PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Comitê de Governança de Segurança da Informação

MATRIZ DE PLANEJAMENTO

PLANO DE TRABALHO DO CGSI – 2026

Versão: 1.0 | Data: 27/01/2026

1. Resumo Executivo

Este plano organiza as prioridades normativas, estratégicas e operacionais do Comitê de Governança de Segurança da Informação (CGSI) para 2026, orientando a implementação da Política de Segurança da Informação (POSIN) e a condução coordenada dos Programas Institucionais (Programa de Governança, Riscos e Conformidade em Segurança da Informação - PGRCSI, Programa de Defesa Cibernética - PDC, Programa de Gestão de Incidentes e Continuidade - PGIC, Programa de Segurança no Desenvolvimento e Aquisição - PSDA, Programa de Cultura em Segurança da Informação - PCSI e Programa de Segurança Física e Ambiental - PSFA), conforme o modelo estratégico–tático–operacional da POSIN e da FIP.

O plano organiza as entregas da FIP, integra o portfólio de Programas/Projetos 2026, define blocos trimestrais de aprovação, atribui responsáveis, registra evidências no SEI e estabelece *KPIs* e *KRIs* para acompanhamento formal pelo CGSI.

2. Diretrizes de Governança e rastreamento rápido (Deliberação CGSI)

Para reduzir gargalos e garantir tempestividade, o CGSI adota o seguinte fluxo normativo:

Todas as normas complementares da POSIN, após revisão técnica pela SECTI/NUDCI e revisão especializada da Central IT, seguirão diretamente para apreciação e deliberação no CGSI, e, aprovadas, serão encaminhadas à DIGER, responsável pelo trâmite à Presidência para publicação.

Fundamento: A POSIN define a pirâmide normativa (Política → Programas → Normas e Projetos Operacionais) e estabelece que o CGSI é a instância de governança responsável por aprovar normas complementares antes do envio para publicação.

3. Prioridades Imediatas - Auditoria e Conformidade (T1/2026)

Prioridade	Ação	Impacto na Maturidade
Crítica	Publicação da POSIN (Ato Mestre)	Requisito Base (Sem ela, nada avança)
Alta	Aprovação da Norma de Vulnerabilidades e NUARTI pelo CGSI	Controle 7 (CIS8): Gestão Contínua e reduz risco operacional contínuo
Alta	Norma de Educação e Cultura	Controle 14 (CIS8): Redução de Risco Humano

Alta	Aprovar reuniões e roteiro de relatos para o Calendário CGSI 2026 e roteiro de Relatos Trimestrais	Conformidade com a Portaria Presi 6 (1582594), que determina a elaboração do plano em até 30 dias
Alta	Aprovar bloco essencial de normas complementares já validadas com as áreas técnicas que cada norma impacta e com a consultoria qualificada (Central IT)	Destrava execução dos Programas e proporciona exequibilidade da POSIN

4. Estratégia de Aprovação em Blocos – Ciclo de Governança 2026

Bloco 1 – até 27/01/2026 (Alicerce)

- Aprovar POSIN (SEI 1479831) e encaminhar para DIGER para avaliar trâmite para a Presidência ou Plenário Administrativo para apreciação e publicação.
- Aprovar normas complementares. Normas essenciais: Tratamento de Vulnerabilidades – 1574705; Uso Aceitável de Recursos de TI (NUARTI) – 1515970; Educação e Cultura em SI – 1579241.

Justificativa de Convocação (NUGTI/ASGES/SUDAS/Escola de Magistratura): Garantir que as normas estejam alinhadas à estratégia do Tribunal (ASGES), sejam tecnicamente exequíveis pela SECTI (NUGTI), e o plano de educação esteja em conformidade com as diretrizes e cronograma da SUDAS e da Escola de Magistratura.

Bloco 2 – Abril/2026

- Discussão dos resultados e andamentos da implementação da POSIN e das normas complementares aprovadas.
- Aprovação das normas complementares já validadas com as áreas técnicas que cada norma impacta e com a consultoria qualificada (Central IT).
- Auditoria Contratual: Revisão de cláusulas de SI em novos editais e renovações.
- Inventário Crítico: Lançamento do Projeto Classifica-JF6. Meta: 100% dos ativos críticos inventariados até dezembro (*Data Discovery ou Data Loss Prevention - DLP*).
- Avaliação de normas complementares necessárias à execução das atividades elencadas no cronograma da FIP.

Bloco 3 – Junho/2026

- Plano de Continuidade (PCN/PRI): Elaboração dos fluxos de continuidade de negócios e resposta a incidentes.
- Segurança no Desenvolvimento: Homologação do Projeto Esteira-Segura (Checklist de segurança para novos sistemas).
- Avaliação de normas complementares necessárias à execução das atividades elencadas no cronograma da FIP.
- Avaliação do relatório semestral sobre o nível de maturidade do SGSI.

Bloco 4 – Outubro/2026

- Capacitação em Massa (Escudo-Humano): Relatório final da execução do treinamento obrigatório para 100% dos usuários.

- Projeto Phishing-Zero: Primeira simulação de ataque controlada para medir a vulnerabilidade humana.
- Teste de recuperação de desastres.
- Avaliação do relatório semestral sobre o nível de maturidade do SGSI.
- Avaliação dos resultados e necessidades de alterações normativas.

5. Programas e Projetos

A execução seguirá os Programas Institucionais: PGRCSI, PDC, PGIC, PSDA, PCSI e PSFA, com os seguintes projetos:

PGRCSI – Governança e Riscos

- Classifica-JF6
- Mapa de Riscos

PDC – Defesa Cibernética

- Acesso-Seguro (MFA)
- Scan-Contínuo
- Zero-Trust
- Threat-Intel

PGIC – Continuidade e Incidentes

- Resposta-Rápida (PRI/Fluxos ETIR)
- DR-Nuvem (1º teste)

PSDA – Desenvolvimento Seguro

- Esteira-Segura (SCA/SAST/DAST)
- Homologa-Seguro (checklist)

PCSI – Cultura e Conformidade

- Escudo-Humano (treinamento obrigatório)
- Phishing-Zero (simulações)

PSFA – Segurança Física e Ambiental

- Fortaleza-Física (áreas críticas de ativos de informação - datacenter)

6. Cronograma Macro (Mês 1 = jan/2026)

Frente/Projeto	**Entrega/Marco**	**Início**	**Fim**	**Responsável/Lotação**	**Influência**
Governança	POSIN – minuta>publicação	M1	M6	NUSIN/DIGER/Presidência/Jurídico	TD/ID
	Availação de maturidade em Segurança da Informação	M6	M12	NUSIN/SECTI/Áreas de Gestão	TD/ID
Governança	Normas complementares – 1ª onda	M7	M12	NUSIN	TD/ID

Ativos e Acesso	Classifica-TRF6 (inventário críticos)	M7	M16	NUSIN/SECTI	TD/ID
Ativos e Acesso	Acesso-Seguro (MFA)	M7	M16	SECTI	TD/ID
Ativos e Acesso	Fortaleza-Física (segurança de áreas físicas do datacenter)	M9	M18	NUSIN/Infra	TD/ID
Ativos e Acesso	Zero-Trust (marcos)	M6	M18	SECTI/NUSIN	TD/ID
Desenvolvimento	Homologa-Seguro	M7	M12	NUSIN/SECTI	ID
Desenvolvimento	Esteira-Segura	M6	M14	SECTI/NUSIN	ID
Defesa	Scan-Contínuo (ferramenta)	M7	M12	NUDCI/SECTI	ID
Defesa	PRI/PCN (v1.0) – Resposta-Rápida	M8	M14	NUSIN/ETIR/NUDCI	TD/ID
Defesa	DR-Nuvem – 1º teste	M10	M18	SECTI/NUSIN/NUDCI	ID
Defesa	Threat-Intel (integração)	M8	M16	NUDCI/SECTI	ID
Cultura	Escudo-Humano (treinamento)	M1	M12	NUSIN/SUDAS/SEFAS/ESMAG/ASCOM	ID
Cultura	Cláusulas de SI em contratos	M7	M15	Jurídico/Contratos	ID
Cultura	Phishing-Zero (simulações)	M6	M18	NUSIN/NUDCI/ASCOM	ID

7. Reuniões CGSI e Relatórios Trimestrais

Para dar maior ritmo e governabilidade, as reuniões passam a ter dois tipos:

7.1 Reuniões Ordinárias (fixas – bimestrais)

Reuniões ordinárias previstas: 27/01, 16/04, 18/06, 20/08, 22/10 e 10/12 (14h–16h).

Objetivos padrão das reuniões ordinárias:

a) Aprovação de normas complementares prontas.
b) Monitoramento dos Programas/Projetos da POSIN (painel de KPIs).
c) Avaliação de riscos e incidentes relevantes (ETIR/NUDCI).
d) Validação de entregas do cronograma FIP.
e) Acompanhamento dos Relatórios Trimestrais: 31/03, 30/06, 30/09 e 17/12 (consolidação anual até 19/12).

7.2 Reuniões Extraordinárias (convocação rápida – *fast track*)

Usadas para:

a) Aprovar normas de alta criticidade.
b) Analisar incidentes graves ou de impacto institucional.
c) Validar decisões de risco (aceitação, transferência, mitigação crítica).
d) Aprovar documentos estruturantes (ex.: PCN, PRI, Metodologia de Riscos).
e) Liberar marcos de contratação de ferramentas essenciais (ex.: varredura contínua).

8. Rito de Aprovação e Publicação

Fluxo oficial:

1) Validação técnica: SECTI/NUDCI/NUSIN;
2) Deliberação: CGSI;
3) Trâmite: Diretoria Geral (DIGER);
4) Apreciação e Publicação: Presidência; e
5) Disponibilização: Repositório institucional (se não sigiloso).

9. Evidências exigidas (Auditoria Interna/TCU/CNJ)

- Portaria POSIN publicada e SEI vinculado; atas do CGSI de aprovação.
- Normas complementares aprovadas e publicadas (ou em SEI) com controle de versão.
- Registro de instalação/integração de ferramenta de vulnerabilidades e relatórios consolidados.
- Atas/exercícios ETIR (PRI/PCN), simulações (*table-top*), e relatório de DR-Nuvem.
- Registros de treinamento (listas de presença/relatórios de conclusão) e campanhas de *phishing*.
- Contratos/termos com cláusulas de segurança incluídas após publicação da POSIN (amostras).

10. Indicadores de Acompanhamento (KPIs/KRIs)

- Publicação POSIN (sim/não).
- Cobertura MFA em sistemas críticos (%).
- Ativos inventariados e classificados (%).
- Vulnerabilidades críticas pendentes e tempo médio de correção.
- Treinamento obrigatório concluído (%).
- Execução de simulações de *phishing* (%).
- Testes de DR realizados (sim/não por semestre).

11. Riscos e Mitigações

- Capacidade limitada do NUSIN: Solicitar 2-3 servidores em apoio; priorização por blocos.

- Atrasos de validação: Cronograma formal com prazos no CGSI.

- Orçamento para ferramentas: gargalo de recursos financeiros, técnicos, jurídicos ou humanos em cada onda de contratação de software, conforme cronograma da FIP. Mitigação: Uso de ferramentas Open Source validadas pela SECTI e CentralIT como medida tempestiva de solução temporária.

- Baixa adesão a treinamentos: Campanhas com ASCOM; gestores como patrocinadores; métricas por unidade.

12. Matriz RACI (síntese)

A – Aprova | R – Responsável | C – Consultado | I – Informado

Atividade	Alta Adm.	CGSI	NUSIN	SECTI/NUDCI	Demais Areas
POSIN e Normas Complementares	A	R	R	C	C
Inventário/Classe de Ativos	I	I	R	C	R (Gestores)
Gestão de Vulnerabilidades	I	I	C	R	I
PCN/PRI/DR	I	A	R	C/R	C
Treinamento e Phishing	I	A	R	I	R (SUDAS/Escola de Magistratura/ASCOM)
Relatório de maturidade em segurança da informação	I	I	R	C	C

Documento assinado eletronicamente por **Thiago Marques Lopes**, **Coordenador(a)**, em 27/01/2026, às 17:07, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Sabrina Araujo Ferreira**, **Membro**, em 27/01/2026, às 17:11, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Arianne Caldeira do Carmo**, **Secretário(a)**, em 28/01/2026, às 11:04, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1602566** e o código CRC **902C90C0**.