TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE SÃO PAULO
PRESIDÊNCIA

PORTARIA Nº 227/2021

Estabelece diretrizes pra atendimento à Portaria CNJ nº 162/2021 no âmbito da Justiça Eleitoral do Estado de São Paulo

O Desembargador Waldir Sebastião de Nuevo Campos Junior, Presidente do Tribunal Regional Eleitoral do Estado de São Paulo, no uso de suas atribuições legais,

CONSIDERANDO a Resolução CNJ nº 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO os termos da Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o disposto na Portaria CNJ nº 162/2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO a Portaria CNJ nº 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário e dispõe sobre a normatização para criação do Centro de Tratamento de Incidentes de Segurança Cibernética (CTISC) do CNJ, que funcionará como canal oficial para orquestração e divulgação de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos;

CONSIDERANDO a Instrução Normativa GSI nº 1/2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

CONSIDERANDO a Instrução Normativa GSI nº 2/2020, que altera a Instrução Normativa GSI nº 1/2020;

CONSIDERANDO a importância de estabelecer objetivos, princípios e diretrizes de Segurança da Informação e de Gestão de Riscos de Segurança da Informação, alinhados às recomendações constantes das normas NBR ISO/IEC 27001:2013 e NBR ISO/IEC 27005:2019;

CONSIDERANDO a necessidade de garantir o cumprimento da Lei Federal nº 12.527/2011 (Lei de Acesso à Informação), bem como, no âmbito do Poder Judiciário, da Resolução CNJ nº 215/2015, cujas normas disciplinam o direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral;

CONSIDERANDO o que dispõe a Lei Federal nº 13.709/2018, com a redação dada pela Lei Federal nº 13.853/2019, sobre a proteção de dados pessoais, que altera a Lei nº 12.965/2014 (Marco Civil da Internet);

CONSIDERANDO o disposto na Resolução CNJ nº 176/2013, que institui o Sistema

Nacional de Segurança do Poder Judiciário;

CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO o alto potencial de prejuízo dos ataques cibernéticos, cujo alcance e complexidade não têm precedentes, bem como que os impactos financeiros, operacionais e de reputação podem ser imediatos e significativos;

RESOLVE:

Art. 1º Estabelecer plano de ação com vistas à implementação do **Protocolo de Gerenciamento de Crises Cibernéticas** no âmbito do Tribunal Regional Eleitoral do Estado de São Paulo, na forma do Anexo I deste normativo.

Art. 2º Estabelecer plano de ação com vistas à implementação do **Protocolo de Investigação para Ilícitos Cibernéticos** no âmbito do Tribunal Regional Eleitoral do Estado de São Paulo, na forma do Anexo II deste normativo.

Art. 3º Estabelecer plano de ação com vistas à implementação do **Protocolo de Prevenção a Incidentes Cibernéticos** no âmbito do Tribunal Regional Eleitoral do Estado de São Paulo, na forma do Anexo III deste normativo.

Art. 4º Determinar que a Secretaria de Tecnologia da Informação (STI) providencie a adoção de medidas previstas nos anexos IV e VI da Portaria CNJ nº 162/2021.

Art. 5º Determinar que a Secretaria de Auditoria Interna (SAI) e a Secretaria de Tecnologia da Informação (STI) providenciem a adoção de medidas previstas no anexo V da Portaria CNJ nº 162/2021.

Art. 6º Determinar que a Secretaria de Gestão de Pessoas (SGP), a Coordenadoria de Comunicação Social (CCS) e a Secretaria de Tecnologia da Informação (STI) providenciem a adoção de medidas previstas no anexo VII da Portaria CNJ nº 162/2021.

Art. 7º Revogar as Portarias TRE-SP nº 44, 45 e 46, todas de 2021.

Art. 8º Esta Portaria entra em vigor na data de sua publicação.

Waldir Sebastião de Nuevo Campos Junior

Presidente

ANEXO I

PLANO DE AÇÃO - GERENCIAMENTO DE CRISES CIBERNÉTICAS

Tópico	Ação	Descrição Macro	Responsável	Data final	% conclusão	Alinhamento Portaria CNJ

				final	**conclusão**	**162/2021**
1. Organização	1.1. Atualizar as competências da ETIR/TRE-SP, para alinhamento com as ações descritas neste Plano	• Atualizar e publicar composição e atividades de competência da ETIR/TRE-SP relacionadas a esta portaria	• ETIR • Comissão de Segurança da Informação	08/2021		Anexo I, itens 5 e 6; Anexo II, item 4, subitem 4.2
2. Identificação e gerenciamento de Crise Cibernética	2.1. Elaborar protocolo de identificação e gerenciamento de crise cibernética	• Identificar grave dano material ou de imagem; • Analisar se é evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses; • Analisar se o incidente vai impactar na atividade finalística ou o serviço crítico mantido pela organização; • Analisar se o evento atraiu grande atenção da mídia e da população em geral • Mapear o protocolo de identificação e gerenciamento de crise cibernética	• ASSPE • ETIR • CCS	12/2021		Anexo II, itens 2 e 3
		• Apresentar minuta do protocolo para o gestor de segurança	• ETIR	12/2021		
		• Apresentar minuta do protocolo para a comissão de segurança	• STI	02/2022		

						Anexo II, item 2
		• Instituir protocolo de identificação e gerenciamento de crise cibernética	• Comissão de Segurança da Informação	02/2022		
		Implementar protocolo de identificação e gerenciamento de crise cibernética	• Unidades da STI	04/2022		
3. Para a fase preparatória (pré-crise)	3.1. Elaborar Plano de Continuidade de Negócio do TRE-SP (PCN)	• Elaborar Plano de Continuidade de Negócio do TRE-SP (PCN), contendo pelo menos as atividades considerados críticas em relação ao negócio	• ASSPE	04/2022		Anexo II, item 4
		• Elaborar Plano de Gestão de Incidentes que Geram Crises Cibernéticas	• ETIR • Unidades da STI	06/2022		
		• Aprovar Plano de Continuidade de Negócio do TRE-SP (PCN)	• TRE	06/2022		
		• Aprovar Plano de Gestão de Incidentes que Geram Crises Cibernéticas	• Comissão de Segurança da Informação	12/2022		
	3.2. Definir uma sala de situação de crises cibernéticas e criar Comitê	• Criar Comitê de Crises Cibernéticas	• Comissão de Segurança da Informação	12/2021		Anexo II, item 2, subitem 4.2
		• Definir e equipar sala de situação de crises cibernéticas	• Comissão de Segurança da Informação	06/2022		

	3.3. Revisar Plano de Continuidade de TIC	• Revisar Plano de Continuidade de TIC - alinhar ao PCN	• GT Continuidade	03/2023		

ANEXO II

PLANO DE AÇÃO - INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS

Tópico	Ação	Descrição Macro	Responsável	Data final	% conclusão	Alinhamento Portaria CNJ 162/2021
1. Organização	1.1. Atualizar as competências da ETIR/TRE-SP, para alinhamento com as ações descritas neste Plano	• Atualizar e publicar composição e atividades de competência da ETIR/TRE-SP relacionadas a esta portaria	• ETIR • Comissão de Segurança da Informação	08/2021		Anexo I, itens 5 e 6
	1.2. Obter subsídios para obtenção do Protocolo	• Pesquisar legislação e normas aplicadas ao caso (NBR 27001 e 27002, dentre outras) • Identificar atividades necessárias para viabilizar investigação de ilícitos	• ETIR	12/2021		
	2.1. Revisar o formato de sincronização dos ativos de informação, de acordo com a HLB – Hora Legal Brasileira	• Verificar com o TSE se a HLB está sendo apontado para o Observatório Nacional (os servidores do TRE estão apontados para o TSE) ou se há orientação do TSE sobre essa questão (para garantir atualização de horários) • Publicar LD com orientações • Verificar se todos os ativos de informação estão sincronizados com a HLB (secretaria, cartórios,	• ScRS • ScNT	09/2021		Anexo III, item 2

		centrais, postos e pontos) • Verificar se a sincronização GMT atende os requisitos solicitados (secretaria, cartórios, centrais, postos e pontos)				
	2.2. Revisar e atualizar o formato de registros dos eventos relevantes de Segurança da Informação e Comunicação (SIC)	• Revisar e atualizar: ◦ autenticação, tanto as bem-sucedidas quanto as malsucedidas; ◦ acesso a recursos e dados privilegiados; e ◦ acesso e alteração nos registros de auditoria.	• ScRS • ScBD • ScDV • ScNT	12/2021		Anexo III, item 2
		• Revisar e atualizar (coleta de dados de ativos - secretaria, cartórios, centrais, postos e pontos): ◦ identificação inequívoca do usuário que acessou o recurso; ◦ natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.; ◦ data, hora e fuso horário, observando o previsto no Anexo III, item 2; e ◦ endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam	• ScRS • ScBD • ScDV • ScNT	12/2022		

		identificar a possível origem do evento.				
		• Mapear processo de gerenciamento de LOGs e eventos	• ScRS • ScBD • ScDV • ScNT	05/2021		Anexo III, item 2
		• Apresentar minuta para o gestor de segurança	• ScRS • ScBD • ScDV • ScNT	06/2021		
		• Apresentar minuta do processo para a comissão de segurança	• STI	07/2021		
		• Instituir o processo de Gerenciamento de LOGs e Eventos de recursos de TIC	• Comissão de Segurança da Informação	08/2021		
		• Pesquisar solução para melhoria de armazenamento e análise de LOGs (todos os ativos, por 6 meses)	• ScRS • ScBD • ScDV • ScNT	10/2021		
		• Inserir previsão de aquisições e investimentos no orçamento de 2022	• Unidades da STI	02/2021		Anexo III, item 2
		• Elaborar documentação para aquisições	• ScRS • ScBD • ScDV • ScNT	12/2021		
2. Dos requisitos para adequação dos ativos de informação	2.3. Registrar eventos	• Adquirir solução de armazenamento e ferramenta de análise de LOGs – licitação	• SAM • Equipe de planejamento de contratação designada	02/2022		
		• Repasse de conhecimento por parte da contratada	• Unidades da STI	07/2022		
		• Implementar a solução da monitoração, de acordo com o plano de aquisição,	• Unidades da STI	12/2022		

		implantação e gerenciamento				
		• Implementar o processo de Gerenciamento de LOGs e Eventos de recursos de TIC (implementação em fases)	• Unidades da STI	12/2022		
	2.4. Identificar ativos de informação que não permitam os registros dos eventos listados no Anexo III, item 2, por meio de mapeamento e documentação quanto ao tipo e formato de registros de auditoria permitidos e armazenados	• Fazer levantamento e catalogação dos ativos que não contemplam o Anexo III, item 2	• ScRS • ScBD • ScDV • ScNT	12/2022		Anexo III, item 2; Anexo IV, Item 8, subitens de 6.1 a 6.8
	2.5. Monitorar os sistemas de redes de comunicação de dados	• Verificar a configuração do monitoramento para atendimento dos itens: ◦ utilização de usuários, perfis e grupos privilegiados; ◦ inicialização, suspensão e reinicialização de serviços; ◦ acoplamento e desacoplamento de dispositivos de *hardware*, com especial atenção para mídias removíveis; ◦ modificações da lista de membros de grupos privilegiados; ◦ modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após	• ScRS • ScBD • ScDV • ScNT	12/2022		Anexo III, item 2

		exceder determinado número de tentativas de autenticação, histórico etc.; ◦ acesso ou modificação de arquivos ou sistemas considerados críticos; e ◦ eventos obtidos por meio de quaisquer mecanismos de segurança existentes.				
	2.6. Configurar os servidores de hospedagem WEB bem como qualquer ativo de informação. Logs devem ser armazenados em formato que permita a identificação do fluxo de dados	• Verificar configurações de logs • Alinhar ao plano de *backup* o prazo de armazenamento (obs.: 6 meses para consulta)	• ScRS • ScBD • ScDV • ScNT	12/2021		Anexo III, item 2
	2.7. Armazenar os registros de auditoria local e remotamente	• Armazenar LOGs na estação e no computador servidor, no TRE • Verificar com o TSE a possibilidade de armazenamento de registros de auditoria na sala cofre ou em outro local remoto que conte com critérios de segurança exigidos	• ScRS • ScBD • ScDV • ScNT	12/2021		Anexo III, item 2
3. Procedimentos para coleta e preservação das evidências para tratamento de incidente	3.1. Elaborar protocolo para investigação de ilícitos cibernéticos	Elaborar minutas do protocolo de investigação de ilícitos cibernéticos	• ETIR	12/2021		Anexo III, item 3
		Apresentar minuta do protocolo para o gestor de segurança	• ETIR	12/2021		
		Apresentar minuta do protocolo para a comissão de segurança	• STI	02/2022		

penalmente relevante		Instituir portaria oficializando o protocolo de investigação de ilícitos cibernéticos	• Comissão de Segurança da Informação	02/2022		
		Implementar protocolo de investigação de ilícitos cibernéticos	• Unidades da STI	04/2022		
4. Processo para avaliar se o incidente é penalmente relevante, encaminhar formalmente ao órgão responsável pelo Poder Judiciário e comunicar ao órgão de polícia judiciária	4.1. Elaborar e instituir processo	Elaborar processo para avaliar se o incidente é penalmente relevante, encaminhar formalmente ao órgão responsável pelo Poder Judiciário e comunicar ao órgão de polícia judiciária	• ETIR	12/2021		Anexo III, item 3 e 4
		Apresentar minuta do processo para o gestor de segurança	• ETIR	12/2021		
		Apresentar minuta do processo para a comissão de segurança	• STI	02/2022		Anexo III, item 3 e 4
		Instituir processo para avaliar se o incidente é penalmente relevante, encaminhar formalmente ao órgão responsável pelo Poder Judiciário e comunicar ao órgão de polícia judiciária	• Comissão de Segurança da Informação	02/2022		
		Implementar processo de investigação de ilícitos cibernéticos	• Unidades da STI	04/2022		
	4.2 Aprovar modelo de relatório de comunicação de incidentes penalmente relevantes de segurança de redes computacionais	• Elaborar modelo de Relatório de Comunicação de Incidentes penalmente relevantes de segurança em redes computacionais, com base no anexo da Portaria CNJ 291/2020	• Comissão de Segurança da Informação	06/2022		Anexo III, item 3 e 4
		• Aprovar o modelo de Relatório de Comunicação de Incidentes penalmente relevantes de segurança em redes	• Comissão de Segurança da Informação	12/2022		

		computacionais				

ANEXO III

PLANO DE AÇÃO - PREVENÇÃO A INCIDENTES CIBERNÉTICOS

Tópico	Ação	Descrição Macro	Responsável	Data final	% conclusão	Alinhamento Portaria CNJ 162/2021
1. Organização	1.1. Atualizar as competências da ETIR/TRE-SP, para alinhamento com as ações descritas neste Plano	• Atualizar e publicar composição e atividades de competência da ETIR/TRE-SP relacionadas a esta portaria (Incluir na portaria da ETIR o previsto nos art. 6, 7 e 8 da Portaria CNJ 292/2020)	• ETIR • Comissão de Segurança da Informação	08/2021		Anexo I, itens 5 e 6
2. Gestão de Incidentes de Segurança da Informação	2.1. Revisar processo para a gestão de incidentes de segurança da informação	• Identificar no processo as fases de detecção, triagem, análise e resposta aos incidentes de segurança da informação	• ETIR	05/2021		Anexo IV, Item 8, subitens de 3.1 a 3.6
		• Apresentar minuta do processo ao gestor de segurança	• ETIR	06/2021		
		• Apresentar minuta do processo para a comissão de segurança	• STI	07/2021		
		• Levantamento das atividades já adotadas pela STI no gerenciamento de vulnerabilidades	• ScDv • ScRS • ScBD • ScNT	04/2021		Anexo IV, Item 8, subitens de 3.1 a 3.6
		• Verificar as soluções aplicadas em	• ScDv • ScRS • ScBD	04/2021		

		outros regionais	• ScNT			
	3.1. Instituir o processo de gestão de vulnerabilidades	• Mapear processo de gerenciamento de vulnerabilidades	• ScDv • ScRS • ScBD • ScNT	05/2021		Anexo IV, Item 8, subitens de 3.1 a 3.6
		• Apresentar minuta do processo ao gestor de segurança	• ScDv • ScRS • ScBD • ScNT	06/2021		
		• Apresentar minuta do processo para a comissão de segurança	• STI	07/2021		
		• Instituir o processo	• Comissão de Segurança da Informação	08/2021		
		• Implementar processo	• ScDv • ScRS • ScBD • ScNT	10/2021		
		• Elaborar documentos de análise de risco em manter sistemas legados e desatualizados	• GTARSI (GT Análise de Riscos SI)	12/2021		Anexo IV, Item 8, subitens de 3.1 a 3.6
		• Análise dos sistemas obsoletos para identificar necessidade de migração para plataforma atualizada	• ScDv • ScRS • ScBD • ScNT	12/2021		
		• Elaborar cronograma para atualização de sistemas (desenvolvimento, migração, implantação)	• ScDv • ScRS • ScBD • ScNT	03/2022		
		• Apresentar proposta ao gestor de segurança	• CID • CSE	04/2022		
3. Gestão de vulnerabilidades		• Apresentar				

		proposta para a comissão de segurança	• STI	04/2022		Anexo IV, Item 8, subitens de 3.1 a 3.6
		• Inserir previsão de aquisições nos orçamentos de 2022/2023	• Unidades da STI	01/2022		
	3.2. Atualizar sistemas legados e sistemas operacionais obsoletos	• Elaborar documentação para viabilizar aquisições de *softwares* e equipamentos com sistema operacional atualizado, para substituir equipamentos obsoletos (computadores servidores e estações de trabalho usados na secretaria, cartórios, centrais, postos e pontos) - anos de 2021, 2022 e 2023	• Unidades da STI	12/2022		
		• Adquirir *softwares* e equipamentos adequados – licitação nos anos de 2021, 2022 e 2023	• SAM • Equipe de planejamento de contratação designada	03/2023		Anexo IV, Item 8, subitens de 3.1 a 3.6
		• Substituir computadores servidores e estações de trabalho obsoletos	• ScNT • ScEI	12/2023		
		• Atualização de sistemas operacionais dos computadores servidores físicos e virtuais	• ScRS	12/2023		
		• Atualização de bancos de dados	• ScBD	12/2023		
		• Migração dos serviços para os novos servidores	• ScRS	12/2023		

		• Desativação de computadores servidores obsoletos	• ScRS	12/2023		
		• Descarte dos computadores obsoletos	• SAM	06/2024		
4. Da segurança Cibernética e boas práticas	4.1. Criar ou adequar os mecanismos de respostas e prevenção	• Verificar os mecanismos existentes de respostas a prevenção e fazer ajustes que forem necessários	• ScRS • ScBD • ScDv • ScNT	12/2021		Anexo I, itens 2, 3 e 7
	4.2. Instituir protocolo para a prevenção a incidentes	• Adequação das novas atividades para as funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas • Levantamento das atividades já adotadas pela STI para a prevenção a incidentes	• ETIR	04/2021		
		• Verificar as soluções aplicadas em outros regionais	• ETIR	04/2021		Anexo I, itens 2, 3 e 7
		• Elaborar protocolo para a prevenção a incidentes	• ETIR	05/2021		
		• Apresentar minuta do protocolo ao gestor de segurança	• ETIR	06/2021		
		• Apresentar minuta do protocolo para a comissão de segurança	• STI	07/2021		
		• Instituir o protocolo para a prevenção a incidentes	• Comissão de Segurança da Informação	08/2021		

		• Implementar protocolo para a prevenção a incidentes	• Unidades da STI	10/2021		

Documento assinado eletronicamente por **WALDIR SEBASTIÃO DE NUEVO CAMPOS JUNIOR**, **PRESIDENTE**, em 28/09/2021, às 18:56, 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 **2969735** e o código CRC **2AAD204A**.