Comissão de Segurança da Informação:

Proposta de agenda de trabalho

1º de agosto de 2018

Sumário

Contexto

Comissões e comitês

Comissão de Segurança da Informação

Comitê Regional de Atenção ao 1º Grau

Comissão de Aplicação da Lei de Acesso à Informação

Política Nacional/Regional de Atenção à Saúde

Comitê Gestor do Planejamento Estratégico 2015/2020

Comissão Permanente de Acessibilidade

Comissão Socioambiental

Comissão de Segurança Permanente

Contexto

Tecnologia da Informação e Comunicação (TIC)

A Tecnologia da Informação e Comunicação (TIC), nos dias atuais, é um dos principais instrumentos de sustentabilidade, crescimento e gerenciamento do valor e risco na maioria das organizações.

Essa posição de relevo tem sido reconhecida pelas instituições de controle – Conselho Nacional de Justiça (CNJ) e Tribunal de Contas da União (TCU) e outras instâncias – Tribunal Superior Eleitoral (TSE).

Nesse sentido, em linha com as melhores práticas, essas instituições têm definido políticas, diretrizes e estruturas organizacionais com vistas ao fortalecimento das atividades de TIC, inclusive com a instituição de instrumentos de planejamento e instâncias de governança próprios.

Contexto

Pressupostos de boa governança

Liderança – “que estabeleça os objetivos e a direção a seguir, sendo capaz de corrigir os possíveis desvios de rumo”

Estratégias e planos – “que materializem a direção estabelecida, de forma a contribuir com o alcance dos objetivos da organização”

Informações – “tempestivas para subsidiar a tomada de decisão, bem como dar transparência das ações às partes interessadas”

Processos – “para implementar as políticas e entregar os resultados esperados, bem como garantir a continuidade das ações”

Pessoas – “capazes de fazer funcionar essa engrenagem organizacional de forma eficiente e efetiva”

Fonte: Relatório de Levantamento de Governança de TI 2016 (TCU TC 008.127/2016-6)

Contexto

Instrumentos de planejamento

Estratégia Nacional do Poder Judiciário 2015/2020
(Res. CNJ 198/14)

Estratégia Nacional de TIC do Poder Judiciário
(Res. CNJ 211/15)

Planejamento Estratégico TREDF 2015/2020 (Res. TREDF 7.656/15)			**Plano Estratégico de TIC TREDF 2017/2020 (Res. 7.760/17)**			
Macrodesafios			**Mapa estratégico**			
Indicadores estratégicos	**Ações/Projetos Estratégicos**	**Plano de Gestão (Metas estratégicas)**	**Indicadores**	**Plano Diretor de TIC 2017/2018 (iniciativas)**	**Política de Segurança da Informação (Res. TSE 23.501/16)**	**Plano de Contratações de Soluções de TIC**

Contexto

Fóruns de governança

Planejamento Estratégico TREDF 2015/2020 (Res. TREDF 7.656/15)

- Comitê Gestor do Plano Estratégico do TRE-DF (art. 2º) – Res. TRE-DF 6.857/09

Estratégia Nacional de TIC do Poder Judiciário (Res. CNJ 211/15)

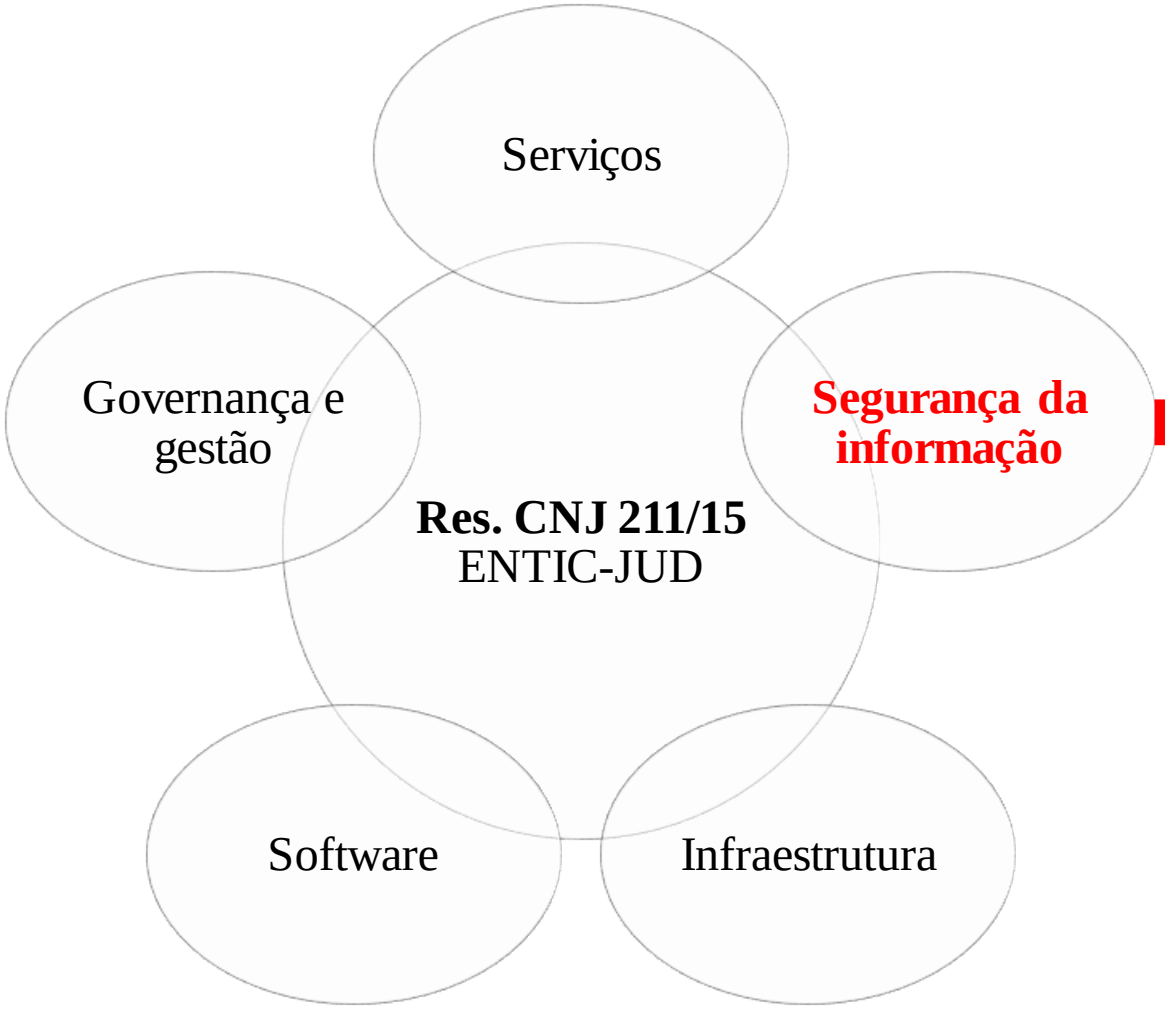
- Comitê de Governança de Tecnologia da Informação e Comunicação (art. 7º) - Port. PR/TRE-DF 187/17, 21/9/17
- Comitê de Gestão (art. 8º) Port. DG/TRE-DF 296/17, 3/1/17
- Comitê Gestor de Segurança da Informação (art. 9º)

Política de Segurança da Informação (Res. TSE 23.501/16)

- Comissão de Segurança da Informação (art. 22) Port. DG/TRE-DF 82/18, 17/5/18
- Gestor de Segurança da Informação (art. 25) Port. DG/TRE-DF 94/17, 30/6/17

Contexto

Complementariedade normativa



Res. TSE 23.501, de 19/12/16 – Institui a **Política de Segurança da Informação** no âmbito da Justiça Eleitoral*

*Res. TSE 22.780, de 24/4/08, Estabelece princípios e valores a serem adotados para assegurar a integridade, a confidencialidade e a disponibilidade das informações no âmbito da Justiça Eleitoral.

Política de Segurança da Informação

Princípios e escopo

Princípios

- Integridade
- Autenticidade
- Confidencialidade
- Disponibilidade
- Irretratabilidade

dos ativos de informação e de processamento

Escopos

I - instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação;

II - promover ações necessárias à implementação e à manutenção da segurança da informação;

III - combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

IV - promover a conscientização e a capacitação de recursos humanos em segurança da informação.

Política de Segurança da Informação

Atribuições

Res. CNJ 211/15

Comitê Gestor de Segurança da Informação - CGSI(art. 9º)

elaborar e aplicar política, gestão e processo de segurança da informação a serem desenvolvidos em todos os níveis da instituição

Res. TSE 23.501/16

Comissão de Segurança da Informação – CSI (art. 22)

Propor em relação à PSI: i) **normas, procedimentos, planos e/ou processos**; ii) **estratégia de implantação**; iii) **fiscalização da aplicação**; iv) realização de análise de riscos; v) modelo de ETIR e promover a divulgação da PSI

Gestor de Segurança da Informação - GSI (art. 25)

Propor : i**) normas relativas à segurança da informação à CSI**; ii) iniciativas para aumentar o nível da segurança da informação à CSI; iii) o uso de novas tecnologias, e iv) implantar, em conjunto com as demais áreas, normas, procedimentos, planos e/ou processos elaborados pela CSI

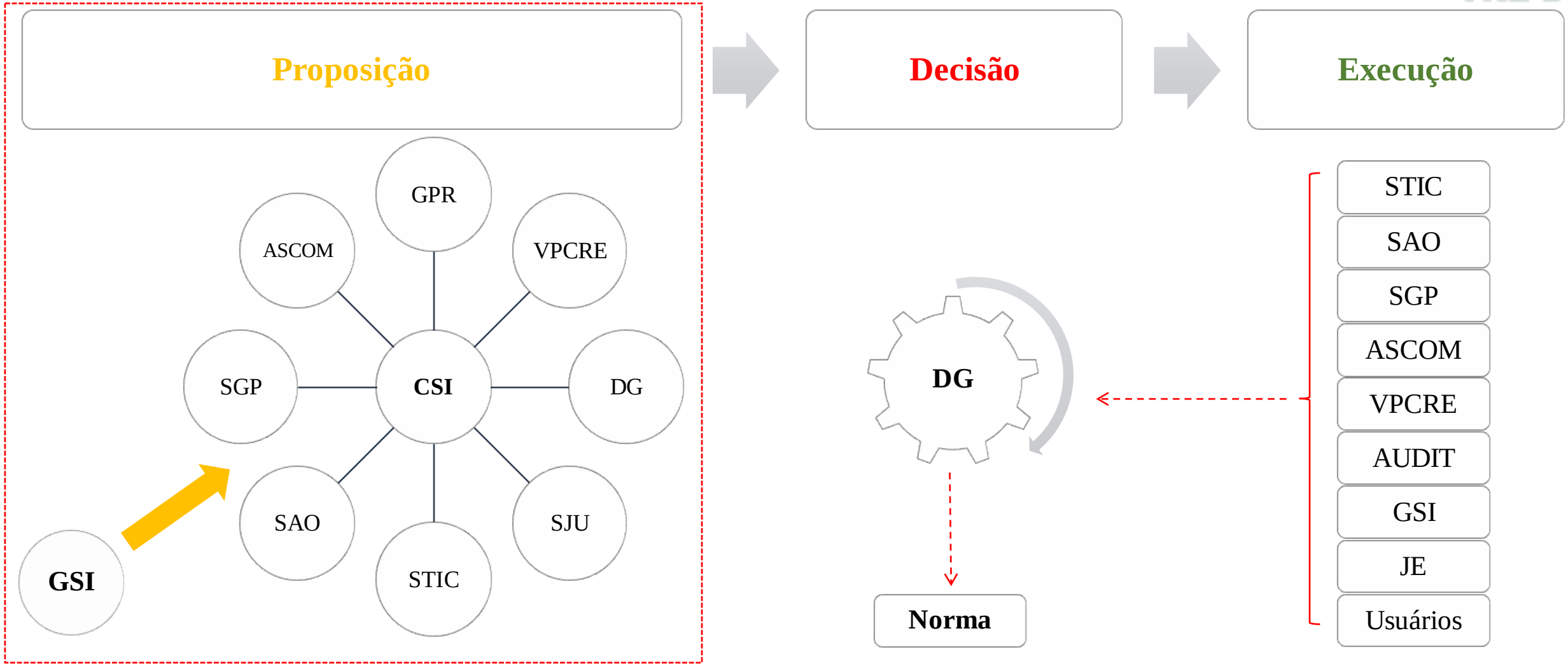
Política de Segurança da Informação

Governança

Res. CNJ 211/15			Res. TSE 23.501/16	
Comitê de Governança de Tecnologia da Informação e Comunicação (art. 7º) - Port. PR/TRE-DF 187/17, 21/9/17 I – o DG; II – o STIC; III – o SJU; IV – o SGP; V – o SAO; VI – o CACRE; e VII – o ASSPLAN.	**Comitê de Gestão de TIC (art. 8º)** Port. DG/TRE-DF 81/18, 17/5/18 I – **Ricardo Negrão de Oliveira**, STIC; II – **Carlos Roberto Menezes**, – COIE/STIC; III – **Rafael Dittberner** - COSC/STIC; IV – **Nelson Antônio Guimarães Neto** - SGTICSTIC; e V – **José Fernando Valim Batelli** – SARSO/STIC.	**Comitê Gestor de Segurança da Informação (art. 9º)**	**Comissão de Segurança da Informação (art. 22)** Port. DG/TRE-DF 82/18, 17/5/18 I – **Tadeu Costa Saenger**, GPR; II – **Paulo Lucena Melo**, VPCRE; III – **Lúcia Carvalho Bitar Yung-Tay**, DG; IV – **Fábio Moreira Lima**, SJU; V – **Ricardo Negrão de Oliveira**, STIC; VI – **Edivan Ismael dos Santos**, SAO ; VII – **Paulo de Tarso Costa de Souza**, SGP; VIII – **Fernando de Castro Velloso Filho**, ASCOM.	**Gestor de Segurança da Informação (art. 25)** Port. DG/TRE-DF 94/17, 30/6/17 **Carlos Roberto de Menezes** – COIE/STIC

Política de Segurança da Informação

Governança



Comissão de Segurança da Informação

Responsabilidades e atribuições

GSI (art. 25)	I - propor normas relativas à segurança da informação à Comissão de Segurança da Informação;
	II - propor iniciativas para aumentar o nível da segurança da informação à Comissão de Segurança da Informação, com base, inclusive, nos registros armazenados pela ETIR;
	III - propor o uso de novas tecnologias na área de segurança da informação;
	IV - implantar, em conjunto com as demais áreas, normas, procedimentos, planos e/ou processos elaborados pela Comissão de Segurança da Informação;

Comissão de Segurança da Informação

Responsabilidades e atribuições

CSI (art. 23)	I - propor melhorias a esta PSI;	VI - propor recursos necessários à implementação das ações de segurança da informação;
	II - propor normas, procedimentos, planos e/ou processos, nos termos do art. 6º, visando à operacionalização desta PSI;	VII - propor a realização de análise de riscos e mapeamento de vulnerabilidades nos ativos;
	III - promover a divulgação desta PSI e normativos, bem como ações para disseminar a cultura em segurança da informação, no âmbito do Tribunal Eleitoral;	VIII - propor a abertura de sindicância para investigar e avaliar os danos decorrentes de quebra de segurança da informação;
	IV - propor estratégias para a implantação desta PSI;	IX - propor o modelo de implementação da Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR), de acordo com a norma vigente;
	V - propor ações visando à fiscalização da aplicação das normas e da política de segurança da informação;	X - propor a constituição de grupos de trabalho para tratar de temas sobre segurança da informação;
		XI - responder pela segurança da informação.

Comissão de Segurança da Informação

Responsabilidades e atribuições

Presidência (art. 27)	I - apoiar a aplicação das ações estabelecidas nesta PSI;	
	II - nomear ou **delegar ao Diretor-Geral** da Secretaria a nomeação:	
	a) do Gestor da Comissão de Segurança da Informação, nos termos do art. 22;	Port. DG/TRE-DF 82/18
	b) do Gestor de Segurança da Informação e seu substituto, nos termos do art. 25, parágrafo único;	Port. DG/TRE-DF 94/17
	c) de integrantes da ETIR, nos termos do art. 26.	Port. PR/TRE-DF 113/18

Comissão de Segurança da Informação

Responsabilidades e atribuições

Diretoria-Geral (art. 28)	I - aprovar normas, procedimentos, planos e/ou processos que lhe forem submetidos pela Comissão de Segurança da Informação;
	II - submeter à Presidência as propostas que extrapolem sua alçada decisória;
	III - apoiar a aplicação das ações estabelecidas nesta PSI;
	IV - viabilizar financeiramente as ações de implantação desta PSI, inclusive a exequibilidade do Plano de Continuidade de Negócios do Tribunal, abrangendo sua manutenção, treinamento e testes periódicos.

Comissão de Segurança da Informação

Responsabilidades e atribuições

STI (art. 29)	I - apoiar a implementação desta PSI;
	II - prover os ativos de processamento necessários ao cumprimento desta PSI;
	III - garantir que os níveis de acesso lógico concedidos aos usuários estejam adequados aos propósitos do negócio e condizentes com as normas vigentes de segurança da informação;
	IV - disponibilizar e gerenciar a infraestrutura necessária aos processos de trabalho da ETIR;
	V - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação.

Comissão de Segurança da Informação

Responsabilidades e atribuições

SAO (art. 30)	I - implantar controles nos ambientes físicos, visando prevenir danos, furtos, roubos, interferência e acesso não autorizado às instalações e ao patrimônio da Justiça Eleitoral;
	II - implantar controles e proteção contra ameaças externas ou decorrentes do meio ambiente, como incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e desastres naturais;
	III - assegurar que os empregados das empresas prestadoras de serviço contratadas conheçam suas atribuições e responsabilidades em relação à segurança da informação;
	IV - adotar as medidas necessárias por ocasião do desligamento de empregados das empresas prestadoras de serviço contratadas e comunicar às demais unidades do Tribunal, com vistas à pertinente remoção dos acessos às informações da Justiça Eleitoral;
	V - executar as orientações técnicas e procedimentos estabelecidos pela Comissão de Segurança da Informação.

Comissão de Segurança da Informação

Responsabilidades e atribuições

SGP (art. 31)	I - apoiar a Comissão de Segurança da Informação na missão de assegurar que os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários conheçam suas atribuições e responsabilidades em relação à segurança da informação;
	II - adotar as medidas necessárias por ocasião do desligamento de pessoal e comunicar às demais unidades do Tribunal, com vistas à pertinente remoção dos acessos às informações da Justiça Eleitoral;
	III - promover a capacitação dos servidores que integram a estrutura de gestão da segurança da informação, no que for pertinente;
	IV - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação.

Comissão de Segurança da Informação

Responsabilidades e atribuições

ASCOM (art. 32)	I - promover campanhas de conscientização sobre a importância da segurança da informação;
	II - divulgar esta PSI;
	III - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;
CRE (art. 33)	I - empreender medidas e expedir normas para adequar as práticas cartorárias a esta PSI;
	II - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;

Comissão de Segurança da Informação

Responsabilidades e atribuições

COCI (art. 34)	I - incluir no escopo do Plano Anual de Auditoria e Conformidade, nos termos estabelecidos no art. 17, a análise do cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes;
	II - realizar auditorias conforme Plano Anual de Auditoria e Conformidade;
	III - executar as orientações técnicas e procedimentos estabelecidos pela Comissão de Segurança da Informação.
SEGED (art. 35)	I - regulamentar e coordenar o processo de classificação da informação no âmbito do Tribunal;
	II - executar as orientações técnicas e os procedimentos estabelecidos.

Comissão de Segurança da Informação

Responsabilidades e atribuições

Juiz Eleitoral (art. 36)	I - apoiar a Comissão de Segurança da Informação na missão de assegurar que os magistrados, servidores efetivos e requisitados, estagiários, prestadores de serviço e colaboradores conheçam suas atribuições e responsabilidades em relação à segurança da informação;
	II - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;
Usuários (art. 37)	I - responder por toda atividade executada com o uso de sua identificação;
	II - ter pleno conhecimento desta PSI;
	III - reportar tempestivamente ao Gestor de Segurança da Informação quaisquer falhas ou indícios de falhas de segurança de que tenha conhecimento ou suspeita;
	IV - proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;
	V - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;
	VI - gerenciar os ativos sob sua responsabilidade.

Diretrizes Gerais

Providências

Normas → **Procedimentos** → **Planos/Processos** → **Ações**

Seção I Da Gestão de Ativos	**Seção II** Do Controle de Acessos	**Seção III** Da Gestão de Riscos	**Seção IV** Da Gestão da Continuidade de Negócios	**Seção V** Do Tratamento de Incidentes de Rede	**Seção VI** Da Gestão de Incidentes de Segurança da Informação

Seção VII Da Auditoria e Conformidade	**Seção VIII** Dos Serviços de Internet e Do Correio Eletrônico Corporativo	**Seção IX** Do Desenvolvimento de Sistemas Seguros	**Seção X** Do Uso de Recursos Criptográficos	**Seção XI** Do Processo de Tratamento da Informação

Diretrizes Gerais

Providências

Seção I

Da Gestão de Ativos

- Inventário e classificação dos ativos de informação e processamento
  - Atualização periódica e definição da unidade responsável
- Há processo de classificação da informação? (Portaria Conjunta TRE-DF/PR/DG/GDG 15/18?)

Seção II

Do Controle de Acessos

- Portaria PR/TRE-DF 112/18

Seção III

Da Gestão de Riscos

- Processo de gestão de Riscos de ativos de informação e de processamento
  - identificação, avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação
  - Atualização periódica

Diretrizes Gerais

Providências

Seção IV

Da Gestão da Continuidade de Negócios

- Plano de Continuidade de Negócios - Portaria PR/TRE-DF 125/18
  - estabelecer procedimentos e definir estrutura mínima de recursos para que se desenvolva uma resiliência organizacional
  - Teste e revisão periódico

Seção V

Do Tratamento de Incidentes de Rede

- Processo de Tratamento e Respostas a Incidentes em Redes de Computadores - Portaria PR/TRE-DF 113/18
  - impedir, interromper ou minimizar o impacto de uma ação maliciosa ou acidental

Seção VI

Da Gestão de Incidentes de Segurança da Informação

- assegurar que fragilidades e incidentes em segurança da informação sejam identificados, permitindo a tomada de ação corretiva em tempo hábil

Diretrizes Gerais

Providências

Seção VII

Da Auditoria e Conformidade

- Plano Anual de Auditoria e Conformidade
  - Inclusão da análise do correto cumprimento da PSI, seus regulamentos e demais normativos
  - Periodicidade: a cada 2 anos

Seção VIII

Dos Serviços de Internet e Do Correio Eletrônico Corporativo

- Política de controle de acesso às informações - Portaria PR/TRE-DF 112/18

Seção IX

Do Desenvolvimento de Sistemas Seguros

- Processo de Desenvolvimento de Software
  - Deve contemplar atividades específicas que garantam maior segurança para os sistemas utilizados, de forma a preservar o ambiente tecnológico, assim como prevenir possíveis incidentes de segurança

Diretrizes Gerais

Providências

Seção X

Do Uso de Recursos Criptográficos

- Toda a informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida pelo Tribunal, em parte ou totalmente, por qualquer meio eletrônico, deverá ser protegida com recurso criptográfico.

Seção XI

Do Processo de Tratamento da Informação

- Abranger todas as fases do ciclo da vida da informação
  - Produção e recepção
  - Organizações
  - Uso e disseminação
  - Destinações

Diretrizes Gerais

Providências - reestruturação

Dos ativos	Da gestão	Da segurança	Do controle
• **Seção I** - Da Gestão de Ativos • **Seção XI** - Do Processo de Tratamento da Informação • **Seção X** - Do Uso de Recursos Criptográficos	• **Seção II** - Do Controle de Acessos • **Seção VIII** - Dos Serviços de Internet e Do Correio Eletrônico Corporativo • **Seção IX** - Do Desenvolvimento de Sistemas Seguros	• **Seção III** - Da Gestão de Riscos • **Seção IV** - Da Gestão da Continuidade de Negócios • **Seção VI** - Da Gestão de Incidentes de Segurança da Informação • **Seção V** - Do Tratamento de Incidentes de Rede	• **Seção VII** • Da Auditoria e Conformidade

Considerações

Questões iniciais

O prazo para adaptação aos termos da PSI venceu em 31/12/17

- "Art. 39. Esta PSI é obrigatória a todos os Tribunais Eleitorais, os quais terão até 31 de dezembro de 2017 para se adaptarem às regras previstas nesta resolução."

Levantamento informal realizado pela STIC indica que os TRE's estão em estágios distintos de implantação da PSI.

O próprio TSE, também informalmente, reconhece a dificuldade de implementar a PSI no prazo originalmente fixado e pretende adequá-lo.

A implementação da PSI, no momento, concorre com as atividades inerentes ao período eleitoral (ago a nov/18)

Considerações

Questões iniciais

A Auditoria Coordenada do CNJ referente à Governança de TI, realizada pela Audit, apontou vários achados de auditoria relacionadas à PSI:

A1 – Inconsistência: Ausência de processo formalizado de gestão de riscos de TI	A2 – Inconsistência: Ausência de política formal de gestão de pessoas	A3– Inconsistência: Ausência de comunicação com partes interessadas sobre os resultados de TI
A5 – Inconsistência: Ausência de processo de software definido	A9 – Inconsistência: Ausência de periodicidade na realização de ações de conscientização, educação e treinamento em segurança da informação para os seus colaboradores	A12 – Inconsistência: Ausência de política de cópia de segurança (backup)
A15 – Inconsistência: Inexistência de plano anual de capacitação na área de TIC	**A16 – Inconsistência: Os comitês a seguir estão apenas aprovados e formalizados, porém, sem operacionalização prática: CGTI e CGSTIC**	A19 – Inconsistência: Inexistência de processos formalmente instituídos de gestão da segurança da informação

Considerações

Questões iniciais

As iniciativas adotadas com vistas ao cumprimento da PSI, de modo geral, têm sido apreciadas no âmbito da CGTIC (fórum técnico-especializado) e instituídas por ato da Presidente do Tribunal, de modo distinto do que estabelece a referida política.

Essa situação configura alguma irregularidade?

- Avaliação da COCI?
- Ratificar pela CSI?

Encaminhamentos

Proposta de plano de trabalho

1º)	• Levantamento das medidas já implementadas: • GPR; DG; STIC; SAO; SGP; ASCOM; VPCRE; COCI; SEGED; GSI
2º)	• Apresentação das medidas já implementadas: • Pós levantamento
3º)	• Proposição de plano de ação (5W2H) – por área – com as medidas a serem adotadas, considerando os seguintes critérios: prioridade, urgência, complexidade, disponibilidade
4º)	• Apresentação da STIC sobre o PETIC e o PDTIC
5º)	• Apresentação da Audit – IgovTI2016 e Relatório de Auditoria de Governança de TI Audit 2018
6º)	• Apresentação de plano de ação das áreas (5W2H)
7º)	• Cronograma de reuniões

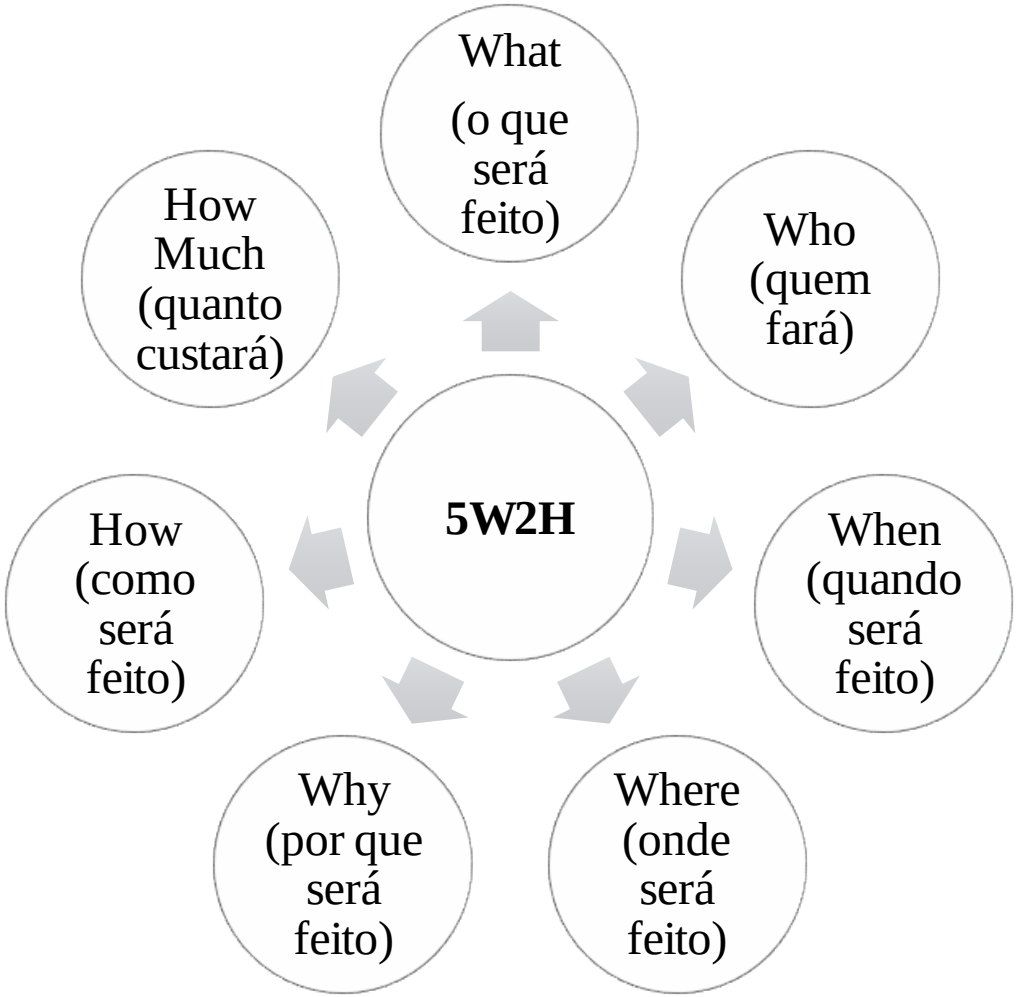
Encaminhamentos

Debates

Slides de apoio

Slides de apoio

Plano de ação



Slides de apoio

Plano de ação

Gestão de Ativos

- ISO 27001 – Sistema de Gestão de Segurança da Informação.
- ISO 27002 – Código de Prática para Gestão de Segurança da Informação.
- **Norma Complementar nº 10/IN01/DSIC/GSIPR**, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Gestão de Riscos

- Norma ABNT NBR ISSO 31000:2009, que estabelece princípios e diretrizes para a gestão de riscos.
- ISO 27005 – Gestão de Risco da Segurança da Informação.
- **Norma Complementar nº 04/IN01/DSIC/GSIPR**, e seu anexo, **(Revisão 01)** Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.
- Res. TRE-PB 11/2017, de 13/7/2017, dispõe sobre a Política de Gestão de Riscos da Justiça Eleitoral da Paraíba.

Da Gestão da Continuidade de Negócios

- **Norma Complementar nº 06/IN01/DSIC/GSIPR**, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- Res. TRE-AL 15.822, de 3/7/2017, Institui a política de continuidade de serviços essenciais de Tecnologia da Informação e Comunicação no âmbito da Justiça Eleitoral de Alagoas

Slides de apoio

Plano de ação

Gestão de Incidentes de Segurança da Informação

- Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 21/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Auditoria e Conformidade

- Inclusão no plano da auditoria

Desenvolvimento de Sistemas Seguros

- Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.

Slides de apoio

Plano de ação

Recursos Criptográficos

- IN03-GSI-PR Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.
- **Norma Complementar nº 09/IN01/DSIC/GSIPR**, **(Revisão 02)** Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta.

Tratamento da informação

- IN02-GSI-PR Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.
- **Norma Complementar nº 20/IN01/DSIC/GSIPR**, **(Revisão 01)**Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Encaminhamentos

Plano de ação - SAO

I - implantar controles nos ambientes físicos, visando prevenir danos, furtos, roubos, interferência e acesso não autorizado às instalações e ao patrimônio da Justiça Eleitoral;

- **Identificar o que já tem**

II - implantar controles e proteção contra ameaças externas ou decorrentes do meio ambiente, como incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e desastres naturais;

- **Identificar o que já tem**

IV - adotar as medidas necessárias por ocasião do desligamento de empregados das empresas prestadoras de serviço contratadas e comunicar às demais unidades do Tribunal, com vistas à pertinente remoção dos acessos às informações da Justiça Eleitoral;

- **Identificar o que já tem**

Encaminhamentos

Plano de ação - SGP

I - apoiar a Comissão de Segurança da Informação na missão de assegurar que os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários conheçam suas atribuições e responsabilidades em relação à segurança da informação;

- **Pensar treinamento**

II - adotar as medidas necessárias por ocasião do desligamento de pessoal e comunicar às demais unidades do Tribunal, com vistas à pertinente remoção dos acessos às informações da Justiça Eleitoral;

- **Pensar procedimentos e rotinas**

III - promover a capacitação dos servidores que integram a estrutura de gestão da segurança da informação, no que for pertinente;

- **Norma Complementar nº 17/IN01/DSIC/GSIPR**, Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

Encaminhamentos

Plano de ação - Ascom

I - promover campanhas de conscientização sobre a importância da segurança da informação;

- **Identificar o que já tem**

II - divulgar esta PSI;

- **Identificar o que já tem**

Encaminhamentos

Plano de ação - Audit

I - incluir no escopo do Plano Anual de Auditoria e Conformidade, nos termos estabelecidos no art. 17, a análise do cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes;

- **Inserir na regulamentação**

Encaminhamentos

Plano de ação – Gestão da informação

I - regulamentar e coordenar o processo de classificação da informação no âmbito do Tribunal;

- **Identificar o que já tem**

Tecnologia da Informação e Comunicação

Planejamento Estratégico 2015/2020

Macrodesafio: Fortalecer a Governança de TI

Indicadores

- Índice de Governança de TI
- Índice de satisfação da sociedade com o portal do TRE-DF na Internet
- Disponibilidade da rede de comunicação de dados da Sede com as Zonas Eleitorais

Ações/Projetos Estratégicos

- Adquirir equipamento e software para a pesquisa de satisfação
- Promover as adaptações necessárias no sítio eletrônico do TRE e sistema de acompanhamento processual a fim de garantir pleno acesso às informações disponíveis às pessoas com deficiência visual
- Incluir no sistema de cadastramento de Mesários Voluntários a pergunta “Possui capacitação em Libras?”
- Elaborar estudos para redistribuição de impressoras na Secretaria do TER
- Elaborar projeto de implantação do SEI.
- Elaborar estudos para a viabilização de descarte de equipamentos eletrônicos
- Criar formulário na internet para receber as avaliações daqueles que acessam o portal do TRE-DF

Plano de Gestão

- Adquirir equipamento e software para a emissão de senhas nos Cartórios Eleitorais
- Publicar painéis do planejamento estratégico na internet
- Elaborar estudos para a viabilização de descarte de equipamentos eletrônicos
- Implantar o Sistema Pardal de fiscalização da propaganda eleitoral
- Elaborar e manter catálogo de serviços de TIC
- Elaborar e publicar norma de gestão de ativos de TIC
- Elaborar e publicar processo de software do TRE-DF
- Elaborar e publicar plano de continuidade de serviços essenciais de TIC

Tecnologia da Informação e Comunicação
ENTIC-JUD

Missão

- melhorar a infraestrutura e a governança de TIC para que o Poder Judiciário cumpra sua função institucional

Visão

- ser reconhecido como um referencial em governança, gestão e infraestrutura da Tecnologia da Informação e Comunicação

Atributos

- a) acessibilidade e usabilidade
- b) celeridade
- c) inovação
- d) responsabilidade social e ambiental
- e) transparência

Objetivos estratégicos

a) Recursos:

- Obj. 1. Aperfeiçoar as competências gerenciais e técnicas de pessoal
- Obj. 2. Prover infraestrutura de TIC apropriada às atividades judiciais e administrativas
- Obj. 3. Aprimorar a gestão orçamentária e financeira

b) Processos Internos:

- Obj. 4. Aperfeiçoar a governança e a gestão
- Obj. 5. Aprimorar as contratações
- Obj. 6. Promover a adoção de padrões tecnológicos
- Obj. 7. Aprimorar e fortalecer a integração e a interoperabilidade de sistemas de informação
- Obj. 8. Aprimorar a segurança da informação

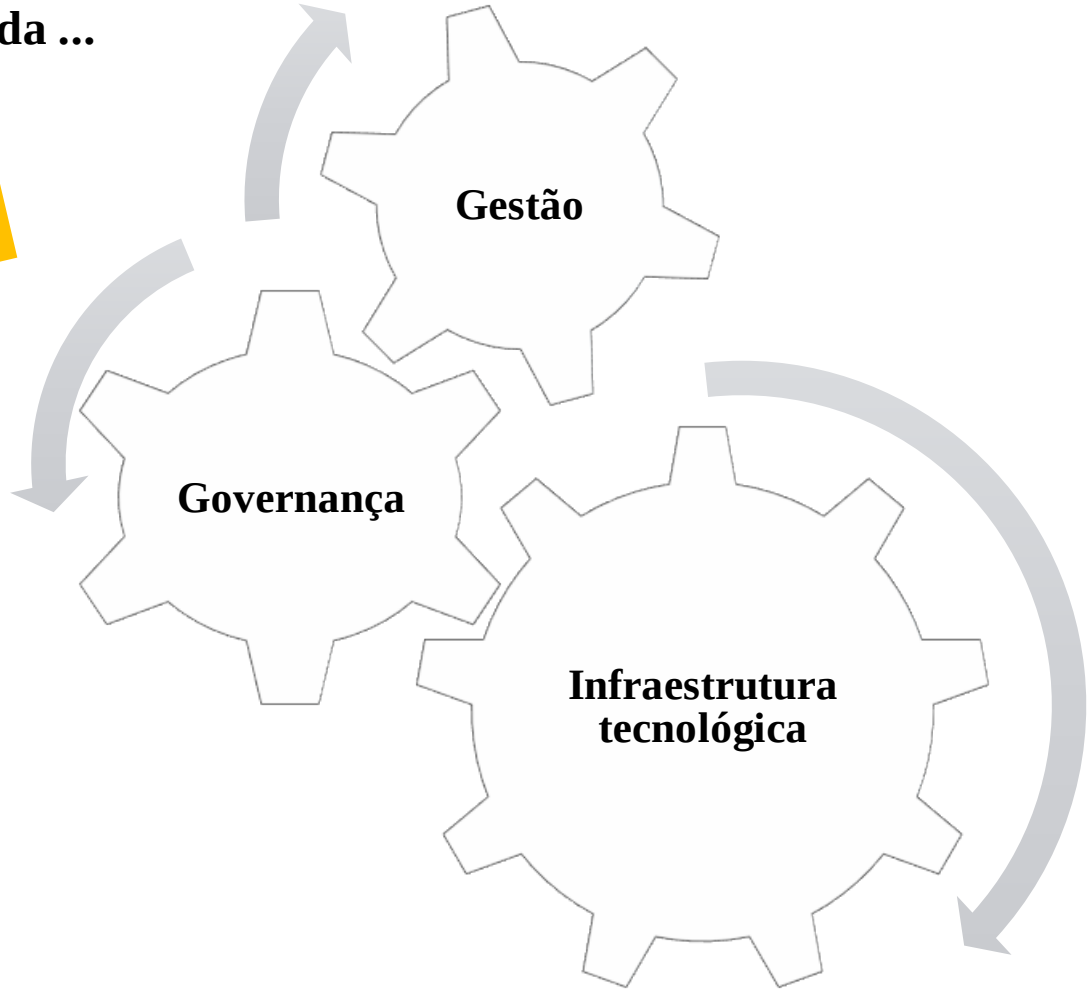
c) Resultados:

- Obj. 9. Primar pela satisfação dos usuários

ENTIC-JUD

Meta

Promover a melhoria da ...



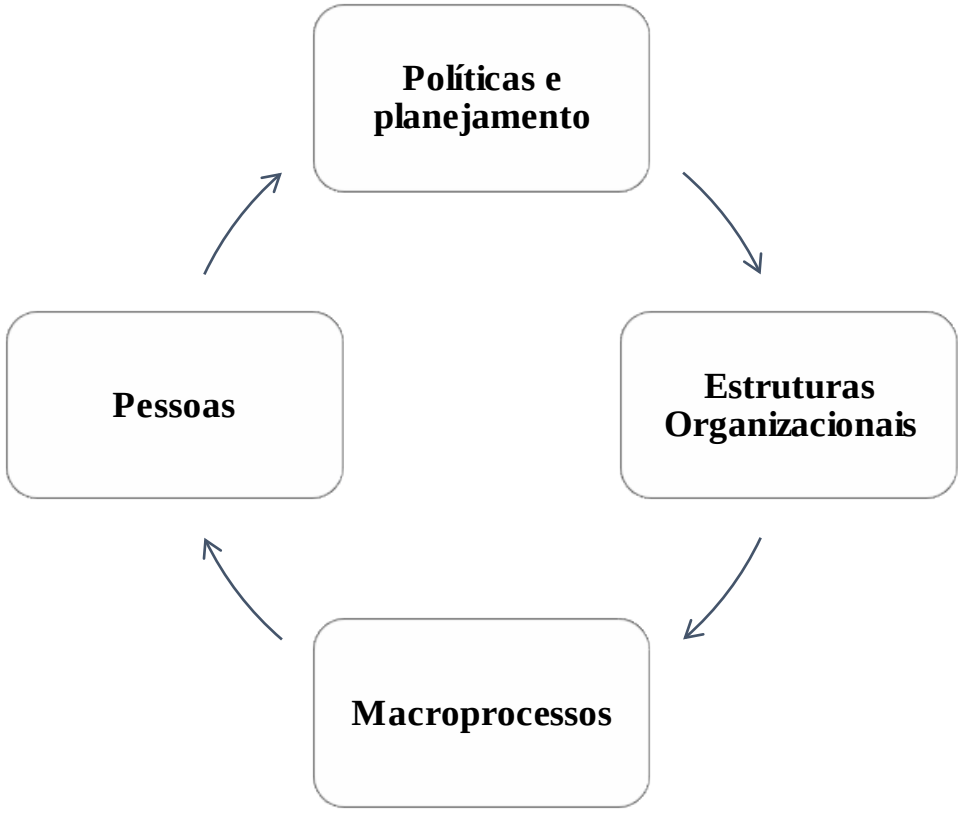
Objetivo amplo

Atinge e compromete toda a instituição

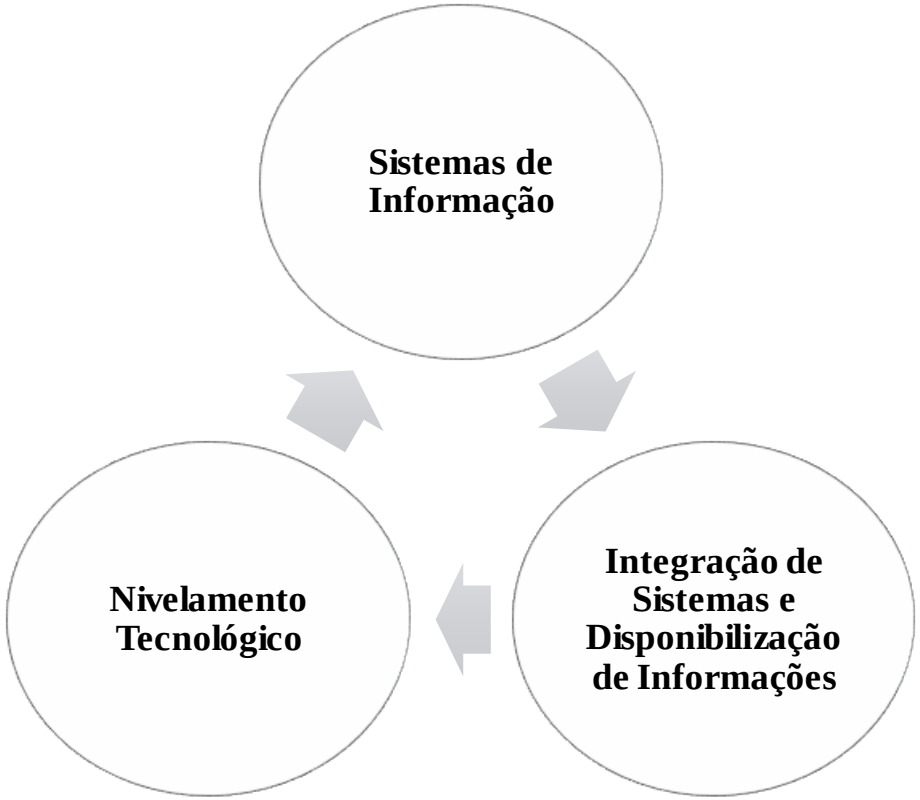
ENTIC-JUD

Diretrizes Estratégicas de Nivelamento

Governança e Gestão



Infraestrutura de TIC



Governança e Gestão

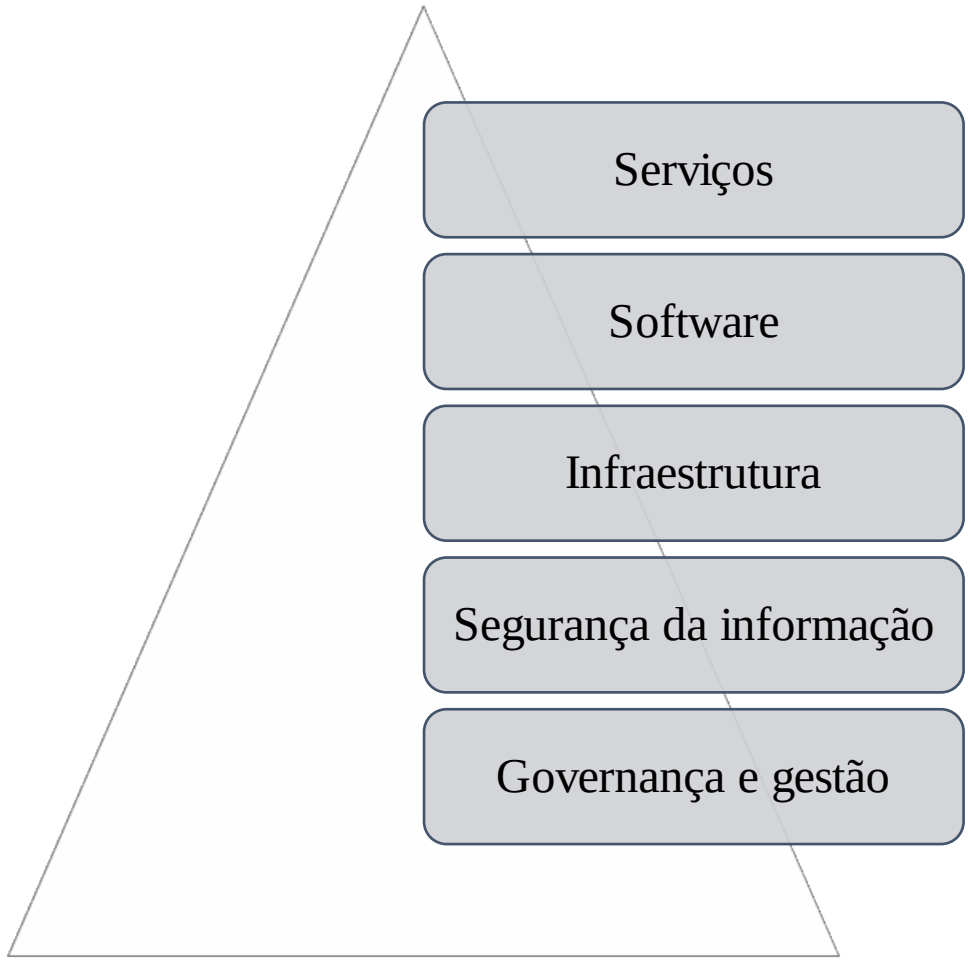
Política e Planejamento

- Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) ✓
- Plano Diretor de Tecnologia da Informação e Comunicação ✓
- Plano de Continuidade de Serviços essenciais ✓
- Processos para gestão de infraestrutura tecnológica ?
- Política de manutenção de documentos eletrônicos ?

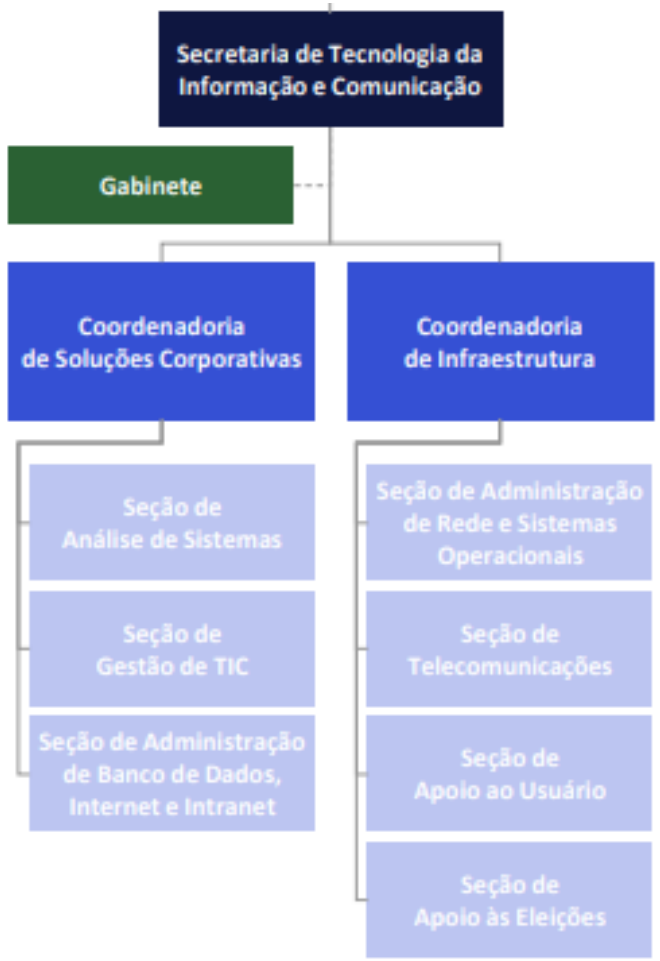
- **Comitê de Governança de Tecnologia da Informação e Comunicação (art. 7º)** ✓
  Port. PR/TRE-DF 187/17, 21/9/17
- **Comitê de Gestão (art. 8º)** ✓
  Port. DG/TRE-DF 296/17, 3/1/17
- **Comitê Gestor de Segurança da Informação (art. 9º)** ✓
  Port. DG/TRE-DF 82/18, 17/5/18
  Port. DG/TRE-DF 94/17, 30/6/17

Governança e Gestão

Estruturas Organizacionais e Macroprocessos

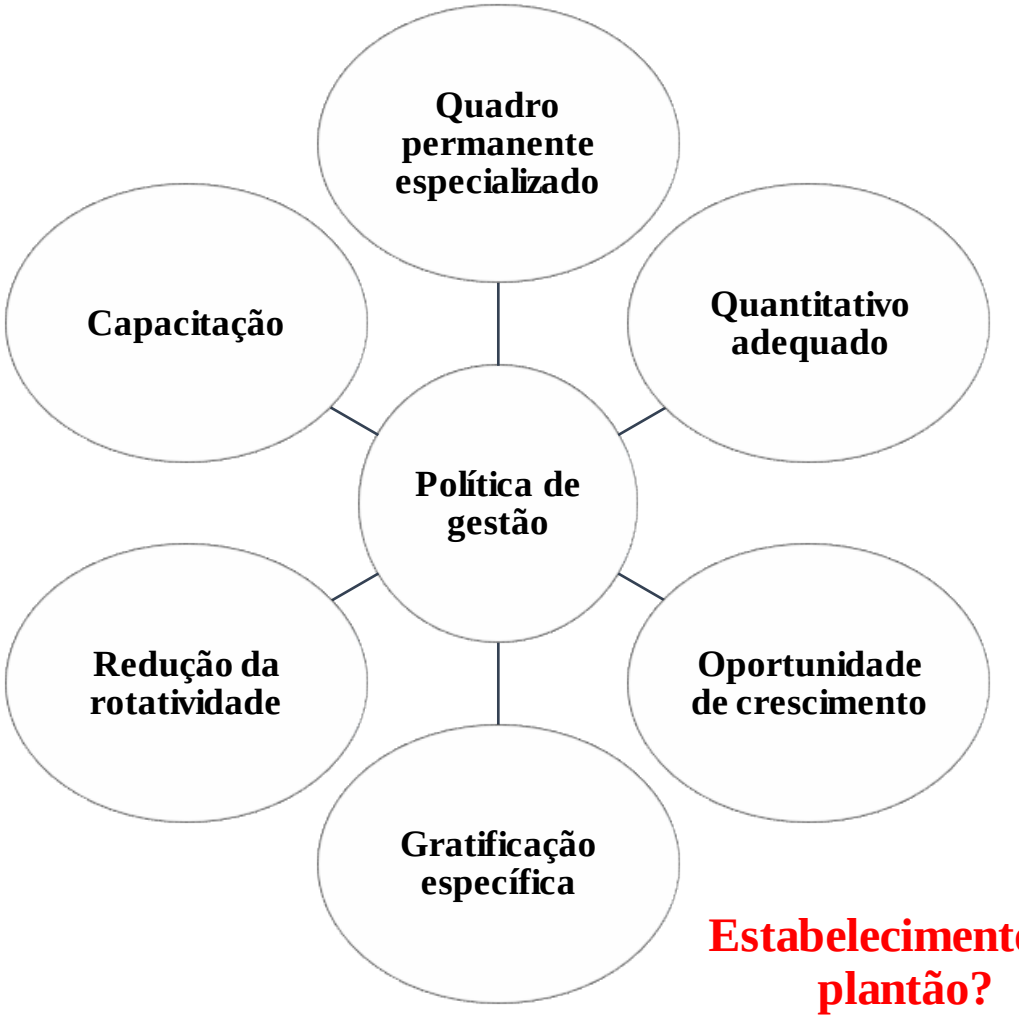


Como as áreas interagem?



Governança e Gestão

Pessoas

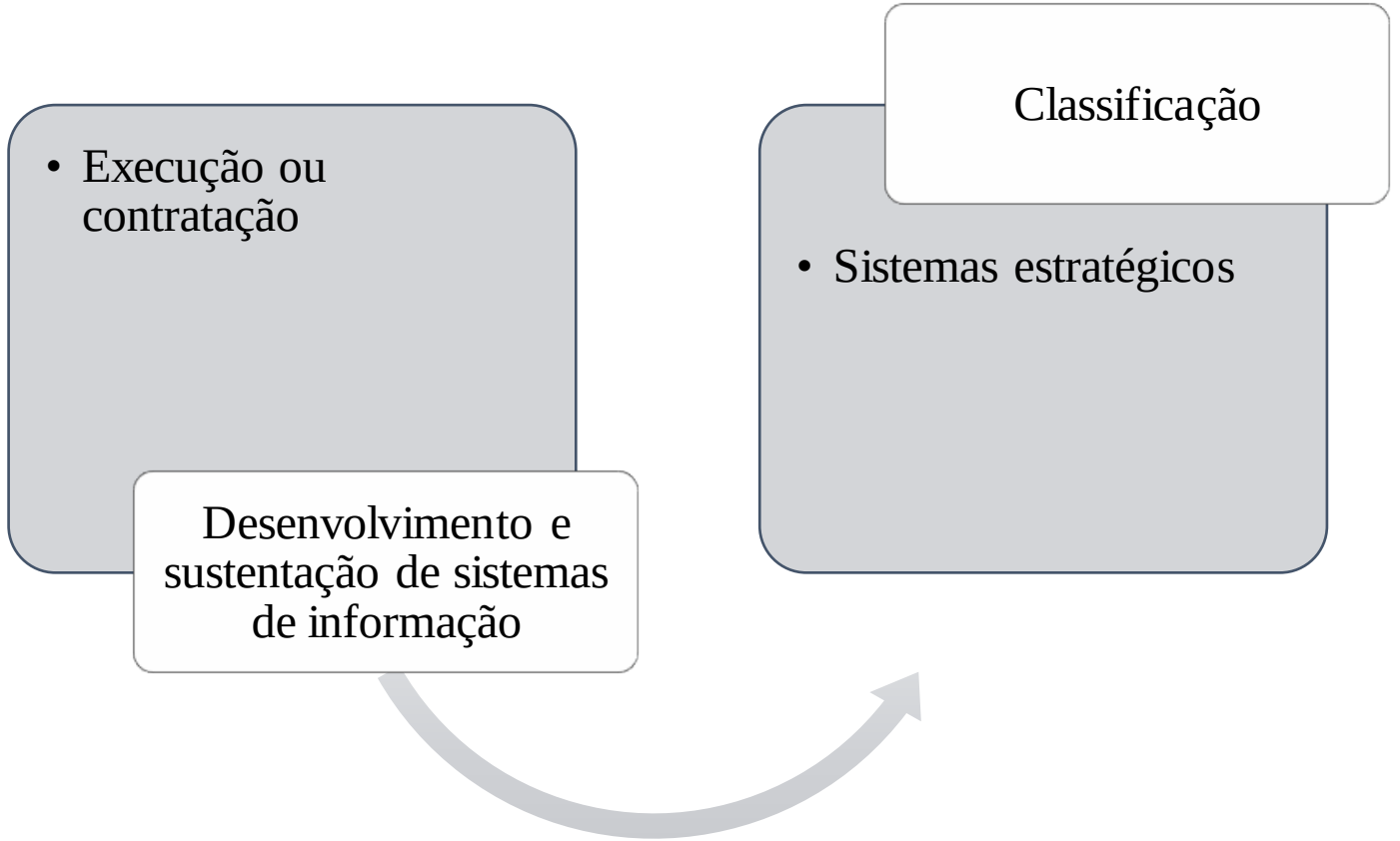


SGP ou STIC?

Estabelecimento de plantão?

Infraestrutura de TIC

Sistemas de Informação



Infraestrutura de TIC

Integração

Garantia de integração entre instâncias

- Modelo Nacional de Interoperabilidade do Poder Judiciário e do Ministério Público

Infraestrutura de TIC

Nivelamento

I – 1 (uma) estação de trabalho do tipo *desktop*

II – 1 (uma) estação de trabalho do tipo *desktop* ou 1 (um) computador portátil com acesso à rede para cada usuário interno nas salas de sessão e de audiência, e uma tela para acompanhamento dos usuários externos

III – equipamento de impressão e/ou de digitalização compatível com as demandas de trabalho

IV – 1 (uma) solução de gravação audiovisual de audiência para cada sala de sessão e de audiência, compatível com o MNI

V - *links* de comunicação entre as unidades e o órgão suficientes para suportar o tráfego de dados e garantir a disponibilidade exigida pelos sistemas de informação

VI – 2 (dois) *links* de comunicação do órgão com a internet, mas com operadoras distintas para acesso à rede de dados

VII – 1 (um) ambiente de processamento central (*DataCenter*) com requisitos mínimos de segurança e de disponibilidade estabelecidos em normas nacionais e internacionais

VIII – 1 (uma) solução de *backup* com capacidade suficiente para garantir a salvaguarda das informações digitais armazenadas

IX – 1 (uma) solução de armazenamento de dados e respectivos *softwares* de gerência

X – 1 (um) parque de equipamentos servidores suficientes para atender às necessidades de processamento de dados dos sistemas e serviços do órgão

XI - pelo menos 1 (uma) solução de videoconferência corporativa para a sede de cada tribunal

XII – 1 (uma) central de serviços de 1º e de 2º níveis para atendimento de requisições efetuadas pelos usuários internos e tratamento de incidentes no que se refere ao uso de serviços e sistemas essenciais

XIII - rede sem fio para a promoção dos serviços ofertados aos usuários e respeitando a política de segurança da informação de cada órgão, sempre que possível

Desdobramentos

Execução

Plano de trabalho			
Grupo 1	**Grupo 2**	**Grupo 3**	**Grupo 4**
Da governança e da gestão de Tecnologia da Informação e Comunicação o prazo é de até 1 (um) ano, contado após a vigência desta Resolução	Dos padrões de desenvolvimento e de sustentação de sistemas de informação é de até 2 (dois) anos, contados após a vigência desta Resolução	Da infraestrutura tecnológica o prazo é de até 3 (três) anos, contados após a vigência desta Resolução	Do quadro permanente de servidores e da elaboração de política de gestão de pessoas prazo é de até 4 (quatro) anos, contados após a vigência desta Resolução

1º/1/16

1º/1/17 → 1º/1/18 → 1º/1/19 → 1º/1/20

Desdobramentos

Acompanhamento e revisão