Departamento de Ciência da Computação
Instituto de Ciências Exatas
Universidade Federal de Minas Gerais

Plano de Trabalho

Desenvolvendo Inteligência para a Cibersegurança em Tempo Real e Defesa de Sistemas Inteligentes

Título Público: Desenvolvendo Inteligência para a Cibersegurança em Tempo Real e Defesa de Sistemas Inteligentes

Descrição Pública: O avanço acelerado das ameaças digitais e a crescente sofisticação dos ataques cibernéticos colocam em risco sistemas críticos e a privacidade de milhões de pessoas, exigindo respostas rápidas, inteligentes e confiáveis. Este projeto visa desenvolver soluções inovadoras baseadas em Inteligência Artificial para a **detecção e resposta a ameaças cibernéticas em tempo real**, enfrentando diretamente um dos maiores desafios atuais da segurança cibernética: **a antecipação e a mitigação proativa de ataques que evoluem rapidamente**. Além de atuar na proteção de infraestruturas digitais, o projeto também se propõe a **fortalecer a segurança dos próprios sistemas de IA**, tornando-os menos suscetíveis a ataques adversariais, manipulações e vazamentos de dados sensíveis. Essa atuação na intersecção entre cibersegurança e proteção de modelos inteligentes representa um **eixo de inovação crítica**, voltado à construção de tecnologias resilientes, éticas e transparentes. A parceria entre a UE DCC/UFMG e o Instituto Kunumi une excelência acadêmica e experiência de mercado para enfrentar esses riscos com soluções concretas. O projeto também visa consolidar o laboratório de Cibersegurança e Inteligência Artificial em criação no DCC/UFMG e promover impacto social ao contribuir para a **formação de recursos humanos especializados**, **o fortalecimento da equidade de gênero em tecnologia** e a **transferência de conhecimento para a sociedade**, consolidando um ecossistema de inovação orientado à segurança e à responsabilidade digital.

Projeto de Pesquisa, Desenvolvimento e Inovação em Parceria com Instituto KUNUMI

Interveniente Administrativo-Financeiro: FUNDEP
Coordenadora: Profa. Michele Nogueira Lima
Subcoordenador: Prof. Adriano Alonso Veloso
Versão: 06/05/2025

Sumário

1. INTRODUÇÃO

Este documento apresenta o Plano de Trabalho do projeto "**Desenvolvendo Inteligência para a Cibersegurança em Tempo Real e Defesa de Sistemas Inteligentes**", a ser realizado mediante uma parceria entre o Instituto Kunumi doravante denominada simplesmente "KUNUMI", e a

Unidade EMBRAPII do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG), doravante denominada simplesmente “UE DCC/UFMG”.

A KUNUMI é um instituto brasileiro, proponente em Inteligência Artificial, Aprendizagem de Máquina e Ciência de Dados, e pretende compartilhar conhecimento e contribuir com o fomento de pesquisa científica de potencial transformador e impacto positivo para a sociedade. Ela possui como fundadora a empresa KUNUMI LTDA, onde desde sua fundação, a empresa atuou em inúmeros parceiros dos segmentos de cidades, cultura, saúde, engenharia e negócios, aportando conhecimento no estado da arte em IA para a solução de problemas complexos e sofisticados. Ao mesmo tempo, se manteve próximo a instituições acadêmicas - brasileiras e internacionais - de ponta, não apenas colaborando em projetos multidisciplinares, aportando conhecimento em IA e/ou recursos financeiros advindos de sua margem obtida no mercado, mas também se mantendo próximo aos avanços na Inteligência Artificial, Aprendizagem de Máquina e/ou aprendendo sobre outros domínios do conhecimento, o que acredita ser o único caminho para a geração de valor dessa tecnologia no mundo real.

A UE DCC/UFMG atua na área de competência Software para Sistemas Ciberfísicos. O foco principal da UE DCC/UFMG é o desenvolvimento de plataformas computacionais para tratar componentes físicos, virtuais e sociais em diferentes escalas e suportadas por tecnologias diversas em todas as atividades humanas. As linhas de atuação da UE DCC/UFMG são:

• Prospecção e Monitoramento de Dados;

• Gestão da Informação;

• Mecanismos para Tomada de Decisão e Atuação.

2. IDENTIFICAÇÃO DO PROJETO

TÍTULO: Desenvolvendo Inteligência para a Cibersegurança em Tempo Real e Defesa de Sistemas Inteligentes

TIPO: Projeto de Pesquisa, Desenvolvimento Tecnológico e Inovação

TIPO DE PROJETO: Produto e processo

ÁREA DE CONHECIMENTO: Cibersegurança, Inteligência Artificial e Aprendizado de Máquina

Identificação do Partícipe 1 - UFMG

CNPJ: 17.217.985/0001-04.

Endereço: Av. Antônio Carlos, 6627, Pampulha, CEP 31.270-901, Belo Horizonte, MG.

Representante legal: Sandra Regina Goulart Almeida.

Cargo: Reitora.

CI:M-2.xxx.517

CPF:452.xxx.xxx-49

Telefone: (31) 3409-4124.

E-mail: reitor@ufmg.br.

Identificação do Partícipe 2 - Instituto Kunumi

Razão Social: Instituto Kunumi

CNPJ: 60.413.662/0001-15

Endereço: R RIO GRANDE DO NORTE 1435 Sala 708, Savassi, Belo Horizonte, MG, Brasil, CEP: 30.130-138

Representantes legais

Nome: Alberto Colares

Cargo: CEO

CPF: 818.xxx.xxx-72

Telefone: (11) 97370-6767

E-mail: alberto@kunumi.ai

Nome: Marcelo Guerra Xavier

Cargo: Diretor de Parcerias

CPF: 042.xxx.xxx-99

Telefone: (11) 97370-6767

E-mail: marcelo@kunumi.ai

Faixa de Faturamento: Entre R$ 4,8 e R$ 300 milhões

Faixa de número de empregados: Entre 01 e 50 empregados

Classificação: Instituto de Médio Porte

COORDENAÇÃO DO PROJETO - UFMG

Coordenadores:

Michele Nogueira Lima

SIAPE: 1750012 **Telefone**: (41) 99800-0990 **Ramal UFMG**- 5857

E-mail: michele@dcc.ufmg.br

Setor de lotação: Departamento de Ciência da Computação - DCC

Adriano Alonso Veloso

SIAPE: 1741193-1 **Telefone:** (32) 984161098 **Ramal UFMG**- 5579

E-mail: adrianov@dcc.ufmg.br

Setor de lotação: Departamento de Ciência da Computação - DCC

COORDENAÇÃO DO PROJETO - Instituto Kunumi

Coordenador(a): Marcelo Xavier

CPF: 042.xxx.xxx-99 **Telefone:** (11) 97370-6767

E-mail: marcelo@kunumi.ai

Cargo: Diretor de Parcerias

Departamento/Setor: Pesquisa e Desenvolvimento

3. OBJETIVO

O Instituto Kunumi é uma associação privada com o foco em desenvolver soluções para problemas complexos e sofisticados envolvendo Inteligência Artificial, tendo atuado em diferentes segmentos da sociedade como cultura, saúde, engenharia e negócios. No escopo deste projeto, o instituto Kunumi visa avançar o estado da arte em cibersegurança, desenvolvendo soluções inovadoras baseadas em Inteligência Artificial para a **detecção e resposta a ameaças cibernéticas em tempo real**, enfrentando diretamente um dos maiores desafios atuais da segurança cibernética: **a antecipação e a mitigação proativa de ataques que evoluem em frações de segundo**. Combinando aprendizado de máquina, processamento de linguagem natural e outras abordagens avançadas de IA, o instituto visa oferecer modelos capazes de lidar em tempo real com a complexidade crescente do ciberespaço e suas múltiplas vulnerabilidades. Além de atuar na proteção de infraestruturas digitais, o projeto também se propõe a **fortalecer a segurança dos próprios sistemas de IA**, tornando-os menos suscetíveis a ataques adversariais, manipulações e vazamentos de dados sensíveis. Essa atuação na intersecção entre cibersegurança e proteção de modelos inteligentes representa um **eixo de inovação crítica**, voltado à construção de tecnologias resilientes, éticas e transparentes. A parceria entre a UE DCC/UFMG e o Instituto Kunumi une excelência acadêmica e experiência de mercado para enfrentar esses riscos com soluções concretas. O projeto também visa consolidar o laboratório de Cibersegurança e Inteligência Artificial em criação no DCC/UFMG e promover impacto social ao contribuir para a **formação de recursos humanos especializados**, **o fortalecimento da equidade de gênero em tecnologia** e a **transferência de conhecimento para a sociedade**, consolidando um ecossistema de inovação orientado à segurança e à responsabilidade digital.

Para que o objetivo geral proposto seja alcançado, serão perseguidos os seguintes objetivos específicos:

1. Desenvolver soluções de IA para detecção e resposta a ameaças cibernéticas em **tempo real**, utilizando técnicas de aprendizado profundo, redes neurais dinâmicas e modelos generativos.

2. Proteger modelos de IA contra ataques adversariais, envenenamento de dados, roubo de modelos e inferência de dados privados.

3. Promover a formação de recursos humanos qualificados e fomentar a transferência de tecnologia para setores estratégicos.

4. Promover e impulsionar a diversidade de gênero nas áreas de Cibersegurança e IA através da atração e formação de meninas e pesquisadoras.

5. Apoiar a criação do laboratório de Cibersegurança e Inteligência Artificial.

4. PESQUISA E DESENVOLVIMENTO

A segurança cibernética (cibersegurança) e a inteligência artificial são áreas em constante evolução, cujas interseções geram novos desafios técnicos e científicos. De um lado, os sistemas de IA oferecem capacidades avançadas de detecção e resposta a ameaças cibernéticas; de outro, eles próprios se tornam alvos de ataques sofisticados, como manipulações adversariais e envenenamento de dados. Atualmente, as soluções existentes ainda apresentam limitações para lidar com ameaças dinâmicas e complexas, além de vulnerabilidades nos próprios modelos de IA implantados em ambientes críticos.

Nesse contexto, este projeto propõe o desenvolvimento de técnicas inovadoras de Inteligência Artificial para fortalecer a capacidade de defesa cibernética em tempo real e, simultaneamente, assegurar a proteção dos próprios sistemas de IA. A pesquisa se concentrará na criação de métodos de detecção de ameaças em tempo real baseados em aprendizado de máquina, redes neurais dinâmicas e modelos generativos, bem como no desenvolvimento de mecanismos de defesa contra ataques adversariais e de proteção à privacidade dos dados utilizados para treinar sistemas inteligentes.

O desenvolvimento visa à antecipação e à mitigação de riscos cibernéticos e de ameaças aos próprios modelos de IA, tornando os processos de segurança digital mais robustos, éticos e transparentes. Com isso, pretende-se impactar positivamente setores estratégicos que dependem de IA em larga escala, como finanças e infraestrutura crítica.

Este projeto se enquadra nas linhas de atuação da UE DCC/UFMG em **Prospecção e Monitoramento de Dados**, **Gestão da Informação**, e **Mecanismos para Tomada de Decisão e Atuação**, assim como nas atividades do **grupo de pesquisa Ciência de Segurança Computacional e de Segurança de Redes (CCSC)**. A UE DCC/UFMG contribuirá com seu conhecimento avançado em IA aplicada à cibersegurança, visando

ao desenvolvimento de soluções inovadoras que agreguem valor à parceria com o Instituto Kunumi e ampliem a competitividade tecnológica nacional.

5. ASPECTOS INOVADORES

Os aspectos de inovação deste projeto de Pesquisa, Desenvolvimento e Inovação (PD&I) estão no desenvolvimento de algoritmos, técnicas e tecnologias de Inteligência Artificial voltados simultaneamente para dois desafios estratégicos: (i) o fortalecimento da defesa cibernética em **tempo real** por meio da detecção inteligente de ameaças e (ii) a proteção dos próprios sistemas de IA contra ataques adversariais, envenenamento de dados e vazamentos de informações sensíveis.

A inovação para o negócio do Instituto Kunumi reside na criação de soluções que vão além da segurança tradicional, incorporando inteligência adaptativa e mecanismos de defesa autônomos que aumentam a capacidade de resposta a ameaças emergentes em tempo real. Estas soluções permitirão à KUNUMI posicionar-se de maneira estratégica no mercado de cibersegurança e IA confiável, fortalecendo sua atuação em setores críticos como saúde, finanças e infraestruturas críticas.

Do ponto de vista de mercado, o projeto contribuirá para diferenciar a KUNUMI pela oferta de tecnologias de segurança cibernética baseadas em IA que são não apenas eficientes, mas também resilientes, éticas e transparentes — atributos cada vez mais valorizados globalmente. A capacidade de proteger tanto os dados quanto os próprios modelos de inteligência artificial representa um diferencial competitivo relevante no cenário atual de crescimento das ameaças digitais e de exigências regulatórias de proteção de dados.

A UE DCC/UFMG possui o conhecimento necessário e experiência para produzir algoritmos, técnicas e tecnologias eficientes e inovadoras em aprendizado de máquina, segurança de redes e defesa contra ataques adversariais, assegurando a excelência científica e tecnológica no desenvolvimento das soluções propostas.

6. RELEVÂNCIA DO PROJETO

O problema central que este projeto busca resolver é a crescente vulnerabilidade de sistemas digitais frente a ameaças cibernéticas cada vez mais sofisticadas, dinâmicas e repentinas, além da fragilidade dos próprios modelos de inteligência artificial frente a ataques adversariais e à violação de dados sensíveis. A falta de soluções integradas que, simultaneamente, aprimorem a capacidade de defesa cibernética em tempo real e protejam os sistemas de IA representa um risco significativo para diversos setores estratégicos da sociedade.

A realização deste projeto beneficiará tanto a sociedade quanto o setor produtivo, ao viabilizar a criação de tecnologias inovadoras que garantam maior segurança, privacidade e confiabilidade em ambientes digitais. O desenvolvimento de sistemas de IA mais resilientes e de defesas cibernéticas baseadas em inteligência artificial terá impacto direto na proteção de infraestruturas críticas, na preservação de dados pessoais e na segurança das transações digitais em áreas como finanças e indústria.

A UFMG, por meio do Departamento de Ciência da Computação, vê neste projeto uma oportunidade estratégica de aplicar seu conhecimento em aprendizado de máquina, cibersegurança e segurança de redes a um problema real de grande impacto social e econômico. O envolvimento da universidade não apenas fortalece sua missão de inovação, transferência de tecnologia e responsabilidade social, como também fomenta a formação de recursos humanos altamente qualificados em áreas tecnológicas de ponta além de promover e fortalecer as ações de equidade de gênero do Departamento.

A parceria com o Instituto Kunumi é essencial, dado o conhecimento prático e os dados que o Instituto traz, possibilitando que as soluções desenvolvidas sejam eficazes, alinhadas às demandas de mercado e orientadas para desafios reais de segurança cibernética em escala nacional e internacional.

7. PLANO DE ATIVIDADES

O projeto será executado em múltiplas etapas e as atividades para o desenvolvimento de cada Macroentrega são descritas a seguir.

ETAPA	DESCRIÇÃO DAS ATIVIDADES	MACROENTREGA
Etapa 1: Instalação do projeto e contratação de pessoal.	Seleção e contratação de equipe de pesquisa (pesquisadores, bolsistas, CLT), treinamento inicial, definição detalhada dos desafios prioritários, reunião de kick-off com o Instituto Kunumi.	**Macroentrega 1:** Relatório de início do projeto, equipe constituída e planejamento detalhado das fases seguintes.
Etapa 2: Levantamento e Análise de Cenários de Cibersegurança e Vulnerabilidades em IA	Estudo dos cenários de aplicação, análise das ameaças cibernéticas relevantes e levantamento dos principais vetores de ataque a modelos de IA. Revisão de literatura científica e técnica.	Relatório técnico com o estado da arte em cibersegurança baseada em IA e vulnerabilidades de modelos de IA, com mapeamento de oportunidades de inovação.
Etapa 3: Definição e projeto de uma solução de IA para detecção de ameaças cibernéticas em tempo real	Definição e projeto do sistema de detecção de ameaças em **tempo real**. Definir sobre as técnicas a serem aplicadas, tais como aprendizado profundo, redes neurais dinâmicas, modelos generativos, data streaming. Definição da metodologia e métodos de avaliação (precisão, recall, robustez).	**Macroentrega 2:** Definição do sistema de detecção inteligente de ameaças cibernéticas em tempo real (descrição, definições e premissas), poderá se

		fazer testes com ambientes e cenários simulados. (documento com definição do sistema)
Etapa 4: Definição e projeto de um mecanismo de defesa de modelos de IA	Projeto do mecanismo de defesa contra ataques adversariais e envenenamento de dados; desenvolvimento de métodos de fortalecimento de modelos (adversarial training, privacidade diferencial, federated learning).	Definição do mecanismo de defesa proposto para modelos de IA com resultados de testes de resiliência em cenários simulados (documento com a descrição do mecanismo, definições e premissas).
Etapa 5: Implementação da solução de IA para detecção de ameaças cibernéticas em tempo real	Implementação do sistema de detecção de ameaças em tempo real utilizando aprendizado profundo, redes neurais dinâmicas e modelos generativos. Definição da metodologia e métodos de avaliação (precisão, recall, robustez).	**Macroentrega 3:** Protótipo inicial de sistema de detecção inteligente de ameaças cibernéticas com relatório de desempenho preliminar.
Etapa 6: Desenvolvimento do mecanismo de defesa de modelos de IA definido na etapa 4.	Implementação de técnicas de defesa contra ataques adversariais e envenenamento de dados; desenvolvimento de métodos de fortalecimento de modelos (adversarial training, privacidade diferencial, federated learning).	**Macroentrega 4:** Protótipo funcional do mecanismo de defesa para modelos de IA, com resultados de testes de resiliência em cenários simulados.
Etapa 7: Integração e Validação de Soluções em Ambientes de Aplicação	Integração das soluções desenvolvidas em cenários reais de operação ou simulações controladas; testes de segurança ofensiva (red teaming) e avaliação de eficácia.	**Macroentrega 5:** Documentação com resultados da validação de protótipos em ambientes simulados e reais, com métricas de desempenho e robustez.
Etapa 8: Transferência de Tecnologia e Disseminação de Resultados	Preparação de documentação técnica, realização de workshops de treinamento para equipe Kunumi, submissão de artigos científicos e relatórios finais do projeto.	Documentação completa das tecnologias desenvolvidas, workshops realizados e submissão de pelo menos quatro artigos científicos em eventos de destaque e um em periódico internacional.

Atividades do INSTITUTO

1. **Definição dos requisitos de aplicação**: Apoiar na definição e priorização dos requisitos técnicos e funcionais dos sistemas de cibersegurança e defesa de IA a serem desenvolvidos, com base em necessidades práticas de mercado e aplicações reais.
2. **Disponibilização de dados e cenários de teste**: Fornecer conjuntos de dados, informações de ameaças e cenários simulados ou reais de operação para o desenvolvimento, validação e avaliação das soluções propostas.

3. **Disponibilização de acesso ao ambiente/cluster de GPUs:** Fornecer acesso ao ambiente de testes composto por GPUs implantados pelo instituto para execução e testes.
4. **Avaliação técnica contínua das entregas**: Participar da avaliação técnica das soluções desenvolvidas (protótipos, algoritmos e frameworks), fornecendo feedback sobre desempenho, aplicabilidade e aderência às necessidades práticas.
5. **Participação em testes de validação e red teaming**: Atuar nos processos de validação funcional e testes ofensivos (testes de intrusão, simulação de ataques adversariais) para medir a robustez das soluções de cibersegurança e proteção de IA.
6. **Ajustes e adequações de integração**: Apoiar na identificação de requisitos para integração das soluções desenvolvidas em suas plataformas e serviços, ajustando aspectos técnicos e operacionais conforme necessário.
7. **Transferência de conhecimento e capacitação da equipe**: Participar de workshops, treinamentos e sessões técnicas organizadas pela UE DCC/UFMG para absorver o conhecimento gerado no projeto e viabilizar a aplicação das soluções no ambiente empresarial.
8. **Gestão administrativa do projeto**: Gerenciar os aportes financeiros previstos no cronograma, participar de reuniões periódicas de acompanhamento do projeto e validar formalmente as macroentregas.

Atividades conjuntas

1. **Definição e detalhamento dos desafios e casos de uso prioritários**: trabalhar em conjunto para identificar os principais desafios de cibersegurança e vulnerabilidades em sistemas de IA, mapeando casos de uso relevantes para aplicação das soluções desenvolvidas.
2. **Avaliações colaborativas de soluções de IA para segurança digital**: trabalhar de forma integrada na avaliação de algoritmos, modelos de aprendizado de máquina e mecanismos de defesa de IA, com troca de conhecimentos técnicos e avaliações iterativas.
3. **Validação e avaliação contínua das soluções desenvolvidas**: definir conjuntamente testes das soluções geradas usando ambientes simulados e reais, com a análise colaborativa de métricas de desempenho, robustez, confiabilidade e adequação às necessidades práticas.
4. **Realização de workshops técnicos, reuniões de avaliação e refinamento de soluções**: organizar workshops técnicos internos para revisão de progresso, troca de feedback e refinamento das abordagens, garantindo alinhamento estratégico e técnico ao longo do projeto.
5. **Publicação de resultados científicos e tecnológicos**: produzir, em parceria, artigos técnicos e científicos para submissão a conferências e periódicos relevantes, promovendo a divulgação do conhecimento gerado no projeto.

8. **CRONOGRAMA DE EXECUÇÃO DAS ATIVIDADES**

A tabela abaixo apresenta a estimativa de duração de cada uma das etapas do projeto. O cronograma de execução deste projeto prevê o prazo de 24 (vinte e quatro) meses apresentados na tabela a seguir.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
ETAPA 1																								
ETAPA 2				**X**																				
ETAPA 3																								
ETAPA 4										**X**														
ETAPA 5																**X**								
ETAPA 6																				**X**				
ETAPA 7																								
ETAPA 8																								**X**

*Tabela 1. Cronograma (em **meses**) mostrando cada uma das etapas do projeto. Células com* **X** correspondem ao bimestre em que ao final ocorrerá uma m*acroentrega*.

9. **PREMISSAS**

As seguintes premissas foram consideradas verdadeiras para o sucesso do projeto:

1. A Kunumi deverá validar as entregas em até 10 (dez) dias úteis, e comunicar quaisquer solicitações de alterações por escrito à equipe da UE DCC/UFMG. Caso nenhuma comunicação seja recebida neste período, as entregas serão consideradas aceitas sem modificações e Termo de Aceite aprovado e assinado.

2. Mudanças no escopo deverão ser acordadas entre ambas as partes.

3. Haverá participação efetiva da equipe técnica da Kunumi na identificação e avaliação dos resultados obtidos, no esclarecimento das dúvidas da equipe da UE DCC/UFMG;

4. A Kunumi se compromete a fornecer os dados de produção e o respectivo desfecho em termos da qualidade observada;

5. A UE DCC/UFMG e a Kunumi estarão comprometidos a fornecer pessoal necessário e adequado para execução do projeto, conforme o acordo estabelecido entre as partes;

6. O cumprimento do cronograma do projeto está condicionado à reserva de agenda pela equipe Kunumi para reuniões, entrevistas, oficinas e validações dos artefatos gerados no projeto;

7. A UE DCC/UFMG terá plena autonomia em relação à definição e gerenciamento de sua equipe;

8. As equipes da UE DCC/UFMG e Kunumi deverão fazer acompanhamento periódico do projeto em relação ao andamento de suas atividades.

9. A UE DCC/UFMG detém conhecimento (know-how) prévio de soluções baseadas em algoritmos de IA e Cibersegurança e a pesquisa feita neste projeto acrescentará ao conhecimento existente especificidades para atender ao escopo do projeto.

10. Para as comunicações do projeto entre as equipes da UE DCC/UFMG e da Kunumi serão utilizados os seguintes recursos:

▪ E-mail: no início do projeto será distribuída uma lista com o endereço eletrônico dos principais envolvidos em cada fase do projeto;

▪ Telefone: será mantida também uma lista com os contatos dos envolvidos;

▪ Reuniões: sempre que julgarem necessário, tanto a equipe técnica da UE DCC/UFMG quanto a equipe da Kunumi poderão solicitar reuniões para esclarecimento de dúvidas e resolução de pendências do projeto. No início do projeto, o cronograma e periodicidade das reuniões de acompanhamento do projeto serão definidos entre UE DCC/UFMG e Kunumi.

10. RESTRIÇÕES

As seguintes restrições são consideradas verdadeiras para o sucesso do projeto:

● Os aportes financeiros recebidos como doação pela Kunumi para a consecução dos objetivos estabelecidos no Plano de Trabalho não serão considerados recursos financeiros aportados no projeto, ainda que utilizados na execução do mesmo, constituindo-se, portanto em mera liberalidade por parte da Kunumi;

● Os resultados e/ou entregas previstos neste projeto pertencem ao nível de maturidade 4 (de acordo com escala TRL[1]), envolvendo prova de conceito e validação funcional do sistema e tecnologia em ambiente de laboratório.

11. RISCOS IDENTIFICADOS

Os riscos inicialmente identificados para este projeto são:

● Atraso no aporte do instituto.

● Possíveis dificuldades na obtenção dos dados, juntamente com o instituto, para avaliação das soluções sendo desenvolvidas.

● Obtenção de resultados abaixo do esperado devido à qualidade dos dados, mudanças de características dos cenários monitorados ou presença de ambientes de monitoramento muito heterogêneos para um dado problema.

● Obtenção de resultados abaixo do esperado pelos módulos desenvolvidos devido a riscos naturais associados à atividade de pesquisa e inovação.

A UE DCC/UFMG juntamente com a Kunumi se compromete na identificação e gerenciamento de riscos durante todo o projeto e no seu tratamento de modo a aumentar a probabilidade e os impactos dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto usando estratégias adequadas de mitigação e ações de resposta aos riscos.

12. RESULTADOS ESPERADOS DO PROJETO

Múltiplos resultados positivos serão alcançados com este projeto. Os mais importantes são:

● **Desenvolvimento e implementação de soluções baseadas em Inteligência Artificial para detecção e resposta a ameaças cibernéticas em tempo real**, utilizando técnicas avançadas de aprendizado de máquina, redes neurais dinâmicas e modelos generativos. Espera-se o desenvolvimento de, pelo menos, três protótipos funcionais validados em cenários reais de aplicação.

● **Criação de mecanismos de defesa robustos para proteção de modelos de IA** contra ataques adversariais, envenenamento de dados, roubo de modelos e inferência de informações sensíveis, com a implementação de pelo menos dois métodos de proteção validados.

● **Solução de problemas práticos apresentados pelo Instituto Kunumi** durante o desenvolvimento do projeto, com entregas intermediárias que respondam a necessidades específicas identificadas em ambientes de cibersegurança e proteção de IA utilizados pelo instituto.

● **Identificação contínua de novas linhas de pesquisa relevantes** na interseção entre cibersegurança e inteligência artificial, com a expectativa de gerar, no mínimo, dois artigos científicos submetidos a conferências ou periódicos de alto impacto, além de relatórios técnicos que documentem os avanços obtidos.

● **Troca de experiência e transferência de tecnologia entre pesquisadores da UE DCC/UFMG e do Instituto Kunumi**, com a realização de workshops técnicos, reuniões de revisão de progresso trimestrais, e treinamentos práticos para a equipe do instituto nas soluções desenvolvidas.

● **Formação de recursos humanos altamente qualificados**, incluindo a participação de estudantes de graduação e pós-graduação, com a previsão de envolvimento direto de pelo menos quatro bolsistas de diferentes níveis, ampliando a capacidade científica e tecnológica da equipe.

● **Consolidação do laboratório de Cibersegurança e IA,** iniciando uma parceria de longo prazo entre Kunumi e UE DCC-UFMG em pesquisa, desenvolvimento e inovação na intersecção entre essas duas áreas de grande importância.

Indicadores de sucesso incluem: número de protótipos desenvolvidos, nível de eficácia dos algoritmos em cenários de validação (medidos por métricas como precisão, recall, F1-score e robustez adversarial), número de artigos científicos submetidos e aceitos, quantidade de tecnologias transferidas e volume de capacitação técnica realizada.

13. CONTRAPARTIDA ECONÔMICA

A contrapartida da UE DCC/UFMG pode incluir custos indiretos com infraestrutura (laboratórios, equipamentos, redes de tecnologia de informação, uso de software de PD&I próprios), depreciação da infraestrutura durante a execução do projeto, despesas com infraestrutura

(água, energia elétrica e segurança), diárias/passagens e despesas de locomoção, serviços de terceiros (pessoa física e jurídica), material de consumo, despesas de suporte operacional, e/ou uso de software de P,D&I próprios. Ainda mais, a Portaria 03/2019 da Pró-Reitoria de Planejamento e Desenvolvimento da UFMG define o percentual de contrapartida levando em consideração os custos indiretos e a depreciação da infraestrutura durante a execução do projeto.

Dessa forma, como contrapartida econômica da UE DCC/UFMG foi adotada uma estimativa média de 12% na composição do orçamento do projeto. Reforçando, não haverá dispêndio direto de recursos pela Universidade. A contrapartida da KUNUMI será financeira.

14. ORÇAMENTO DO PROJETO

Este projeto utilizará a modalidade de financiamento padrão da Embrapii.

O valor total do orçamento do projeto é de **R$3.516.298,73** (Três milhões, quinhentos e dezesseis mil, duzentos e noventa e oito reais e setenta e três centavos) e é composto da seguinte forma:

Recursos Financeiros		**Contrapartida Econômica (Não Financeira) ***
EMBRAPII	**KUNUMI***	**UE DCC/UFMG**
R$1.160.378,58	R$1.933.964,30	R$421.955,85

As despesas previstas para este projeto são:

Rubricas	**Valor**
Pessoal	R$2.537.598,08
Material de consumo (componentes protótipo/solução)	R$0,00
Passagens e despesas de locomoção	R$29.300,00
Serviços de terceiros - pessoa física e jurídica	0,00
Despesas operacionais incluindo remuneração da FUNDEP	R$527.444,81
Contrapartida Econômica UE DCC/UFMG	R$421.955,85
TOTAL DO ORÇAMENTO	**R$3.516.298,73**

Os recursos financeiros serão administrados pela FUNDEP. Para isto será repassado para a FUNDEP o valor total de R$ 527.444,81 (quinhentos e vinte e sete mil, quatrocentos e quarenta e quatro reais e oitenta e um centavos) em decorrência da gestão administrativa e despesas de suportes operacionais do projeto conforme Manual de Operações da EMBRAPII versão 6.

15. CRONOGRAMA DE DESEMBOLSO

O aporte (desembolso) dos recursos financeiros para a execução deste projeto será feito conforme a tabela abaixo:

	MÊS	**KUNUMI**	**EMBRAPII**
Macro Entrega 1	1	R$539.195,10	R$323.517,06
Macro Entrega 2	5	R$418.430,76	R$251.058,46
Macro Entrega 3	11	R$418.430,76	R$251.058,46
Macro Entrega 4	17	R$278.953,84	R$167.372,30
Macro Entrega 5	21	R$278.953,84	R$167.372,30

Os aportes devem ser feitos pela KUNUMI até o quinto dia útil, após a emissão da fatura emitida e enviada pela FUNDEP.

O aporte referente a macroentrega 1 deverá ser realizado no início do projeto, assim que for assinado o Acordo de Parceria. O projeto somente será iniciado após a realização deste primeiro aporte. Os demais aportes também serão sempre no início da macroentrega e após aceitação da macroentrega anterior.

16. COORDENAÇÃO E EQUIPE DO PROJETO

Para a coordenação do projeto a UE DCC/UFMG designa a Profa. Michele Nogueira Lima, CPF: 853.802.023-49 e Adriano Alonso Veloso, CPF: 037.336.476-88, que serão os responsáveis pelo bom andamento do projeto no que se refere à orientação da equipe, definição das diretrizes técnicas e de pesquisa durante todo o projeto, bem como o cumprimento das metas acordadas entre as partes.

A KUNUMI por sua vez, designa Marcelo Xavier, CPF: 042.958.596-99, como coordenador técnico de sua parte, que será responsável pela interlocução com a UE DCC/UFMG nos assuntos relacionados à execução do projeto e que tem como atribuições o acompanhamento do

projeto na totalidade, além do aporte dos recursos financeiros como definido neste plano de trabalho.

Para a execução do projeto será necessária uma equipe de pesquisadores e profissionais, executando tarefas específicas, como descrito na tabela abaixo.

Membro da Equipe*	**CPF ou SIAPE**	**Tarefas**
Professora Pesquisadora Coordenadora Michele Nogueira Lima	853.802.023-49	Responsável pelo acompanhamento do projeto e orientação da criação e desenvolvimento das soluções para os problemas objetos do projeto.
Professor Pesquisador Subcoordenador Adriano Veloso	037.336.476-88	Responsável pela coordenação da pesquisa e do projeto, orientação da criação e desenvolvimento das soluções para os problemas objetos do projeto.
Professor Pesquisador Aldri Luiz dos Santos	014.531.347-60	Responsável pela orientação da criação e desenvolvimento das soluções para os problemas objetos do projeto.
03 Bolsistas de Pós-doutorado a definir		Responsáveis pelas pesquisas mais avançadas, liderança na escrita dos artigos científicos e direcionamentos nos avanços científicos em conjunto com os pesquisadores.
04 Bolsistas de doutorado a definir		Responsáveis pelas atividades de pesquisa e desenvolvimento do projeto.
03 Bolsistas de mestrado a definir		Responsáveis pelas atividades de pesquisa, implementação e desenvolvimento do projeto.
10 Bolsistas de Graduação a definir		Responsáveis pelas atividades de pesquisa, implementação e desenvolvimento do projeto.
Gerente de Projeto a definir		Responsável pelo gerenciamento do projeto e liderar o desenvolvimento e criação dos algoritmos, preparação das entregas e interação com a equipe técnica da KUNUMI.

*A atuação dos pesquisadores se dará através de atividades de inovação científica e tecnológica, com concessão de bolsas, sendo que a quantidade de meses, horas dedicadas mensalmente e valores estão no documento de Formalização de Projeto, e atende as Resoluções pertinentes da UFMG.

Belo Horizonte, data da assinatura digital.

Pela UFMG:

Professora Sandra Regina Goulart Almeida

Reitora

Pela KUNUMI:

Marcelo Guerra Xavier

Diretor de Parcerias

Alberto Henrique Duarte Colares

Diretor Presidente

Pela FUNDEP:

Professor Jaime Arturo Ramírez

Presidente

TESTEMUNHAS:

1- UFMG
Michele Nogueira Lima
Coordenador do Projeto

2- Fundação
Leonardo de Souza Esteves
FUNDEP

3- INSTITUTO
Nome: Marina Sasaki
Instituto Kunumi

[1] Com base na norma ISO 16290:2013 (ISO/FDIS 16290:2013(E) Space systems - Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment. International Organization for Standardization, Switzerland, 2013. 12p.)

Documento assinado eletronicamente por **Alberto Henrique Duarte Colares**, **Usuário Externo**, em 07/07/2025, às 16:38, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marina Barreto Sasaki**, **Usuário Externo**, em 08/07/2025, às 11:01, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo Guerra Xavier**, **Usuário Externo**, em 08/07/2025, às 12:24, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Leonardo de Souza Esteves**, **Usuário Externo**, em 08/07/2025, às 15:50, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Michele Nogueira Lima**, **Professora do Magistério Superior**, em 08/07/2025, às 17:17, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Sandra Regina Goulart Almeida**, **Reitora**, em 15/07/2025, às 17:06, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Jaime Arturo Ramírez**, **Usuário Externo**, em 21/08/2025, às 10:25, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4360489** e o código CRC **0373052C**.

Referência: Processo nº 23072.229064/2025-17 SEI nº 4360489

Criado por janainaoliveira, versão 2 por janainaoliveira em 07/07/2025 15:59:40.