Poder Judiciário

Conselho Nacional de Justiça

ANEXO IV – Manual de Referência – Proteção de infraestruturas críticas de TIC

Manual de Referência

Proteção de Infraestruturas Críticas de TIC

Material de Referência com os Principais Controles de Segurança Cibernética necessários para proteção estratégica de infraestruturas de TIC

Sumário

1. Motivação e Origem

1.1. O cenário tecnológico atual propicia avanços em todos os setores da sociedade, inclusive nos serviços prestados pelo Poder Judiciário. Nos últimos anos o Judiciário vem passando por grandes avanços tecnológicos, conferindo-lhe mais agilidade e ampliando o acesso à Justiça. De forma quase natural os ambientes tecnológicos tornaram-se maiores, mais complexos, bem como os processos de negócio se tornaram mais dependentes da tecnologia. Nesse contexto os riscos relacionados à segurança da informação tendem a amplificar-se e, em muitos casos, materializar-se.

1.2. Esse cenário tecnológico é reforçado pela Resolução CNJ n. 345, de 9 de outubro de 2020, que autoriza os tribunais a adotarem o Juízo 100% Digital para viabilizarem a execução de todos os atos processuais exclusivamente por meio eletrônico e remoto. A medida segue um dos principais eixos definidos pelo CNJ, voltada para o incentivo à inovação tecnológica, eficiência na prestação do serviço jurisdicional e a redução de custos do Judiciário.

1.3. Os fatores citados somados às novas exigências legais, como, por exemplo, a LGPD, motivam o CNJ, por meio do Comitê Gestor de Segurança Cibernética do Poder Judiciário (CGSCPJ), a apoiar os órgãos do Judiciário, estabelecendo padrões mínimos para proteção de sua infraestrutura tecnológica. Esses padrões foram organizados neste Manual, que conta com orientações organizacionais sobre sua aplicação e uma lista de controles mínimos exigidos para implantação pelos órgãos do Judiciário.

2 Estrutura do Documento

2.1 Este documento foi organizado no intuito de facilitar sua leitura e entendimento, incrementando sua aplicabilidade em ambientes reais e está dividido nas seguintes seções:

2.1.1 Motivação e Origem: descreve a motivação e a autoria do documento.

2.1.2 Estrutura do Documento: trata-se desta seção.

2.1.3 Referência Normativa: lista as referências relevantes utilizadas na elaboração do documento.

2.1.4 Campo de Aplicação: descreve quais órgãos estão submetidos aos requisitos mínimos descritos.

2.1.5 Finalidade e Escopo: descreve de forma geral a finalidade e os limites de aplicabilidade deste documento.

2.1.6 Termos e Definições: lista termos e suas definições aplicáveis no âmbito deste documento e das discussões acerca dele.

2.1.7 Princípios: lista os princípios que devem nortear a leitura e as atividades baseadas neste documento.

2.1.8 Diretrizes Gerais: descreve as diretrizes gerais norteadoras da construção deste documento.

2.1.9 Competências e Responsabilidades: descreve de maneira geral as responsabilidades envolvidas no processo de implantação.

2.1.10 Controles Mínimos Exigidos: lista informações sobre os controles que cada órgão do Judiciário deve implementar em seu ambiente.

2.1.11 Atualização: descreve a expectativa de atualização deste Manual.

3 Referência Normativa

a) Resolução CNJ n. 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)

b) Portaria CNJ n. 242 de 10 de novembro de 2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário;

c) Portaria CNJ n. 249 de 13 de novembro de 2020, que designa os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);

d) Norma técnica Gestão de Riscos de Segurança da Informação associada às recomendações constantes da norma NBR ISO/IEC 27005:2019;

e) *Framework – CIS Controls* – Versão 7.1, https://www.cisecurity.org/;

f) *Framework – National Institute of Standards and Technology* (NIST) – Versão 1.1, https://www.nist.gov/cyberframework/framework.

4 Campo de Aplicação

4.1. Este Manual é de aplicação mandatória no âmbito do Poder Judiciário, com exceção do Supremo Tribunal Federal. Portanto, todo órgão do Judiciário que conte com

infraestrutura tecnológica, inclusive mantida ou administrada por terceiros, deve seguir as orientações e implantar os controles mínimos aqui recomendados.

5 Finalidade e Escopo

5.1. Este Manual tem por finalidade estabelecer as diretrizes estratégicas para a implementação dos controles de segurança cibernética necessários para proteção de infraestruturas de TIC de forma a preservar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

5.2. As orientações e os controles recomendados neste Manual 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.

5.3. Cabe ainda ressaltar que as orientações e os controles aqui expostos consistem em base mínima para a proteção de infraestruturas críticas de TI, não limitando a evolução do modelo de segurança da informação de cada órgão, bem como a adoção de outros controles, processos e *frameworks* que possam contribuir nesse contexto.

5.4. Ainda, considerando que os controles foram selecionados a partir do conjunto de boas práticas denominado *CIS Controls*, versão 7.1, recomenda-se que a instituição avalie a pertinência e a oportunidade de aplicar os demais controles por ele preconizados.

6. Princípios

6.1. Está disposta a seguir uma lista com os princípios que devem nortear a leitura e as atividades baseadas neste documento.

6.1.1 Eficiência: propriedade de que a Política de Segurança da Informação e das Comunicações – POSIC e suas Normas busquem o melhor resultado possível, por meio das suas diretrizes e normatizações, visando a auxiliar para que a atividade administrativa seja exercida com presteza, perfeição e rendimento funcional.

6.1.2 Ética: propriedade de que a POSIC e suas Normas devem seguir os valores morais de conduta. São todos os direitos e interesses legítimos de usuários.

6.1.3 Impessoalidade: propriedade de que a POSIC e suas Normas devem servir para todos, sem preferências ou aversões pessoais ou partidárias.

6.1.4 Legalidade: propriedade de que a POSIC e suas Normas devem atuar no âmbito das leis.

6.1.5 Moralidade: propriedade de que as diretrizes estabelecidas nesta POSIC e suas Normas preservarão a moral dos princípios éticos, da boa-fé e da lealdade.

6.1.6 Publicidade: propriedade de que a POSIC e suas Normas terão publicidade e serão levadas ao conhecimento de toda a Entidade, buscando garantir atuação transparente do Poder Público.

7 Controles Mínimos Recomendados

7.1. O Poder Judiciário conta com um cenário heterogêneo em relação à diversidade de características entre seus órgãos integrantes, embora existam similaridades reconhecidas pelo fato de todos comporem um mesmo Poder. As variações entre eles estão presentes em vários aspectos, tais como finalidade para a qual cada um existe, distribuição geográfica, dimensão de recursos disponíveis, peculiaridades do seu ambiente tecnológico, características de competências do corpo funcional, entre outros. Tomando como base as similaridades, diversidades e boas práticas de segurança da informação corporativa reconhecidas na atualidade, este Manual baseia-se em um conjunto de controles mínimos exigidos compreendidos como pertinentes e condizentes com a realidade do Judiciário.

7.2. Os controles selecionados como linha base (recomendações iniciais mínimas) para a versão inicial deste Manual 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.

7.3. Dessa maneira, segundo o *framework*, por meio da adoção desses controles, estima-se que cerca de 85% (oitenta e cinco por cento) dos principais ataques praticados quando do lançamento do *CIS* versão 7.1 poderiam ser evitados.

Optou-se também por se manter a escala de aplicabilidade de cada controle em relação ao porte da organização, categorizado por Grupo 1, Grupo 2 e Grupo 3, esses grupos fornecem uma forma simples e acessível de ajudar as organizações de diferentes portes a direcionar seus recursos com o melhor custo × benefício, alcançando os melhores resultados na busca pela mitigação do risco. Os critérios aplicáveis para a classificação do órgão quanto ao porte estão detalhados no quadro seguinte.

Grupo	Sugestão de ordem de implantação
Grupo 1	Organizações com nível limitado de recursos disponíveis e pouca experiência em segurança cibernética
Grupo 2	Organizações com nível moderado de recursos disponíveis e experiência média em segurança cibernética
Grupo 3	Organizações com nível elevado de recursos disponíveis e alta experiência em segurança cibernética

7.4. Cabe ressaltar que a classificação por grupos é uma sugestão para direcionamento e priorização dos esforços de segurança da informação a serem operacionalizados, e que tal abordagem deve ter sua aplicabilidade e aderência sempre validadas\adequadas para o contexto de cada organização.

7.5. A categorização pelo *NIST CSF* também foi incluída para apoiar o entendimento sobre em que fase de um incidente o controle se enquadra.

7.6. Os controles disponíveis para trabalho a partir deste Manual são essencialmente técnicos. Entretanto, para alcançar sua implementação, os órgãos precisam de medidas organizacionais que apoiem a efetivação de cada um deles. A descrição dessas medidas não faz parte do escopo deste Manual, mas é importante considerar o patrocínio e o acompanhamento pela alta administração, que deve entender a aplicação desses controles como estratégica para o órgão.

7.7. Considerando que as tecnologias mudam rapidamente e as ameaças cibernéticas crescem exponencialmente, a busca pela adequação dos órgãos ao atendimento dos requisitos mínimos deve ser contínua. Portanto, é imprescindível que a aplicação dos *checklists* pela organização seja periódica (anualmente, pelo menos), e que esses *checklists* tenham níveis de atendimento/maturidade, possibilitando a melhoria contínua da segurança digital de cada dependência.

8 Checklist para utilização dos Controles Mínimos Recomendados

ID	Requisito	Controle	NIST CSF	Maturidade de SI		
				Grupo 1	Grupo 2	Grupo 3
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*.		Identificar		X	X
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*.		Identificar		X	X
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.		Identificar	X	X	X
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.		Identificar		X	X
1.5	Garantir que ativos não autorizados sejam removidos da rede ou colocados em quarentena, ou que o inventário seja atualizado em tempo hábil.		Responder	X	X	X
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.	Identificar	X	X	X
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.	Identificar	X	X	X
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.	Identificar		X	X
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.	Identificar		X	X
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.	Identificar			X
2.6	Garantir que qualquer *software* não autorizado seja removido, ou que o inventário seja atualizado em tempo hábil.	Identificar	X	X	X
2.7	Sistemas segregados física ou logicamente devem ser utilizados para isolar e executar *softwares* que sejam necessários às operações do negócio, mas que não tragam maior risco à organização.	Proteger			X
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.	Detectar		X	X

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.	Detectar		X	X
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.	Detectar		X	X
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.	Proteger	X	X	X
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.	Proteger	X	X	X
3.6	Utilizar um processo de classificação de riscos para priorizar a remediação de vulnerabilidades descobertas.	Responder		X	X
Uso controlado de privilégios administrativos					
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.	Detectar		X	X
4.2	Antes de ativar qualquer novo ativo, modificar todas as senhas padrão de forma consistente com contas de nível administrativo.	Proteger	X	X	X

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.	Proteger	X	X	X
4.4	Utilizar autenticação multifator e canais criptografados para todos os acessos de contas administrativas.	Proteger		X	X
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.	Proteger		X	X
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.	Proteger		X	X
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.	Detectar		X	X
4.8	Configurar os sistemas para efetuarem um registro no *log* e um alerta no caso de *logins* sem sucesso de uma conta administrativa.	Detectar		X	X
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.	Proteger	X	X	X

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*.	Proteger		X	X
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*.	Proteger		X	X
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.	Proteger		X	X
Manutenção, Monitoramento e Análise de *Logs* de Auditoria					
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.	Detectar		X	X
6.2	Garantir que o *log* local tenha sido habilitado em todos os sistemas e dispositivos de rede.	Detectar	X	X	X
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.	Detectar		X	X
6.4	Garantir que todos os sistemas que armazenem *logs* tenham espaço de armazenamento adequado para os *logs* gerados.	Detectar		X	X
6.5	Garantir que os *logs* apropriados sejam agregados em um sistema central de gerenciamento de *logs* para análises e revisões.	Detectar		X	X

6.6	Implantar *Security Information and Event Management* (SIEM) ou ferramenta analítica de *logs* para correlação e análise de *logs*.	Detectar		X	X
6.7	Em uma base regular, revisar os *logs* para identificar anomalias ou eventos anormais.	Detectar		X	X
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.	Detectar			X
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.	Proteger	X	X	X
7.2	Desinstalar ou desabilitar *plug-ins* ou aplicações *add-on* não autorizados para navegadores *web* e clientes de e-mail.	Proteger		X	X
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.	Proteger		X	X
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.	Proteger		X	X
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.	Detectar		X	X
7.6	Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.	Proteger	X	X	X

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).	Proteger		X	X
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.	Proteger		X	X
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.	Proteger		X	X
8.2	Garantir que o *software antimalware* atualize seu motor de varredura e base de assinaturas de *malware* de forma regular.	Proteger	X	X	X
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.	Proteger		X	X
8.4	Configurar os dispositivos de forma que automaticamente conduzem uma varredura *antimalware* em mídias removíveis assim que sejam inseridas ou conectadas.	Detectar	X	X	X
8.5	Configurar os dispositivos para que não autoexecutem conteúdo em mídia removível.	Proteger	X	X	X
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.	Detectar		X	X

8.7	Habilitar *log* de pesquisas sobre *Domain Name System* (DNS) de forma a detectar buscas por nomes de *hosts* em domínios reconhecidamente maliciosos.	Detectar		X	X
8.8	Habilitar *log* de auditoria sobre ferramentas de linha de comando, tais como *Microsoft Powershell* e *Bash*.	Detectar		X	X
Capacidades de recuperação de dados					
9.1	Garantir que todos os dados dos sistemas tenham cópias de segurança (*backups*) realizados automaticamente de forma regular.	Proteger	X	X	X
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.	Proteger	X	X	X
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.	Proteger		X	X
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 (*backup*s) remotas e em serviços de nuvem.	Proteger	X	X	X
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.	Proteger	X	X	X
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.	Identificar	X	X	X
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.	Proteger	X	X	X
10.3	Permitir apenas o acesso de *cloud storage* e\ou provedores de e-mail autorizados.	Proteger		X	X
10.4	Utilizar ferramentas aprovadas para criptografia total dos discos rígidos de todos os dispositivos móveis.	Proteger	X	X	X
10.5	Configurar os sistemas para não gravar dados em mídia externa removível, caso não haja requisito de negócio que exija tais dispositivos.	Proteger			X
10.6	Caso seja necessária a utilização de dispositivos de armazenamento USB, todos os dados devem ser armazenados de forma criptografada.	Proteger			X