nº 13.853/2019, sobre a proteção de dados pessoais, que altera a Lei nº 12.965/2014 (Marco Civil da Internet);

RESOLVE:

Art. 1º Estabelecer planos de ação com vistas ao cumprimento dos manuais de Proteção de Infraestruturas Críticas de TIC, Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital e Gestão de Identidades, estabelecida nos Anexos IV, V e VI da Portaria CNJ nº 162, de 10 de junho de 2021, na forma do Anexo deste normativo.

Art. 2 Esta Portaria entra em vigor na data de sua publicação.

Waldir Sebastião de Nuevo Campos Junior

Presidente

ANEXO I

PLANO DE AÇÃO - Proteção de Infraestruturas Críticas de TIC

ID	Requisito	Atividades necessárias	Área	Prazo previsto	Referência
1	**Inventário e controle de ativos de hardware**				
1.1	Utilizar uma ferramenta de descoberta ativa para identificar dispositivos conectados à rede da organização, e atualizar o inventário de hardware.	– Aquisição da solução – Treinamento – Implantação	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
1.2	Utilizar os registros (logs) do Dynamic Host Configuration Protocol (DHCP) em todos os servidores ou utilizar ferramentas de gerenciamento de endereços IP para atualizar o inventário de ativos de hardware.	Integração com a solução a ser adquirida no item 1.1	ScRS	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
1.3	Manter inventário atualizado e preciso de todos os ativos de tecnologia que detenham o potencial de armazenamento ou processamento de informações. Esse inventário deve incluir ativos de hardware, conectados ou não à rede da organização.	Integração com a solução a ser adquirida no item 1.1	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
1.4	Garantir que o inventário de ativos de hardware armazene o endereço de rede, endereço de hardware, nome do equipamento,	Integração com a solução a ser	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria

1.4	proprietário do ativo e departamento para cada ativo, registrando ainda se foi aprovada ou não a conexão do ativo à rede.	solução a ser adquirida no item 1.1	CID/CSE	30/06/23	CNJ nº 162/2021 – NIST CSF
1.5	Garantir que ativos não autorizados sejam removidos da rede ou colocados em quarentena, ou que o inventário seja atualizado em tempo hábil.	– Revisão da PSI. – Projeto de estudo para implantar esse controle.	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
2	**Inventário e controle de ativos de software**				
2.1	Manter uma lista atualizada de todos os softwares autorizados que sejam necessários à organização para qualquer propósito ou sistema de negócios.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado – Revisão da PSI	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
2.2	Garantir que apenas aplicações ou sistemas operacionais atualmente suportados pelo fabricante sejam adicionados ao inventário de softwares autorizados. Softwares sem suporte devem ser indicados no sistema de inventário.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado – Revisão da PSI	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
2.3	Utilizar ferramentas de inventário de software em toda a organização de forma a automatizar a documentação de todos os softwares que componham sistemas de negócio.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado – Revisão da PSI	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
2.4	O sistema de inventário de software deve registrar nome, versão, fabricante e data de instalação para todos os softwares, incluindo sistemas operacionais autorizados pela organização.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
2.5	O sistema de inventário de software deve ser vinculado ao inventário de ativos de hardware, de forma que todos os dispositivos e softwares associados possam ser rastreados a partir de uma única localidade.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado – Revisão da PSI – Configuração do CITSmart para gerenciamento de ativos (atender servidores Linux)	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
2.6	Garantir que qualquer software não autorizado seja removido, ou que o inventário seja atualizado em tempo hábil.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado – Revisão da PSI	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
2.7	Sistemas segregados física ou logicamente devem ser utilizados para isolar e executar softwares que sejam necessários às	– Identificar sistemas que possam trazer riscos à organização – Projeto na ScRS	CID/CSE	30/06/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº

	operações do negócio, mas que não tragam maior risco à organização.	para rever as configurações de segurança de perímetro			CNJ nº 162/2021 – NIST CSF
3	**Gerenciamento Contínuo de Vulnerabilidade**				
3.1	Utilizar uma ferramenta atualizada e compatível com o SCAP para efetuar varreduras automatizadas em todos os ativos conectados à rede com frequência semanal ou inferior. para identificar todas as vulnerabilidades potenciais nos sistemas da organização.	– Projeto de gerenciamento de vulnerabilidade	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
3.2	Realizar varreduras por vulnerabilidades com contas autenticadas em agentes executados localmente em cada sistema, ou varreduras por scanners remotos que sejam configurados com privilégios elevados nos sistemas que estejam sendo testados.	– Projeto de gerenciamento de vulnerabilidade	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
3.3	Utilizar uma conta dedicada para as varreduras por vulnerabilidades autenticadas, que não deve ser utilizada para quaisquer outras atividades administrativas e que deve ser vinculada a equipamentos específicos, em endereços IP específicos.	– Projeto de gerenciamento de vulnerabilidade	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
3.4	Implantar ferramentas de atualização automatizada de software, de forma a garantir que os sistemas operacionais sejam executados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado – Revisão da PSI	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
3.5	Implantar ferramentas de atualização automatizada de software de forma a garantir que os softwares de terceiros em todos os equipamentos sejam utilizados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	– Aquisição de ferramenta apropriada – Manter catálogo de sistemas atualizado – Revisão da PSI	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
3.6	Utilizar um processo de classificação de riscos para priorizar a remediação de vulnerabilidades descobertas.	– Levantar as vulnerabilidades – Mapear os riscos para as vulnerabilidades identificadas. – Execução do Processo de Gestão de Riscos – Integração com a solução a ser adquirida no item 3.4	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF

4	**Uso controlado de privilégios administrativo**				
4.1	Utilizar ferramentas automatizadas para inventariar todas as contas administrativas, incluindo contas de domínio e contas locais, para garantir que apenas indivíduos autorizados tenham privilégios elevados.	– Elaborar estudos para aquisição de ferramenta	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
4.2	Antes de ativar qualquer novo ativo, modificar todas as senhas padrão de forma consistente com contas de nível administrativo.	– Criar processo de ajuste de senhas padrão e de nível administrativo	CID/CSE	30/06/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
4.3	Garantir que todos os usuários com contas administrativas utilizem uma conta secundária para atividades de privilégio elevado. Essa conta deve ser utilizada somente para atividades administrativas e não para navegação na internet, correio eletrônico ou atividades similares.	– Mapear contas administrativas – Remover acesso a contas administrativas de acesso remoto – Revisão da PSI	CID/CSE	30/06/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF – ISO 27002
4.4	Utilizar autenticação multifator e canais criptografados para todos os acessos de contas administrativas.	– Projeto para implantar o multifator – Projeto para rever configurações de segurança do AD.	CID/CSE	30/04/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
4.5	Garantir que administradores utilizem um equipamento dedicado para todas as tarefas administrativas ou tarefas que requeiram acesso administrativo. Tal equipamento deve estar em rede segregada da rede principal da organização e não deve ter permitido o acesso à internet. Esse equipamento não deverá ser utilizado para a leitura de e-mails, elaboração de documentos, ou navegação na internet.	– Projeto para implantar micros dedicados à administração – Projeto para rever configurações de segurança do AD.	CID/CSE	30/06/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
4.6	Limitar o acesso a ferramentas de scripting (tais como Microsoft PowerShell and Python) exclusivamente a usuários administrativos ou de desenvolvimento que necessitem acessar tais funcionalidades.	– Projeto para rever configurações de segurança do AD.	CID/CSE	30/04/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
4.7	Configurar os sistemas para efetuarem um registro no log e um alerta quando uma conta for adicionada ou removida de qualquer grupo com privilégios administrativos.	– Projeto para rever configurações de segurança do AD. – Implementar o alerta na ferramenta – Implementar processo de gerenciamento de	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF

		LOGs			
4.8	Configurar os sistemas para efetuarem um registro no log e um alerta no caso de logins sem sucesso de uma conta administrativa.	– Projeto para rever configurações de segurança do AD. – Implementar o alerta na ferramenta	CID/CSE	17/12/21	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
5	**Configuração segura para hardware e software em dispositivos móveis, laptops, estações de trabalho e servidores**				
5.1	Manter padrões documentados de configuração segura para todos os sistemas operacionais e softwares autorizados.	– Elaborar Documentação necessária	CID/CSE	30/04/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
5.2	Manter imagens ou templates seguros para todos os sistemas na organização com base nos padrões de configuração aprovados. Todos os novos sistemas implantados ou sistemas existentes que venham a ser comprometidos devem ser instalados ou restaurados a partir dessas imagens ou templates.	– Projeto para implementar imagens ou templates de servidores e serviços – Identificar possíveis falhas nos processos envolvidos – Verificar adequada realização de versionamento e de backup	CID/CSE	30/04/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021 – NIST CSF
5.3	Armazenar as imagens e templates em servidores configurados de forma segura, validados por meio de ferramentas de monitoramento de integridade, de forma a garantir apenas modificações autorizadas nas imagens e templates.	– Projeto para implementar imagens ou templates de servidores e serviços	CID/CSE	30/04/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
5.4	Implantar ferramentas de gerência de configuração de sistemas que automaticamente imponham e reapliquem opções de configuração sobre os sistemas em intervalos regulares agendados.	– Projeto para definir ferramenta e configurações	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
6	**Manutenção, Monitoramento e Análise de Logs de Auditoria**				
6.2	Garantir que o log local tenha sido habilitado em todos os sistemas e dispositivos de rede.	– Implementar processo de gerenciamento de LOGs	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
6.3	Habilitar o log dos sistemas de forma a incluir informações detalhadas, tais como origem do evento, data, usuário, horário, endereços de origem, endereços de destino e outros elementos úteis.	– Implementar processo de gerenciamento de LOGs	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
	Garantir que todos os sistemas que	– Implementar			– Itens 7 e 8 do Anexo IV

6.4	armazenem logs tenham espaço de armazenamento adequado para os logs gerados.	processo de gerenciamento de LOGs	CID/CSE	19/12/22	do Anexo IV da Portaria CNJ nº 162/2021
6.5	Garantir que os logs apropriados sejam agregados em um sistema central de gerenciamento de logs para análises e revisões.	– Implementar processo de gerenciamento de LOGs	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
6.6	Implantar Security Information and Event Management (SIEM) ou ferramenta analítica de logs para correlação e análise de logs.	– Implementar processo de gerenciamento de LOGs	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
6.7	Em uma base regular, revisar os logs para identificar anomalias ou eventos anormais.	– Implementar processo de gerenciamento de LOGs	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
6.8	Em uma base regular, ajustar as configurações do SIEM de forma a melhor identificar eventos que requeiram ações e diminuir o ruído proveniente de eventos não importantes.	– Implementar processo de gerenciamento de LOGs	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
7	**Proteções de e-mail e navegadores web**				
7.1	Garantir que apenas navegadores web e clientes de e-mail suportados possam ser executados na organização, idealmente utilizando apenas a versão mais recente disponibilizada pelo fabricante.	Projeto de atualização do parque de computadores e licenças.	CID/CSE	17/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
7.2	Desinstalar ou desabilitar plug-ins ou aplicações add-on não autorizados para navegadores web e clientes de e-mail.	– Estudo de ferramenta de gerenciamento de ativos (controle de software) – Avaliar ferramentas disponíveis e necessidade de aquisição	CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
7.3	Utilizar filtros de URL baseados em rede de forma a limitar a possibilidade de sistemas se conectarem a websites não aprovados pela organização. Tais filtros devem ser impostos a todos os sistemas da organização, quer se encontrem dentro do espaço físico da organização, quer não.	– Avaliação e ajustes nos sistemas de Proxy e Firewall – Estudo e implementação em equipamentos que usam a VPN com acesso direto a rede do TRE.	CID/CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
7.4	Subscrever serviços de categorização de URLs de forma a garantir que o filtro esteja atualizado com base nas mais recentes definições de categorias de sítios eletrônicos disponíveis	– Avaliação e ajustes nos sistemas de Proxy e Firewall – Estudo e implementação em equipamentos que	CID	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº

	de sítios eletrônicos disponíveis. Sites não categorizados devem ser bloqueados por padrão.	usam a VPN com acesso direto a rede do TRE.			162/2021
7.5	Realizar registros de log de todas as requisições a URLs a partir de cada um dos sistemas da organização, quer nas dependências corporativas, quer em dispositivos móveis, de forma a identificar potenciais atividades maliciosas e auxiliar operadores de incidentes com a identificação de sistemas potencialmente comprometidos.	– Avaliação e ajustes nos sistemas de Proxy e Firewall – Estudo e implementação em equipamentos que usam a VPN com acesso direto a rede do TRE.	CID	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
7.6	Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.	– Projeto para implantar controle e filtragem de DNS	CID	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
7.7	Com o objetivo de diminuir a possibilidade de recebimento de e-mails forjados ou modificados de domínios válidos, implementar políticas e verificações com base no padrão Domain-based Message Authentication, Reporting and Conformance (DMARC), iniciando pela implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM).	– Estudo para implantar, no serviço de e-mail, políticas e verificações com base no padrão DMARC	CID	30/06/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
7.8	Bloquear todos os anexos de e-mail no gateway de correio eletrônico para os tipos de arquivos que sejam desnecessários ao negócio da organização.	– Estudo para avaliação e ajuste, no serviço de e-mail para bloqueio de arquivos/anexos desnecessários ao negócio	CID	17/12/21	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
8	**Defesas contra malware**				
8.1	Utilizar software antimalware gerenciado de forma central para monitorar continuamente e defender cada uma das estações de trabalho e servidores.– Projeto para adequação de todos os servidores com segurança antimalware – Elaborar estudos para aquisição de ferramenta com suporte a Linux, Windows e MAC	– Projeto para adequação de todos os servidores com segurança antimalware – Elaborar estudos para aquisição de ferramenta com suporte a Linux, Windows e MAC	CID/CSE	31/05/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
8.2	Garantir que o software antimalware atualize seu motor de varredura e base de assinaturas de malware de forma regular.	– Elaborar estudos para aquisição de ferramenta com suporte a Linux, Windows e MAC	CID/CSE	31/05/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
	Habilitar funcionalidades anti-exploits, tais como Data Execution Prevention (DEP) ou Address	– Elaborar estudo			

8.3	Space Layout Randomization (ASLR) que estejam disponíveis no sistema operacional, ou implantar ferramentas apropriadas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.	– Elaborar estudo para implementação nos sistemas Linux, MAC e nos servidores corporativos.	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
8.4	Configurar os dispositivos de forma que automaticamente conduzem uma varredura antimalware em mídias removíveis assim que sejam inseridas ou conectadas.	– Elaborar estudo para implementação nos sistemas Linux , MAC e nos servidores corporativos.	CID/CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
8.6	Enviar todos os eventos de detecção de malware para as ferramentas de administração de antimalware e para servidores de logs, para análises e alertas.	– Implementar processo de gerenciamento de LOGs – Projeto de Integração da ferramenta de detecção (TREND) com o servidor de LOGs.	CSE	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
8.7	Habilitar log de pesquisas sobre Domain Name System (DNS) de forma a detectar buscas por nomes de hosts em domínios reconhecidamente maliciosos.	– Estudo para implantar log de pesquisa DNS relativos a domínios maliciosos	CID	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
8.8	Habilitar log de auditoria sobre ferramentas de linha de comando, tais como Microsoft Powershell e Bash.	– Habilitar no Kibana o registro deste tipo de auditoria	CID/CSE	17/12/21	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
9	**Capacidades de recuperação de dados**				
9.1	Garantir que todos os dados dos sistemas tenham cópias de segurança (backups) realizados automaticamente de forma regular.	Levantamento dos backups realizados: ativos administrados pela STI	CID e Gestores dos ativos de TIC	31/03/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
9.2	Garantir que todos os sistemas chave da organização tenham suas cópias de segurança (backups) realizadas como um sistema completo, por meio de processos como a geração de imagem, de forma a permitir uma rápida recuperação de todo o sistema.	Levantamento dos backups realizados dos sistemas essenciais dos ativos administrados pela STI	CID	31/03/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
9.3	Testar a integridade dos dados nas mídias das cópias de segurança de forma regular, por meio da realização de um processo de restauração dos dados, de forma a garantir que o processo de cópia de segurança (backup) esteja sendo executado de forma apropriada.	Projeto para implementar testes de mídias de backups	CID	31/05/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021

9.4	Garantir que as cópias de segurança (backups) sejam apropriadamente protegidas por meio de segurança física ou criptografia quando forem armazenadas, assim como quando são movimentadas através da rede. Isso inclui cópias de segurança (backups) remotas e em serviços de nuvem.	Melhoria do processo: avaliar se tem criptografia para a cópia dos dados para o dataprotector	CID	31/05/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
9.5	Garantir que todas as cópias de segurança contenham ao menos uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.	Aquisição de solução de backup em andamento	CID	31/07/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
10	**Proteção de dados**				
10.1	Manter um inventário de todas as informações sensíveis armazenadas, processadas ou transmitidas pelos sistemas de tecnologia da organização, incluindo aquelas localizado nas próprias dependências da organização ou em um provedor de serviços remoto.	– Elaboração do questionário – Desenvolvimento do sistema para coleta das informações – Orientação para Unidades do TRE-SP – Coleta e Análise das respostas – Validação de alterações – Publicação do resultados	STI/GT-LGPD	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
10.2	Remover da rede dados sensíveis ou sistemas não acessados regularmente pela organização. Tais sistemas devem ser utilizados somente como sistemas isolados (desconectados da rede) pela unidade de negócios que necessite de acesso ocasional, ou devem ser completamente virtualizados e desligados até que sejam necessários.	– Projeto de gerenciamento do ciclo de vida dos sistemas	CID e Gestores de sistemas	19/12/24	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
10.3	Permitir apenas o acesso de cloud storage e\ou provedores de e-mail autorizados.	– Definição dos sistemas que podem ser utilizados – Revisão da PSI	STI/CSI/GT-LGPD	19/12/22	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
10.4	Utilizar ferramentas aprovadas para criptografia total dos discos rígidos de todos os dispositivos móveis.	– Projeto de estudo e implantação de ferramenta de criptografia – Revisão PSI	CSE	19/12/23	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
10.5	Configurar os sistemas para não gravar dados em mídia externa removível, caso não haja requisito de negócio que exija tais dispositivos.	– Estudo de bloqueio por conta da adoção do serviço em nuvem.	CID/CSE	17/12/21	– Itens 7 e 8 do Anexo IV da Portaria CNJ nº 162/2021
	Caso seja necessária a utilização de dispositivos de armazenamento	– Projeto de implantação de			– Itens 7 e 8 do Anexo IV

10.6	USB, todos os dados devem ser armazenados de forma criptografada.	ferramenta de criptografia. – Revisão PSI	CSE	19/12/22	da Portaria CNJ nº 162/2021

ANEXO II

PLANO DE AÇÃO - Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

ID	Requisito	Atividades necessárias	Área	Prazo previsto	Referência
1	**Padrões mínimos de Gestão de Riscos de Segurança da Informação**				
1.3	O Processo de Gestão de Riscos de Segurança Cibernética está associado ao Sistema de Gestão de Segurança da Informação.	Implementar Resolução CNJ 396/2021	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.4	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Estabelecimento de Contexto Definida.	– Estudo de adequação do escopo do GTARSI e do Grupo de Continuidade de Negócio na Gestão de Risco de TIC, para atender a segurança cibernética.	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.5	O Processo de Gestão de Riscos de Segurança Cibernética possui um subprocesso de Avaliação de Riscos Definido	– Revisão do Gestão de Riscos de Segurança da Informação (Portaria TRE-SP 289/2020)	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.5.1	O subprocesso de Avaliação de Riscos contempla atividade de Identificação de Riscos.	– Revisão do Gestão de Riscos de Segurança da Informação (Portaria TRE-SP 289/2020)	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.5.2	O subprocesso de Avaliação de Riscos contempla atividade de Análise de Riscos.	– Revisão do Gestão de Riscos de Segurança da Informação (Portaria TRE-SP 289/2020)	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.5.3	O subprocesso de Avaliação de Riscos contempla atividade de Avaliação de Riscos.	– Revisão do Gestão de Riscos de Segurança da Informação (Portaria TRE-SP 289/2020)	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
		– Estudo de adequação do			

1.5.4	Critérios para determinação do impacto/criticidade e probabilidade dos riscos de segurança cibernética estão definidos.	escopo do GTARSI e do Grupo de Continuidade de Negócio na Gestão de Risco de TIC, para atender a segurança cibernética.	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.5.5	Critérios para aceitação de riscos de segurança cibernética estão definidos.	– Estudo de adequação do escopo do GTARSI e do Grupo de Continuidade de Negócio na Gestão de Risco de TIC, para atender a segurança cibernética.	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.6	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Tratamento de Riscos definida.	– Estudo de adequação do escopo do GTARSI e do Grupo de Continuidade de Negócio na Gestão de Risco de TIC, para atender a segurança cibernética.	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.7	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Monitoramento e Análise Crítica definida.	– Estudo de adequação do escopo do GTARSI e do Grupo de Continuidade de Negócio na Gestão de Risco de TIC, para atender a segurança cibernética.	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019
1.8	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Comunicação e Consulta definida.	– Estudo de adequação do escopo do GTARSI e do Grupo de Continuidade de Negócio na Gestão de Risco de TIC, para atender a segurança cibernética.	STI/CSI	19/12/22	– Anexo V da Portaria CNJ nº 162/2021 – NBR 27.005:2019

ANEXO III

PLANO DE AÇÃO - Gestão de Identidade e Controle de Acesso

ID	Requisito	Atividades necessárias	Área	Prazo previsto	Referência

1	**Gestão de identidade e controle acesso**				
1.1	Formalizar Política de Gestão de Identidade e Controle de Acesso em conformidade com as diretrizes previstas neste Manual e boas práticas de segurança.	– Revisar PSI – Revisar processo	CID	17/12/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.3	Realizar processo de revisão para identificar privilégios excessivos de usuários, administradores de TI e de contas de serviço.	– Revisar o processo – Identificar quais casos – Solicitar justificativa de cada caso – Excluir privilégios desnecessários	CID	30/04/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.4	Definir e utilizar um processo para a revogação de direitos de acesso, desabilitando imediatamente as contas no momento do término do vínculo ou da alteração das responsabilidades de um servidor ou prestador de serviços.	– Elaborar processo para a revogação de direitos de acesso	CID	30/04/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.5	Manter um inventário de cada um dos sistemas de autenticação da organização, incluindo aqueles internos ou em provedores de serviços remotos.	– Mapear sistemas de autenticação	CID/CSE	28/02/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.6	Adotar modelo de controle de acesso baseado em funções (RBAC).	– Estudar a implantação do modelo de acesso baseado em funções (RBAC)	CID/CSE	17/12/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.7	Registrar em logs acessos, operações e período para fins de auditoria.	– Implementar processo de gestão de LOGs	CID	17/12/21	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.8	Garantir que todas as contas tenham uma data de expiração de senha e que isso seja configurado e monitorado.	– Projeto para rever configurações de segurança do AD.	CID	17/12/21	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.9	Gerenciar acessos e ações executadas com credenciais privilegiados, não utilizando credenciais genéricas e de uso Compartilhado	– Propor aos Gestor de SI adoção da política	CID	17/12/21	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.10	Criptografar ou embaralhar (hash) com a utilização de salt as credenciais de autenticação armazenadas.	– Projeto para rever configurações avançadas de – segurança do AD.	CID	17/12/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.11	Utilizar criptografia no canal de comunicação ao trafegar credenciais de acesso.	– Implementar https em aplicações internas e externas administradas pela STI	CID	17/12/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
		– Realizar estudo			

1.14	Configurar o acesso a todas as contas por meio da menor quantidade de pontos de autenticação centralizados possível, incluindo sistemas de rede, segurança e sistemas em nuvem.	para avaliar pontos de autenticação centralizados – Elaboração de projeto de adequação para a menor quantidade possível na estrutura atual	CID	19/12/23	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.15	Garantir que todas as contas (usernames) e senhas sejam transmitidas em rede utilizando canais criptografados.	– Projeto para rever configurações de segurança do AD. – Implementar https em aplicações internas e externas administradas pela STI	CID/CSE	17/12/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.16	Manter um inventário de todas as contas organizadas por sistema de autenticação.	– Realizar estudo para avaliar recursos dos mecanismos de autenticação	CID	19/12/23	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.18	Desabilitar qualquer conta que não possa ser associada a um processo de negócio ou a um usuário.	– Mapear contas	CID	28/02/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.19	Desabilitar automaticamente contas não utilizadas após um período de inatividade pré-definido.	– Realizar estudo para avaliar recursos dos mecanismos de autenticação	CID/CSE	31/05/23	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.20	Bloquear automaticamente as estações de trabalho após um período de inatividade pré-definido.	– Estudo de implementação – Estudo de aquisição aquisição de ferramenta de gerenciamento de ativos.	CSE	17/12/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.21	Monitorar tentativas de acesso a contas desativadas, por meio de logs de auditoria.	– Projeto para rever configurações de segurança do AD.	CID	30/04/22	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1
1.22	Segregar as redes de comunicação a depender do grupo dos serviços, sistemas ou usuários.	– Estudo de implementação – Estudo de aquisição aquisição de ferramenta	CID	19/12/23	– Anexo VI da Portaria CNJ nº 162/2021 – CIS Controls v7.1

Documento assinado eletronicamente por **WALDIR SEBASTIÃO DE NUEVO CAMPOS JUNIOR**, **PRESIDENTE**, em 27/09/2021, às 18:47, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

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