

Motivação:

- Ataques ao Judiciário
- Eleição sob suspeita
- Segurança Cibernética é feita por todos. Empreendimento coletivo.
- Fundamentar contratações
- Novos Normativos CNJ
- Auditoria dos Órgãos de Controle – TCU e CNJ
- Auditoria Interna

NORMATIVOS	
Resolução 396 de 7 de JUNHO de 2021 CNJ	Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)
Portaria 162 de JUNHO de 2021 CNJ	Protocolos e Manuais criados pela Resolução CNJ no 396/2021
Resolução 363 de 12 de JANEIRO de 2021 CNJ	Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.
Lei 13.709/2021	Lei Geral de Proteção de Dados Pessoais - LGPD
Resolução TSE 23644 de 1º de JULHO de 2021	Política de Segurança da Informação - PSI
Resolução 23.650 TSE	Política Geral de Privacidade e Proteção de Dados Pessoais JE
Resolução TSE nº 23.656 , de 7 de outubro de 2021	Dispõe sobre o acesso a dados pessoais constantes dos sistemas informatizados da Justiça Eleitoral (JE)
Resolução 370 de 28 de janeiro de 2021 CNJ	Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação (ENTIC-JUD) do Poder Judiciário

Resolução 396/2021 Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)	
Visão	Alcançar a excelência em segurança cibernética
Objetivo	Aprimorar o nível de maturidade em segurança cibernética no Judiciário Específico: I – tornar o Judiciário mais seguro e inclusivo no ambiente digital; II – aumentar a resiliência às ameaças cibernéticas; III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível
Ações	Deve ter engajamento da alta administração I – fortalecer as ações de governança cibernética; II – eleva o nível de segurança das infraestruturas críticas; III – estabelecer rede de cooperação do Judiciário para a segurança cibernética; e IV – estabelecer modelo centralizado de governança cibernética nacional.
Elevar o Nível de Segurança	I – estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão; II – instituir e manter Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR); III – elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa; IV – utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança; V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet; VI – providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em formato que permita a investigação de incidentes; VII – elaborar requisitos específicos de segurança cibernética relativos aos ativos sob sua jurisdição, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive computadores portáteis e telefones celulares; VIII – elaborar requisitos específicos de segurança cibernética relacionados com o trabalho remoto; IX – adotar práticas e requisitos de segurança cibernética no desenvolvimento de novos projetos, tais como dupla verificação do acesso externo; X – realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos; XI realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo; e XII – estabelecer troca de informações e boas práticas com outros membros do poder público em geral e do setor privado com objetivo colaborativo.
Estrutura Nacional	Modelo Centralizado De Governança Nacional Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ) Rede Nacional de Cooperação do Poder Judiciário
Ações da PSI de cada Tribunal	I – realizar a Gestão dos Ativos de Informação e da Política de Controle de Acesso; II – criar controles para o tratamento de informações com restrição de acesso; III – promover treinamento contínuo e certificação internacional dos profissionais diretamente envolvidos na área de segurança cibernética; IV – estabelecer requisitos mínimos de segurança cibernética nas contratações e nos acordos que envolvam a comunicação com outros órgãos;

	V – utilizar os recursos de soluções de criptografia , ampliando o uso de assinatura eletrônica , conforme legislações específicas; e VI – comunicar e articular as ações de segurança da informação com a alta administração do órgão.
Gestão de Usuários	I – gerenciamento de identidades; II – gerenciamento de acessos; e III – gerenciamento de privilégios.
Conscientização	Política De Cultura E Educação Em Segurança cibernética
Orçamento	Rubrica Específica

Resolução 162/2021	
Protocolos	I - Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ); II – Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRCPJ); III – Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).
Manuais	I – Proteção de Infraestruturas Críticas de TIC; II – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital; III – Gestão de Identidades; e IV – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.

Resolução 162/2021 ANEXO I Prevenção de Incidentes Cibernéticos do Poder Judiciário – PPINC-PJ	
Funções	1 – Identificar • Gerenciar riscos de ativos críticos. • Concentração e priorização de esforços na gestão de ativos
	2 – Proteger • desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, e de ativos de informação, bem como a prestação de serviços críticos
	3 – Detectar • desenvolvimento e implementação de atividades para descoberta oportuna de eventos ou detecção de incidentes. (monitoramento contínuo)
	4 – Responder • Adoção de medidas em resposta incidentes detectados
	5 – Recuperar • desenvolvimento, implementação e manutenção dos planos de resiliência e de restauração
Gestão de Incidentes	• Através de processo definido e constituído formalmente • Fases: detecção, triagem, análise e resposta
Competência de Atuação	• Instituir ETIR (Equipe de Tratamento e Resposta a Incidentes)
Funcionamento da ETIR	Instrução normativa 8/2018 – atualizar https://www.tre-ma.jus.br/o-tre/goveranca-gestao/seguranca-da-informacao

Resolução 162/2021 ANEXO II Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ)	
Escopo	Prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses.
Identificação	O gerenciamento de crise se inicia quando: a) ficar caracterizado grave dano material ou de imagem; b) restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses; c) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou d) o incidente atrair grande atenção da mídia e da população em geral
Fases	O Gerenciamento de Crises pode ser dividido em 3 (três) fases: a) planejamento (pré-crise); b) execução (durante a crise); e c) melhoria Contínua (pós-crise).
	Planejamento da Crise (pré-crise) 1 - Estabelecer um Programa de Gestão da Continuidade de Serviços que contemple: a) observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário; b) definir as atividades críticas que são fundamentais para a atividade finalística do órgão; c) identificar os ativos de informação críticos, ou seja, aqueles que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação; d) avaliar continuamente os riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio; e) categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos; f) priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade. Tais atividades deverão ser detalhadas e consolidadas em um plano de contingência que contemple diversos setores, em razão de possíveis cenários de crise, a fim de se contrapor à escalada de uma eventual crise e com o objetivo de manter os serviços prestados pela organização; e g) realizar simulações e testes para validação dos planos e procedimentos. 2 - Definir a sala de situação e criar um Comitê de Crises Cibernéticas, com suporte da ETIR
	Execução (durante a crise) Crise = longa duração ou grande impacto • ETIR aciona o Comitê de Crise • Executa-se os planos de contingência visando a continuidade • Comunicar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) • Definir estratégias de comunicação • Aplicar Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário • Solicitar colaboração de especialistas • Elaborar plano de retorno à normalidade
	Melhoria contínua (lições aprendidas no pós-crise) • Identificação das lições aprendidas • Elaboração de Relatório de Comunicação de Incidente de Segurança Cibernética • Revisar procedimentos

Resolução 162/2021 ANEXO III Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ)	
Objetivo	Procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal
Requisitos	• O horário dos ativos de tecnologia da informação deve ser ajustado por meio de mecanismos de sincronização de tempo • Registrar (SISLOG, SIEM) todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), tais como: a) autenticação, tanto as bem-sucedidas quanto as malsucedidas; b) acesso a recursos e dados privilegiados; e c) acesso e alteração nos registros de auditoria. • Monitoramento de sistemas e redes de comunicações a) utilização de usuários, perfis e grupos privilegiados; b) inicialização, suspensão e reinicialização de serviços; c) acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis; d) modificações da lista de membros de grupos privilegiados; e) modificações de política de senhas, como, por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico etc.; f) acesso ou modificação de arquivos ou sistemas considerados críticos; e g) eventos obtidos por meio de quaisquer mecanismos de segurança existentes. • Serviços de hospedagem e ativos de informação deve ter log que possibilite identificação de fluxos de dados • Armazenar por 6 meses • Armazenar logs localmente e remotamente
Coleta e Preservação de Evidências	• ETIR sob a supervisão do seu responsável deve coletar e preservar: a) as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses; b) os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e c) todos os registros de eventos citados neste documento • As ações de restabelecimento não devem comprometer a coleta e a preservação da integridade das evidências. • O material coletado será lacrado e custodiado pelo responsável pela ETIR
Comunicação	• Comunicar à polícia judiciária • Responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética

Resolução 162/2021 ANEXO IV MANUAL de Referência – Proteção de Infraestruturas Críticas de TIC	
Objetivo	Estabelecer: • padrões mínimos para proteção de sua infraestrutura tecnológica • diretrizes para implementação de controles de segurança cibernética (CIS Controls versão 7.1)
Campo de Aplicação	Manual é de aplicação mandatória
	Checklist para utilização dos Controles Mínimos Recomendados por Grupo

Resolução 162/2021 ANEXO V Manual de referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital	
Objetivo	Estabelecer: • melhores práticas reconhecidas no mercado e uma lista de controles mínimos exigidos para implantação pelos órgãos do Judiciário
	• Capítulo 1: Principais frameworks de referência utilizados • Capítulo 2: Padrões mínimos de Gestão de Riscos de Segurança da Informação • Capítulo 3: Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas • Capítulo 4: Confiança digital, prevenção e mitigação de ameaças cibernéticas • Capítulo 5 e Anexo I: Modelo de checklist
Principais frameworks de referência utilizados	MITRE ATT&CK Norma ABNT NBR ISO/IEC 27000:2018 - visão geral dos sistemas de gerenciamento de segurança da informação e os termos e definições comumente usados na família de normas ISO/IEC 27001 Norma ABNT NBR ISO/IEC 27001:2013 - Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação Norma ABNT/NBR ISO/IEC 27005:2019 - diretrizes para o processo de gestão de riscos de segurança da informação Norma ABNT NBR ISO/IEC 27007:2018 - diretrizes sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação Norma ABNT NBR ISO/IEC 19011:2018 - orientação sobre a auditoria de sistemas de gestão, incluindo os princípios de auditoria, a gestão de um programa de auditoria e a condução de auditoria de sistemas de gestão Norma Complementar nº 11/IN01/DSIC/GSIPR, de 2012 - diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta NIST SP 800-160 Vol. 2- publicação NIST Special Publication 800-160, Volume 2 (Desenvolvendo Sistemas Cyber Resilientes: Uma – Abordagem de engenharia de Segurança de Sistemas) é usada em conjunto com a ISO/IEC/IEEE 15288: 2015 (Engenharia de sistemas e <i>software</i> - processos de ciclo de vida de sistemas), NIST <i>Special Publication</i> 800-160 volume 1 (Engenharia de segurança de sistemas – Considerações para uma abordagem multidisciplinar na engenharia de confiabilidade Sistemas Seguros) e NIST <i>Special Publication</i> 800-37 (Estrutura de Gerenciamento de Risco para Sistemas de Informação e Organizações – uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade)
Estrutura e Competências	É imprescindível que esta norma seja compreendida e aplicada pela área de Controle Interno ou Auditoria de cada órgão.
	Checklist

Resolução 162/2021 ANEXO VI Manual de Referência – Gestão de Identidade e de Controle de Acessos	
Objetivo	Estabelecer: • Este Manual estabelece as diretrizes principais para a gestão de identidades e credenciais eletrônicas bem como para o controle de acessos aos sistemas, serviços e equipamentos de tecnologia da informação (TI).
Frameworks de referência	• CIS Controls 7.1 • MITRE ATT&CK • Norma ABNT NBR ISO/IEC 27001:2013 • NIST SP 800-53
	Checklist

Resolução 162/2021 ANEXO VII Manual de Referência – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário	
Objetivo	Estabelecer: • visa estabelecer as diretrizes necessárias consubstanciadas em ações permanentes de capacitação, de educação, de engenharia social e de formação de cultura especializada