TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE SÃO PAULO
PRESIDÊNCIA

PORTARIA Nº 46/2021

Estabelece o Plano de Ação para construção do Protocolo de Investigação para Ilícitos Cibernéticos 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 os termos da Resolução CNJ nº 362/2020, que institui o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário;

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

CONSIDERANDO o disposto nos incisos X e XII do art. 5º da Constituição da República, que instituem os direitos à privacidade;

CONSIDERANDO a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados; a Lei nº 12.965/2014 – Marco Civil da Internet; o Decreto nº 8.771/2016, e a Lei nº 12.527/2011 – Lei de Acesso à Informação; bem como as Resoluções CNJ nº 121/2010 e nº 215/2015 e a Recomendação do CNJ nº 73/2020;

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;

RESOLVE:

Art. 1º Estabelecer plano de ação com vistas à construção do **Protocolo de Investigação para Ilícitos Cibernéticos** no âmbito do Tribunal Regional Eleitoral do Estado de São Paulo, alinhado à Portaria CNJ nº 291, de 17 de dezembro de 2020, na forma do Anexo deste normativo.

Art. 2 Esta Portaria entra em vigor na data de sua publicação.

Waldir Sebastião de Nuevo Campos Junior

Presidente

ANEXO
PLANO DE AÇÃO - INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS

Tópico	Ação	Descrição Macro	Responsável	Data final	% conclusão	Alinhamento Portaria CNJ 291
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	06/2021		Art. 3, 12, 13, 14, 15 e 16
	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		
		• Verificar com o TSE se a HLB está sendo apontado para o Observatório Nacional (os				

	2.1. Revisar o formato de sincronização dos ativos de informação, de acordo com a HLB – Hora Legal Brasileira	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, centrais, postos e pontos) • Verificar se a sincronização GMT atende os requisitos solicitados (secretaria, cartórios, centrais, postos e pontos)	• ScRS • ScNT	06/2021		Art. 5
	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		Art. 6
		• 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 art. 5º; e • endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.	• ScRS • ScBD • ScDV • ScNT	12/2022		Art. 7
		• Mapear processo de gerenciamento de LOGs e eventos	• ScRS • ScBD • ScDV • ScNT	03/2021		
		• Apresentar minuta para o gestor de segurança	• ScRS • ScBD • ScDV • ScNT	03/2021		
	2.3. Registrar eventos	• Apresentar minuta do processo para a comissão de segurança	• STI	04/2021		
		• Instituir o processo de Gerenciamento	• Comissão de Segurança da	05/2021		

		de LOGs e Eventos de recursos de TIC	Segurança da Informação	05/2021		
		• Pesquisar solução para melhoria de armazenamento e análise de LOGs (todos os ativos, por 6 meses)	• ScRS • ScBD • ScDV • ScNT	07/2021		
2. Dos requisitos para adequação dos ativos de informação		• Inserir previsão de aquisições e investimentos no orçamento de 2022	• Unidades da STI	02/2021		
		• Elaborar documentação para aquisições	• ScRS • ScBD • ScDV • ScNT	12/2021		
		• 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, implantação e gerenciamento	• Unidades da STI	12/2022		
		• 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 art. 7, 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 art. 07	• ScRS • ScBD • ScDV • ScNT	12/2022		Art. 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 exceder determinado número de tentativas de autenticação, histórico etc.; • acesso ou	• ScRS • ScBD • ScDV • ScNT	12/2022		Art. 9

		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		Art. 10
	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		Art. 11
3. Procedimentos para coleta e preservação das evidências para tratamento de incidente penalmente	3.1. Elaborar protocolo para investigação de ilícitos cibernéticos	Elaborar minutas do protocolo de investigação de ilícitos cibernéticos	• ETIR	12/2021		Art. 12, 13, 14, 15 e 16
		Apresentar minuta do protocolo para o gestor de segurança	• ETIR	12/2021		Art. 12, 13, 14, 15 e 16
		Apresentar minuta do protocolo para a comissão de segurança	• STI	02/2022		Art. 12, 13, 14, 15 e 16
		Instituir portaria oficializando o protocolo de	• Comissão de Segurança da	02/2022		Art. 12, 13, 14, 15 e 16

relevante		investigação de ilícitos cibernéticos	Informação			14, 15 e 16
		Implementar protocolo de investigação de ilícitos cibernéticos	• Unidades da STI	04/2022		Art. 12, 13, 14, 15 e 16
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		Art. 17 e 19
		Apresentar minuta do processo para o gestor de segurança	• ETIR	12/2021		
		Apresentar minuta do processo para a comissão de segurança	• STI	02/2022		
		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		Art. 17 e 19
		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		Art. 18
		• Aprovar o modelo de Relatório de Comunicação de Incidentes penalmente relevantes de segurança em redes	• Comissão de Segurança da Informação	12/2022		Art. 18

		computacionais				

Documento assinado eletronicamente por **WALDIR SEBASTIÃO DE NUEVO CAMPOS JUNIOR**, **PRESIDENTE**, em 11/02/2021, às 19:05, 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 **2611397** e o código CRC **4FE24A3F**.