TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE SÃO PAULO

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		
2. Dos requisitos para adequação dos ativos de informação	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, centrais, postos e pontos)	• ScRS • ScNT	06/2021		Art. 5

		• 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		Art. 6
	2.3. Registrar eventos	• 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	• ScRS • ScBD • ScDV • ScNT	12/2022		Art. 7

		informações que possam identificar a possível origem do evento.				
		• 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		
		• Apresentar minuta do processo para a comissão de segurança	• STI	04/2021		
		• Instituir o processo de Gerenciamento de LOGs e Eventos de recursos de TIC	• Comissão de 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		
		• 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:	• ScRS • ScBD • ScDV • ScNT	12/2022		Art. 9

		○ 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 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 relevante	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 investigação de ilícitos cibernéticos	• Comissão de Segurança da Informação	02/2022		Art. 12, 13, 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	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		

Judiciário e comunicar ao órgão de polícia judiciária		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 computacionais	• Comissão de Segurança da Informação	12/2022		Art. 18