# Argos - Analisador Forense
# Documento de Visão

## 1. Introdução

O presente documento visa fornecer uma visão geral do projeto que será desenvolvido ao longo da disciplina de Análise e Projeto de Software. Os desenvolvedores são alunos do curso de Ciência da Computação da Universidade Católica de Brasília: Gustavo Horestee Santos Barros, Maria Clara Fernandes Rangel, Matheus Vinycius Vieira Batista, Pedro Henrique Oliveira Marques e Nathalia Gonçalves Silva.

O projeto consiste no desenvolvimento de um software multicliente voltado para auxiliar empresas no monitoramento e controle interativo de logs, permitindo a identificação de eventos suspeitos por meio de regras baseadas em análise heurística além de relatórios de conformidade prontos para auditorias. A iniciativa surge da necessidade de apoiar equipes de SOC (Centro de Operações de Segurança) na realização de análises mais eficazes, rápidas e objetivas, possibilitando uma resposta ágil na prevenção de ataques cibernéticos.

## 2. Contexto de negócio

Devido ao crescente aumento da virtualização de processos em empresas públicas e privadas, houve um aumento expansivo na geração de dados digitais, principalmente em logs de sistemas, arquivos e registros de rede. Esses dados são essenciais para analisar e preservar evidências digitais em investigações de crimes cibernéticos, fraudes internas, vazamento de dados e outros incidentes.

Com base nos estudos feitos pelas organizações IBM, Verizon, Ponemon Institute e Identity Theft Resource Center o número de violações de dados aumentou significantemente em relação a outros anos, no ano de 2022 o número de vazamentos foi de 1,801 para 3,205 em 2023 significado um aumento de 78% conforme demonstrado na figura 1. Cerca de 82% dessas violações ocorrem em armazenamento em Cloud, gerando um prejuízo de US$ 4,75 milhões (IBM, 2023). Esses dados ficam ainda mais preocupantes quando avaliamos que quase metade desses dados(46%) envolvem informações pessoais identificáveis (PII) do cliente, que podem incluir nome completo, endereço, email, hash de senha, número do cartão, etc.

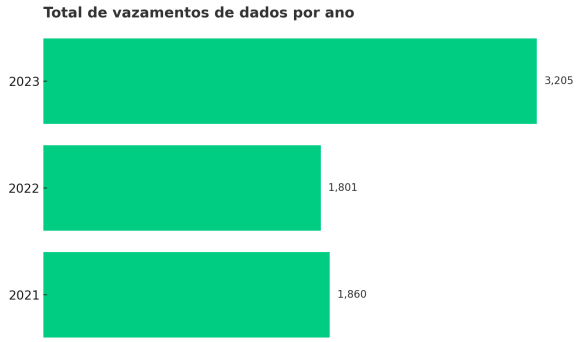


Figura 1 - Theft Resource Center 2023 Data Breach Report

Atualmente o maior vazamento de dados ocorreu na empresa de CAM4, onde por volta de 10 bilhões de registros foram vazados, afetando 106 milhões de usuários, em comunicado oficial a empresa divulgou que o erro ocorreu, pois o banco de dados estava sem senha, sendo possível acessar todos os dados pessoais dos usuários sem nenhuma dificuldade. A segunda maior violação de dados da história até o momento, a do Yahoo, ocorreu em 2013. A empresa relatou inicialmente cerca de um bilhão de registros de dados expostos, mas após uma investigação, atualizou o número, revelando que três bilhões de contas foram afetadas. A Violação Nacional de Dados Públicos foi anunciada em agosto de 2024. O incidente se tornou público quando informações de identificação pessoal de indivíduos foram disponibilizadas para venda na dark web. No total, os profissionais de segurança estimam o vazamento de quase três bilhões de registros pessoais.

Pesquisas feitas pela Clearinghouse demonstram que os setores com maior número de vazamentos de dados são: serviços financeiros, bancários e de seguros; manufatura, tecnologia e comunicações; e saúde e provedores médicos. Esses dados podem ser visualizados na figura 2. Além disso, os principais vetores de ataques cibernéticos em 2023, segundo o Centro de Recursos para Roubo de Identidade, foram: phishing e comprometimento de e-mail corporativo (18,5%); ransomware (10,4%); malware (4,9%); ataques de dia zero (4,6%); preenchimento de credenciais (1,2%); ambientes de nuvem não seguros (0,5%); e outras causas (1,2%). Ressalta-se ainda que 58% dos incidentes reportados não tiveram o vetor de ataque especificado.

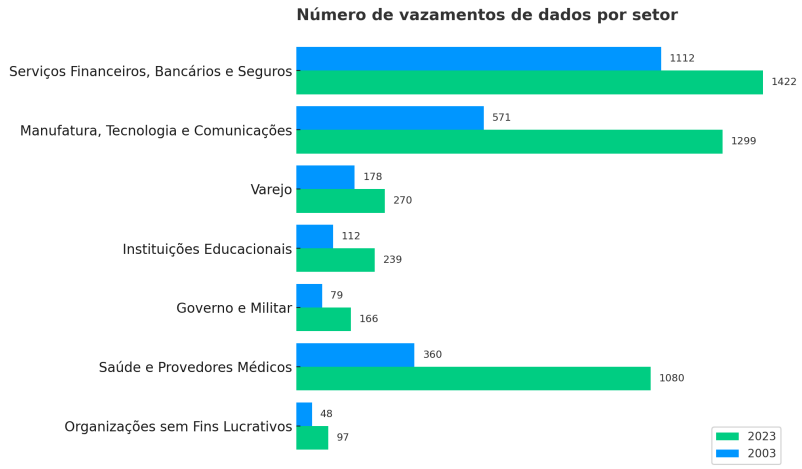


Figura 2 - Clearinghouse, 2023

Atualmente, é possível classificar a análise forense digital em dois grandes grupos: a pericial, voltada para investigações criminais e utilizada por órgãos como a polícia; e a não pericial, aplicada em contextos corporativos ou acadêmicos, sem vínculo direto com processos judiciais. Independente do grupo, eles possuem semelhanças básicas, o processo de análise forense digital pode ser dividido em quatro fases principais: **coleta**, **extração**, **análise** e **apresentação** como demonstrado na figura 3. A fase de **coleta** envolve a obtenção dos logs relevantes, assegurando a integridade das informações e identificando corretamente o host envolvido. Em seguida, na **extração**, os dados são identificados, extraídos, filtrados e documentados de forma sistemática. A fase de **análise** consiste em examinar os logs, correlacionar eventos e também registrar tudo de maneira estruturada. Por fim, na etapa de **apresentação**, é elaborado o relatório final, com identificação dos registros e anexação das evidências pertinentes, garantindo a clareza e a rastreabilidade das informações para possíveis ações legais ou administrativas. Dentre os softwares de florence não perícias existem aqueles que possuem uma quinta fase, **intervenção** onde o próprio serviço executa tarefas a fim de mitigar o problema.

Além das fases da análise forense, diversas ferramentas são utilizadas no processo de investigação. Entre elas, destacam-se o IPED, desenvolvido por peritos brasileiros, que permite recuperar arquivos, detectar palavras-chave, cruzar informações e lidar com grandes volumes de dados. Já o EnCase, usado pelo FBI e Polícia Federal, oferece investigações completas com geração de relatórios e recuperação de arquivos, sendo amplamente reconhecido internacionalmente. O FTK, da AccessData, é conhecido pela facilidade de uso e análise rápida de discos e documentos. Para dispositivos móveis, o UFED Touch, da Cellebrite, extrai dados até mesmo de aparelhos bloqueados ou criptografados. Outras opções incluem o DFF, de código aberto, que preserva evidências em Windows e Linux, e o Xplico, voltado à análise de protocolos de rede como HTTP, TCP e UDP. Essas ferramentas auxiliam peritos e analistas na coleta e interpretação de evidências digitais com eficiência e precisão (IPOG, 2023).

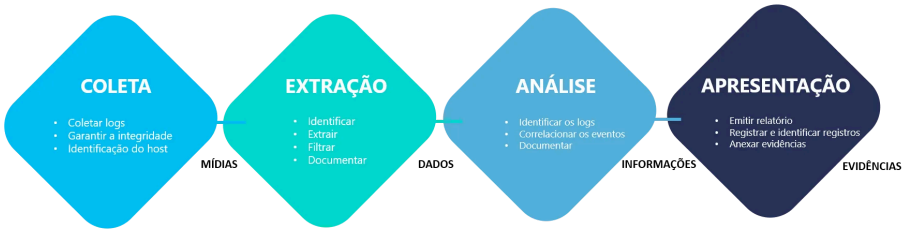

Figura 3 – Ilustração do uso de logs em análise forense (KRYPTUS, 2025).

O ManageEngine e EventLog Analyzer se destaca como uma solução robusta para análise de logs e resposta a incidentes em ambientes corporativos, com foco claro na conformidade, segurança e automação. Ao realizar um benchmarking com softwares não periciais, ou seja, voltados à administração e segurança de TI sem o rigor judicial da perícia forense, percebemos que o EventLog oferece ampla cobertura de funcionalidades, desde a coleta centralizada e normalização de logs, até a resposta automatizada a ameaças e integração com sistemas ITSM. Seus pontos fortes incluem a variedade de formatos suportados, dashboards interativos, inteligência de ameaças integrada e **relatórios de conformidade prontos para auditorias.** No entanto, sua **complexidade** pode ser uma barreira para pequenas empresas ou profissionais com menos experiência técnica, além de exigir infraestrutura para escalar. Há uma oportunidade clara para o desenvolvimento de softwares mais acessíveis, com interfaces simplificadas, foco em casos de uso específicos (como pequenas redes ou dispositivos IoT) e custos reduzidos, mantendo ainda a capacidade de detecção de anomalias e geração de visões de segurança, o que pode democratizar o acesso à análise de logs fora do universo corporativo tradicional.

# 3. Posicionamento

## 3.1 Declaração do problema

| | |
|---|---|
| O problema de | Sobrecarga de dados que resulta em análises manuais lentas e propensas a erros, dificultando a detecção eficaz de ameaças reais, como acessos não autorizados, falhas frequentes de acesso e a presença de malware. A falta de visibilidade, causada pela manutenção de logs descentralizados, impede a correlação de eventos de diferentes fontes e contribui para respostas lentas a incidentes. Além do desafio de manter a conformidade regulatória exigida pelas leis brasileiras (a exemplo da LGPD e do Marco Civil da Internet), além dos custos e da complexidade elevados associados às soluções tradicionais on-premise. |
| Afeta | Devido a complexidade dos problemas, nesse cenário temos uma cadeia de afetados. Dentro de uma empresa que possui soluções digitais de uso interno a equipe técnica de SOC que realiza a gestão de cibersegurança é a principal afetada pois é responsável por manter a segurança de forma eficaz e ágil, assegurando que atividades suspeitas sejam detectadas antes que causem maiores prejuízos. Por conseguinte temos a equipe de compliance que é responsável por manter a conformidade legal, atendendo as exigências jurídicas e garantindo a confiança dos clientes. |
| Seu impacto é | A falha em gerenciar e analisar logs de forma eficaz causa impacto em diferentes setores da empresa, no âmbito operacional temos um aumento significativo no tempo de detecção e resposta a incidentes, dificultando investigações e causando uma ineficiência na operação. Na área financeira e legal temos prejuízos com violação de dados, risco de danos concretos, como fraudes, chantagens e prejuízos reputacionais. |
| Uma solução de sucesso deveria | Com base em análises, uma boa solução deve conter:<br>1. Detecção rápida e inteligente de comportamentos suspeitos, permitindo a entidade contratante responda de forma ágil e eficaz;<br>2. Interface simplificada e acessível para diferentes perfis de usuários, desde analistas de SOC até diretores de compliance;<br>3. Geração de relatórios de conformidade automatizados, que poupam tempo e garantem alinhamento com exigências legais;<br>4. Capacidade de monitoramento em tempo real sem comprometer a infraestrutura da empresa, graças à integração via API; |

| | |
|---|---|
| | 5. Estrutura de visualização hierárquica, que promove controle e governança sobre os dados analisados;<br>6. Histórico e análise comportamental, essenciais para auditorias e estratégias preventivas de segurança; |

## 3.2 Declaração da visão do software

| | |
|---|---|
| Para | Entidades que buscam maior segurança digital e aprimorar suas próprias capacidades, evitando prejuízo, entidades essas que podem ser: universidades, órgãos públicos, serviços financeiros, manufatura, tecnologia e saúde. Com foco principal em pequenos negócios e(ou) profissionais com menos experiência técnica. |
| Que | Há uma necessidade crescente por soluções que transformem grandes volumes de dados técnicos, como logs, em informações acionáveis e compreensíveis, para equipes técnicas (SOC). Empresas enfrentam o desafio de identificar riscos de segurança digital e atender a exigências legais sem sobrecarregar suas equipes. A oportunidade está em oferecer uma ferramenta que automatize a vigilância, gere visões forenses e produza relatórios estratégicos, garantindo agilidade na resposta a incidentes e suporte à conformidade regulatória. |
| O | Argos |
| É um | É um SaaS(Software como serviço) de cibersegurança para análise inteligente de logs. |
| Que | Objetivo principal é uma plataforma que faça uma análise tática e estratégica baseada em dados de logs de acesso. Análise tática é a capacidade de averiguar dados em tempo real, tais como, acesso fora de hora, IP suspeito e acessos constantes. Já análise estratégica, serve para gerar relatórios de conformidade prontos para auditorias. |
| Diferente de | Existem algumas plataformas que oferecem serviços semelhantes ao nosso, algumas delas são: |

| IBM QRadar | CloudFlare | ManageEngine |
|---|---|---|
| Coleta, Agregação e Normalização de Dados de Segurança (Eventos e Fluxos). | Rede de Distribuição de Conteúdo (CDN - Content Delivery Network) | Gerenciamento Unificado de Endpoints e Segurança (UEM) |

| | |
|---|---|
| | <table><tr><td>Detecção de Ameaças em Tempo Real e Análise de Comportamento.</td><td>Proteção contra ataques DDoS (Distributed Denial of Service)</td><td>Gerenciamento de Serviços de TI (ITSM) e Suporte ao Cliente</td></tr><tr><td>Gerenciamento de Ofensas e Suporte à Resposta a Incidentes.</td><td>Firewall de Aplicativos Web (WAF)</td><td>Gerenciamento de Operações de TI (ITOM) e Observabilidade</td></tr></table> Essas empresas oferecem uma gama completa de ferramentas para segurança digital, o que acaba, inevitavelmente, gerando uma complexidade exagerada e expulsiva para pequenos negócios e profissionais com pouca experiência técnica. Outro ponto é que não geram relatórios estratégicos a fim de análises mais detalhadas. |
| Nosso produto | Argos é um analisador de logs que se destaca como um "intérprete inteligente" com foco em observação forense, oferecendo tanto análise tática (SOC) com alerta em tempo real e detecção de padrões incomuns, quanto visão estratégica (Compliance) com relatórios de conformidade e análise de comportamento. Nossos diferenciais incluem a implementação local - garantindo privacidade, UI/UX simplificada e uso de IA para relatórios. |

## 4. Descrição das partes interessadas

| Nome | Descrição | Responsabilidades |
|---|---|---|
| Equipe técnica SOC (Security Operations Center) | Equipe encarregada da segurança operacional dos sistemas de TI da empresa contratante. | ● Monitora os alertas emitidos pelo sistema Argos.<br>● Responde a eventos suspeitos identificados nos logs.<br>● Garante que o sistema esteja alinhado com as necessidades de detecção tática.<br>● Trabalha com rapidez e eficiência diante de incidentes relatados. |

| Nome | Descrição | Responsabilidades |
|---|---|---|
| Clientes (Empresas Contratantes) | | ● Obter uma solução eficaz e acessível (Argos) para aprimorar suas capacidades de monitoramento de segurança, detecção de ameaças e conformidade regulatória.<br>● Reduzir o tempo e o esforço gastos em análises manuais de logs, aumentando a agilidade na resposta a incidentes.<br>● Assegurar que o sistema Argos contribua para a proteção de seus ativos digitais e para a manutenção da confiança de seus próprios clientes.<br>● Fornecer feedback sobre a utilidade e adequação do Argos às suas necessidades operacionais e de negócio. |
| Desenvolvedor Front-end | Responsável por implementar a interface gráfica do sistema Argos. | ● Assegurar que a interface do usuário do Argos seja intuitiva, acessível (conforme requisitos WCAG), performática e atenda eficazmente às necessidades de visualização dos analistas de SOC e diretores.<br>● Garantir a viabilidade técnica da interface proposta e sua correta integração com os serviços de back-end, contribuindo para a satisfação do usuário final.<br>● Interesse em aplicar as melhores práticas de desenvolvimento front-end para criar um produto de alta qualidade e fácil manutenção. |
| Desenvolvedor back-end | Constrói a lógica de negócios e gerência a manipulação de dados. | ● Garantir que a lógica de negócios do Argos para processamento, análise de logs e detecção de ameaças seja robusta, segura, eficiente e escalável.. |

| Nome | Descrição | Responsabilidades |
|---|---|---|
| | | ● Responsável por construir e manter a fundação tecnológica que permite ao Argos entregar análises táticas e estratégicas confiáveis.<br>● Assegurar a integridade e a performance da API que serve de base para as funcionalidades do sistema. |
| Desenvolvedor de banco de dados (DBA) | Responsável pela modelagem e manutenção dos dados. | ● Garantir que a arquitetura de dados do Argos seja eficiente, segura, escalável e otimizada para suportar o armazenamento de grandes volumes de logs e as consultas necessárias para análises em tempo real e geração de relatórios.<br>● Responsável pela integridade, disponibilidade e segurança dos dados armazenados, assegurando que as informações críticas do sistema e dos clientes estejam protegidas e acessíveis conforme necessário.<br>● Zelar pela performance do banco de dados, garantindo que ele não se torne um gargalo para as funcionalidades analíticas e de monitoramento do Argos. |
| Arquiteto de Software | Define a estrutura da aplicação e suas tecnologias. | ● Definir e zelar por uma arquitetura de software para o Argos que seja sustentável, escalável, manutenível e alinhada com os objetivos de longo prazo do produto e as restrições não funcionais.<br>● Garantir que as escolhas tecnológicas e de design promovam a qualidade e a viabilidade do Argos, mitigando riscos técnicos.<br>● Facilitar a integração coesa dos |

| Nome | Descrição | Responsabilidades |
|---|---|---|
| | | diferentes componentes do sistema, assegurando a solidez técnica do produto final. |
| Especialista em Inteligência Artificial | Profissional responsável por projetar, treinar e manter os modelos de IA usados na interpretação dos logs. | ● Garantir que os componentes de Inteligência Artificial do Argos sejam eficazes na detecção de padrões anômalos e comportamentos suspeitos, fornecendo análises contextualizadas, acionáveis e que agreguem valor significativo à capacidade de resposta tática e estratégica dos usuários.<br>● Responsável pela evolução contínua e pela acurácia dos modelos de IA, assegurando que se mantenham relevantes diante de novas ameaças e volumes de dados, sem comprometer o desempenho geral do sistema.<br>● Promover o uso ético e eficaz da IA dentro do Argos, garantindo que suas análises sejam compreensíveis e confiáveis para os usuários finais. |
| Analista de Dados | Responsável por transformar os logs brutos em informações estratégicas e operacionais para os usuários. | ● Garantir a qualidade, integridade, relevância e oportunidade dos dados transformados e apresentados pelo Argos, assegurando que as informações fornecidas sejam estratégicas e operacionais para os usuários.<br>● Responsável por definir e manter os processos de ingestão, tratamento e enriquecimento de dados que sustentam as capacidades analíticas e de IA do Argos, viabilizando insights precisos.<br>● Colaborar ativamente com as equipes de SOC e Compliance para que os dados e relatórios gerados pelo Argos |

| Nome | Descrição | Responsabilidades |
|---|---|---|
| | | atendam efetivamente às suas necessidades de auditoria, conformidade e tomada de decisão. |

## 5. Visão geral do produto

### 5.1 Necessidades e funcionalidades

| Tag | Descrição |
|---|---|
| Alta | Essencial para o sucesso do produto ou solução. |
| Média | Importante, mas não crítica no momento. |
| Baixa | Desejável, mas não impacta diretamente o sucesso imediato do projeto. |

| Necessidade | Funcionalidade | Prioridade | Responsável |
|---|---|---|---|
| A equipe técnica (SOC), precisa garantir que apenas usuários autorizados acessem as informações de análise forense. | F1. Manter cadastro de usuários; | Alta | Nathalia G. Silva |
| | F2. Manter perfil de acessos; | Alta | Nathalia G. Silva |
| | F3. Realizar controle lógico de acesso; | Alta | Matheus Vinycius V. Batista |
| Suporte à equipe técnica (SOC), na detecção de atividades suspeitas. | F4. Monitoramento em tempo real de logs de acesso; | Alta | Nathalia G. Silva |

| | | | |
|---|---|---|---|
| | F5. Emitir alerta para atividades suspeitas, como acesso fora de hora, diversas tentativas de acesso ou IP suspeito; | Alta | Pedro Henrique O. Marques |
| | F6. Gerar relatório diário de atividades suspeitas. | Média | Pedro Henrique O. Marques |
| Suporte a equipe técnica (SOC), equipe DPO e equipe de compliance à condução de investigação de segurança. | F7. Visualizar ameaças por níveis de severidade. | Alta | Maria Clara F. Rangel |
| | F8. Consultar histórico de incidentes; | Média | Maria Clara F. Rangel |
| | F9. Gerar insights de tendências sobre incidentes; | Média | Gustavo Horeste S. Barros |
| Apoio a equipe técnica (SOC), equipe DPO e equipe de compliance na geração de relatórios de conformidade para auditorias. | F10. Gerar relatório de tendências sobre incidentes; | Alta | Matheus Vinycius V. Batista |
| | F11. Gerar relatório sobre incidentes com dados pessoais. | Média | Gustavo Horeste S. Barros |
| | F12. Gerar relatório de Atividade de Login Bem-Sucedido. | Baixa | Maria Clara F. Rangel |

| | | | |
|---|---|---|---|
| | F13. Relatório de Tentativas de Login Falhadas. | Baixa | Gustavo Horeste S. Barros |

## 5.2 Requisitos não funcionais

| ID | Categoria | Requisito não funcional | Prioridade |
|---|---|---|---|
| RNF 001 | Desempenho | *O sistema deve apresentar visualizações de dados na interface com latência inferior a 2 segundos.* | Alta |
| RNF 002 | Desempenho | *O sistema deve processar análises em tempo real com latência inferior a 5 segundos para um volume de dados de até 1 milhão de registros.* | Alta |
| RNF 003 | Segurança | *O sistema deve proteger dados sensíveis, como credenciais de acesso e informações do cliente, contra acesso e modificação não autorizados, através de criptografia e controles de acesso.* | Alta |
| RNF 004 | Segurança | *O sistema deve registrar as principais atividades dos usuários, como logins, acessos a dados sensíveis e alterações de configuração, para criar uma trilha de auditoria que será retida por 1 ano.* | Média |
| RNF 005 | Usabilidade | *O sistema deve permitir que usuários com papéis de 'Analista' ou 'Diretor' personalizem a disposição de widgets e visualizações nos dashboards e salvem estas configurações personalizadas para acesso futuro.* | Baixa |
| RNF 006 | Desempenho | *O tempo de resposta para consultas analíticas complexas (envolvendo agregação de múltiplos dados) utilizadas nos dashboards/relatórios não deve exceder 30 segundos para um volume de dados correspondente aos últimos 30 dias de ingestão.* | Baixa |
| RNF 007 | Usabilidade | *O sistema deve estar em conformidade com WCAG 2.1 Nível AA* | Baixa |

| | | | |
|---|---|---|---|
| RNF 008 | Confiabilidade | *O sistema deve ter uma disponibilidade mínima de 99,5% em ambiente de produção, calculada mensalmente.* | Alta |
| RNF 009 | Confiabilidade | *O sistema deve ser tolerante a falhas em seus componentes críticos e ser capaz de se recuperar de falhas em até 1 hora, com perda máxima de dados de 15 minutos.* | Média |
| RNF 010 | Manutenibilidade | *O tempo médio para identificar e corrigir um defeito crítico deve ser inferior a 5 horas* | Média |
| RNF 011 | Manutenibilidade | *Novas funcionalidades de complexidade média (conforme definido no backlog do projeto) devem ser integráveis com menos de 2 dias de esforço.* | Média |
| RNF 012 | Portabilidade | *O sistema deve ser capaz de ser implantado em diferentes ambientes operacionais, como windows, linux e macOS, sem necessidade de alterações no código fonte principal.* | Média |
| RNF 013 | Usabilidade | *A interface do sistema deve permitir que* analista de segurança *(nível 1, 2 e 3) ou especialista forense ou analista de risco ou DPO, configurem um alerta padrão em no máximo 5 passos.* | Baixa |
| RNF 014 | Segurança | *O sistema deve garantir a integridade dos dados de log e das análises geradas, detectando e alertando sobre quaisquer alterações não autorizadas nos dados armazenados.* | Média |
| RNF 015 | Confiabilidade | *O sistema deve ser capaz de armazenar dados históricos de logs pelo período mínimo de 1 ano, considerando um volume máximo anual de até 10 Terabytes de dados brutos.* | Média |
| RNF 016 | Escalabilidade | *O sistema deve escalar horizontalmente para suportar um aumento de 50% no volume de logs e 40% no número de usuários concorrentes em 7 meses, mantendo os tempos de resposta definidos nos requisitos de desempenho.* | Baixa |
| RNF 017 | Usabilidade | *O sistema deve fornecer uma documentação que explique como implementar o sistema Argos.* | Média |
| RNF 018 | Segurança | *O sistema deve incluir validação rigorosa na entrada de dados para mitigar riscos de ataques comuns, como injeção de código e scripts maliciosos.* | Média |

| | | | |
|---|---|---|---|
| RNF 019 | Manutenibilidade | *O processo de atualização para novas versões do software do sistema deve ser realizado com um tempo de inatividade planejado máximo de 30 minutos.* | Média |
| RNF 020 | Compatibilidade | *A interface web do sistema deve ser totalmente funcional e com layout consistente nos navegadores web mais utilizados (Chrome, Firefox, Edge e safari).* | Média |

## 6. Referências


KRYPTUS. Coleta de Logs de Máquinas Custodiadas para Análise Forense. Disponível em: https://kryptus.com/collector-log-para-analise-forense/. Acesso em: 5 maio 2025.

KRYPTUS. O que é o PCI PIN SECURITY. Disponível em: https://kryptus.com/o-que-e-o-pci-pin-security/?related_post_from=1294. Acesso em: 5 maio 2025.

IPOG. Conheça as principais ferramentas utilizadas na investigação forense computacional. Disponível em: https://blog.ipog.edu.br/tecnologia/principais-ferramentas-utilizadas-na-investigacao-forense-computacional/. Acesso em: 5 maio 2025.

IPOG. O que é: Análise de Logs na Forense Digital. Disponível em: https://forense.io/glossario/o-que-e-analise-de-logs-forense-digital/. Acesso em: 5 maio 2025.

MANAGEENGINE. EventLog Analyzer - SIEM Log management software. Disponível em: https://www.manageengine.com/br/eventlog/. Acesso em: 5 maio 2025.

MANAGEENGINE. Software de Gerenciamento de Serviços e Operações de TI. Disponível em: https://www.manageengine.com/br/?pos=commonpage&loc=MElogo. Acesso em: 5 maio 2025.

SECUREFRAME. 110+ of the Latest Data Breach Statistics [Updated 2025]. Disponível em: https://secureframe.com/blog/data-breach-statistics. Acesso em: 5 maio 2025.