a mais crítica, pois é nela que a organização constrói sua capacidade de resposta. Envolve o desenvolvimento de políticas e procedimentos de segurança, a formação de uma equipe de resposta a incidentes (CSIRT), a definição de ferramentas e tecnologias de suporte (como sistemas de detecção de intrusão e plataformas SIEM), o treinamento da equipe e a preparação da infraestrutura tecnológica. A preparação também inclui a criação de um plano de comunicação claro e de uma base de conhecimento para incidentes.

1.2. Detecção e Análise: Esta fase envolve a identificação de um evento de segurança e a determinação se ele constitui um incidente. Atividades cruciais incluem o monitoramento contínuo de logs e tráfego de rede, a análise de alertas de segurança, a triagem de incidentes para priorização e a coleta de dados forenses para entender a natureza, a causa e o escopo do ataque. O objetivo é responder às perguntas básicas: O que aconteceu? Quando? Como? Qual o impacto?

1.3. Contenção, Erradicação e Recuperação: Uma vez que o incidente é confirmado e analisado, a equipe deve tomar medidas para limitar seu dano e restaurar os sistemas ao seu estado normal. A Contenção busca isolar o sistema comprometido para evitar que o incidente se espalhe. A Erradicação foca em eliminar

a causa raiz do problema, como a remoção de *malware* ou o fechamento de uma vulnerabilidade. A Recuperação envolve a restauração dos sistemas a partir de backups confiáveis, a aplicação de patches e a verificação de que o ambiente está seguro antes de retornar à operação normal.

1.4. Atividade Pós-Incidente: Esta fase encerra o ciclo e é essencial para a melhoria contínua. Envolve a documentação completa do incidente, a realização de uma reunião de lições aprendidas para identificar o que funcionou e o que não funcionou, e a implementação de ações corretivas para fortalecer a segurança da organização e prevenir futuros incidentes semelhantes.

O NIST também reconhece que, em situações de crise grave e urgente, pode não haver tempo para seguir o processo formal. Para esses casos, o guia apresenta um roteiro simplificado e direto para guiar profissionais que precisam agir imediatamente.

Apêndice G — Etapas de Gerenciamento de Crise

Esta é uma lista das principais etapas que devem ser executadas quando um profissional técnico acredita que um incidente grave ocorreu e a organização não possui capacidade de resposta a incidentes disponível. Isso serve como uma referência básica sobre o que fazer para alguém que está enfrentando uma crise e não tem tempo para ler este documento inteiro - NIST SP 800-61.

1. **Documente tudo.** Esse esforço inclui todas as ações realizadas, todas as evidências e todas as conversas com usuários, proprietários do sistema e outras pessoas relacionadas ao incidente.
2. **Encontre um colega de trabalho que possa ajudar.** Lidar com o incidente será muito mais fácil se duas ou mais pessoas trabalharem juntas. Por exemplo, uma pessoa pode realizar ações enquanto a outra as documenta.
3. **Analise as evidências para confirmar que ocorreu um incidente.** Realize pesquisas adicionais, conforme necessário (por exemplo, mecanismos de pesquisa na Internet, documentação de software), para entender melhor as evidências. Entre em contato com outros profissionais técnicos da organização para obter ajuda adicional.
4. **Notifique as pessoas apropriadas dentro da organização.** Isso deve incluir o diretor de informação (CIO), o chefe de segurança da informação e o gerente de segurança local. Use discrição ao discutir detalhes de um incidente com outras pessoas; informe apenas as pessoas que precisam saber e use mecanismos de

comunicação que sejam razoavelmente seguros. (Se o invasor comprometeu os serviços de e-mail, não envie e-mails sobre o incidente.)

5. **Notifique o US-CERT** e/ou outras organizações externas para obter ajuda no tratamento do incidente.

6. **Interrompa o incidente se ele ainda estiver em andamento.** A maneira mais comum de fazer isso é desconectar os sistemas afetados da rede. Em alguns casos, pode ser necessário modificar as configurações do firewall e do roteador para interromper o tráfego de rede que faz parte de um incidente, como um ataque de negação de serviço (DoS).

7. **Preserve as evidências do incidente.** Faça backups (de preferência backups de imagem de disco, não backups do sistema de arquivos) dos sistemas afetados. Faça cópias dos arquivos de log que contêm evidências relacionadas ao incidente.

8. **Elimine todos os efeitos do incidente.** Esse esforço inclui infecções por malware, materiais inadequados (por exemplo, software pirata), arquivos de cavalo de Tróia e quaisquer outras alterações feitas nos sistemas por incidentes. Se um sistema tiver sido totalmente comprometido, reconstrua-o do zero ou restaure-o a partir de um backup válido conhecido.

9. **Identifique e mitigue todas as vulnerabilidades que foram exploradas.** O incidente pode ter ocorrido aproveitando-se de vulnerabilidades em sistemas operacionais ou aplicativos. É fundamental identificar essas vulnerabilidades e eliminá-las ou mitigá-las para que o incidente não se repita.

10. **Confirme se as operações foram restauradas ao normal.** Certifique-se de que os dados, aplicativos e outros serviços afetados pelo incidente tenham voltado a operar normalmente.

11. Esse relatório deve detalhar o processo de tratamento do incidente. Ele também deve fornecer um resumo executivo do que aconteceu e como uma capacidade formal de resposta a incidentes teria ajudado a lidar com a situação, mitigar o risco e limitar os danos mais rapidamente.

O Framework do SANS (SysAdmin, Audit, Network and Security)

O SANS Incident Handler's Handbook é um guia prático e operacional, focado em fornecer um roteiro claro e acionável para os profissionais de segurança. Embora sua estrutura seja conceitualmente semelhante à do NIST, o SANS é mais direto e orientado para a execução técnica. O modelo é dividido em seis fases:

2.1. **Preparação**: Similar ao NIST, esta fase enfatiza a necessidade de ter as ferramentas, as pessoas e os processos prontos antes que um incidente ocorra. Inclui a construção da equipe, a definição de políticas e a preparação técnica do ambiente.

2.2. **Identificação:** Esta fase é focada na detecção e confirmação de um incidente. O SANS enfatiza o uso de logs, alertas de segurança e a comunicação interna para identificar atividades suspeitas e determinar o escopo do incidente.

2.3. **Contenção:** O SANS divide a contenção em estágios: contenção de curto prazo (desconexão rápida do sistema) e contenção de longo prazo (análise e reconstrução do sistema em um ambiente de quarentena). O foco é sempre em minimizar o impacto imediato.

2.4. **Erradicação:** Nesta fase, a equipe remove a causa do incidente, seja um código malicioso ou uma vulnerabilidade explorada. O guia SANS oferece dicas práticas sobre como limpar o ambiente e garantir que o invasor não tenha retornado.

2.5. **Recuperação:** A recuperação no modelo SANS visa colocar os sistemas de volta em operação de forma segura. A equipe deve validar a correção dos sistemas, monitorá-los de perto e garantir que o risco de um novo ataque seja minimizado.

2.6. **Lições Aprendidas:** Esta fase é um ponto central no modelo SANS, onde a equipe de resposta se reúne para analisar o incidente, discutir o que poderia ter sido feito melhor e criar um relatório de melhorias para a organização.

O Framework da ISO/IEC 27035

O padrão ISO/IEC 27035 adota uma perspectiva de governança e gestão. Ele não se concentra apenas nas ações técnicas, mas em como o processo de resposta a incidentes se encaixa em um sistema de gestão de segurança da informação (SGSI), como o da ISO 27001. Suas cinco fases são:

3.1. **Planejamento e Preparação:** Esta fase vai além da preparação técnica, enfatizando a necessidade de uma política de gestão de incidentes de segurança da informação (ISIMS) e a definição clara de papéis e responsabilidades em nível estratégico.

3.2. **Detecção e Notificação:** A norma ISO foca na detecção de eventos e na notificação formal a partes interessadas, tanto internas quanto externas. O processo é menos sobre a análise técnica e mais sobre o fluxo de informação e comunicação.

3.3. **Avaliação e Decisão:** Esta é uma fase central e distintiva da ISO 27035. Antes de iniciar a resposta técnica, a equipe deve avaliar o evento para determinar se ele é, de fato, um incidente de segurança e, em caso afirmativo, qual a sua prioridade.

Esta etapa exige uma decisão gerencial, garantindo que os recursos sejam alocados de forma adequada.

3.4. **Resposta:** A resposta é a execução das ações técnicas e gerenciais. A norma ISO não prescreve um conjunto de passos técnicos, mas orienta que a organização deve ter procedimentos para contenção, erradicação e recuperação, delegando as ações específicas à equipe responsável.

3.5. **Lições Aprendidas:** Semelhante aos outros frameworks, a ISO 27035 exige que a organização documente os incidentes e os analise para identificar oportunidades de melhoria em seus controles de segurança e em seu SGSI.

Análise Comparativa e Discussão

A análise aprofundada dos três frameworks revela que eles não são mutuamente exclusivos, mas sim complementares, cada um com uma contribuição única para a gestão de incidentes.

- **Foco e Público-Alvo:** A principal distinção reside no público-alvo e no foco. O NIST é um guia abrangente para gestores e técnicos que desejam construir um programa completo. O SANS é um "manual de campo" para o analista que está na linha de frente, focado em ações práticas. A ISO 27035 é um padrão de gestão para líderes e diretores que precisam integrar a resposta a incidentes com os objetivos estratégicos e de conformidade da organização.
- **Nível de Detalhe:** O NIST é o mais detalhado e prescritivo em termos de estrutura e recomendações de alto nível. O SANS é mais detalhado nas ações técnicas e operacionais. A ISO é mais orientadora e menos técnica, focando no "o que" deve ser feito, e não no "como".
- **Flexibilidade:** O SANS é o mais flexível e adaptável a incidentes de naturezas distintas. O NIST também oferece flexibilidade, mas dentro de uma estrutura mais rígida. A ISO é a menos flexível, pois exige conformidade com um padrão de gestão para ser eficaz.
- **Sinergia e Complementaridade:** A literatura consultada sugere que a combinação dos três frameworks pode criar um programa de resposta a incidentes otimizado. Por exemplo, uma organização pode utilizar a estrutura de governança da ISO 27035 para a definição de políticas e responsabilidades, a abordagem detalhada do NIST para a criação do plano de resposta e os procedimentos táticos do SANS para o treinamento e a execução das ações pela equipe técnica.

CONSIDERAÇÕES

A presente revisão da literatura demonstrou que as metodologias de resposta a incidentes de segurança cibernética, representadas pelos frameworks NIST SP 800-61, SANS Incident Handler's Handbook e ISO/IEC 27035, constituem pilares essenciais para a resiliência de qualquer organização no ambiente digital contemporâneo. A análise comparativa revelou que, apesar de compartilharem um núcleo comum de fases cíclicas e inter-relacionadas, cada framework possui um enfoque distinto, atendendo a diferentes necessidades e níveis de maturidade em segurança.

O modelo do NIST destaca-se por sua formalidade e abrangência, sendo ideal para a criação de programas de resposta robustos e formais. O SANS, por outro lado, oferece um guia prático e operacional, focado nas ações táticas e na capacitação técnica das equipes, tornando-o um recurso valioso para o cotidiano de analistas de segurança. Já o padrão ISO 27035 adota uma perspectiva de governança, integrando a resposta a incidentes a um sistema de gestão de segurança da informação mais amplo e alinhado aos objetivos estratégicos do negócio.

A principal conclusão deste estudo é que não existe uma única metodologia superior para todos os cenários. A escolha e a implementação de um framework de resposta a incidentes devem ser guiadas pelo perfil da organização, seu tamanho, setor de atuação, requisitos regulatórios e maturidade em segurança. Em muitos casos, uma abordagem híbrida, que combine a estrutura e a formalidade do NIST, a praticidade e o foco técnico do SANS e a visão estratégica e de melhoria contínua da ISO, pode oferecer o modelo mais completo e eficaz.

Esta pesquisa reforça a importância da documentação e da análise contínua de frameworks existentes para que as organizações possam adaptar suas estratégias, fortalecendo sua capacidade de resposta e minimizando os impactos de futuros incidentes de segurança. O estudo contribui para a literatura acadêmica ao consolidar as características de cada modelo e fornecer um roteiro para a tomada de decisão em um tema de crescente relevância. Para pesquisas futuras, sugere-se a realização de estudos de caso para avaliar a eficácia de modelos híbridos em contextos organizacionais reais.

REFERÊNCIAS

NIST. **Computer Security Incident Handling Guide**: SP 800-61 Rev. 2.
Gaithersburg: National Institute of Standards and Technology, 2012. Disponível em:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Acesso em: 15 set. 2025.

SANS INSTITUTE. **The Incident Handler's Handbook**. Bethesda: SANS Institute, 2020. Disponível em: https://www.sans.org/white-papers/33901/. Acesso em: 18 set. 2025.

ISO/IEC. **ISO/IEC 27035-1:2023**: Information security, cybersecurity and privacy protection — Information security incident management — Part 1: Principles and process. Geneva: International Organization for Standardization, 2023. Disponível em: https://www.iso.org/standard/79014.html. Acesso em: 22 set. 2025.