TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

PORTARIA PRESIDÊNCIA Nº 56/2021 TRE-AL/PRE/AEP

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de formalização de plano de ação com vistas à construção de Protocolo de Investigação para Ilícitos Cibernéticos no âmbito deste Tribunal, em atenção ao art. 4º, da Resolução nº 362, de 17 de dezembro de 2020, do Conselho Nacional de Justiça;

CONSIDERANDO o disposto no Processo SEI nº 0000273-40.2021.6.02.8000,

RESOLVE:

Art. 1º Aprovar o plano de ação para a construção do Protocolo de Investigação para Ilícitos Cibernéticos do Tribunal Regional Eleitoral de Alagoas, conforme o Anexo Único deste ato normativo.

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

Desembargador OTÁVIO LEÃO PRAXEDES
Presidente

ANEXO ÚNICO

PLANO DE AÇÃO PARA A CONSTRUÇÃO DO PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

Tópico	Ação	Descrição Macro	Responsável	Data final	Alinhamento Portaria CNJ 291
1. Organização	1.1. Atualização das competências da ETIR para alinhamento das ações descritas neste Plano de Ação	• Atualização e publicação de portaria para a fixação das novas atividades da ETIR	• Comitê de Governança de TIC • ETIR	10/02/2021	
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 Nacional	• Verificar se todos os ativos de informação estão sincronizados com a HLB. • Verificar se a sincronização GMT atende os requisitos solicitados	• COINF	Ciclo contínuo	Art. 5º

2.2. Revisar e atualizar o formato de registros dos eventos relevantes de Segurança da Informação e Comunicação (SIC)	• Revisar e atualizar: ◦ autenticações realizadas e negadas ◦ acesso a recursos e dados privilegiados; e ◦ acesso e alteração nos registros de auditoria.	• COINF	Ciclo contínuo	Art. 6º
2.3. Registros de eventos	• Revisar e atualizar: ◦ 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.	• COINF • CSCOR	Ciclo contínuo	Art. 7º
2.4. Identificar ativos de informação que não permitam os registros dos eventos listados no art. 7º, por meio de mapeamento e documentação quanto ao tipo e formato de registros de auditoria permitidos e armazenados	• Fazer um levantamento de todos os ativos que não contemplam o art. 7º	• COINF • CSCOR	Ciclo contínuo	Art. 8º
2.5. Os sistemas e redes de comunicação de dados devem ser monitorados	• 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	• COINF • CSCOR	Ciclo contínuo	Art. 9º

		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. Os servidores de hospedagem WEB, bem como qualquer ativo de informação, devem ser configurados para armazenar logs em formato que permita a identificação do fluxo de dados	• Verificar a configuração de logs • Alinhar ao plano de backup o prazo de armazenamento	• COINF • CSCOR	Ciclo contínuo	Art. 10
	2.7. Armazenar os registros de auditoria local e remotamente	• Armazenar os registro de auditoria em site backup	• COINF • CSCOR	Ciclo contínuo	Art. 11
3. Procedimentos para coleta e preservação das evidências	3.1. Revisar os procedimentos que objetivem a coleta e a preservação das evidências	• Criar processo para utilizar termo de custódia dos ativos de informação • Propor eventual adequação, se necessário, do modelo disponibilizado pelo CNJ do Termo de Custódia dos Ativos de Informação	• ETIR	15/02/2021	Arts. 12, 13, 14, 15 e 16
4. Comunicação do Incidente de segurança	4.1. Definir o processo de envio de informações ao órgão de polícia judiciária.	• Definir critérios objetivos para definição para um incidente de rede computacional penalmente relevante • Definir os elementos que devem ser coletados para a comunicação ao órgão de polícia judiciária	• Comitê de Governança de TIC	15/02/2021	Arts. 17,18 e 19
	4.2 Efetivar comunicação ao órgão de polícia judiciária	• Criar processo para utilizar o Relatório de Comunicação de Incidentes de segurança em redes computacionais • Avaliar a adoção do modelo disponibilizado pelo CNJ do Relatório de Comunicação de Incidentes de segurança em redes computacionais	• Presidência	15/02/2021 (Ciclo contínuo para fins de comunicação)	Arts. 17, 18 e 19

		• Comunicar ao órgão de polícia judiciária			
5. Construção do protocolo de investigação para ilícitos cibernéticos	5.1. Instituição do protocolo de investigação para ilícitos cibernéticos	• Elaborar, aprovar e publicar ato normativo para a instituição do protocolo de investigação para ilícitos cibernéticos	• Presidência • Comitê de Crise	30 dias após Instituição do Comitê de Crise	Art. 21

Maceió, 08 de fevereiro de 2021.

Documento assinado eletronicamente por **OTÁVIO LEÃO PRAXEDES**, **Presidente**, em 08/02/2021, às 19:40, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-al.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0851866** e o código CRC **E2C2CB05**.