TRIBUNAL REGIONAL ELEITORAL DO ACRE
Alameda Ministro Miguel Ferrante, 224 - Bairro Portal da Amazônia - CEP 69915-632 - Rio Branco - AC

PLANO DE AÇÃO Nº 0609820 / 2023 - PRESI/DG/STI/ASPGOVTI

IMPLEMENTAÇÃO DOS ITENS DO MANUAL DE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TI

1. APRESENTAÇÃO

Nos últimos anos o Judiciário vem passando por grandes avanços tecnológicos, proporcionando agilidade e ampliando o acesso à Justiça. A criação do Juízo 100% digital para viabilizar a execução de todos os atos processuais exclusivamente por meio eletrônico e remoto foi impulsionado com a publicação da Resolução CNJ n. 345/2020. Tais fatores somados às exigências legais, tais como a LGPD, motivara o CNJ a elaboração de Protocolos e Manuais para apoiar os órgãos do Poder Judiciário, estabelecendo padrões mínimos para proteção de sua infraestrutura tecnológica com orientações organizacionais sobre a sua aplicação e lista de controle mínimos exigidos para implementação pelos órgãos do Judiciário.

2. OBJETIVO GERAL

Implementação dos itens do Manual de Proteção de Infraestruturas Críticas de TI, constantes do anexo IV, da Portaria CNJ n. 162/2021.

3. REFERÊNCIA NORMATIVA

- Resolução CNJ no 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Portaria CNJ n. 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário;
- Portaria CNJ n. 249/2020, que designa os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);
- Portaria TRE/AC n. 165/2023, que institui o Protocolo Protocolo de Prevenção de Incidentes Cibernéticos;
- Portaria TRE/AC n. 163/2023, que institui o Protocolo de Investigação para Ilícitos Cibernéticos;
- Portaria TRE/AC n. 156/2023, que institui o Protocolo Protocolo de Gerenciamento de Crises Cibernéticas;
- Recomendações constantes da norma técnica ABNT NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação;
- CIS Controls Framework – Versão 7.1, Center for Internet Security (CIS), https://www.cisecurity.org/controls/”
- NIST Cybersecurity Framework – Versão 1.1, National Institute of Standards and Technology (NIST), https://www.nist.gov/cyberframework/framework”

4. CAMPO DE APLICAÇÃO

- Tribunal Regional Eleitoral do Acre.

5. FINALIDADE E ESCOPO

Estabelecer as diretrizes estratégicas para implementação dos controles de segurança cibernética necessários para proteção de infraestrutura de TI de forma a preservar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

As orientações e os controles recomendados no Manual de Referência do CNJ – Proteção de Infraestruturas Críticas de TIC, aplicam-se a todos os membros do órgão, sejam eles magistrados ou magistradas, servidores ou servidoras, colaboradores ou colaboradoras, fornecedores, prestadores ou prestadoras de serviços, estagiários ou estagiárias que, oficialmente, executem atividades relacionadas ao órgão.

As orientações e os controles constantes do Manual supra consistem em base mínima para a proteção de infraestruturas críticas de TI determinados pelo CNJ, não limitando a evolução do modelo de segurança da informação do TRE/AC, podendo adotar outros controles, processos e frameworks que possam contribuir para a Proteção de Infraestruturas Críticas de TI.

6. CONTROLES MÍNIMOS RECOMENDADOS

Os controles selecionados como linha base (recomendações iniciais mínimas) para a versão inicial do Manual de Referência do CNJ – Proteção de Infraestruturas Críticas de TIC, foram selecionados a partir do framework denominado CIS Controls, versão 7.1. Considerando a visão de adequação a médio prazo na busca de linha base mínima de controles para os diferentes órgãos do Judiciário, considerou-se para este momento os controles do agrupamento Basic do CIS Control 7.1 e, adicionalmente, os seguintes controles desse framework: E-mail e Proteções de Navegador web; Defesas contra malware; Capacidade de Recuperação de Dados; e Proteção de Dados. Dentro desses destaques ainda houve uma segunda seleção e eventuais ajustes de texto em alguns controles para adequação ao contexto e a normativos já existentes

7. ORÇAMENTO

As despesas relacionadas a esse plano que por ventura venham a ter gastos, serão providas com recursos provenientes do orçamento corrente do TRE-AC.

8. PLANO DE AÇÃO PARA UTILIZAÇÃO DOS CONTROLES MÍNIMOS RECOMENDADOS

Inventário e controle de ativos de hardware					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
1.1	Utilizar uma ferramenta de descoberta ativa para identificar dispositivos conectados à rede da organização, e atualizar o inventário de hardware.	SEREDE	out/2021	mar/2022	Finalizado
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.	SEREDE	out/2021	mar/2022	Finalizado
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.	SEREDE	out/2021	mar/2022	Finalizado
1.4	Garantir que o inventário de ativos de hardware armazene o endereço de rede, endereço de hardware, nome do equipamento, proprietário do ativo e departamento para cada ativo, registrando ainda se foi aprovada ou não a conexão do ativo à rede.	SEREDE	out/2021	mar/2022	Finalizado
1.5	Garantir que ativos não autorizados sejam removidos a rede ou colocados em quarentena, ou que o inventário seja atualizado em tempo hábil.	SEREDE	out/2021	mar/2022	Finalizado
	Garantir que o inventário de ativos de				

1.6	hardware armazene o endereço de rede, endereço de hardware, nome do equipamento, proprietário do ativo e departamento para cada ativo, registrando ainda se foi aprovada ou não a conexão do ativo à rede.	SEREDE	out/2021	mar/2022	Finalizado
1.7	Garantir que ativos não autorizados sejam removidos da rede ou colocados em quarentena, ou que o inventário seja atualizado em tempo hábil.	SEREDE	out/2021	mar/2022	Finalizado
Inventário e controle de ativos de software					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
2.1	Manter uma lista atualizada de todos os softwares autorizados que sejam necessários à organização para qualquer propósito ou sistema de negócios.	SEREDE	out/2021	mar/2022	Finalizado
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.	SEREDE	out/2021	mar/2022	Finalizado
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.	SEREDE	out/2021	mar/2022	Finalizado
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.	SEREDE	out/2021	mar/2022	Finalizado
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.	SEREDE	out/2021	mar/2022	Finalizado
2.6	Garantir que qualquer software não autorizado seja removido, ou que o inventário seja atualizado em tempo hábil.	SEREDE	out/2021	mar/2022	Finalizado
Gerenciamento Contínuo de Vulnerabilidade					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
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.	SEREDE	jan/2023	dez/2023	Não iniciada
	Realizar varreduras por vulnerabilidades com contas autenticadas em agentes executados localmente em cada sistema,				

3.2	ou varreduras por scanners remotos que sejam configurados com privilégios elevados nos sistemas que estejam sendo testados.	SEREDE	jan/2023	dez/2023	Não iniciada
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.	SEREDE	jan/2023	dez/2023	Não iniciada
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.	SEREDE	jan/2023	dez/2023	Finalizado
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.	SEREDE	jan/2023	dez/2023	Não iniciada
3.6	Utilizar um processo de classificação de riscos para priorizar a remediação de vulnerabilidades descobertas.	SEREDE	jan/2023	dez/2023	Não iniciada

Uso controlado de privilégios administrativo

ID da Ação	Descrição das Ações	Responsável	Data de Início	Data de Término	Situação
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.	SEREDE	jan/2023	dez/2023	Finalizada
4.2	Antes de ativar qualquer novo ativo, modificar todas as senhas padrão de forma consistente com contas de nível administrativo.	SEREDE	jan/2023	dez/2023	Finalizada
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.	SEREDE	jan/2023	dez/2023	Finalizada
4.4	Utilizar autenticação multifator e canais criptografados para todos os acessos de contas administrativas.	SEREDE	jan/2023	dez/2023	Finalizada
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	SEREDE	jan/2023	abr/2024	Não iniciada

	documentos, ou navegação na internet.				
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.	SEREDE	jan/2023	dez/2023	Finalizada
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.	SEREDE	jan/2023	abr/2024	Não iniciada
4.8	Configurar os sistemas para efetuarem um registro no log e um alerta no caso de logins sem sucesso de uma conta administrativa.	SEREDE	jan/2023	dez/2023	Finalizada
Configuração segura para hardware e software em dispositivos móveis, laptops, estações de trabalho e servidores					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
5.1	Manter padrões documentados de configuração segura para todos os sistemas operacionais e softwares autorizados.	SEREDE	jan/2023	dez/2023	Finalizada
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.	SEREDE	jan/2023	dez/2023	Finalizada
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.	SEREDE	jan/2023	dez/2023	Finalizada
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.	SEREDE	jan/2023	abr/2024	Não iniciada
Manutenção, Monitoramento e Análise de Logs de Auditoria					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
6.1	Utilizar ao menos três fontes de horário sincronizadas, a partir das quais todos os servidores e dispositivos de rede atualizem informações sobre horário de forma regular, a fim de que os timestamps dos logs sejam consistentes.	SEREDE	jan/2023	abr/2024	Não iniciada
6.2	Garantir que o log local tenha sido habilitado em todos os sistemas e dispositivos de rede.	SEREDE	jan/2023	abr/2024	Finalizada
	Habilitar o log dos sistemas de forma a				

6.3	incluir informações detalhadas, tais como origem do evento, data, usuário, horário, endereços de origem, endereços de destino e outros elementos úteis.	SEREDE	jan/2023	abr/2024	Finalizada
6.4	Garantir que todos os sistemas que armazenem logs tenham espaço de armazenamento adequado para os logs gerados.	SEREDE	jan/2023	abr/2024	Finalizada
6.5	Garantir que os logs apropriados sejam agregados em um sistema central de gerenciamento de logs para análises e revisões.	SEREDE	jan/2023	abr/2024	Finalizada
6.6	Implantar Security Information and Event Management (SIEM) ou ferramenta analítica de logs para correlação e análise de logs.	SEREDE	jan/2023	abr/2024	Não iniciada
6.7	Em uma base regular, revisar os logs para identificar anomalias ou eventos anormais.	SEREDE	jan/2023	abr/2024	Não iniciada
Proteções de e-mail e navegadores web					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
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.	SEREDE	jan/2023	abr/2024	Finalizada
7.2	Desinstalar ou desabilitar plug-ins ou aplicações add-on não autorizados para navegadores web e clientes de e-mail.	SEREDE	jan/2023	ago/2024	Não iniciada
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.	SEREDE	jan/2023	abr/2024	Finalizada
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. Sites não categorizados devem ser bloqueados por padrão.	SEREDE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	abr/2024	Finalizada
7.6	Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.	SEREDE	jan/2023	abr/2024	Finalizada
	Com o objetivo de diminuir a possibilidade de recebimento de e-mails				

7.7	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).	SEREDE/TSE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	abr/2024	Finalizada
Defesas contra malware					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
8.1	Utilizar software antimalware gerenciado de forma central para monitorar continuamente e defender cada uma das estações de trabalho e servidores.	SEREDE	jan/2023	abr/2024	Finalizada
8.2	Garantir que o software antimalware atualize seu motor de varredura e base de assinaturas de malware de forma regular.	SEREDE	jan/2023	abr/2024	Finalizada
8.3	Habilitar funcionalidades anti-exploits, tais como Data Execution Prevention (DEP) ou Address 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.	SEREDE	jan/2023	ago/2024	Não iniciada
8.4	Configurar os dispositivos de forma que automaticamente conduzem uma varredura antimalware em mídias removíveis assim que sejam inseridas ou conectadas.	SEREDE	jan/2023	abr/2024	Finalizada
8.5	Configurar os dispositivos para que não autoexecutem conteúdo em mídia removível.	SEREDE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	abr/2024	Finalizada
8.7	Habilitar log de pesquisas sobre Domain Name System (DNS) de forma a detectar buscas por nomes de hosts em domínios reconhecidamente maliciosos.	SEREDE	jan/2023	ago/2024	Não iniciada
8.8	Habilitar log de auditoria sobre ferramentas de linha de comando, tais como Microsoft Powershell e Bash.	SEREDE	jan/2023	ago2024	Não iniciada
Capacidades de recuperação de dados					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
	Garantir que todos os dados dos sistemas				

9.1	tenham cópias de segurança (backups) realizados automaticamente de forma regular.	SEREDE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	abr/2024	Finalizada
Proteção de dados					
ID da Ação	**Descrição das Ações**	**Responsável**	**Data de Início**	**Data de Término**	**Situação**
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.	SEREDE	jan/2023	abr/2024	Finalizada
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.	SEREDE	jan/2023	ago2024	Não iniciada
10.3	Permitir apenas o acesso de cloud storage e\ou provedores de e-mail autorizados.	SEREDE	jan/2023	abr/2024	Finalizada
10.4	Utilizar ferramentas aprovadas para criptografia total dos discos rígidos de todos os dispositivos móveis.	SEREDE	jan/2023	abr/2024	Finalizada

9. PREMISSAS E RESTRIÇÕES DO OBJETO

- Apoio da Administração, Diretoria Geral e Secretarias do Tribunal
- Disponibilidade orçamentária;

- Cumprimento dos prazos previamente fixados para realização das tarefas pelas unidades envolvidas;

- Comprometimento de todas as áreas impactadas;

Controle de versões:

Plano de Ação

versão preliminar 1.0

Responsável: ASPGOVTI/SEREDE/SCSEG