PLANO DE AÇÃO - GOVERNANÇA E GESTÃO DE TECNOLOGIA E INFORMAÇÃO - TCU 2024

PAGINA	QUESTAO	UNIDADE GESTORA	RESPOSTAS DAS QUESTÕES E SUBQUESTÕES 2024	EVIDÊNCIAS DAS QUESTÕES E SUBQUESTÕES	ATÉ QUANDO PODERÁ SER IMPLANTADO?	STATUS	ANOTAÇÕES
4210. Realizar planejamento de tecnologia da informação	4211. A organização executa processo de planejamento de tecnologia da informação	STI	Adota em maior parte ou totalmente				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) as áreas demandantes de soluções de TI participam do processo de planejamento de tecnologia da informação.	STI	Sim	A construção do Plano Diretor de TI 2023/2025 contou com a participação das demais unidades do Tribunal, sobretudo para a elaboração do Anexo - Demandas de Soluções, que por sua vez é precedido de um levantamento anual de soluções de TI, no qual se assegura o alinhamento ao planejamento estratégico.			
	b) a organização estabeleceu critérios para orientar a seleção e a priorização das iniciativas de TI (projetos e ações) e os mantêm atualizados.	STI	Sim	Foram utilizados critérios de priorização no PDTI 2023/2025 definidos no Procedimento SEI n. 0000254-56.2024.6.01.8000, a título de exemplo.			
	c) as análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações).	STI	Adota em maior parte ou totalmente	Os formulários preenchidos pelas unidades, apresentam os requisitos do item.			
	d) o processo de planejamento de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).	STI	Adota em maior parte ou totalmente	Resolução TRE-AC n. 1.755/2022 e Planejamento Estratégico Institucional 2021/2026 (0620569). Por meio da Portaria DG n. 126/2023 aprovou o Plano Diretor de TI 23/25. (procedimento SEI nº 0001960-11.2023.6.01.8000)			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Planejamento de Tecnologia da Informação; Risco; TI (Tecnologia da Informação).						
4210. Realizar planejamento de tecnologia da informação	4212. A organização possui plano de tecnologia da informação vigente	STI	Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/planejamento-de-servicos-de-ti/tre-ac-plano-diretor-de-tecnologia-da-informacao/@@download/file/PLANO%20DIRETOR%20DE%20TECNOLOGIA%20DA%20INFORMA%C3%87%C3%83O%202023%202.pdf			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) o plano de tecnologia da informação (plano de TI) é aprovado pelo dirigente máximo da organização ou por dirigente ou colegiado que integra a alta administração.		Sim	Portaria DG n. 126/2023			
	b) o plano de TI é publicado na internet, para fácil acesso de partes interessadas e da sociedade.		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/planejamento-de-servicos-de-ti/tre-ac-plano-diretor-de-tecnologia-da-informacao/@@download/file/PLANO%20DIRETOR%20DE%20TECNOLOGIA%20DA%20INFORMA%C3%87%C3%83O%202023%202.pdf			
	c) o plano de TI fundamenta a proposta orçamentária da área de TI e o plano de contratações.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	d) as iniciativas de TI (projetos e ações) constantes do plano de TI alinham-se aos objetivos e iniciativas definidos no plano estratégico e demais planos institucionais, assim como, quando aplicável, às estratégias e objetivos estabelecidos por instâncias de governança superiores (p. ex.: Estratégia de Governança Digital - EGD, Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD).		Sim	https://sgpweb2.tre-ac.jus.br/paginaib/index.html?IB=monitoramento-tic			
	e) é feito acompanhamento concomitante à execução do plano de TI, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessário.		Sim	https://sgpweb2.tre-ac.jus.br/paginaib/index.html?IB=monitoramento-tic			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Dirigente máximo; Estratégia; Partes interessadas; Planejamento de Tecnologia da Informação; Plano de Tecnologia da Informação; TI (Tecnologia da Informação).						
4220. Gerir serviços de tecnologia da informação	4221. A organização elabora um catálogo de serviços de tecnologia da informação e monitora níveis de serviço		Sim				
	a) o catálogo contém as metas definidas para cada serviço (p. ex.: prazos de entrega, horários de serviço e de suporte, bem como pontos de contato para solicitação do serviço, envio de sugestões, esclarecimento de dúvidas e reporte de incidentes).		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	b) o catálogo está atualizado e as informações que nele constam são compatíveis com os Acordos de Níveis de Serviço (ANS) estabelecidos pela área de tecnologia da informação e as áreas de negócio da organização.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	c) o catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	d) são formalizados ANS contendo metas de nível de serviço acordadas com representantes das áreas de negócio clientes.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	e) a área de gestão de tecnologia da informação monitora continuamente o alcance dos níveis de serviço estabelecidos nos ANS.		Sim	Monitora via sistema interno - GLPI			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Área de gestão de tecnologia da informação; Catálogo de serviços de TI; Gestão de serviços de tecnologia da informação; Meta; Serviços de tecnologia da informação; TI (Tecnologia da Informação); Usuário.						
4220. Gerir serviços de tecnologia da informação	4222. A organização executa processo de gestão de mudanças		Sim				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização estabeleceu critérios para orientar a aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais).		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	b) mudanças são previamente comunicadas a todas as partes que possam ser afetadas.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	c) identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	d) a realização de cada mudança é precedida de planejamento e testes.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	e) mudanças executadas são rastreáveis e monitoradas, com vistas à avaliação de sua efetividade e para permitir ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e testes.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	f) o processo de gestão de mudanças está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Efetividade; Prática de habilitação de mudança.						
4220. Gerir serviços de tecnologia da informação	4223. A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)		Sim				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização mantém uma base de dados consolidada e atualizada com as configurações dos serviços e ativos de TI e o relacionamento entre eles.		Sim	Utilização das ferramentas: GLPI			
	b) a base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças.		Sim	Utilização da ferramenta: GLPI			
	c) o processo de gestão de configuração e ativos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).		Sim	Portaria Presidência n. 138/2023 https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de serviços de tecnologia da informação; Prática de gerenciamento de configuração e ativos; Serviços de tecnologia da informação; TI (Tecnologia da Informação).						
4220. Gerir serviços de tecnologia da informação	4224. A organização executa processo(s) de gestão de incidentes de serviços de tecnologia da informação e de incidentes de segurança da informação		Adota em maior parte ou totalmente				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização definiu regras para a priorização e o escalamento de incidentes.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/gestao-de-identidade-e-de-controle-de-acessos/@@download/file/Gest%C3%A3o%20de%20Identidade%20e%20de%20Controle%20de%20Acessos.pdf			
	b) a resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/gestao-de-identidade-e-de-controle-de-acessos/@@download/file/Gest%C3%A3o%20de%20Identidade%20e%20de%20Controle%20de%20Acessos.pdf			

	c) há base(s) de conhecimento que registra(m) erros conhecidos e problemas, de modo a tornar eficiente e efetiva a resolução de incidentes.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/gestao-de-identidade-e-de-controle-de-acesso/@@download/file/Gest%C3%A3o%20de%20Identidade%20e%20de%20Controle%20de%20Acesso.pdf			
	d) o(s) processo(s) de gestão de incidentes está(ão) formalizado(s) (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/gestao-de-identidade-e-de-controle-de-acesso/@@download/file/Gest%C3%A3o%20de%20Identidade%20e%20de%20Controle%20de%20Acesso.pdf			
	e) a organização definiu procedimentos e responsabilidades quanto à notificação e ao tratamento das notificações de incidentes de segurança da informação, bem como quanto à adoção de ações emergenciais, diretrizes para escalamento e comunicação interna e externa.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/gestao-de-identidade-e-de-controle-de-acesso/@@download/file/Gest%C3%A3o%20de%20Identidade%20e%20de%20Controle%20de%20Acesso.pdf			
	f) a organização definiu procedimentos e responsabilidades quanto à análise dos incidentes, identificação de causas raízes e planejamento e implementação de ações corretivas.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/gestao-de-identidade-e-de-controle-de-acesso/@@download/file/Gest%C3%A3o%20de%20Identidade%20e%20de%20Controle%20de%20Acesso.pdf			
	g) a organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente.		Sim	https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/gestao-de-identidade-e-de-controle-de-acesso/@@download/file/Gest%C3%A3o%20de%20Identidade%20e%20de%20Controle%20de%20Acesso.pdf			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Gestão de serviços de tecnologia da informação; Prática de gestão de incidentes; Segurança da Informação; Serviços de tecnologia da informação; TI (Tecnologia da Informação).						
4230. Gerir riscos de tecnologia da informação e riscos de segurança da informação	**4231. A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio**		**Adota em maior parte ou totalmente**	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/plano-de-gestao-de-riscos-de-			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização identifica e avalia os riscos associados com o uso de Tecnologia da Informação nos processos organizacionais críticos para o negócio (Riscos de TI).		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/plano-de-gestao-de-riscos-de-ti/@@download/file/plano%20de%20gestao%20de%20riscos%20de%20ti%20versao%20final.pdf			
	b) a organização trata os Riscos de TI com base em um plano de tratamento de risco.		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/vie			
	c) o processo de gestão dos riscos de tecnologia da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Critérios de análise e avaliação de riscos; Fonte de risco; Gestão de riscos; Identificação de riscos; Limites de exposição ao risco; Mitigar risco; Processo de gestão de riscos; Resposta a risco; Risco de Tecnologia da Informação; TI (Tecnologia da Informação); Tratamento de risco.						
4230. Gerir riscos de tecnologia da informação e riscos de segurança da informação	**4232. A organização executa processo de gestão de riscos de segurança da informação**		**Sim**	**https://www.tre-ac.jus.br/institucional/planejamento-estrategico/tecnologia-da-informacao-e-comunicacao-tic**			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização identifica e avalia riscos de segurança da informação.		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/plano-de-gestao-de-riscos-de-ti/@@download/file/plano%20de%20gestao%20de%20riscos%20de%20ti%20versao%20final.pdf			
	b) a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos.		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/plano-de-gestao-de-riscos-de-ti/@@download/file/plano%20de%20gestao%20de%20riscos%20de%20ti%20versao%20final.pdf			
	c) a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação.		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/plano-de-gestao-de-riscos-de-ti/@@download/file/plano%20de%20gestao%20de%20riscos%20de%20ti%20versao%20final.pdf			
	d) o processo de gestão de riscos de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)		Sim	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/plano-de-gestao-de-riscos-de-ti/@@download/file/plano%20de%20gestao%20de%20riscos%20de%20ti%20versao%20final.pdf			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Critérios de análise e avaliação de riscos; Fonte de risco; Gestão de riscos; Identificação de riscos; Limites de exposição ao risco; Mitigar risco; Processo de gestão de riscos; Resposta a risco; Risco de Segurança da Informação; Segurança da Informação; Tratamento de risco.						
4230. Gerir riscos de tecnologia da informação e riscos de segurança da informação	**4233. A organização executa processo de gestão de continuidade de serviços de tecnologia da informação**		**Adota em maior parte ou totalmente**				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização elabora um plano de continuidade de serviços de TI.		Sim	SEI N. 269279			
	b) as ações e os prazos definidos no plano de continuidade de serviços de TI fundamentam-se em análises de impacto no negócio (AIN/BIA) realizadas sobre os processos organizacionais críticos.		Sim				
	c) o plano de continuidade de serviços de TI é testado e revisado periodicamente.		Não				
	d) o processo de gestão de continuidade de serviços de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).		Sim	SEI N. 269279			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Análise de impacto no negócio; Gestão de continuidade do negócio; Plano de continuidade do negócio; Serviços de tecnologia da informação; TI (Tecnologia da Informação).						
4240. Definir políticas de responsabilidades para a	**4241. A organização dispõe de uma política de segurança da informação**		**Sim**	https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a política declara o comprometimento da alta administração e estabelece princípios, diretrizes, objetivos, estruturas e responsabilidades relativos à segurança da informação.		Sim	Portaria TRE-AC n. 1.776/2022 https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-			
	b) a política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação.		Sim	Portaria TRE-AC n. 1.776/2022 https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-			
	c) a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação.		Sim	Portaria TRE-AC n. 1.776/2022 https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-			
	d) a política é mantida atualizada por meio de revisões periódicas e é amplamente comunicada a empregados, servidores, colaboradores e partes externas relevantes.		Sim	Portaria TRE-AC n. 1.776/2022 https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Colaboradores; Gestão de riscos; Política de segurança da informação; Risco de Segurança da Informação; Segurança da Informação.						
4240. Definir políticas de responsabilidades para a gestão da segurança da informação	**4242. A organização dispõe de comitê de segurança da informação**		**Adota em maior parte ou totalmente**	nenhum			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo.		Adota em maior parte ou totalmente	Procedimento de registro de reuniões da CSI 0002223-19.2018.6.01.8000			
	b) o comitê formula diretrizes para a segurança da informação.		Adota em maior parte ou totalmente	Implementação do Manual de Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.			

	c) o comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação, como resultado do monitoramento do ambiente interno e externo.		Sim	0002171-23.2018.6.01.8000 – Política de Backup 0002323-71.2018.6.01.8000 – Controle de Acesso físico e lógico 0003710-24.2018.6.01.8000 – Política de uso de ativos de TIC 0002322-86.2018.6.01.8000 – Plano de Continuidade dos Serviços de TIC 0001779-49.2015.6.24.8000 - 0165055 - IN 29 / 2017 -Dispõe sobre o os procedimentos para o tratamento e resposta a incidentes em redes computacionais no âmbito do TRE/AC.			
	d) o comitê é composto por representantes de áreas relevantes da organização.		Sim	Portaria 51/2022 - https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/legislacao/TREAC_portarias_presidencia_2022/tre-ac-portaria-presidencia-51-2022/@@download/file/PORTARIA%20PRESID%C3%BANCIA%20N%C2%BA%2051_2022.pdf			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Comitê de segurança da informação; Segurança da Informação.						
4240. Definir políticas de responsabilidades para a gestão da segurança da informação	**4243. A organização possui um gestor institucional de segurança da informação**		**Adota em maior parte ou totalmente**	Portaria PRESI 51/2022 https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/legislacao/TREAC_portarias_presidencia_2022/tre-ac-portaria-presidencia-51-2022/@@download/file/PORTARIA%20PRESID%C3%BANCIA%20N%C2%BA%2051_2022.pdf			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) o gestor institucional de segurança da informação foi designado formalmente pela alta administração.		**Adota em maior parte ou totalmente**	Portaria PRESI 51/2022			
	b) o gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional.		**Adota em maior parte ou totalmente**	A ACSEG é a Assistência da Cibersegurança. O Servidor Silvio é responsável pela gestão juntamente com a STI.			
	c) o gestor institucional de segurança da informação promove e coordena ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e colaboradores.		**Adota em maior parte ou totalmente**	Realiza reuniões 0596791 e 0598378			
	d) o gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências (nível hierárquico adequado, pessoal suficiente alocado etc.).		**Adota em maior parte ou totalmente**	A ACSEG é a Assistência da Cibersegurança. O Servidor Silvio é responsável pela gestão juntamente com a STI.			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Colaboradores; Competências; Gestão de riscos; Gestor; Gestor institucional de segurança da informação; Partes interessadas; Processo de gestão de riscos; Risco de Segurança da Informação; Segurança da Informação.						
4250. Estabelecer processos e atividades para a gestão da segurança da informação	**4251. A organização executa processo de controle de acesso à informação e aos ativos associados à informação**		**Adota em maior parte ou totalmente**	Controle de acesso é realizado por meio do uso de senhas, certificados digitais (em alguns casos), duplo fator de autenticação para acesso remoto, etc.			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização mantém um inventário dos ativos associados à informação e identifica as informações críticas que os ativos armazenam, processam ou transmitem.		**Sim**	O inventário de ativos é realizado pelo Plugin do FOG.			
	b) a organização implementa controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio.		**Sim**	Controle de acesso é realizado por meio do uso de senhas, certificados digitais (em alguns casos), duplo fator de autenticação para acesso remoto, etc.			
	c) os controles de acesso implementados na organização aplicam o princípio 'necessidade de conhecer', o qual prescreve que deve haver necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio 'privilégio mínimo', o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades.		**Sim**	Sim, quando é feita a qualificação e identificação do usuário para acesso aos sistemas, por meio de requisição formal do superior imediato, com pedido e justificativa registrados no sistema de chamados:			
	d) a organização aplica o modelo de segurança de 'confiança zero' (zero trust), o qual preconiza que uma identidade não é confiável até que seja adequadamente verificada para cada acesso pretendido, independentemente de perímetros.		**Não**	não há			
	e) a organização analisa criticamente, a intervalos regulares, os direitos de acesso lógicos e físicos existentes, com vistas à remoção de direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos.		**Sim**	não há			
	f) a organização instituiu uma Política de Controle de Acesso (PCA), a qual estabelece princípios, objetivos, diretrizes, principais atividades e responsabilidades relativos ao processo de controle de acesso.		**Sim**	0002323-71.2018.6.01.8000 – Controle de Acesso físico e lógico			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Política.						
4250. Estabelecer processos e atividades para a gestão da segurança da informação	**4252. A organização executa processo para classificação e tratamento de informações**						
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) as informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção.			Galvão, essas questões são de competência da LGPD. Reinaldo.			
	b) a organização informa em seu sítio eletrônico as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, bem como fornece informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas de tratamento que utiliza.			Galvão, essas questões são de competência da LGPD. Reinaldo.			
	c) informações sigilosas em razão de sua imprescindibilidade à segurança da sociedade ou do Estado são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção.			Galvão, essas questões são de competência da LGPD. Reinaldo.			
	d) informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção.			Galvão, essas questões são de competência da LGPD. Reinaldo.			
	e) informações críticas para a organização em razão de necessidades do negócio (p. ex.: requisitos associados à integridade, disponibilidade, autenticidade ou a outros atributos da informação) são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção.			Galvão, essas questões são de competência da LGPD. Reinaldo.			
	f) o processo de classificação e tratamento de informações está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).			Galvão, essas questões são de competência da LGPD. Reinaldo.			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Competências; Processo para classificação e tratamento de informações; Tratamento de dados pessoais.						
4250. Estabelecer processos e atividades para a gestão da segurança da informação	**4253. A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem**		**Adota em maior parte ou totalmente**				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização gerencia (inventaria e controla) os softwares instalados nos dispositivos conectados em sua rede.		**Sim**	Realizado pelo GLPI.			
	b) a organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio.		**Sim**	Realizado pelo GLPI.			
	c) a organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio.		**Sim**	Realizado pelo GLPI.			
	d) a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio.		**Adota em maior parte ou totalmente**	Realizado pelo SYSLOG-NG. A análise ralizada pela SCSEG.			
	e) a organização aplica controles compensatórios para o uso de privilégios administrativos em seus ativos de software, de hardware e de rede críticos para o negócio.		**Sim**	Utiliza segmentação de rede para o gerenciamento dos ativos críticos, bem como multiplo fator de autenticação.			
	f) a organização implementa cópias regulares de segurança (backup) das informações em meio digital, conforme as melhores práticas e as necessidades de negócio, incluindo a realização periódica de testes de recuperação das informações.		**Sim**	É realizado pelo sitema Bacula.			
	g) a organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração).		**Há decisão formal ou plano aprovado para adotá-lo**	Contratação em andamento.			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Gestão de ativos; Segurança dos recursos de processamento da informação.						
4260. Gerir desenvolvimento de soluções e inovação	**4261. A organização executa um processo de software**		**Adota em maior parte ou totalmente**	Portaria TRE-AC n. 60/2023 https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/portaria-diretoria-geral-no-60-2023/@@download/file/PORTARIA%20DIRETORIA-GERAL%20N%C2%BA%2060%202023%20-%20SEI_0000799_97.2022.6.01.8000.pdf			
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) o processo de software utilizado pela organização promove a participação de representante da área de negócio como integrante da equipe de desenvolvimento ou aquisição de software, desde sua concepção até a aceitação final.		**Adota em maior parte ou totalmente**				
	b) o processo de software da organização promove desde a concepção a identificação de requisitos de segurança da informação, bem como a gestão permanente desses requisitos durante todo o ciclo de vida do software.		**Sim**	Portaria TRE-AC n. 60/2023 https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/portaria-diretoria-geral-no-60-2023/@@download/file/PORTARIA%20DIRETORIA-GERAL%20N%C2%BA%2060%202023%20-%20SEI_0000799_97.2022.6.01.8000.pdf			
	c) o processo de software da organização promove desde a concepção a identificação de requisitos de acessibilidade e de usabilidade, bem como a gestão permanente desses requisitos durante todo o ciclo de vida do software.		**Adota em maior parte ou totalmente**				
	d) a organização assegura os seus direitos autorais, de propriedade e de uso relativamente ao software que desenvolve por meio de contratação.		**Não se aplica**				

	e) o processo de software está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).		**Sim**	Portaria TRE-AC n. 60/2023 https://www.tre-ac.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tre-ac.jus.br/institucional/planejamento-estrategico/normativos-de-ti/portaria-diretoria-geral-no-60-2023/@@download/file/PORTARIA%20DIRETORIA-GERAL%20N%C2%BA%2060%202023%20-%20SEI_0000799_97.2022.6.01.8000.pdf			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área de negócio; Processo de software; Segurança da Informação.						
4260. Gerir desenvolvimento de soluções e inovação	**4262. A organização executa processo de gestão de projetos de tecnologia da informação**		**Há decisão formal ou plano aprovado para adotá-lo**				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) a organização possui base de dados consolidada (portfólio) de projetos de tecnologia da informação.		**Há decisão formal ou plano aprovado para adotá-lo**	Processo SEI n. 0000893-74.2024.6.01.8000 para adotar a gestão de projetos.			
	b) escopo, custos, uso de recursos e cumprimento de prazos são gerenciados em cada projeto.		**Há decisão formal ou plano aprovado para adotá-lo**	Processo SEI n. 0000893-74.2024.6.01.8000 para adotar a gestão de projetos.			
	c) é realizada a gestão de riscos de cada um dos projetos de alta materialidade ou alta relevância.		**Há decisão formal ou plano aprovado para adotá-lo**	Processo SEI n. 0000893-74.2024.6.01.8000 para adotar a gestão de projetos.			
	d) o processo de gestão de projetos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades).		**Há decisão formal ou plano aprovado para adotá-lo**	Processo SEI n. 0000893-74.2024.6.01.8000 para adotar a gestão de projetos.			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de riscos; Política; Projeto; TI (Tecnologia da Informação).						
4260. Gerir desenvolvimento de soluções e inovação	**4263. A organização faz uso de Inteligência Artificial em seus processos internos ou finalísticos**		**Sim**				
	Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:						
	a) há colaboradores que experimentaram e testaram projetos de IA, embora com pouca ou sem padronização.		**Sim**	A utilização do sistema JANUS de automação de processos judiciais			
	b) há projetos iniciais de prova de conceito (POC) elaborados e em fase piloto.		**Não**				
	c) há projetos de IA em produção.		**Sim**	O sistema JANUS de automação de processos judiciais está em produção.			
	d) a alta administração patrocina projetos de IA ou há orçamento exclusivo para projetos de IA.		**Sim**	A adoção do JANUS foi determinação da alta administração do Tribunal.			
	e) há unidade especializada em inteligência artificial, com especialistas em IA e capacidade para desenvolver projetos.		**Não**				
	f) os novos projetos digitais, incluindo revisões de processo para otimização, consideram a utilização de IA como forma de agregar valor		**Não se aplica**				
	g) o uso de inteligência artificial é costumeiro e esperado na execução dos processos de negócio, sendo que os aplicativos que utilizam 'IA' interagem de forma produtiva dentro da organização e com o ecossistema de negócios.		**Adota em maior parte ou totalmente**	O uso de IA é incipiente, porém já produz otimização dos processos.			
	Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Adicionar/criar valor; Alta Administração; Gestão de riscos; Colaboradores; Projeto.