



PLANO DE TRABALHO

1. DADOS CADASTRAIS

PARTÍCIPE 1: SECRETARIA-EXECUTIVA DO MINISTÉRIO DA GESTÃO E DA 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: CILAIR RODRIGUES DE ABREU

Cargo: Secretário-Executivo

Nomeado pelo Decreto de 6 de janeiro de 2026, publicado na Seção 2 do Diário Oficial da União de 7 de janeiro de 2026.

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: ROGÉRIO 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

Processo SEI-MTE nº: 19958.243935/2024-83

Início: 18 de setembro de 2026

Término: 18 de março de 2028

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 TI e do aperfeiçoamento do monitoramento de falhas dos serviços, aplicações e sistemas.

3. DIAGNÓSTICO

A Medida Provisória nº 1.058, publicada em 27 de julho de 2021, convertida na Lei nº 14.261, de 16 de dezembro de 2021, criou o Ministério do Trabalho e Previdência - MTP. Após as eleições presidenciais de 2022, em 1º de janeiro de 2023, ocorreu a divisão ministerial do MTP em (1) Ministério do Trabalho e Emprego - MTE e (2) Ministério da Previdência Social - MPS. O MTE foi estruturado pelo Decreto nº 11.779, de 13 de novembro de 2023, e é integrante da Administração Pública Federal direta. Diante dos desafios impostos pela limitada capacidade operacional do quadro de pessoal do MTE para gerir e monitorar múltiplos projetos críticos simultaneamente, a necessidade de fortalecer a maturidade e conformidade de atendimento dos serviços digitais tornou-se evidente.

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 em *data centers* de empresas públicas contratadas pelo órgão (DATAPREV e SERPRO). Os diversos serviços e sistemas de informação, de acesso via Internet e Intranet, atendem aos programas de alta 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 MTE tem direta relação com a respectiva segurança da informação e com a qualidade do ambiente de infraestrutura associado, que deve garantir a

confidencialidade, integridade e a disponibilidade das informações corporativas. O MTE possui aproximadamente 27 superintendências, 89 gerências e 307 agências 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), acessível em <https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros>, mostra um cenário preocupante no que diz respeito à segurança cibernética. Em 2023, o total de notificações de incidentes e vulnerabilidades atingiu seu pico com 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 19/08/2024, com destaque para vazamentos de dados. Entre os incidentes mais críticos de 2024, vazamentos de dados se destacam, com 3.701 registros, seguidos por vulnerabilidades em *softwares* e ataques DDoS - *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 dos dados sob a responsabilidade do Ministério não é apenas uma questão de integridade institucional, mas também de garantir a privacidade e a segurança das informações pessoais e sensíveis dos cidadãos.

Proteger essas informações é essencial para manter a confiança pública nos serviços digitais oferecidos pelo MTE. Ao reduzir a exposição a vulnerabilidades e mitigar o impacto de incidentes, o MTE assegura que os serviços públicos permaneçam disponíveis e resilientes, proporcionando ao cidadão um atendimento mais seguro, contínuo e eficiente. A 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 tem como público-alvo:

- O próprio Ministério do Trabalho e Emprego – MTE, por meio de seus profissionais de TI;
- Usuários internos do MTE;
- Usuários externos;
- Prestadores de serviços;
- Fornecedores de tecnologia;
- Coordenação de Planejamento e empresas contratadas do MTE; e
- Ministério da Gestão e da Inovação em Serviços Públicos – MGI.

5. JUSTIFICATIVA

O CyberGuard está alinhado aos objetivos estratégicos do MTE ao fortalecer a proteção dos ativos de informação, apoiar a transformação digital segura, promover a continuidade dos serviços prestados à sociedade, ampliar a capacidade institucional de gestão de riscos cibernéticos e fornecer subsídios para uma governança baseada em indicadores e evidências. Dessa forma, o projeto contribui diretamente para a confiabilidade, disponibilidade e integridade dos serviços digitais e das informações sob responsabilidade do Ministério.

Com a prorrogação da execução do projeto Cyberguard, o objetivo é contribuir de forma significativa para o aumento da maturidade de Segurança da Informação do Ministério do Trabalho e Emprego ao atuar como impulsionador para evolução da política, normas, processos, projetos, controles, monitoramento e governança de segurança.

O projeto tem como fundamento os controles de segurança da informação estabelecidos no

Programa de Privacidade e Segurança da Informação - PPSI e nas ações de continuidade e evolução das iniciativas estratégicas estabelecidas no âmbito do Projeto CyberGuard, em colaboração com o Programa Startup gov.br e o Ministério da Gestão e da Inovação em Serviços Públicos - MGI.

Embora o Projeto CyberGuard tenha proporcionado avanços significativos na estruturação da Segurança da Informação do Ministério, com a implantação de controles, processos e melhorias relevantes na proteção do ambiente tecnológico, a evolução constante do cenário de ameaças cibernéticas torna imprescindível a continuidade dessa iniciativa. O surgimento contínuo de novas técnicas de ataque, o aumento da sofisticação de agentes maliciosos, a ampliação da superfície de exposição decorrente da transformação digital e a necessidade de atendimento a novos requisitos regulatórios exigem um processo permanente de evolução dos mecanismos de defesa.

Ao longo da execução do projeto, foram identificadas diversas fragilidades relevantes no ambiente tecnológico e de segurança da informação, evidenciando a necessidade de evolução da maturidade dos controles, processos e mecanismos de proteção institucional. Entre os principais apontamentos, destacam-se:

- elevado volume de credenciais expostas ou potencialmente comprometidas;
- fragilidades no ambiente de *Active Directory* - AD;
- exposição e comprometimento de credenciais e acessos relacionados à VPN;
- necessidade de fortalecimento do gerenciamento de identidades e acessos - IAM;
- necessidade de evolução dos mecanismos de autenticação; ausência ou insuficiência de padronização de processos e serviços de TI e Segurança da Informação;
- elevada dependência operacional de terceiros, necessidade de aprimoramento da gestão de ativos tecnológicos;
- necessidade de fortalecimento do gerenciamento de vulnerabilidades e correções;
- necessidade de melhoria na gestão e resposta a incidentes de segurança;
- necessidade de maior integração entre processos de infraestrutura, segurança, gestão de identidades, ativos, vulnerabilidades e incidentes;
- necessidade de formalização e documentação dos processos críticos.

Nesse contexto, a continuidade do projeto representa uma medida estratégica para assegurar que os controles de segurança permaneçam atualizados e eficazes diante das novas ameaças, evitando que os resultados já alcançados sejam comprometidos pela obsolescência tecnológica ou pela ausência de evolução dos processos de segurança.

Além disso, o Ministério do Trabalho e Emprego é responsável pelo tratamento de informações institucionais críticas e de um elevado volume de dados pessoais de cidadãos, empresas e servidores públicos. A proteção desses ativos informacionais constitui um desafio permanente e uma responsabilidade institucional, exigindo investimentos contínuos em prevenção, detecção, resposta e recuperação diante de incidentes cibernéticos.

Dessa forma, a continuidade do Projeto CyberGuard contribuirá para fortalecer a capacidade do MTE em proteger seus dados e serviços digitais, reduzir riscos operacionais, preservar a disponibilidade, integridade e confidencialidade das informações, assegurar a continuidade dos serviços públicos prestados à sociedade e aumentar a confiança dos cidadãos na capacidade do Ministério de proteger as informações sob sua responsabilidade.

6. OBJETIVOS GERAL E ESPECÍFICO

Objetivo Geral:

Contribuir de forma significativa para o aumento da maturidade de Segurança da Informação do Ministério do Trabalho e Emprego ao atuar como impulsionador para evolução da política, normas, processos, projetos, controles, monitoramento e governança de segurança.

Objetivos Específicos:

- Realizar estudo para projetar a identificação e implementação de mecanismos de Gestão de Identidades e Acessos - IAM, Autenticação Multifator - MFA e Gestão de Acessos Privilegiados - PAM no Ministério para fortalecer o controle sobre as identidades, credenciais e privilégios utilizados para acesso aos sistemas e ativos institucionais;
- Projetar a segmentação do *Active Directory* - AD, *baselines* de segurança e um processo formal de homologação de *softwares* fortalece a arquitetura de segurança do Ministério, reduzindo a superfície de ataque e limitando os impactos decorrentes de eventuais comprometimentos;
- Apoiar a estruturação e o fortalecimento da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETIR para garantir uma atuação institucional rápida, coordenada, padronizada e assertiva diante de incidentes cibernéticos. A crescente complexidade das ameaças e a necessidade de preservar a continuidade dos serviços públicos exigem que a resposta a incidentes deixe de depender exclusivamente de ações manuais e reativas, evoluindo para um modelo baseado em processos formalizados, automação, monitoramento contínuo, inteligência e tomada de decisão orientada por evidências;
- Realizar um estudo e desenvolver um projeto para a implementação de uma Gestão Institucional de Ativos de Tecnologia da Informação visando garantir visibilidade, controle e governança sobre todos os recursos tecnológicos utilizados pelo Ministério. Um inventário atualizado e confiável permite identificar estações de trabalho, servidores, equipamentos de rede, dispositivos, sistemas, softwares e demais ativos, bem como seus responsáveis, localização, características, status e nível de criticidade;
- Realizar estudo de uma Gestão Institucional de Proteção de Dados é fundamental para garantir que as informações tratadas pelo Ministério sejam coletadas, utilizadas, armazenadas, compartilhadas e descartadas de forma segura, controlada e alinhada às necessidades institucionais e aos requisitos legais aplicáveis;
- Desenvolver o Programa de Gestão Contínua de Vulnerabilidades para fortalecer a capacidade interna do Ministério de identificar e tratar, de forma antecipada e sistemática, as fragilidades existentes em seu ambiente tecnológico. Uma infraestrutura continuamente avaliada e protegida reduz a superfície de ataque e diminui substancialmente a probabilidade de incidentes;
- Desenvolver o Programa de Gestão e Monitoramento de Registros de Auditoria, abrangendo os sistemas, *firewalls* e *Active Directory* do Ministério, com o objetivo de estabelecer uma capacidade institucional de rastreabilidade, monitoramento e análise contínua das atividades realizadas no ambiente tecnológico.

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;
- Oferta dos serviços de pesquisa e *design* de experiência do usuário, por meio do Laboratório de Qualidade de Serviços Públicos - LabQ, voltados para melhorias centradas no cidadão. As atividades são focadas no diagnóstico de problemas, sugestões de melhorias e no (re)desenho do produto/serviço, com base na análise das características e necessidades do 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 da startup;
- 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 do MGI - ROGÉRIO SOUZA MASCARENHAS

Diretor de Tecnologia da Informação do MTE – HEBER MAIA FIALHO JUNIOR

Líder do projeto no MTE:

Nome: Juliana Rocha Munita Moreira

Cargo: Coordenadora-Geral de Segurança da Informação

Telefone: (61) 2031-4619

E-mail: juliana.munita@trabalho.gov.br

Ponto Focal (Escritório de Projetos Secretaria de Governo Digital)

Nome: Jackeline Paula de Godoi Degani

Cargo: Coordenadora-Geral de Projetos Estratégicos

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

Telefone: (61) 2020-2405

E-mail: jackeline.degani@gestao.gov.br

Ponto Focal no MTE (pessoa que manterá contato constante com a SGD)

Nome: Ismael Rodrigues Pereira Junior

Cargo: Chefe de Divisão de Segurança da Informação

Telefone: (61) 2021-6535

E-mail: ismael.junior@trabalho.gov.br

9. RESULTADOS ESPERADOS

O CyberGuard pode ser apresentado como um instrumento de apoio direto ao alcance dos objetivos estratégicos do MTE, especialmente aqueles relacionados à transformação digital, continuidade dos serviços públicos, proteção de dados e fortalecimento da governança

institucional, correlacionando-se a:

Fortalecimento da transformação digital do MTE, pois o Ministério depende cada vez mais de serviços digitais para atender trabalhadores, empregadores e cidadãos. O CyberGuard tem como objetivo aumentar a maturidade da segurança desses serviços ao identificar vulnerabilidades, monitorar ameaças e reduzir riscos operacionais, criando um ambiente mais confiável para a transformação digital.

Garantia da continuidade dos serviços públicos Sistemas críticos como os relacionados ao emprego, relações do trabalho, inspeção do trabalho e gestão administrativa precisam permanecer disponíveis e íntegros. O CyberGuard contribui para a prevenção de incidentes cibernéticos que possam causar interrupções ou indisponibilidade dos serviços.

Aprimoramento da governança e da gestão institucional. O projeto fornece indicadores, métricas e informações consolidadas sobre riscos, vulnerabilidades e conformidade, apoiando a tomada de decisão da alta administração e fortalecendo a governança de Segurança da Informação.

Proteção de dados e conformidade regulatória. O MTE trata grandes volumes de informações institucionais e dados pessoais. O CyberGuard auxilia na implementação de controles de segurança, contribuindo para a conformidade com a LGPD, normativos do GSI/PR, requisitos do TCU e demais diretrizes aplicáveis à Administração Pública Federal.

Gestão baseada em riscos. O projeto permite que o MTE priorize ações de segurança de acordo com o impacto e a criticidade dos ativos institucionais, direcionando recursos para os riscos mais relevantes e aumentando a eficiência dos investimentos em segurança.

Desenvolvimento da resiliência cibernética Além de identificar vulnerabilidades, o CyberGuard fortalece a capacidade de detecção, resposta e recuperação diante de incidentes, elevando o nível de resiliência institucional e reduzindo impactos sobre a missão do órgão.

10. PLANO DE AÇÃO

Área de Interesse	Macro Entrega	Micro Entrega	Prazo estimado
9.1. Controle de Acesso e Gerenciamento de Identidades	Política de Senhas	Elaborar documento de boas práticas para criação, utilização e gestão de senhas no Ministério.	MÊS 1
	Matriz de perfis de acesso	Elaborar documento contendo uma matriz de todos os perfis de acesso de contas privilegiadas.	MÊS 3
	MFA – <i>Multi-Factor Authentication</i> em todos os sistemas críticos	Elaborar documento com um estudo preliminar.	MÊS 8 e MÊS 9
		Realizar levantamento, documentando todos os sistemas críticos identificando a possibilidade de implantação de MFA.	MÊS 10, MÊS 11 e MÊS 12
		Elaborar planejamento dos processos de implementação de MFA.	MÊS 10, MÊS 11 e MÊS 12
		Elaborar documento de Procedimento Operacional Padrão com as melhores práticas aprendidas.	MÊS 16
	Gerenciamento de Acessos Privilegiados - PAM integrada à VPN e solução de Jump Server	Elaborar documento com um estudo preliminar.	MÊS 1 e MÊS 2
		Elaborar planejamento dos processos de implementação.	MÊS 3 e MÊS 4

		Elaborar documento de Procedimento Operacional Padrão com as melhores práticas aprendidas.	MÊS 13
9.2. Gestão de infraestrutura de rede	Segmentação do <i>Active Directory</i> - AD	Elaborar documento com um estudo preliminar.	MÊS 1 e MÊS 2
		Elaborar planejamento dos processos de implementação de segmentação.	MÊS 3, MÊS 4 e MÊS 5
		Elaborar documento de Procedimento Operacional Padrão com as melhores práticas aprendidas.	MÊS 16
	Configuração segura de ativos institucionais e soluções de <i>software</i>	Elaborar documento para definição e padronização de <i>baselines</i> de segurança para ativos de TI do Ministério.	MÊS 8
		Elaboração de documento técnico para estabelecer critérios e procedimentos de classificação, avaliação de riscos, análise de segurança e homologação dos <i>softwares</i> utilizados no âmbito do Ministério.	MÊS 10
9.3. Gestão de Incidentes	Continuidade do projeto ETIR – Equipe de Prevenção, Tratamento e Resposta a Incidentes	Estudo para melhoria nos processos de tratamento e resposta de incidentes.	MÊS 5 e MÊS 6
		Estudo para automatização dos tratamentos de incidentes.	MÊS 6 e MÊS 7
		Estudo para melhoria no processo de tratamento de credenciais vazadas.	MÊS 8 e MÊS 9
		Elaborar documento de Procedimento Operacional Padrão com as melhores práticas aprendidas.	MÊS 15
		Elaborar documento de análise dos resultados dos testes de intrusão (<i>Pentests</i>) realizados pela empresa terceirizada, no contexto das atividades da ETIR.	MÊS 7
9.4. Gestão de Ativos	Inventário dos Ativos de Informação	Estudo para implantação de solução independente e gratuita para gestão de ativos e <i>softwares</i> .	MÊS 2
9.5. Gestão de Proteção de Dados	Proteção de Dados	Estudo para procedimentos de <i>hardening</i> no Ministério.	MÊS 13
		Elaborar documento de políticas e procedimentos para descarte seguro de dados e informações.	MÊS 14
		Elaborar documento política e diretrizes para implementação e aplicação de DLP (<i>Data Loss Prevention</i>).	MÊS 14 e MÊS 15
9.6. Gestão contínua de vulnerabilidades de segurança	Vulnerabilidades de segurança	Elaborar um documento contendo um Programa de Gestão Contínua de Vulnerabilidades de Segurança.	MÊS 5
		Elaborar um projeto de implantação de Gestão Contínua de Vulnerabilidades de Segurança.	MÊS 6
		Elaborar documento de Procedimento Operacional Padrão com as melhores práticas aprendidas.	MÊS 14

9.7. Gestão e monitoramento de registros de auditoria	Monitoramento de registros de auditoria	Elaborar um documento contendo um Programa de Gestão e Monitoramento de Registros de Auditoria para os sistemas, <i>firewall</i> e <i>Active Directory</i> do Ministério.	MÊS 7
		Elaborar um projeto de implantação de Gestão e Monitoramento de Registros de Auditoria para os sistemas, <i>firewall</i> e <i>Active Directory</i> do Ministério.	MÊS 11
		Elaborar documento de Procedimento Operacional Padrão com as melhores práticas aprendidas.	MÊS 17

11. EQUIPE NECESSÁRIA

DETALHAMENTO DA EQUIPE

Perfil	Quantitativo	Órgão de origem
<i>Especialista em Gestão de Projetos</i>	1	Equipe SGD
<i>Especialista em infraestrutura</i>	4	Equipe SGD
<i>Especialista em Segurança da Informação e Proteção de Dados</i>	5	Equipe SGD
Total	10	

12. RISCOS

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

DETALHAMENTO DE RISCOS

Risco	Probabilidade	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 sobre o andamento do projeto;
- Pontos de controle entre líderes do projeto, gerente do escritório de projetos ágeis da Secretaria de Governo Digital e pontos focais dos órgãos parceiros;
- Reuniões do Comitê Estratégico do Plano, 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 (técnicos) entre a equipe do projeto;
- Pontos de controle (gerenciais) com a equipe do projeto e o Gerente de Projetos;
- Avaliação da evolução dos indicadores de desempenho, resultado e impacto:

Indicador Macro Entregas	Fórmula / Cálculo	Unidade de Medida	Meta * (em 18 meses)
Política de Senhas	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Matriz de perfis de acesso	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
MFA – <i>Multi-Factor Authentication</i> em todos os sistemas críticos	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Gerenciamento de Acessos Privilegiados - PAM integrada à VPN e solução de <i>Jump Server</i>	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Segmentação do <i>Active Directory</i> - AD	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Configuração segura de ativos institucionais e soluções de <i>software</i>	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Continuidade do projeto ETIR – Equipe de Prevenção, Tratamento e Resposta a Incidentes	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Inventário dos Ativos de Informação	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Proteção de Dados	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %

Vulnerabilidades de segurança	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %
Monitoramento de registros de auditoria	(qtd micro entrega realizada x 100) / qtd micro entrega programada	Percentual (%)	100 %

Aprova-se o presente Plano de Trabalho.

CILAIR RODRIGUES DE ABREU

Secretário-Executivo

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 **Francisco Macena da Silva, Usuário Externo**, em 17/09/2026, às 12:01, 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 **Adauto Modesto Junior, Secretário(a) Executivo(a) Adjunto(a)**, em 17/09/2026, às 16:14, 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 **Rogério Souza Mascarenhas, Secretário(a)**, em 17/09/2026, às 22:11, 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://colaboragov.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **64482688** e o código CRC **A6CD2060**.

Referência: Processo nº 14021.003219/2025-93.

SEI nº 64482688