TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Ata de Reunião Nº 12 - TRE/PRESI/DG/STI

ATA DE REUNIÃO DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO

IDENTIFICAÇÃO DA REUNIÃO

Data	Horário		Local	Coordenador da Reunião
05/06/2023	10:00h	11:40h	Videoconferência	Anderson Lima

PAUTA

1. Encontro de STI de 30 e 31 de maio de 2023;
2. Acompanhamento do Plano de Capacitação de Tecnologia da Informação - PAC de TI;
3. Transformação Digital;
4. Análise do Manual do Processo de Gestão de Segurança da Informação.

PARTICIPANTES

Nome	Unidade
Anderson Cavalcanti de Lima	GABSTI
Ana Caroline Carvalho Portela	GABSTI
Nadja Marcela Melo Silva Santiago	COSUT
Jairo Mendes Soares Martins	SEGSIE
Etevaldo Cândido Custódio	SEAU
Márcio Igo Carvalho Ribeiro Gonçalves	COELEI
Francisco Diógenes Façanha Pires	SELOGI
Rosemberg Maia Gomes	CODIN
Carlos Alberto Ribeiro do Nascimento Júnior	SEINF
Paulo das Neves e Silva Junior	SEDESC
Antônio Manoel Silveira de Sousa	NSEGI
Leonardo Saraiva e Silva	NSCIB

APRESENTAÇÃO

Discussão	Decisão / Pendência	Responsável	Data Limite
Abertura	Recepcionados os presentes, o Secretário apresentou a pauta da reunião.	Anderson Lima	Não se aplica
Encontro de STI de 30 e 31 de maio de 2023	Apresentação dos principais tópicos abordados no Encontro de Secretários de TI, ocorrido nos dias 30 e 31 de maio de 2023.	Anderson Lima	Não se aplica
	Diante da relevância e da grande quantidade de temas, o Comitê deliberou pelo agendamento de reunião exclusiva pra tratar dessa pauta.	Membros do Comitê	Não se aplica
Plano de Capacitação de Tecnologia da Informação - PAC de TI	Apresentação da execução do orçamento destinado ao PAC de TI 2023, conforme apresentação de slides 0001849545. Exibição dos painéis disponibilizados pela Alura, que permitem o acompanhamento dos treinamentos realizados pelos servidores na plataforma.	Anderson Lima	Não se aplica
Transformação Digital	Apresentação dos ajustes no cronograma de execução do Plano de Transformação Digital, de acordo com evento SEI 0001849545.	Anderson Lima	Não se aplica
Manual do Processo de Gestão de Segurança da Informação	Apresentação da minuta do Manual do Processo de Gestão de Segurança da Informação, evento 0001849896.	Antônio Manoel	Não se aplica
	O Comitê deliberou pela realização de ajustes no Manual, que deverá ser aprovado na próxima reunião do CGTI.	Membros do Comitê	Não se aplica

Discussão	Decisão / Pendência	Responsável	Data Limite
Outras Informações	Como parte integrante dessa ata, segue a apresentação utilizada na reunião, evento 0001849545 e o Manual do Processo de Gestão de Segurança da Informação, evento 0001849896.	Anderson Lima	Não se aplica
	Não havendo outros assuntos a serem tratados, o Secretário de Tecnologia da Informação agradeceu aos presentes e finalizou a reunião.	Anderson Lima	Não se aplica

ASSINATURA DOS MEMBROS DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO

Nome	Unidade	Assinatura
Anderson Cavalcanti de Lima	GABSTI	Assinatura Eletrônica
Rosemberg Maia Gomes	CODIN	Assinatura Eletrônica
Márcio Igo Carvalho Ribeiro Gonçalves	COELEI	Assinatura Eletrônica
Nadja Marcela Melo Silva Santiago	COSUT	Assinatura Eletrônica
Ana Caroline Carvalho Portela	GABSTI	Assinatura Eletrônica

Em 05 de junho de 2023.

Documento assinado eletronicamente por **Anderson Cavalcanti de Lima**, **Secretário de Tecnologia da Informação**, em 13/06/2023, às 12:05, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Rosemberg Maia Gomes**, **Coordenador de Desenvolvimento e Infraestrutura**, em 14/06/2023, às 09:29, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Nadja Marcela Melo Silva Santiago**, **Coordenador(a) de Suporte Técnico**, em 14/06/2023, às 10:03, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Ana Caroline Carvalho Portela**, **Técnico Judiciário**, em 20/06/2023, às 09:55, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Márcio Igo Carvalho Ribeiro Gonçalves**, **Coordenador(a), em exercício**, em 20/06/2023, às 10:10, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0001847373** e o código CRC **C751698B**.

--

Comitê Gestor de Tecnologia da Informação

Reunião Ordinária – SEI nº 0007697-21.2023.6.18.8000

05 de junho de 2023

Tribunal Regional Eleitoral
do Piauí

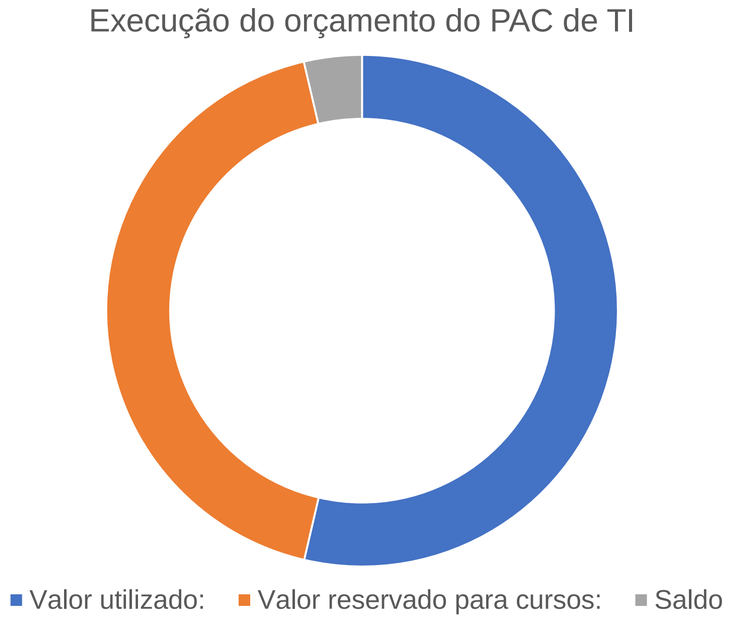
Pauta

TRE-PI

1. Plano de Capacitação de Tecnologia da Informação - PAC de TI
2. Transformação Digital
3. Análise do Manual do Processo de Gestão de Segurança da Informação

Acompanhamento do Plano de Capacitação de TI

- Valor Aprovado PAC: 180.000,00
- Valor utilizado: 96.538,20
- Valor reservado para cursos: 76.880,00
- Saldo R$ 6.581,80



Acompanhamento do Plano de Capacitação de TI

TRE-PI

Pontos Relevantes

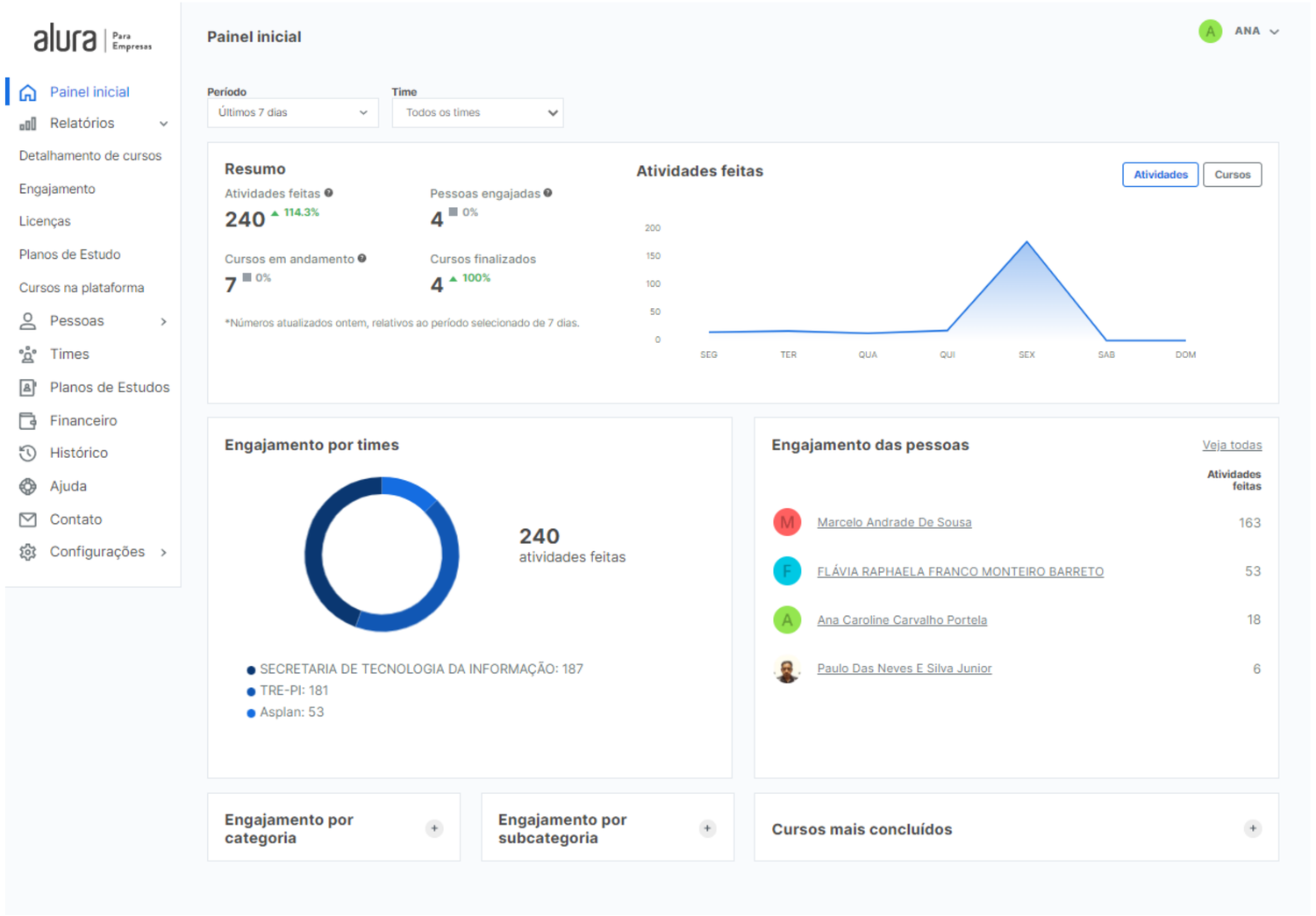
- Adiamento de abertura de turma para o treinamento “Aperfeiçoando a Gestão de TI no Poder Judiciário” para o período de **12 a 15.09.2023.**
- Valor previsto R$ 10.600,00
- Substituir a demanda por outro curso
- Melhorias na gestão dos treinamentos realizados pela plataforma da Alura.

Acompanhamento do Plano de Capacitação de TI

TRE-PI

Painel da Alura

- Acompanhamento dos cursos em realização pelas equipes



Transformação Digital

TRE-PI

Contextualização

- O Plano de Transformação Digital (PTD) é uma exigência da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário 2021-2026 (ENTIC-JUD) – Resolução CNJ nº 370/2021
- Instituído pela Portaria TRE-PI nº 903/2022

Transformação Digital

Transformação Digital dos Serviços

Transformação Digital

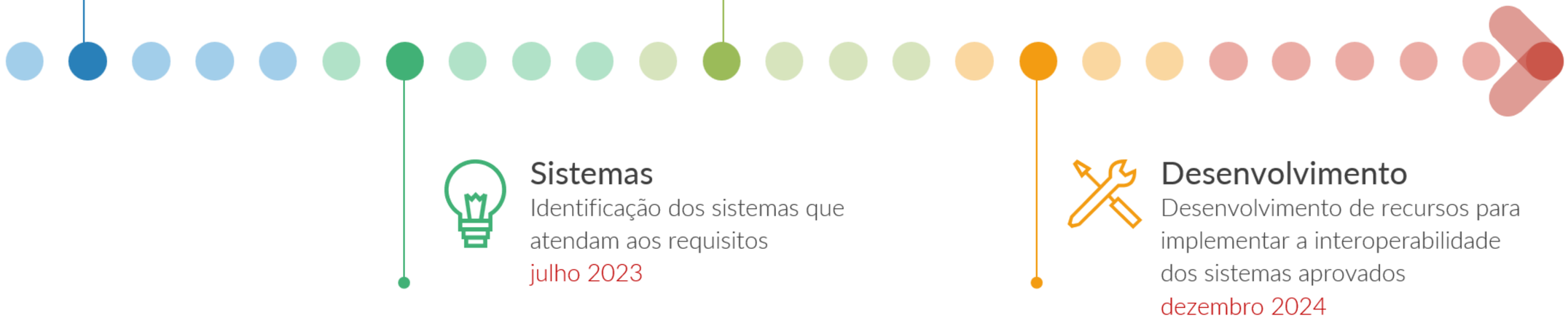
TRE-PI

Integração de Canais Digitais

Transformação Digital

TRE-PI

Estratégia de Monitoramento



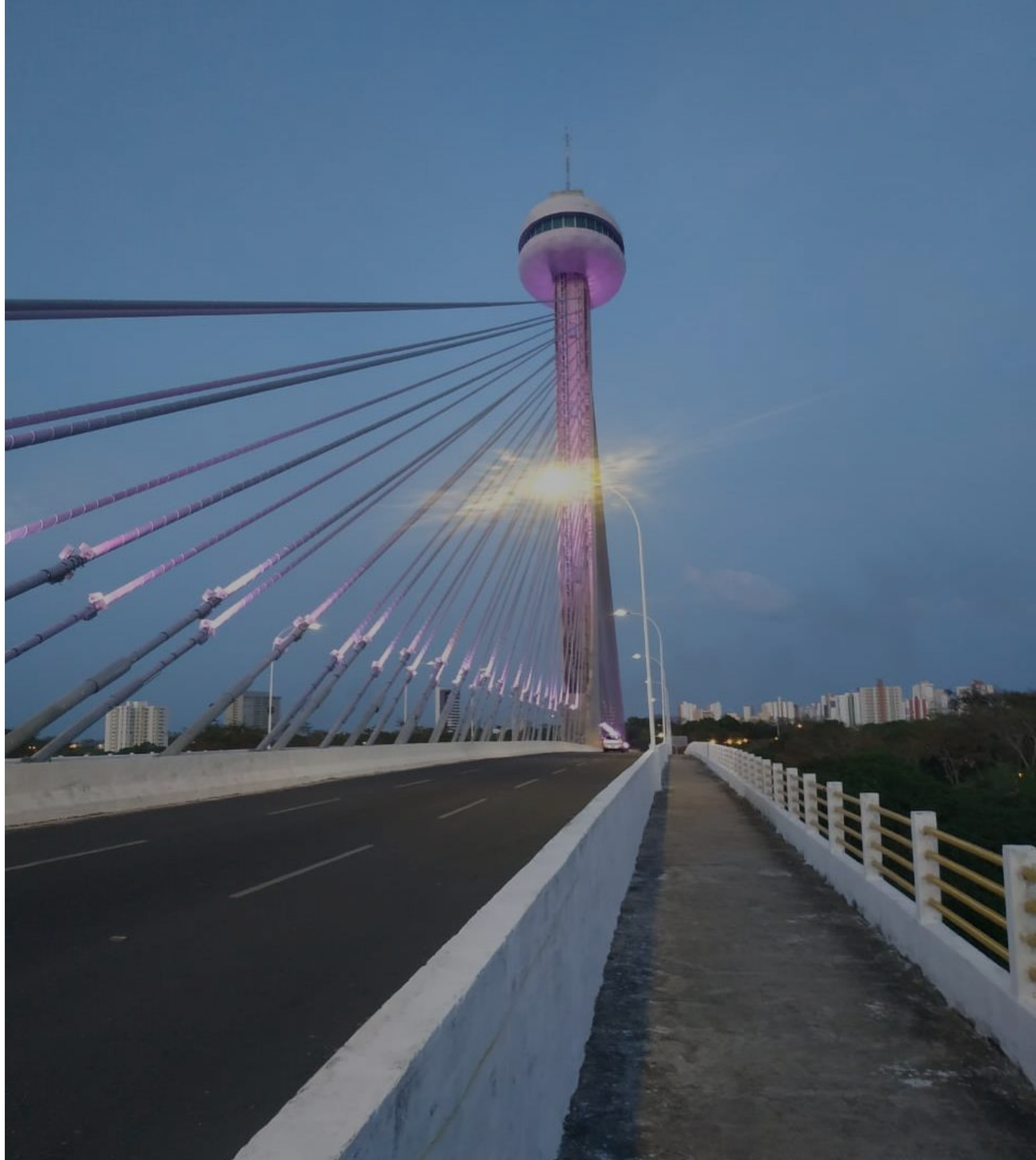
Requisitos
Definição dos requisitos de interoperabilidade de sistemas
maio 2023

Portfólio
Aprovação do portfólio de sistemas para implementação de mecanismos de interoperabilidade
setembro 2023

Sistemas
Identificação dos sistemas que atendam aos requisitos
julho 2023

Desenvolvimento
Desenvolvimento de recursos para implementar a interoperabilidade dos sistemas aprovados
dezembro 2024

Secretaria de Tecnologia da Informação
sti@tre-pi.jus.br
(86) 2107-9760



Tribunal Regional Eleitoral
do Piauí

Processo de Gestão de Segurança da Informação

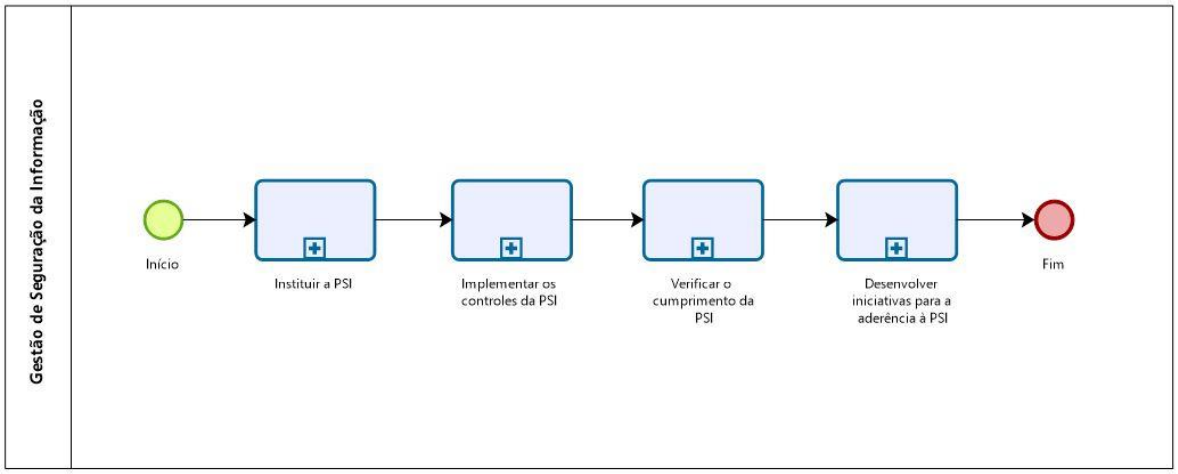
Bizagi Modeler

Índice

1. APRESENTAÇÃO

É importante destacar que todos os fluxos apresentados neste Manual foram desenvolvidos na ferramenta Bizagi.

2. Macroprocesso de Gestão de Segurança da Informação



O Macroprocesso de Gestão de Segurança da Informação tem basicamente os quatro subprocessos apresentados na imagem acima, ou seja:

Instituir a PSI: reúne as atividades necessárias para instituir a Política de Segurança da Informação (PSI) no âmbito do TRE-PI.

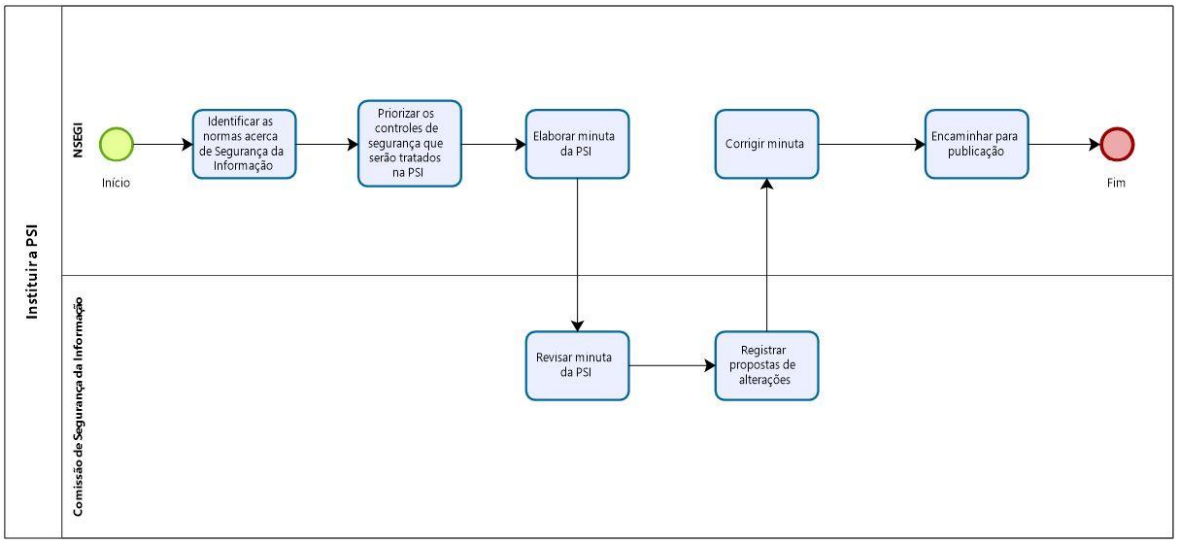
Implementar os controles da PSI: reúne as atividades necessárias para implementar os controles da Política de Segurança da Informação.

Verificar o cumprimento da PSI: reúne as atividades necessárias para verificar o cumprimento da PSI.

Desenvolver iniciativas para aderência à PSI: reúne as atividades necessárias para desenvolver iniciativas para aderência à PSI.

A responsabilidade por cada tarefa constante nos subprocessos supracitados está descrita no detalhamento de cada subprocesso apresentados neste Manual.

2.1 Instituir a PSI



O subprocesso **Instituir a PSI** apresenta em seu fluxo as atividades a seguir:

2.1.1 **Identificar as normas acerca da Segurança da Informação**: esta atividade exige que durante a fase de desenvolvimento de uma Política de Segurança da Informação sejam identificados os principais normativos para verificar necessidade de alinhamento. Não será relacionado neste documento as versões de tais normativos, visto que são atualizados periodicamente. A seguir, apresentaremos os principais normativos considerando o contexto em que o TRE-PI se encontra:

- ✓ ABNT ISO/IEC 27001: *especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação, dentro do contexto da organização*. [ABNT 27.001:2013]
- ✓ ABNT ISO/IEC 27002: *fornece diretrizes para as práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco de segurança da informação da organização*. [ABNT 27.002:2013]
- ✓ Resoluções do Conselho Nacional de Justiça (CNJ) sobre o tema Segurança da Informação: O CNJ instituiu normativos estabelecendo diretrizes para todo o Poder Judiciário. Esses normativos devem ser considerados durante a elaboração de uma PSI.

- ✓ Política de Segurança da Informação da Justiça Eleitoral: o Tribunal Superior também instituiu normativos estabelecendo diretrizes de segurança da informação para toda a Justiça Eleitoral. Esses normativos também devem ser considerados durante a elaboração de uma PSI.
- ✓ *CIS Controls*: A empresa *Center for Internet Security (CIS)* desenvolveu um framework que estabelece as melhores práticas para a segurança da informação nas empresas. Esse framework orienta quais são os principais controles a serem implementados de acordo com o porte da empresa. A observação do CIS Controls durante a elaboração da PSI serve de orientação para estabelecer quais os principais controles de segurança que devem ser tratados pela organização.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.1.2 **Priorizar os controles de segurança que serão tratados na PSI**: nesta atividade o NSEGI identificará os principais controles que devem ser tratados na PSI. Na prática é comum a adoção dos controles estabelecidos pelo TSE, entretanto a boa prática recomenda que após uma avaliação dos riscos da organização sejam estabelecidos os controles que serão reunidos na PSI, ou seja, é possível acrescentar controles identificados como necessários para o TRE-PI.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.1.3 **Elaborar minuta da PSI**: ao final desta atividade o NSEGI deverá apresentar uma minuta de PSI para posterior aprovação pela Comissão de Segurança da Informação (CSI).

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.1.4 **Revisar minuta da PSI**: nesta atividade a minuta da PSI deverá ser revisada por todos os membros da CSI. Essa revisão deverá ser realizada em reunião oficial.

Responsável: Comissão de Segurança da Informação (CSI).

2.1.5 **Registrar propostas de alterações**: as alterações propostas pelos membros da CSI, durante a reunião, devem ser registradas em Ata para fins de evidências.

Responsável: Comissão de Segurança da Informação (CSI).

2.1.6 **Corrigir minuta**: nesta atividade o NSEGI corrige a minuta da PSI com base nas propostas de alterações apresentadas durante a reunião da CSI. A nova minuta deverá constar em

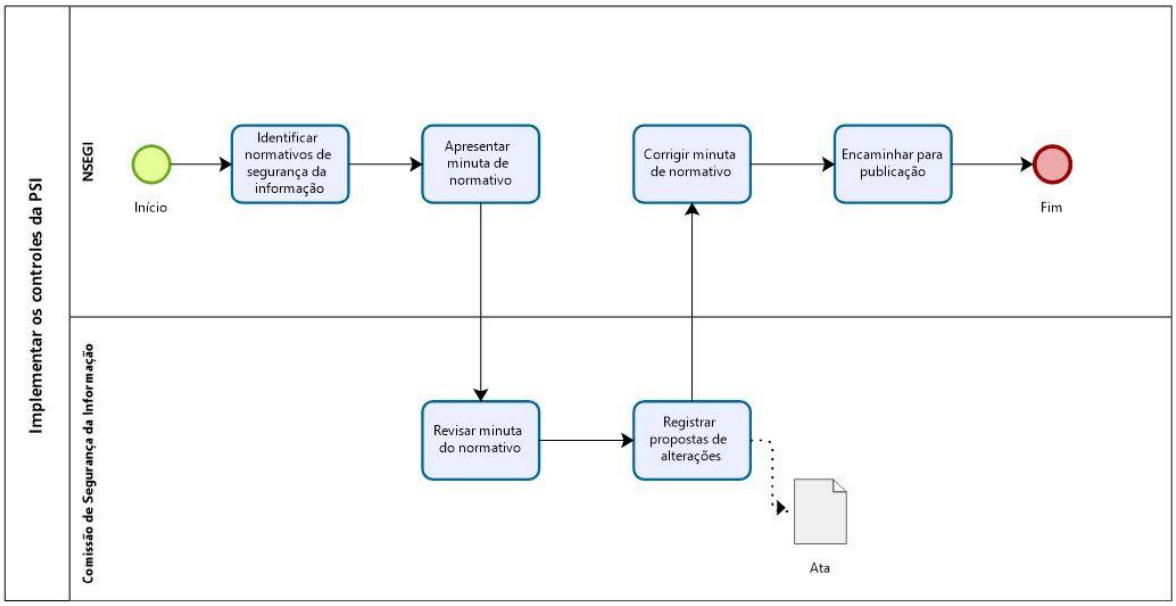
processo SEI para que os membros da CSI possam ter conhecimento da nova redação antes do encaminhamento para a publicação.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.1.7 **Encaminhar minuta para publicação**: nesta atividade o NSEGI, após todas as correções realizadas no conteúdo original, encaminha a nova minuta para publicação da PSI. A minuta deverá ser encaminhada à Diretoria-Geral para que sejam adotados os procedimentos visando a publicação do normativo.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.2 Implementar os controles da PSI



O subprocesso **Implementar os controles da PSI** apresenta em seu fluxo as atividades a seguir:

2.2.1 **Identificar os normativos de segurança da informação**: nesta atividade o NSEGI antes de elaborar uma proposta de minuta de normativo para instituir ou revisar um controle de segurança previsto na PSI deve identificar referências normativas suficientes para a elaboração de proposta embasada nas melhores práticas recomendadas sobre o tema. Para isto devem ser observados normas técnicas, resoluções, portarias e outras fontes bibliográficas que podem dar suporte ao tema que será tratado no normativo.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.2.2 **Apresentar minuta de normativo**: ao final desta atividade o NSEGI deverá apresentar uma minuta de normativo para o controle de segurança da informação para posterior aprovação pela Comissão de Segurança da Informação (CSI).

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.2.3 **Revisar minuta do normativo**: nesta atividade a minuta do normativo para o controle de segurança da informação deverá ser revisada por todos os membros da CSI. Essa revisão deverá ser realizada em reunião oficial.

Responsável: Comissão de Segurança da Informação (CSI).

2.2.4 **Registrar propostas de alterações**: as alterações propostas pelos membros da CSI, durante a reunião, devem ser registradas em Ata para fins de evidências.

Responsável: Comissão de Segurança da Informação (CSI).

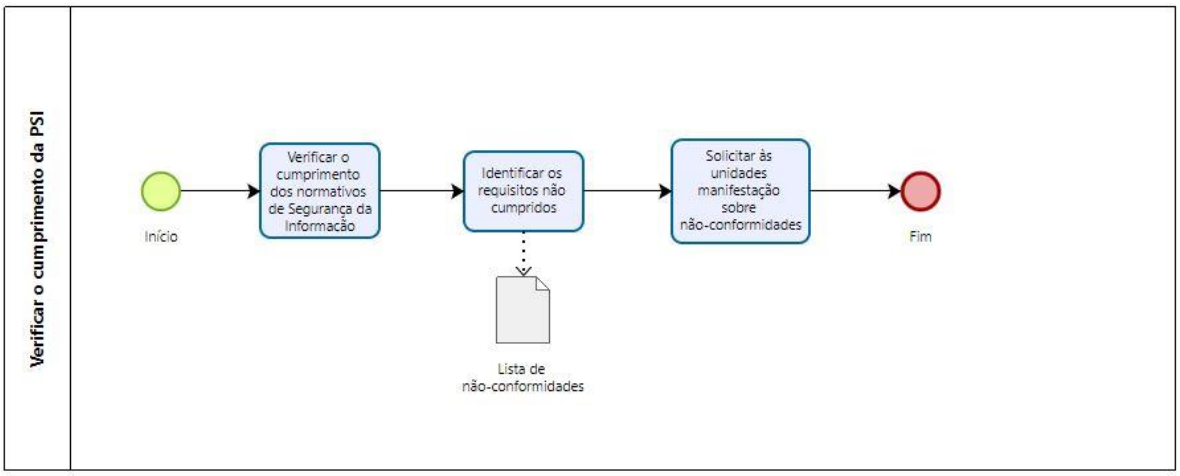
2.2.5 **Corrigir minuta de normativo**: nesta atividade o NSEGI corrige a minuta do normativo considerando as alterações apresentadas, pelos membros da CSI, durante a reunião. A nova minuta deverá constar em processo SEI para que os membros da CSI possam ter conhecimento da nova redação antes do encaminhamento para a publicação.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.2.6 **Encaminhar para publicação**: nesta atividade o NSEGI, após todas as correções realizadas no conteúdo original, encaminha a nova minuta de normativo relacionado ao controle de segurança da informação da PSI. A minuta deverá ser encaminhada à Diretoria-Geral para que sejam adotados os procedimentos visando a publicação do normativo.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.3 Verificar o cumprimento da PSI



O subprocesso **Verificar o cumprimento da PSI** apresenta em seu fluxo as atividades a seguir:

2.3.1 **Verificar o cumprimento dos normativos de segurança da informação**: nesta atividade o NSEGI, realizará, por meio de processo SEI, o acompanhamento junto às unidades acerca do cumprimento da Política de Segurança da Informação e de normativos referentes aos controles de segurança da informação estabelecidos na Política ou priorizados pela Comissão de Segurança da Informação.

Essa atividade pode acontecer de forma conjunta ou separadamente, para verificar o cumprimento de um normativo específico.

Responsável: Núcleo de Segurança da Informação (NSEGI).

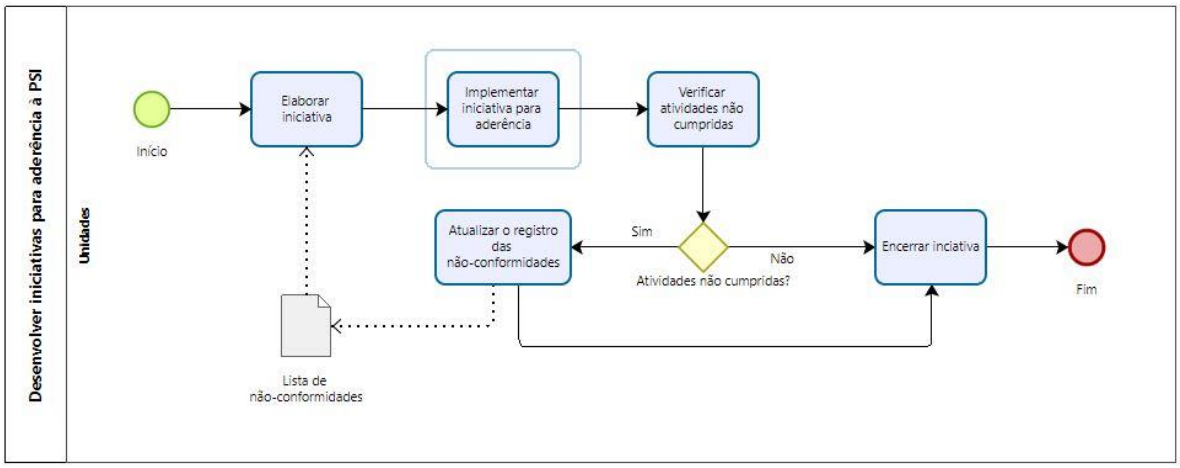
2.3.2 **Identificar os requisitos não cumpridos**: após o levantamento acerca do cumprimento dos normativos de segurança da informação, o NSEGI, registrará os requisitos não cumpridos para controle e próximas ações que serão desenvolvidas a fim de regularizar a situação.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.3.3 **Solicitar às unidades, manifestações sobre não-conformidades**: o NSEGI, solicitará às unidades que se manifestem sobre as não-conformidades, ou seja, sobre os requisitos não cumpridos.

Responsável: Núcleo de Segurança da Informação (NSEGI).

2.4 Desenvolver iniciativas para aderência à PSI



O subprocesso **Desenvolver iniciativas para aderência à PSI** apresenta em seu fluxo as atividades a seguir:

2.4.1 **Elaborar iniciativa**: o NSEGI ou qualquer outra unidade que tenha um normativo que afeta diretamente as atividades sob sua responsabilidade deve apresentar iniciativa, projeto ou plano de ação, visando implementar atividades que permitirão o cumprimento dos requisitos estabelecidos.

A iniciativa poderá exigir a contratação de um serviço ou aquisição de um bem que possa colaborar para o cumprimento dos requisitos previstos no normativo a que está diretamente associada.

Responsável: Todas as unidades.

2.4.2 **Implementar iniciativa**: a iniciativa deverá ser implementada. observando o cumprimento dos requisitos estabelecidos no normativo que está sendo tratado.

Responsável: Todas as unidades.

2.4.3 **Verificar atividades não cumpridas**: a unidade deve avaliar se todas as atividades previstos nas iniciativa foram cumpridas.

Responsável: Todas as unidades.

2.4.4 **Atualizar o registro das não-conformidades**: caso haja atividade não cumprida, a unidade responsável pela iniciativa deve atualizar a lista de não-conformidades.

Essa lista deve ser encaminhada para o NSEGI e será utilizada como fonte de informação para futuras iniciativas.

2.4.5 **Encerrar iniciativa**: a iniciativa deve ser encerrada e devem ser registradas todas as lições aprendidas a fim de permitir um processo de melhoria contínua.

Caso a iniciativa tenha sido encerrada com não-conformidades, a unidade deverá avaliar o impacto das não-conformidades no resultado final, bem como a necessidade de mais recursos (pessoas, prazo ou orçamento), a fim de cumprir a iniciativa em sua integralidade.