Planos de Ação – Portaria 162/2021 CNJ Anexos I, II e III					
Protocolo de Prevenção a Incidentes Cibernéticos (PPICiber/PJ)					
Portaria CNJ Nº 162/2021 Anexo I					
Dispositivo Legal	Ação	Detalhamento	Responsável	Situação	Evidência
4.1 A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.	P1.1 - Revisar Processo de Gerenciamento de Incidentes de Segurança e aprovar alterações, se necessário.	Efetuar revisão do processo, estabelecendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança, conforme determina a Portaria.	CSI / ETIR / SAGGI	Concluído	Processo SEI: 0003644-44.2021.6.08.8000
		Aprovar formalmente o novo processo, dar ciência aos interessados e publicá-lo	CGTIC	Concluído	Processo SEI: 0003644-44.2021.6.08.8001
5.1 Deverá ser formalmente instituída Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), em todos os órgãos do Poder Judiciário, à exceção do STF.	P1.2 - Revisar os termos do Ato que institui a ETIR e normatiza seu funcionamento. Aprovar novo Ato, se necessário.	Efetuar revisão do Ato de instituição e funcionamento da ETIR, adequando-o, se necessário	ETIR / SAGGI / CSI	Concluído	Processo SEI: 0004479-32.2021.6.08.8000 / Ato 339/2022 - Dispõe sobre a ETIR
		Aprovar alterações, publicar novo Ato e dar ciência aos interessados	PRE	Concluído	Processo SEI: 0004479-32.2021.6.08.8000 / Ato 339/2022 - Dispõe sobre a ETIR

Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/ PJ).					
Portaria CNJ Nº 162/2021 Anexo II					
Dispositivo Legal	Ação	Detalhamento	Responsável	Situação	Evidência

4.1 Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:	P2.1 - Instituir Programa de Gestão de Continuidade de Negócios	Criar e consolidar um programa de continuidade de negócios do Órgão, contemplando as atividades descritas nas alíneas "a" até "g" do item 4.1	APECI	Concluído	Processo SEI nº 0005069-38.2023.6.08.8000
a) observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário; (...) g) realizar simulações e testes para validação dos planos e procedimentos.		Definir as atividades críticas que são fundamentais para a atividade finalística do TRE/ES	APECI / CGTI	Concluído	Processo SEI nº 0005069-38.2023.6.08.8001
		Identificar os ativos de informação críticos (que suportam as atividades primordiais), incluindo as pessoas, os processos, a infraestrutura e os recursos de TIC	APECI / CGTI	Concluído	Processo SEI nº 0005069-38.2023.6.08.8002
		Elaborar Matriz de Riscos das atividades críticas e plano de contingência, instituindo processo de avaliação continua desses documentos.	APECI / CSI	Concluído	Processo SEI nº 0005069-38.2023.6.08.8003
		Categorizar incidentes e estabelecer procedimentos de resposta específicos para cada tipo (essa atividade apoia P2.4)	APECI / ETIR	Concluído	Processo SEI nº 0005069-38.2023.6.08.8004

4.2 Deve-se definir a sala de situação e criar um Comitê de Crises Cibernéticas, composto por representantes da alta administração e por representantes executivos, com suporte da ETIR e de especialistas: a) da área Jurídica; b) da área de Comunicação Institucional; c) da área de Tecnologia da Informação e Comunicação; d) da área de Privacidade de Dados Pessoais; e) da área de Segurança da Informação; f) das unidades administrativas de apoio à contratação; e g) da área de Segurança Institucional.	P2.2 - Definir sala de situação	Definir um espaço físico que constituir-se-á a sala de situação	Alta Administração / CSI	Concluído	Processo SEI: 0002846-49.2022.6.08.8000
	P2.3 - Instituir o Comitê de Crises Cibernéticas	Criar o Comitê de Crises Cibernéticas, sendo composto conforme estipulado no item 4.2	Alta Administração / CSI	Concluído	Processo SEI: 0002846-49.2022.6.08.8001 / Portaria 236/2022
4.3 O Plano de Gestão de Incidentes Cibernéticos deve possuir, no mínimo, as categorias de incidentes a que os ativos críticos estão sujeitos; a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência do incidente; e a severidade do incidente.	P2.4 - Instituir o Plano de Gestão de Incidentes Cibernéticos	Elaborar o Plano de Gestão de Incidentes Cibernéticos, com, no mínimo, a categoria do incidente, a indicação do procedimento de resposta específico e a severidade	NSC	Em Execução Previsão: DEZ/24	Processo SEI nº 0009712-44.2020.6.08.8000, aprovado na Ata de Reunião 29 da CSI em 02/04/2024

Protocolo de investigação para ilícitos cibernéticos (PGCC/PJ).					
Portaria CNJ Nº 162/2021 Anexo III					
Dispositivo Legal	Ação	Detalhamento	Responsável	Situação	Evidência

2.1. O horário dos ativos de tecnologia da informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).	P3.1 - Implementar mecanismos de sincronização de tempo nos ativos de TIC	Estudar e adquirir, se necessário, ferramentas de TIC para prover a sincronização de tempo dos ativos críticos do TRE/ES	SGIR	Concluído	Todos os servidores Linux (por cliente NTP) e Windows (registro), assim como os computadores de trabalho são configurados para sincronizar a data e a hora com o Active Directory
2.2. Os ativos de tecnologia da informação devem ser configurados de forma a registrar 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.	P3.2 - Adquirir ferramenta de centralização de logs	Estudar e adquirir ferramenta SIEM para centralização de logs	SGIR	Concluído	Utilização de software livre, Graylog, para centralização dos logs. Processo SEI para aquisição do SIEM: 0001600-81.2023.6.08.8000

2.3. Os registros dos eventos previstos no item 2.2 devem incluir as seguintes informações: a) identificação inequívoca do usuário que acessou o recurso; b) natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.; c) data, hora e fuso horário, observando-se a HLB; e d) endereço IP (Internet Protocol), porta de	P3.3 - Elaborar e aprovar norma técnica de segurança para gerenciamento de Logs	Elaborar norma técnica que determine os eventos, o tempo de guarda, as ferramentas usadas e procedimentos de gestão dos logs	NSC	Concluído	Link para a norma (NSI 007): https://treesjusbr.sharepoint.com/sites/segurancaInformacao2/Normas%20de%20Segurana%20da%20Informao/NSI-007%20-%20TRE-ES%20-%20Norma%20de%20gerenciamento%20de%20logs.pdf?web=1
		Aprovar Norma Técnica de Segurança de gerenciamento de logs	CSI / Administração	Concluído	Ata da CSI: 0771026, processo SEI: 0003623-05.2020.6.08.8000
2.5. Os sistemas e as redes de comunicação de dados devem ser monitorados, registrandose, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes: (...) 2.6. Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o	P3.4 - Elaborar e Aprovar norma técnica de segurança para monitoramento e registro de eventos em ativos críticos	Elaborar norma técnica de segurança que determine como os ativos críticos serão monitorados e como se dará o registro de eventos	NSC	Concluído	Link para a norma (NSI 007): https://treesjusbr.sharepoint.com/sites/segurancaInformacao2/Normas%20de%20Segurana%20da%20Informao/NSI-007%20-%20TRE-ES%20-%20Norma%20de%20gerenciamento%20de%20logs.pdf?web=1
		Aprovar Norma Técnica de Segurança para monitoramento e registro de eventos em ativos críticos	CSI	Concluído	Ata da CSI: 0771026, processo SEI: 0003623-05.2020.6.08.8000

ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (logs) em formato que possibilite a completa identificação dos fluxos de dados.	P3.5 - Estudar e adquirir, se necessário, ferramentas de TIC para monitoramento e registro de eventos em ativos críticos	Estudar e adquirir, se necessário, ferramenta para monitoramento e registro de eventos em ativos críticos,	SGIR / CSGIT	Concluído	Utilização de software livre, Graylog, para centralização dos logs. Processo SEI para aquisição do SIEM: 0001600-81.2023.6.08.8000
3.1. A ETIR, sob a supervisão de seu responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, 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. (...) 3.6. Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante.	P3.6 - Revisar os termos do Ato que institui a ETIR e normatiza seu funcionamento. Aprovar novo Ato, se necessário OBS: Efetuar em conjunto com P1.2	Efetuar revisão do Ato de instituição e funcionamento da ETIR, adequando-o, se necessário,	ETIR / SAGGI	Concluído	Processo SEI: 0004479-32.2021.6.08.8000 / Ato 339/2022 - Dispõe sobre a ETIR
		Aprovar alterações, publicar novo Ato e dar ciência aos interessados	PRE	Concluído	Processo SEI: 0004479-32.2021.6.08.8000 / Ato 339/2022 - Dispõe sobre a ETIR