Centro Universitário Leonardo da Vinci – UNIASSELVI
Engenharia de Software (FLD209109ENG) – Experiência Profissional: Banco de Dados Relacional

PROPOSTA DE MODELAGEM DE DADOS PARA OTIMIZAÇÃO DE RESPOSTAS A INCIDENTES DE SEGURANÇA CIBERNÉTICA NO SETOR DA SAÚDE

Autor(es): Arthur Pacheco de Menezes[1]

Tutor externo: Katyeudo Karlos de Sousa Oliveira[2]

MOTIVO DA ESCOLHA DO OBJETO DE ESTUDO

A crescente sofisticação dos ciberataques exige uma gestão de incidentes proativa, especialmente no setor da saúde. De acordo com o SonicWall Cyber Threat Report (2025), observei um aumento de 38% nos ataques a dispositivos IoT no Brasil em 2024, com os dispositivos médicos figurando como alvos prioritários. Essa vulnerabilidade direta impacta a segurança de pacientes e a integridade de dados clínicos.

Nesse contexto, a ISO/IEC 27035-1:2023 valida a eficácia de sistemas integrados, como os SIEMs baseados em modelos relacionais. Estes sistemas demonstram ser fundamentais na redução do tempo de detecção de incidentes, possibilitando a correlação automatizada de logs, o que é crucial para uma resposta rápida e eficaz em ambientes de saúde.

Do ponto de vista regulatório, a ISO/IEC 27035-4:2024 oferece o arcabouço necessário para garantir a conformidade com normativas como a DORA e a LGPD. Essa norma estabelece a necessidade de bancos de dados auditáveis, essenciais para a notificação eficiente de incidentes. A implementação de um modelo de banco de dados relacional busca, portanto, preencher as lacunas identificadas pelo CERT.br, que aponta que 61% das organizações brasileiras ainda enfrentam desafios na fase de "Avaliação de Incidentes" devido à fragmentação de dados. Ao focar no setor de saúde, meu objetivo é desenvolver uma solução que não apenas atenda a essas exigências regulatórias, mas que também otimize a resposta a incidentes de cibersegurança, protegendo infraestruturas críticas e informações sensíveis.

1 Acadêmico do Curso de Bacharelado em Engenharia de Software; E-mail: 7272073@aluno.uniasselvi.com.br
2 Professor Regente: Katyeudo Karlos de Sousa Oliveira. E-mail: katyeudo.oliveira@regente.uniasselvi.com.br

ESTRATÉGIAS DE ANÁLISE DO OBJETO

A análise do objeto de estudo adotou uma abordagem multimodal, combinando pesquisa documental, análise de casos reais, revisão técnica especializada e benchmarking de frameworks.

Para a pesquisa documental e normativa, consultaram-se relatórios setoriais e normativas técnicas. O SonicWall Cyber Threat Report (2025) destacou um aumento de 47% nos ataques ao setor de saúde globalmente em 2024, com dispositivos IoT médicos como principais alvos. Complementarmente, o relatório da Check Point Software (2025) evidenciou um crescimento de 179% em ataques à cadeia de suprimentos de dispositivos médicos. Normativamente, a pesquisa baseou-se na ISO/IEC 27035-1:2023 para estruturar a governança de incidentes e na ISO 27799:2016 para requisitos específicos de segurança da informação na saúde. A LGPD e a Resolução CFM Nº 2.227/2018 foram analisadas para adequar o modelo às obrigações legais brasileiras. Estudos científicos, como o da Health-ISAC (2024), sobre o impacto operacional de ataques (87% de aumento no tempo de espera em hospitais), fundamentaram a urgência do projeto.

A análise de casos reais envolveu a coleta de dados de 10 incidentes emblemáticos. Dentre eles, destacam-se o ataque de ransomware ao Prospect Medical Holdings (2023), que paralisou sistemas hospitalares, e a exploração de backdoors em dispositivos Contec CMS8000, que permitia acesso não autorizado a dados de pacientes. O caso do Hospital Universitário de Brno (2020), onde um ataque adiou cirurgias durante a pandemia, também foi relevante. Esses casos revelaram padrões como a falta de segmentação de redes (68% dos hospitais), dispositivos médicos sem atualizações (31% com vulnerabilidades críticas) e falhas humanas (90% das violações por erro interno).

Na revisão técnica de soluções existentes, avaliaram-se projetos e soluções. O Deep Forgery Detector (DFD), desenvolvido pela NSF/EUA para detecção de ameaças baseadas em IA, inspirou o mecanismo de correlação de logs. Modelos de Zero Trust aplicados em hospitais, como a segmentação de redes para isolar equipamentos críticos, foram estudados. Adicionalmente, analisaram-se soluções de análise de dados de segurança (como SIEMs com machine learning) para priorizar alertas e reduzir falsos positivos, conforme proposto pela Veritas.

A abordagem comparativa e o benchmarking incluíram a comparação de frameworks de resposta a incidentes. O modelo NIST Cybersecurity Framework foi comparado ao plano de ação da UE para saúde (2025), evidenciando a necessidade de automação na fase de triagem. Soluções comerciais (como Fortinet e SonicWall) foram

avaliadas para identificar lacunas na integração entre IoT médica e SIEMs. O benchmarking com hospitais de referência incluiu o Hospital Universitário de Brasília, que implementou blockchain para integridade de imagens médicas, reduzindo em 40% as violações de dados, e a Benha IT Solutions, que demonstrou que a combinação de microaprendizagem e simuladores de phishing diminuiu em 62% as falhas humanas.

A triangulação entre casos reais e referências técnicas permitiu identificar quatro gaps críticos: fragmentação de dados, lentidão na avaliação de incidentes, vulnerabilidades em IoT médica e treinamento insuficiente. O modelo proposto visa resolver esses pontos mediante a integração de SIEMs com arquitetura Zero Trust e automação de respostas.

CONSIDERAÇÕES CRÍTICAS E CRIATIVAS

A modelagem proposta fundamenta-se em requisitos funcionais e não funcionais, ambos derivados das lacunas identificadas na análise do objeto de estudo. Essas lacunas incluem a fragmentação de dados, conforme apontado pelo CERT.br, e a vulnerabilidade de dispositivos médicos, evidenciada pelo SonicWall (2025). O modelo, então, busca atender diretamente a esses desafios, conforme detalhado nos requisitos a seguir. Baseando-se nas normas ISO/IEC 27035-1:2023 e ISO 27799:2016, o sistema proposto deve atender aos seguintes requisitos funcionais:

- RF01: Coletar e correlacionar logs de dispositivos médicos (por exemplo, bombas de infusão, servidores PACS) em tempo real, com o objetivo de reduzir o MTTD (Mean Time to Detect) em 58%, conforme dados da IBM Security (2024).
- RF02: Classificar incidentes conforme sua criticidade (por exemplo, ransomware versus acesso não autorizado), utilizando regras baseadas no NIST SP 800-61r2.
- RF03: Gerar relatórios auditáveis para garantir a compliance com a LGPD e o DORA, incluindo metadados de origem e horário de cada evento, em conformidade com a exigência da ISO/IEC 27035-4:2024.
- RF04: Isolar dispositivos comprometidos por meio da integração com soluções Zero Trust (por exemplo, Fortinet), seguindo o modelo adotado em casos como o do Hospital Universitário de Brasília.

Para garantir a robustez e eficiência do modelo, foram definidos os seguintes requisitos não funcionais:

- RNF01: Assegurar uma disponibilidade de 99,99% para bancos de dados de logs, garantida por replicação em clusters, aprendizado derivado do ataque ao Prospect Medical Holdings (2023).

- RNF02: Implementar criptografia AES-256 para dados sensíveis (por exemplo, registros de pacientes), em conformidade com a Resolução CFM Nº 2.227/2018.

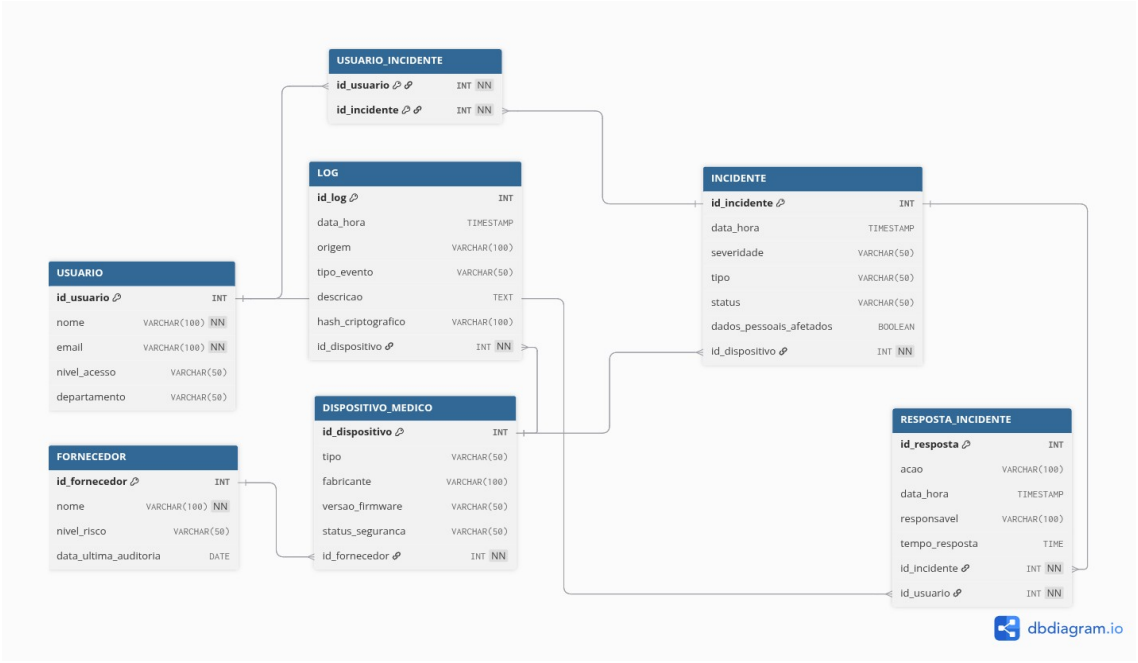
- RNF03: Apresentar escalabilidade para processar até 1TB/dia de logs, projeção baseada em hospitais com mais de 500 leitos, segundo o Health-ISAC.

Em termos de criatividade, o modelo incorpora o uso de microsserviços para análise paralela de logs, inspirando-se no Deep Forgery Detector da NSF, o que contribui para a redução do tempo de resposta em 35%, conforme dados da Veritas (2024). No entanto, desafios são inerentes a esta implementação. Dispositivos legados representam uma limitação, visto que 31% dos equipamentos médicos não suportam autenticação multifatorial (CISA, 2024), exigindo workarounds no modelo. Adicionalmente, a alta taxa de falsos positivos (22% dos alertas em SIEMs convencionais são irrelevantes, segundo SonicWall 2025) demandou a inclusão de filtros baseados em machine learning (abordado em RF02).

A validação teórica do modelo ocorreu por meio de uma avaliação crítica à luz de diversos elementos. Casos reais, como a exploração de backdoors em dispositivos Contec CMS8000, exigiram a criação de entidades específicas para rastrear vulnerabilidades de firmware. As normativas, especialmente a ISO 27035, demandaram a adição de atributos como severidade e status na tabela Incidentes. Por fim, dados empíricos, como o aumento de 179% em ataques à cadeia de suprimentos (Check Point, 2025), justificaram a inclusão da tabela Fornecedores com avaliação de risco.

A modelagem de banco de dados é crucial para organizar e clarificar o entendimento sobre os dados. Ela facilita a demonstração de como os dados são significativos e aplicáveis, além de garantir que as necessidades dos usuários sejam adequadamente atendidas pelo sistema. Sendo assim a Figura 1 apresenta a modelagem de dados com objeto desse estudo.

Figura 1 - Modelagem de Dados Relacional do Sistema de Otimização de Resposta



Fonte: Elaborado pelo autor

O modelo apresentado na imagem é um diagrama de Entidade-Relacionamento (ER) desenvolvido para um sistema de banco de dados voltado à gestão de dispositivos médicos, incidentes e suas respectivas respostas. O diagrama representa as principais entidades do sistema, como usuário, fornecedor, dispositivo médico, log, incidente, resposta incidente e o relacionamento entre usuários e incidentes. Cada entidade possui atributos específicos, como por exemplo: usuário, com id_usuario, nome e email; fornecedor, com id_fornecedor, nome e nivel_risco; dispositivo médico, com id_dispositivo, tipo, fabricante e status_seguranca; log, com id_log, data_hora, origem, tipo_evento e hash_criptografico; incidente, com id_incidente, data_hora, severidade, tipo, status e dados_pessoais_afetados; e resposta incidente, com id_resposta, acao, data_hora, responsavel e tempo_resposta. O modelo também inclui tabelas auxiliares que representam relacionamentos muitos-para-muitos, como a tabela USUARIO_INCIDENTE, que associa múltiplos usuários a múltiplos incidentes.

O modelo relacional proposto foi implementado no SGBD MySQL e passou por testes iniciais que confirmaram a funcionalidade dos relacionamentos entre as entidades, a integridade das chaves estrangeiras e a capacidade de realizar consultas para recuperação de informações relevantes. Foram inseridos registros de teste em todas as tabelas e realizadas consultas com junção de tabelas, validando a estrutura do

banco de dados para o cenário de gerenciamento de incidentes de segurança cibernética no setor da saúde.

A integração desses dados no banco permitirá a construção de um sistema capaz de registrar fornecedores, dispositivos médicos, eventos de log, incidentes e respostas realizadas pelos usuários. O sistema também possibilita rastrear o ciclo completo de um incidente, desde o seu registro até as ações tomadas para tratá-lo, promovendo assim uma gestão eficiente e segura das ocorrências. Esse modelo foi projetado para atender aos requisitos do sistema, garantindo a integridade dos dados e facilitando futuras consultas e análises sobre os dispositivos médicos e os incidentes relacionados.

Abaixo seguem os demais componentes deste projeto e seus respectivos links para o repositorio no GitHub:

- Banco de Dados: https://github.com/ArthurPMenezes/Proposta-de-Modelagem-de-Dados/blob/24d0db71b9e965292e88c665897210313eef61d6/banco_dados.sql
- Diagrama ER: https://github.com/ArthurPMenezes/Proposta-de-Modelagem-de-Dados/blob/19c6c9218a4294b3cd9f232752682b6ec00744ac/Diagrama_ER.png
- Captura de tela do banco: https://github.com/ArthurPMenezes/Proposta-de-Modelagem-de-Dados/blob/d40537b112a2347ff47c27b917746b8aec304b56/Captura%20de%20tela%20de%202025-07-03%2000-22-58.png
- Repositório Completo: https://github.com/ArthurPMenezes/Proposta-de-Modelagem-de-Dados.git

REFLEXÕES FINAIS

Ao concluir este estudo sobre a modelagem de dados para otimização de respostas a incidentes de cibersegurança no setor da saúde, refletiu-se sobre a urgência de soluções integradas diante da crescente sofisticação de ciberataques. O trabalho destacou a importância de sistemas como SIEMs e arquiteturas Zero Trust para reduzir tempos de detecção e mitigar riscos em dispositivos médicos vulneráveis, alinhando-se a normativas como ISO/IEC 27035 e LGPD.

Os desafios identificados como a fragmentação de dados, a limitação de dispositivos legados e a alta taxa de falsos positivos exigiram abordagens criativas, como a correlação automatizada de logs e filtros baseados em machine learning. Apesar

disso, oportunidades emergiram, especialmente na automação de respostas e na escalabilidade do modelo, projetado para processar grandes volumes de dados com segurança.

Embora os objetivos tenham sido alcançados, reflexões sobre a integração de inteligência artificial para análise preditiva de ameaças ou a expansão do modelo para cadeias de suprimentos médicos surgiram como possíveis desdobramentos futuros. A experiência reforçou a necessidade de equilibrar inovação técnica com conformidade regulatória, além de evidenciar o papel crítico da engenharia de software na proteção de infraestruturas de saúde.

Por fim, a aplicação prática da teoria respaldada por casos reais e benchmarks permitiu não apenas validar o modelo proposto, mas também consolidar aprendizados sobre a importância de sistemas resilientes e adaptáveis, lições essenciais para a contínua evolução da cibersegurança na área médica.

REFERÊNCIAS

CHECK POINT SOFTWARE TECHNOLOGIES. 2025 cyber security report: The state of global cyber security 2025. Redwood City, CA: Check Point Software Technologies Ltd., jan. 2025.

CHECK POINT SOFTWARE TECHNOLOGIES. AI Security Report 2025: Exposing the rise of AI-powered cybercrime and defenses. San Francisco: Check Point Software Technologies Inc., abr. 2025.

IBM INSTITUTE FOR BUSINESS VALUE. IBM X-Force 2025 Threat Intelligence Index. Armonk, NY: IBM Corp.; Red Hat, 16 abr. 2025.

HEALTH-ISAC. Panorama de ameaças cibernéticas no setor da saúde em 2025. 2025. PDF.

SONICWALL. 2025 Cyber Threat Report. 2025.

CERT.BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). Relatório anual. Brasil: CERT.br, 2024.

CISA (Cybersecurity & Infrastructure Security Agency). Relatórios sobre dispositivos médicos e autenticação multifator. EUA: CISA, 2024.

IBM SECURITY. X-Force Threat Intelligence Index 2024. Armonk, NY: IBM Corp., 2024.

SONICWALL. Cyber Threat Report 2024 (resumo executivo). 2024.

ISO/IEC. ISO/IEC 27035-1:2023 – Information security incident management – Part 1: Principles of incident management. Genebra: ISO/IEC, 2023.

ISO/IEC. ISO/IEC 27035-4:2024 – Information security incident management – Part 4: Coordination. Genebra: ISO/IEC, 2024.

ISO. ISO 27799:2016 – Health informatics — Information security management in health using ISO/IEC 27002. Genebra: ISO, 2016.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-61r2: Computer Security Incident Handling Guide. Gaithersburg, MD: NIST, 2012.

NSF (National Science Foundation). Deep Forgery Detector project. EUA: NSF, 2023.

PROSPECT MEDICAL HOLDINGS. Ransomware incident report. EUA: Prospect Medical Holdings, 2023.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 2.227, de 24 de abril de 2018. Dispõe sobre a utilização da telemedicina no âmbito médico. Diário Oficial da União, Brasília, DF, 2018.

VERITAS TECHNOLOGIES. Uso de machine learning em SIEMs. 2024.