MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

PLANO DE TRABALHO

1 – DADOS CADASTRAIS

PARTÍCIPE 1: SECRETARIA EXECUTIVA DO MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS PÚBLICOS

CNPJ: 00.489.828/0001-55

ENDEREÇO: Esplanada dos Ministérios, Bloco K - Bairro Zona Cívico-Administrativa

CIDADE/UF: Brasília/DF

CEP: 70.040-906

DDD/Fone: (61) 2020-4021

Esfera Administrativa: Federal

Nome do responsável: CRISTINA KIOMI MORI

Cargo: Secretária-Executiva

Nomeada pelo Decreto de 1º de janeiro de 2023, publicado na Edição 1-A/Seção 2 – Extra do Diário Oficial da União de 1º de janeiro de 2023.

PARTÍCIPE 2: SECRETARIA DE GOVERNO DIGITAL – SGD/MGI

CNPJ: 00.489.828/0074-00

ENDEREÇO: SEPN 516, Bloco D, lote 8, 1º andar

CIDADE/UF: Brasília/DF

CEP: 70.770-524

DDD/Fone: (61) 2020-2398

Esfera Administrativa: Federal

Nome do responsável: ROGERIO SOUZA MASCARENHAS

Cargo: Secretário de Governo Digital

Nomeado pela Portaria nº 1.092, de 23 de janeiro de 2023, publicada no Diário Oficial da União de 24 de janeiro de 2023.

PARTÍCIPE 3: MINISTÉRIO DO TRABALHO E EMPREGO - MTE

CNPJ: 37.115.367/0001-60

Endereço: Esplanada dos Ministérios, Bloco F - Bairro Zona Cívico-Administrativa

Cidade/UF: Brasília/DF

CEP: 70.056-900

DDD/Fone: (61) 2031-6439

Esfera Administrativa: Federal

Nome do responsável: FRANCISCO MACENA DA SILVA

Cargo/função: Secretário-Executivo
Nomeado pelo Decreto de 11 de janeiro de 2023, publicado no Diário Oficial da União de 11 de janeiro de 2023, Seção 2, Edição 8-A, Extra A.

2. IDENTIFICAÇÃO DO OBJETO

Título do Projeto de Transformação Digital: CyberGuard

Processo SEI-MGI nº: 14021.003219/2025-93

Início (mês/ano): Março/2025

Término (mês/ano): Setembro/2026

O projeto visa aumentar a maturidade da segurança da informação no Ministério do Trabalho e Emprego por meio da melhoria da gestão de incidentes de segurança e de vulnerabilidades, do aumento da confiança e segurança dos dados, do aumento da disponibilidade dos sistemas de Tecnologia da Informação e do aperfeiçoamento do monitoramento de falhas dos serviços, aplicações e sistemas.

3. DIAGNÓSTICO

Para viabilizar a execução das políticas públicas da Pasta do Trabalho e Emprego, o MTE possui um portfólio de sistemas hospedados em seu data center, bem como empresas públicas contratadas pelo órgão (DATAPREV e SERPRO). Os diversos serviços e sistemas de informação, de acesso via Internet e Intranet, atendem aos critérios de criticidade e visibilidade nacional, tais como:

- eSocial;
- Seguro Desemprego;
- Abono Salarial;
- FGTS Digital;
- Cadastro Geral de Empregados e Desempregados – CAGED;
- Relação Anual de Informações Sociais – RAIS;
- Cadastro Nacional de Entidades Sindicais – CNES;
- Mediador;
- Sistema Federal de Inspeção do Trabalho;
- Sistema de Serviço Especializado em Segurança e Medicina do Trabalho.

A preservação das informações trocadas no Ministério do Trabalho e Emprego tem direta relação com a respectiva segurança da informação e com a qualidade do ambiente de infraestrutura buscando garantir a confidencialidade, integridade e a disponibilidade das informações coorporativas. O MTE possui aproximadamente 27 superintendências e 89 gerências, totalizando 423 pontos de conectividade em todo o território nacional.

As estatísticas do CTIR Gov (Centro de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos de Governo) mostram um cenário preocupante no que diz respeito à segurança cibernética. Em 2023, o total de notificações de incidentes e vulnerabilidades atingiram 15.128 ocorrências, refletindo um aumento de 29,24% em relação ao ano anterior. Em 2024, os dados mostram um total de 8447 notificações, até agosto de 2024, com vazamentos de dados. Entre os incidentes mais críticos de 2024, vazamentos de dados se destacam com 3.701 registros, seguidos por vulnerabilidades em software (Denial Of Service, também conhecido com ataque de negação de serviço).

Esses números evidenciam a crescente sofisticação e frequência das ameaças, demonstrando a urgência em fortalecer as camadas de segurança do MTE. A proteção e responsabilidade do Ministério não é apenas uma questão de integridade institucional, mas também de garantir a privacidade e a segurança das informações pessoais do cidadão.
Proteger essas informações é essencial para manter a confiança pública nos serviços digitais oferecidos pelo MTE. Ao reduzir a exposição a vulnerabilidades e incidentes, o MTE assegura que os serviços públicos permaneçam disponíveis e resilientes, proporcionando ao cidadão um atendimento mais seguro, contínuo, implementação de medidas robustas de segurança cibernética é, portanto, vital para preservar os direitos dos cidadãos e a integridade dos serviços públicos.

4. ABRANGÊNCIA

O projeto será desenvolvido pelo Ministério do Trabalho e Emprego e terá como público-alvo:

- O próprio Ministério do Trabalho e Emprego (MTE), através de seus profissionais de Tecnologia da Informação;
- Usuários internos do MTE;
- Usuários externos;
- Prestadores de serviços;
- Fornecedores de tecnologia;
- Coordenação de Planejamento e empresas contratadas do MTE;
- Ministério da Gestão e Inovação em Serviços Públicos.

5. JUSTIFICATIVA

Diante da criação do Ministério do Trabalho e Emprego e da crescente demanda por modernização e segurança nos serviços digitais, é imperativo aprimorar a infraestrutura tecnológica e mitigar os riscos cibernéticos associados aos sistemas críticos da Pasta. O portfólio de sistemas do MTE, que salta relevância nacional, como eSocial, Seguro Desemprego, Abono Salarial e FGTS Digital, está diretamente ligado à execução de políticas públicas essenciais.

O aumento nas notificações de incidentes cibernéticos em 2023, conforme dados do CTIR Gov, é um cenário preocupante para a segurança da informação do MTE. Esses riscos não apenas ameaçam a confidencialidade, integridade e disponibilidade das informações como também comprometem a privacidade de dados pessoais de milhões de cidadãos.
Com 423 pontos de conectividade em todo o território nacional e a responsabilidade de gerenciar informações sensíveis em um contexto de ameaças cibernéticas sofisticadas, a modernização das camadas de segurança digital e o fortalecimento da infraestrutura tecnológica do MTE são cruciais para:

- Proteger a privacidade e os direitos dos cidadãos , assegurando a confiança nos serviços digitais;
- Garantir a continuidade e a resiliência dos serviços públicos, reduzindo a exposição a vulnerabilidades e os impactos de incidentes cibernéticos; e
- Aumentar a eficiência e a maturidade operacional do MTE, viabilizando a execução das políticas públicas com maior conformidade e segurança.

A implementação de medidas robustas de segurança cibernética é, portanto, essencial para a integridade institucional do MTE e para a proteção do cidadão refletindo em confiança no Governo e no atendimento ao público de forma eficiente.

6. OBJETIVOS GERAL E ESPECÍFICO

Objetivos Gerais:

- Aumentar a maturidade em segurança cibernética;
- Reduzir os incidentes de segurança graves;
- Melhorar o monitoramento do ambiente de Tecnologia da Informação do MTE;
- Elevar o nível de proteção no ambiente computacional do MTE .

Objetivos Específicos:

- Melhoria na prestação de serviços: unificação e simplificação do atendimento dos serviços digitais do MTE, gerando uma central que vai orientar o cidadão de forma eficiente.

- Acesso facilitado e desburocratizado: com a melhoria do atendimento dos serviços digitais os usuários terão um acesso mais ágil e seguro aos serviços da realização de procedimentos como admissões, comunicações de acidentes de trabalho, cadastros em programas de formação profissional e trabalhistas e previdenciárias.

- Promoção da transparência: a iniciativa contribuirá para uma maior transparência nas operações e serviços do MTE, possibilitando aos usuário o acompanhamento e controle sobre seus processos relacionados ao MTE, tais como a situação de requerimentos do Seguro-Desemprego, registro e atualizações cadastrais.

- Desenvolvimento econômico e social: ao assegurar um ambiente digital mais acessível e intuitivo, robusto, seguro e confiável, o projeto estimula emprego e o acesso a direitos trabalhistas e previdenciários, contribuindo para o desenvolvimento econômico e social do país, ao facilitar a interação entre empresas e governo.
- Economia de recursos públicos: a eficiência operacional e a redução de processos de atendimento ao público, bem como processos relacionados ao atendimento de forma integrada e sistematizada o que pode gerar significativamente economia de recursos públicos, evitando possíveis atendimentos presenciais, por exemplo, fluxo de atendimentos avulsos, além de otimizar o uso dos recursos tecnológicos disponíveis, tendo a possibilidade de unificar os processos.

7. METODOLOGIA DE INTERVENÇÃO

A Secretaria de Governo Digital atuará no projeto nas seguintes frentes:

- Participação do Secretário (ou substituto indicado) no Comitê Estratégico;

- Acompanhamento pela equipe de projetos do Programa Startup gov.br, para orientar e facilitar a atuação do Líder do projeto e monitorar o projeto nas reuniões de gestão;

- Fornecimento dos especialistas de tecnologia da informação, conforme perfis definidos no Acordo de Cooperação Técnica, para atuação no projeto.

O Ministério do Trabalho e Emprego atuará no projeto nas seguintes frentes:

- Disponibilização de equipe de negócio para identificação de processos e requisitos da solução;

- Disponibilização de equipe de técnicos para apoiar a atuação do projeto;

- Fornecimento de espaço físico e recursos para a atuação presencial da equipe do projeto;

- Disponibilização de todos os documentos, manuais técnicos e acessos a sistemas necessários à consecução do projeto;

- Atuação junto a fornecedores para viabilizar as integrações necessárias à solução;

- Interlocução com demais órgãos de Governo, nas três esferas, no que se fizer necessário.

8. UNIDADE RESPONSÁVEL E GESTOR DO ACORDO DE COOPERAÇÃO TÉCNICA

Comitê Estratégico do Projeto

Secretário de Governo Digital/MGI - ROGÉRIO SOUZA MASCARENHAS

Diretor de Tecnologia da Informação/MTE - HEBER FIALHO MAIA JUNIOR

Líder do projeto (Ministério do Trabalho e Emprego)

Nome: CARLOS ALBERTO JACOME MENEZES

Cargo: Chefe da Divisão de Segurança da Informação

Telefone: (61) 2031-4226

E-mail: [redacted]

Ponto Focal (Escritório de Projetos Secretaria de Governo Digital)

Nome: JACKELINE PAULA DE GODOI DEGANI

Cargo: Coordenadora-Geral de Projetos Estratégicos

Endereço: SEPN 516 Bloco D lote 8, 1º andar

Telefone: (61) 2020-2405

E-mail: [redacted]

Ponto Focal (Ministério do Trabalho e Emprego)

Nome: RAFAEL FREITAS REALE

Cargo: Professor Ensino Básico Técnico

Telefone: (61) 2021-6535

E-mail: [redacted]

9. RESULTADOS ESPERADOS

São esperados os seguintes resultados:

- Fortalecimento das camadas de segurança do MTE;
- Redução da exposição a vulnerabilidades e mitigar o impacto de incidentes;
- Assegurar que os serviços públicos permaneçam disponíveis;
- Implementação de medidas robustas de segurança cibernética.

10. PLANO DE AÇÃO

Ação	Responsável	Prazo	Situação
Planejamento de sanitização de Firewall	MTE	1º Trim 2025	Em planejamento
Planejamento de sanitização de contas do AD	MTE	1º Trim 2025	Em planejamento

Planejamento de implementação de MFA na VPN e SEI	MTE	1º Trim 2025	Em planejamento
Estudo para Melhoria na Segmentação de VLAN na SEDE	MTE	1º Trim 2025	Em planejamento
Desenvolvimento de Parecer Técnico para Melhoria dos Controles do PPSI	MTE	1º Trim 2025	Em planejamento
Estudo e Artefato de contratação de SOC – parte 1	MTE	1º Trim 2025	Em planejamento
Estudo e Artefato de contratação d GBIC´S para Firewall Palo Alto – parte 1	MTE	1º Trim 2025	Em planejamento
Relatório de Auditoria para Desativação de Estações Windows 7	MTE	1º Trim 2025	Em planejamento
Estudo para habilitar UAC em todas as estações.	MTE	1º Trim 2025	Em planejamento
Ciclo 1 de Auditoria do AD	MTE	2º Trim 2025	Em planejamento
Implementação de MFA para usuários SEI e VPN	MTE	2º Trim 2025	Em planejamento
Planejamento de Melhoria de VLAN na Sede	MTE	2º Trim 2025	Em planejamento
Estudo de Melhorias Práticas de ETIR + Proposta de POP	MTE	2º Trim 2025	Em planejamento
Estudo e artefato de contratação – parte 2	MTE	2º Trim 2025	Em planejamento
Estudo e artefato para contratação de GBIC ´S para Firewall PALO ALTO – parte 2	MTE	2º Trim 2025	Em planejamento
Organização de Campanha de Comunicação	MTE	2º Trim 2025	Em planejamento
Acompanhamento da Desativação de Estações Windows 7	MTE	2º Trim 2025	Em planejamento
Estudo para desativação do Protocolo SMBV1	MTE	2º Trim 2025	Em planejamento
Revisão de 3 Normas	MTE	3º Trim 2025	Em planejamento
Ciclo 1 de Auditoria de Firewall	MTE	3º Trim 2025	Em planejamento
Planejamento de Sanitização e			

Reorganização de Contas de VPN	MTE	3º Trim 2025	Em planejamento
Projeto de Implementação de VLAN Sede	MTE	3º Trim 2025	Em planejamento
Ciclo 1 de auditoria dos Processos ETIR	MTE	3º Trim 2025	Em planejamento
Estudo e Artefato de Contratação SOC – parte 3	MTE	3º Trim 2025	Em planejamento
Estudo e Artefato para contratação de GBIC´S para FirewallPALO ALTO – parte 3	MTE	3º Trim 2025	Em planejamento
Plano para atualização de 50% das estações para Windows11 – CICLO 1	MTE	3º Trim 2025	Em planejamento
Relatório 1 de auditoria na instalação de antimalware em estações e servidores	MTE	3º Trim 2025	Em planejamento
Revisão de 3 normas – Parte2	MTE	4º Trim 2025	Em planejamento
Ciclo 2 de auditoria do AD	MTE	4º Trim 2025	Em planejamento
Ciclo 2 de auditoria de VPN	MTE	4º Trim 2025	Em planejamento
Estudo para melhoria na segmentação de VLAN nas regionais	MTE	4º Trim 2025	Em planejamento
CICLO 2 de auditoria dos processos ETIR + estudo de melhoria no processo	MTE	4º Trim 2025	Em planejamento
Estudo e artefato de contratação SOC – parte 4	MTE	4º Trim 2025	Em planejamento
POP de atualização e correção de patches em virtualizadores + servidores	MTE	4º Trim 2025	Em planejamento
Relatório 2 de auditoria na instalação de antimalware em estações e servidores	MTE	4º Trim 2025	Em planejamento
Organização de palestra e conscientização	MTE	4º Trim 2025	Em planejamento
Revisão de 3 procedimentos operacionais	MTE	1º Trim 2026	Em planejamento
Ciclo 2 de auditoria de Firewall	MTE	1º Trim 2026	Em planejamento

Pop com as melhores práticas aprendidas da sanitização das contas de AD	MTE	1º Trim 2026	Em planejamento
Ciclo 2 de auditoria de VPN	MTE	1º Trim 2026	Em planejamento
Planejamento de melhoria de VLAN nas regionais	MTE	1º Trim 2026	Em planejamento
BI de monitoramento das métricas do PPSI	MTE	1º Trim 2026	Em planejamento
POP de atualização e correção de patches em servidores + estações	MTE	1º Trim 2026	Em planejamento
Plano para atualização de 50% das estações para Windows 11 – Ciclo 2	MTE	1º Trim 2026	Em planejamento
Relatório 3 de auditoria na instalação de antimalware em estações e servidores	MTE	1º Trim 2026	Em planejamento
Revisão de 3 procedimentos operacionais – Parte 2	MTE	2º Trim 2026	Em planejamento
POP com as melhores práticas aprendidas da sanitização do firewall	MTE	2º Trim 2026	Em planejamento
Pop com as melhores práticas aprendidas da sanitização de contas de VPN	MTE	2º Trim 2026	Em planejamento
Projeto de implementação de VLAN nas regionais	MTE	2º Trim 2026	Em planejamento
Parecer técnico de ações para melhoria nos índices do PPSI	MTE	2º Trim 2026	Em planejamento
POP com as melhores práticas aprendidas quanto da conformidade na instalação de antimalware em servidores e estações.	MTE	2º Trim 2026	Em planejamento
Organização de curso	MTE	2º Trim 2026	Em planejamento
Relatório de auditoria da desabilitação do protocolo SMBv1	MTE	2º Trim 2026	Em planejamento
Relatório de auditoria da ativação do UAC em todas as estações.	MTE	2º Trim 2026	Em planejamento

11 – EQUIPE NECESSÁRIA

DETALHAMENTO DA EQUIPE

Perfil	Quantitativo	Órgão de Origem
Especialista em Gestão de Projetos	1	Squad-SGD
Especialista em infraestrutura	2	Squad-SGD
Especialista em Segurança da Informação	3	Squad-SGD
TOTAL	6	

12 - RISCOS

Neste projeto foram identificados eventuais riscos, dentre os quais destacam-se:

DETALHAMENTO DE RISCOS

Risco	Probabilidade de ocorrer	Gravidade
Falta de pessoal qualificado	Alta	Alta
Resistência à mudança por parte dos usuários	Média	Alta
Dependência de fornecedores externos	Alta	Média
Incidentes de segurança durante a fase de implementação	Média	Alta
Dificuldade na adaptação de sistemas legados ao novo ambiente	Alta	Alta
Interrupções nos serviços durante a migração e implementação	Média	Alta

Com o intuito de dirimir os riscos aqui identificados, foram definidos a metodologia de intervenção, a estratégia de gerenciamento e o monitoramento do projeto, incluindo-se a mensuração de indicadores.

13 - ESTRATÉGIA DE MONITORAMENTO

O monitoramento do projeto se dará por meio da disponibilização e acompanhamento de informações em meio eletrônico e complementadas por reuniões presenciais ou virtuais de acompanhamento, abrangendo o que segue:

- Preenchimento de informações semanais sobre o andamento do projeto;

- Pontos de controle quinzenais entre líderes do projeto, gerente do escritório de projetos ágeis da Secretaria de Governo Digital e pontos focais dos órgãos parceiros;

- Reuniões mensais do Comitê Estratégico do Plano, ou conforme a periodicidade julgada mais adequada pelos partícipes diante do cronograma de entregas pactuado.

No âmbito do Ministério do Trabalho e Emprego:

- Alimentação periódica de informações em sistema próprio (MS Project, por exemplo);

- Pontos de controle semanais (técnicos) entre a equipe do projeto;

- Pontos de controle quinzenais (gerenciais) com a equipe do projeto e o Gerente de Projetos;

- Avaliação da evolução dos indicadores de desempenho, resultado e impacto:

Indicadores	Fórmula do cálculo	Periodicidade
De Desempenho		
Execução do projeto	Total de entregas realizadas (ER) / total de entregas previstas (EP)	Mensal
Entregas realizadas no prazo	Total de entregas realizadas no prazo(ERP) /total de entregas realizadas (ER)	Mensal
De Resultado		
Normativos publicados	(qtd de normativos publicados x 100) / (qtd de normativos propostos)	Anual
Procedimentos operacionais publicados	(qtd de procedimentos publicados x 100) / (qtd de procedimentos propostos)	Anual
De Impacto		
Melhoria da Segurança da Informação nos Servidores de Rede	qtddvc x 100) / qtdvd	Trimestral
Conscientização dos colaboradores da importância da Segurança da Informação	qtdcolt x 100) / qtdcolpt	Anual

Os valores das metas previstas e as fórmulas de cálculos podem ser alterados no decorrer do projeto.
A correção de vulnerabilidades de servidores que são máquinas responsáveis por prover serviços na Instituição, está ligada diretamente a disponibilidade dos serviços prestados ao cidadão.
Dados da DFTI - POC-ASRM-trend-relatorio_V2_windows 1.xlsx (sharepoint.com)
* qtdvd = qtd de SERVIDORES com vulnerabilidades detectados até a data de início do projeto CyberGuard
* qtdvc = qtd de SERVIDORES com vulnerabilidades corrigidas após o término do projeto CyberGuard
* qtdcolpt = qtd de COLABORADORES previstos para treinamento até a data de início do CyberGuard
* qtdcolt = qtd de COLABORADORES treinados após o término do projeto CyberGuard

CRISTINA KIOMI MORI

Secretária-Executiva

Ministério da Gestão e da Inovação em Serviços Públicos

FRANCISCO MACENA DA SILVA

Secretário-Executivo

Ministério do Trabalho e Emprego

ROGÉRIO SOUZA MASCARENHAS

Secretário de Governo Digital

Ministério da Gestão e da Inovação em Serviços Públicos

Documento assinado eletronicamente por **Rogerio Souza Mascarenhas**, **Secretário(a)**, em 07/03/2025, às 18:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Francisco Macena da Silva**, **Usuário Externo**, em 11/03/2025, às 19:08, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cristina Kiomi Mori**, **Secretário(a) Executivo(a)**, em 18/03/2025, às 18:26, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **49082207** e o código CRC **50CDF92C**.

Referência: Processo nº 14021.003219/2025-93. SEI nº 49082207