SÃO PAULO TECH SCHOOL

Ciência da Computação

GABRIEL LEAL CEGATTO

GABRIELLY SILVA CAMPOS

ISABELA TEIXEIRA RODRIGUES

LUIZ FELIPE HIPOLITO PARAISO

MATHEUS DE SOUZA RODRIGUES

RICHARD DIEZ ARAÚJO

PROJETO ARGOS

PROJETO DE PESQUISA E INOVAÇÃO

SÃO PAULO

2026

GABRIEL LEAL CEGATTO

GABRIELLY SILVA CAMPOS

ISABELA TEIXEIRA RODRIGUES

LUIZ FELIPE HIPOLITO PARAISO

MATHEUS DE SOUZA RODRIGUES

RICHARD DIEZ ARAÚJO

PROJETO ARGOS

PROJETO DE PESQUISA E INOVAÇÃO

Trabalho apresentado à disciplina de Pesquisa e Inovação, sob orientação do professor Fernando Brandão e da monitora Júlia Araripe Lopes, como parte dos requisitos para a aprovação do segundo semestre do curso de Ciência da Computação da instituição São Paulo Tech School.

SÃO PAULO

SUMÁRIO

Sumário

1 CONTEXTO

Quando falamos sobre ligações de emergência, como o número 190 da Polícia Militar, não podemos aceitar nenhum tipo de queda ou falha nos sistemas responsáveis pelo atendimento, pois qualquer interrupção pode custar não apenas a imagem da corporação, mas também vidas humanas.

Os atendimentos de emergência dependem de servidores que recebem as ligações, processam os dados, registram ocorrências em sistemas internos, relacionam informações com GPS, rádio e mapas, despacham viaturas e armazenam dados em bancos de dados críticos. Todo esse processo ocorre em tempo real e exige alta disponibilidade e estabilidade dos sistemas.

Entretanto, apesar da importância desses servidores, não há um acompanhamento contínuo e automatizado das condições físicas do ambiente onde os equipamentos estão instalados. Isso pode resultar em falhas inesperadas causadas por superaquecimento, instabilidade elétrica, degradação de hardware ou outros problemas físicos sem aviso prévio.

Além dos fatores físicos, existe também a ameaça de ataques cibernéticos direcionados a tornar os servidores indisponíveis. Esses ataques podem ter como objetivo prejudicar a reputação da instituição ou explorar vulnerabilidades no sistema, abrindo brechas de segurança e comprometendo dados sensíveis.

A gravidade dessas situações já foi evidenciada em diversos casos no Brasil. No Rio de Janeiro, o serviço 190 da Polícia Militar ficou fora do ar por mais de quatro(4h) horas devido a falhas operacionais, obrigando a população a recorrer a canais alternativos enquanto o sistema era restabelecido. Em Mato Grosso do Sul, foram registradas mais de 370 ocorrências de falhas nos serviços emergenciais, incluindo os números 190 e 193, relacionadas a instabilidades técnicas na infraestrutura de telecomunicações. Em Santa Catarina, o sistema da Polícia Militar também apresentou instabilidade com impactos no atendimento do 190.

Há ainda registros de ataques hackers que derrubaram sistemas de órgãos de segurança pública e até mesmo ocasionaram exclusão de dados em instituições federais, demonstrando que falhas de segurança podem comprometer tanto a disponibilidade quanto a integridade das informações.

1.1 COPOM (Centro de Operações da Polícia Militar)

COPOM é o órgão responsável pelo atendimento de emergências e chamados à Polícia Militar do estado de São Paulo, assim como coordena as viaturas da corporação. Subordinado à Polícia Militar, opera no atendimento 24h aos chamados referentes à segurança pública, recebendo diariamente cerca de 50 mil ligações.

Neste sentido, O COPOM utiliza sistemas críticos como o SIOPM (Sistema de Irradiação e Operação da Polícia Militar), o Detecta (monitoramento de câmeras/placas) e agora novas camadas de Inteligência Artificial para triagem. Todos rodam em clusters de servidores que precisam de alta disponibilidade.

Este sistema está ligado diretamente com a DTIC (Diretoria de Tecnologia da Informação e Comunicação) é o órgão responsável pelo gerenciamento, planejamento, infraestrutura e segurança das ferramentas tecnológicas em diversas instituições como o PMESP e COPOM. Ela atua na manutenção de sistemas, redes, segurança cibernética e suporte técnico para otimizar o trabalho interno e a prestação de serviços à sociedade.

1.2 Diretoria de Tecnologia da Informação e Comunicação (DTIC)

A DTIC (Diretoria de Tecnologia da Informação e Comunicação) é o órgão central de inteligência tecnológica da Polícia Militar do Estado de São Paulo (PMESP) responsável pelo ciclo de vida tecnológico e pela disponibilidade dos serviços críticos de segurança pública. O órgão atua na camada de governança e execução de toda a infraestrutura de rede, centros de processamento de dados e sistemas de software que sustentam a operação 190.

1.3 Arquitetura e Governança de Dados

A DTIC gerencia um dos maiores ecossistemas de dados policiais da América Latina, integrando sistemas complexos que exigem alta performance de hardware.

- **Ecossistema Integrado:** Coordena a interconexão entre o SIOPM (Sistema de Informação e Operação da Polícia Militar) e o Sistema Detecta. Essa integração atua na correlação de dados em tempo real, permitindo que as atividades operacionais e investigativas das polícias acessem diversos banco de dados institucionais. O sistema processa bilhões de registros, correlacionando informações e imagens de locais, pessoas e veículos para promover ações policiais coordenadas e subsidiar a tomada de decisões estratégicas.
- **Inteligência de Borda e IA:** Gerencia a infraestrutura que suporta a IA Mike, sistema que utiliza o processamento de linguagem natural para triagem automatizada, atuando no atendimento de ocorrências de perturbação do sossego, com capacidade de atender até 200 chamadas simultâneas, liberando atendentes humanos para casos mais graves.
- **Continuidade e Resiliência:** A DTIC implementa estratégias de segurança para garantir que o atendimento 190 nunca seja interrompido, mesmo em caso de falhas graves ou desastres naturais. Para isso, é utilizado um sistema de alta disponibilidade, onde o banco de dados de ocorrência é replicado para servidores localizados em diferentes pontos geográficos. Assegurando que se um equipamento falha ou um prédio sofrer um incidente, terá outro servidor que irá assumir o processamento instantaneamente, preservando a integridade das informações e a continuidade do serviço.

1.3.1 Segurança e Monitoramento

Para assegurar a integridade do fluxo de informações, a DTIC estabelece padrões rigorosos de segurança cibernética e física:

- **Criptografia de Gestão:** Adota o protocolo SNMP v3 como padrão para o monitoramento de seus ativos, garantindo que as métricas de saúde do hardware (temperatura, ciclos de CPI e disco) sejam transmitidos via canais autenticados e criptografados, reduzindo o risco de espionagem ou sabotagem técnica,
- **Geoprocessamento em tempo real:** Sustenta a tecnologia de Localização Móvel Avançada (AML), que exige integração perfeita entre servidores de telecomunicações e banco de dados geoespaciais para o envio imediato de socorro via GPS.

1.3.2 Fundamentação Tecnológica do Monitoramento

O monitoramento de hardware para os servidores de banco de dados da DTIC se baseia na adoção de padrões técnicos universais de mercado e protocolos de comunicação voltados à continuidade dos serviços essenciais. Essa abordagem garante a compatibilidade com infraestruturas de diversos fabricantes e segue as diretrizes de governança de TI do setor público.

1.3.3 Protocolo de Comunicação

A SNMP (Simple Network Management Protocol) é o padrão global de interoperabilidade adotado para o gerenciamento dos ativos de rede e servidores da DTIC. Na infraestrutura de segurança pública, o SNMP v3 é o referencial técnico exigido, visto que em ambientes de alta sensibilidade demandam os recursos de autenticação e criptografia oferecidos por esta versão. O protocolo funciona como a interface de comunicação para a extração de métricas vitais de hardware, como o estado da CPU, RAM e Disco, permitindo que a saúde dos sistemas que sustentam o 190 e o SIOPM seja interpretada pelas plataformas de gestão de redes da corporação.

2 OBJETIVO

Desenvolver uma solução de monitoramento de hardware aplicada a servidores de banco de dados responsáveis pelo processamento e armazenamento de ocorrências policiais em tempo real, visando identificar falhas físicas, sobrecargas de CPU, consumo excessivo de memória e riscos relacionados ao armazenamento, garantindo alta disponibilidade, integridade dos dados e continuidade operacional dos sistemas de missão crítica da segurança pública.

3 JUSTIFICATIVA

A indisponibilidade dos servidores de emergência gera impactos não apenas operacionais e sociais, mas também leva perdas financeiras ao estado, e consequentemente, ao contribuinte. Entre os prejuízos diretos estão os custos com manutenção corretiva emergencial, pagamento de horas extras para equipes técnicas, contratação de suporte externo especializado e substituição de equipamentos danificados. Além disso, quando a infraestrutura depende de empresas terceirizadas de telecomunicação ou data center, há possibilidade da ocorrência de multas contratuais e penalidades por descumprimento de níveis de serviço.

Neste sentido, há também ocorrência de impactos de causas indiretas, como possíveis ações judiciais decorrentes de falhas no atendimento, danos à reputação institucional e necessidade de investimentos emergenciais em segurança da informação após os incidentes.

Sendo assim, a implementação de um sistema de monitoramento preventivo contribui não apenas na redução de custos operacionais, mas também gera aumento e confiabilidade na infraestrutura tecnológica, assim como garante maior estabilidade no atendimento à população do estado de São Paulo.

4 ESCOPO

O projeto tem como objetivo, através de uma plataforma de monitoramento de hardware coletar métricas de servidores de banco de dados da segurança pública. O foco é identificar falhas e sobrecargas em tempo real no processamento de ocorrências policiais, visando reduzir o tempo de inatividade e prevenir o corrompimento de dados críticos, garantindo que o sistema esteja disponível 24/7 para suporte às operações policiais.

4.1 Resultados Esperados

Por meio da implementação de agentes de monitoramento e análise de performance, serão consolidados dados sobre o estado físico dos servidores. Permitindo a detecção precoce de gargalos da CPU e memória, além de prever falhas em discos de armazenamento antes da interrupção do registro de ocorrência.

4.2 Requisitos do Projeto

- Desenvolvimento da arquitetura do sistema de monitoramento.
- Criação do site institucional.
- Criação de página de login e cadastro.
- Criação de painel administrativo com níveis de acesso.
- Dashboard de telemetria em tempo real.
- Sistema de alerta via interface e notificações.
- Estruturação de banco de dados para histórico de performance.
- Integração do banco de dados.
- Provisionamento de ambiente da VM na Nuvem para hospedar a aplicação.
- Criação de registros automáticos da aplicação para auditoria e composição de chamados técnicos.
- Implementação das APIs necessárias.
- Alocamento do projeto no Github.

4.3 Limites e Restrições

Incluso:

- Monitoramento focado exclusivamente no hardware de servidores de banco de dados.
- Acesso ao dashboard e site institucional via navegador web.
- Notificações de incidentes apenas quando os limites de hardware forem atingidos.
- Geração de arquivos .CSV para auditoria e histórico local
- Manutenção e suporte técnico da plataforma de monitoramento.

Isento:

- Reparo físico ou substituição de peças de hardware (servidores, memórias, disco).
- Responsabilidade por falhas ocorridas antes da instalação completa do sistema.
- Monitoramento de sistemas que não sejam do ecossistema de banco de dados da aplicação.
- Responsabilidade por interrupções no fornecimento de serviços de terceiros.
- Garantia de segurança contra ataques cibernéticos externos que não competem à aplicação de monitoramento de hardware.

4.4 Cronograma

Etapas	Tempo
Desenvolvimento	60 Dias
Testes e homologação	30 dias
Levantamento de Requisitos	15 Dias
Implantação	1 Dia
Acompanhamento	15 Dias
Total	121 Dias

4.5 4.5 Recursos Necessários

Recurso	Quantidade	Carga horária
Dispositivo Desktop ou Notebook	6	150 Horas
Google Planner	1	Acesso Integral
Máquina virtual terceirizada	1	Acesso contínuo
Softwares de Desenvolvimento da aplicação (IntelliJ, VScode, MYsql WORKBANCH)	6 (cada)	Acesso contínuo

4.6 Riscos e Restrições

Riscos:

- Limitação no projeto caso não haja acesso à infraestrutura e ferramentas necessárias;
- Os softwares usados podem ficar obsoletos com o tempo;
- Não garantia de funcionamento do software se implementado em dispositivos para os quais não foi projetado;

Restrições:

- Necessidade de energia constante para funcionamento da aplicação;
- Acesso à rede é necessário para a consulta aos dados;
- Interpretação de pessoal instruído é necessária para uso efetivo da ferramenta e seus respectivos recursos;
- A equipe não poderá implementar recursos não solicitados com antecedência;

5 METODOLOGIAS UTILIZADAS

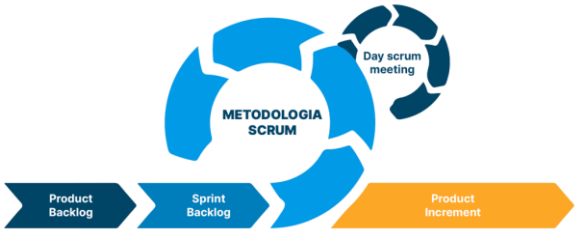
5.1 KANBAN

A **Metodologia Kanban** foi criada por volta de 1940 por Taiichi Ohno na Toyota como parte de um Sistema Toyota de Produção. A metodologia visava dividir as tarefas no quesito de: A fazer, fazendo e feitas. No Projeto, essa metodologia será implementada junto da Ferramenta de Gestão de Projeto, **Planner**. Irá se ter um Quadro com diversos “buckets” pra representar tanto os estados das tarefas, quanto as ATA’s semanais.

5.2 SCRUM

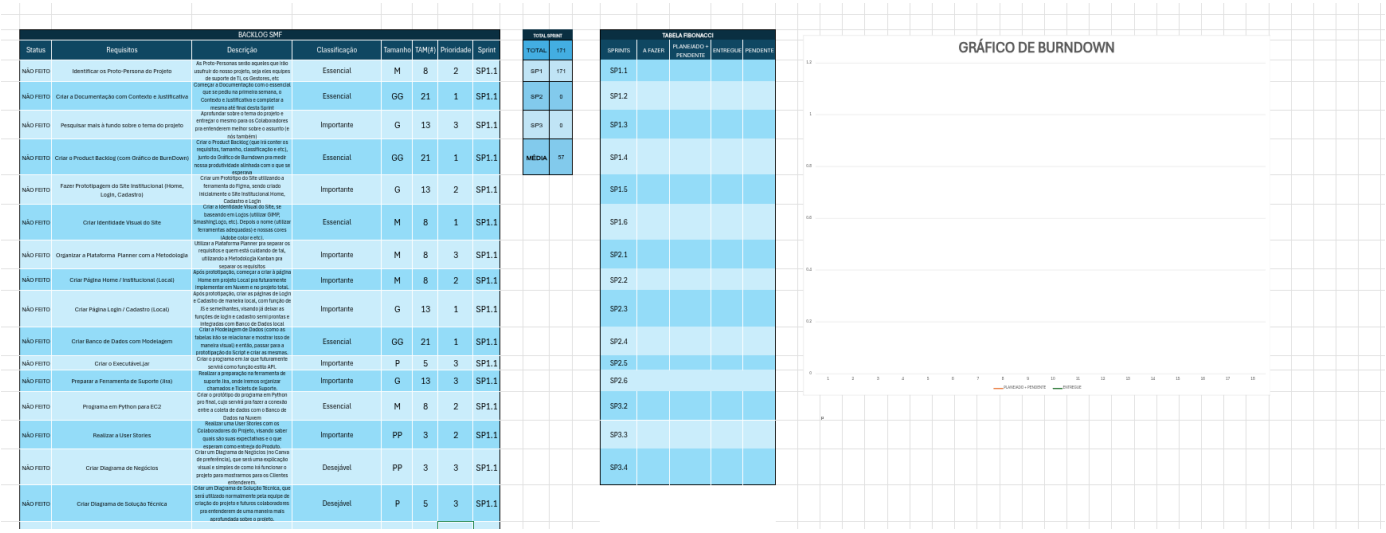
Junto do restante, a **Metodologia Scrum** tem uma forte ligação com um clássico movimento do Futebol Americano, onde todos estão unidos em

formação, com a metodologia representando a união entre todas as partes pra um trabalho bem empenhado. A mesma divide as entregas em Sprints, onde definem um tempo (de 3 em 3 semanas por exemplo) pra entrega parcial do produto até o final. Contudo, que apresenta outras questões como as **Daily** (reuniões diárias de pouca duração para alinhar as entregas e tempo com todo o grupo), **Backlogs** (uma forte gestão de valores de cada tarefa, seus prazos, sua importância e adversos), etc.



6 BACKLOG

O Backlog foi feito utilizando a Ferramenta de Criação de Planilhas, Excel, onde foi ordenado junto dos requisitos, os seus status, prioridade, tamanho (#) e a Sprint na qual está, automatizando a mesma para que não precise perder tanto tempo em outros quesitos (como colocar o valor de Fibonacci em cada tamanho). Além de contudo, possuir um Gráfico de Burndown para definir quais foram as metas para conclusão da Sprint e quais eram as esperadas.



7 STEAKHOLDERS

Equipe de Desenvolvimento:

- **Product Owner (PO)**: Responsável por definir as prioridades do Backlog no Planner e validar a inovação útil do projeto.
- **Desenvolvedores:** Responsáveis pela criação do executável .jar, scripts de captura de hardware e integração com a AWS.
- **Analista de Infraestrutura:** Responsável pelo provisionamento da instância EC2 e política de gestão de acessos.
- **Designer:** Responsável pela usabilidade, responsividade do site.

8 REFERÊNCIAS

SÃO PAULO (Estado). Polícia Militar. Diretoria de Tecnologia da Informação e Comunicação. Edital de Pregão Eletrônico nº 002/211/19. São Paulo: Imprensa Oficial, 08 out. 2019. Disponível em: www.imprensaoficial.com.br.

GOMES, P. R.; SILVA, J. R. Gerenciamento de Redes utilizando o Protocolo SNMP. Tecnologia em Metalurgia, Materiais e Mineração, São Paulo, v. 3, n. 1, p. 1-6, jul./set. 2006. Disponível em: tecnologiammm.com.br.

SÃO PAULO (Estado). Secretaria da Segurança Pública. Cartilha de Adesão ao Sistema DETECTA. São Paulo: Assembleia Legislativa do Estado de São Paulo (ALESP), 2019. Disponível em: www.al.sp.gov.br

Amaral, I. (18 de 03 de 2025). *Nova tecnologia possibilita localização precisa de vítimas durante chamadas de emergência à polícia*. Fonte: Secretária da Segurança Pública: https://www.ssp.sp.gov.br/noticia/58806

Gov, E. d. (23 de 10 de 2017). *Redução de risco de SNMP Abuse*. Fonte: GOV: https://www.gov.br/ctir/pt-br/centrais-de-conteudo/publicacoes/alertas/2017/alerta_2017_08_reducaoderiscodesnmpabuse.pdf

Nascimento, F. F. (06 de 2019). *INTEGRAÇÃO TECNOLÓGICA* . Fonte: Polica Militar: https://policiamilitar.sp.gov.br/unidades/ambiental/SegAmb/ed5/ed5art3.pdf

Nascimento, W. (21 de 06 de 2024). *PM cria sistema de inteligência artificial para agilizar atendimentos em chamados do 190*. Fonte: Secretária da Segurança Pública: https://www.ssp.sp.gov.br/noticia/57580

Novo Serviço de Localização de Emergência está em operação no Brasil. (16 de 12 de 2024). Fonte: GOV: https://www.gov.br/anatel/pt-br/assuntos/noticias/novo-servico-de-localizacao-de-emergencia-esta-em-operacao-no-brasil