TRIBUNAL REGIONAL ELEITORAL DO ACRE

INFORMAÇÃO Nº 0408224 - PRESI/CSI

Em cumprimento ao Despacho CNJ 0405878, a seguir está elencado o Plano de Ação, para a produção dos artefatos que regulamentam as ações executivas, realizadas durante uma eventual crise cibernética.

Considerando que o prazo de resposta àquele Conselho Nacional, se extingue hoje dia 23 de fevereiro de 2020.

	Plano de Ação para atender Resoluções CNJ 360/2020, 361/2020 e 362/2020 – Protocolo de Gerenciamento de Crises Cibernéticas - Planilha 5W2H							
	WHAT	**WHY**	**WHERE**	**WHO**	**WHEN**	**HOW**	**HOW MUCH**	**STATUS**
	O Quê?	**Porquê?**	**Onde?**	**Quem?**	**Quando?**	**Como?**	**Quanto Custa?**	**Status / Obs.**
RES. 360/2020 - Crises Cibernéticas	Revisar atividades críticas	Definir prioridades	CSI	Membros da CSI e COSET	jun/21	Definir e publicar nova portaria com a priorização de serviços críticos	sem custos	a iniciar
	Criar processo formal de Gestão de ativos	Para poder definir quais ativos são críticos e quais devemos envidar esforços para proteção	CSI	MEMBROS DA CSI E STI	ago/21	1. Mapear e formalizar o processo de gestão de ativos; 2. Realizar o inventário dos ativos por meio de ferramentas adequadas.	sem custos iniciais	em andamento
	Revisar a PCN - Politica de Continuidade de Negócios	Mitigar riscos de incidentes disruptivos e aumentar a resiliência institucional, a revisão é necessária para que a mesma contemple o solicitado na portaria 290 do CNJ	CSI	Membros da CSI e STI	ago/21	Definir e Publicar o PCN e os principais procedimentos	sem custos iniciais	a iniciar
	Criar/revisar a Política de Gestão de Riscos de Segurança da Informação	Estabelecer o processo específco de gestão de riscos de SI	CSI	Membros da CSI e COSET	dez/21	Definir e Publicar a Política de Gestão de Riscos de Segurança da Informação	sem custos	a iniciar
	Criar o Comitê de Crises Cibernéticas	Pré-estabelecer as pessoas responsáveis pelas definições em momentos de	CSI	CSI E COSET	mai/21	Definir e Publicar portaria com os membros do Comitê de Gestão de Crises Cibernéticas	sem custos	a iniciar (colocar na PCN)

		crises cibernéticas						
	Treinamentos Técnicos para equipes de TI	Aumentar a capacidade operacional para resposta a ataques cibernéticos	STI	CSI E COSET	dez/22	Contratação de treinamentos com empresas especializadas		a iniciar
	Adequação da estrutura organizacional para segurança da informação	Criar unidade organizacional para gestão de segurança da informação, apoio técnico a LGPD e a Politica de Continuidade de Negócios	TRE-AC	COSET	dez/21	Alocação de equipe especializada, com criação de unidade organizacional ligada a presidencia ou a diretoria geral e também a contratação de serviços de suporte a infraestrutura de 1º, 2º níveis - 000522-52.2020-01 -	Realocação de recursos humanos e Funções Comissionadas	a iniciar
	Criação de protocolos complementares de gerenciamento de crises cibernéticas	Elaborar protocolos e procedimentos operacionais para sistematizar as atividades durante crises	CSI	Gestor de Segurança da Informação	dez/21	Discussão das propostas na CSI e com as áreas técnicas afetadas, como STI	sem custos	a iniciar (colocar na PCN)
RES. 362/2020 - Investigação Ilícitos Cibernéticos	Criar norma técnica para gerenciamento de logs	Definir padrões e boas práticas	CSI	Gestor de Segurança da Informação	dez/21	Apresentação da proposta para CSI e posterior avaliação da COSET	a dimensionar	a iniciar
	Criar servidor de LOGS centralizado	para melhor gestão e segurança dos logs dos ativos de informação	CSI e STI	Membros da CSI e da STI e gestores de infraestrutura	dez/21	Utiilizar ferramental opensource e padrão de mercado como o SYSLOG-NG	a dimensionar	iniciado
	Criação de protocolos complementares para investigação de ilícitos cibernéticos	Definir padrões e boas práticas	CSI	Gestor de Segurança da Informação	dez/22	Apresentação da proposta da CSI e posterior avaliação da COSET	sem custos	a iniciar
	Revisão das permissões de usuários em sistemas, serviço de diretório e bancos de dados	Garantir a legitimidade dos acessos aos ativos de informação	CSI	Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados	dez/21	Levantamento dos ativos, revisão dos usuários e suas permissões	sem custos no primeiro momento.	iniciado

RES. 361/2020 - Prevenção Incidentes Ciber	Atualização de sistemas legados	Garantir o nível mínimo de segurança para cada ativo de informação disponibilizado	CSI	Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados	dez/22	Levantamento dos ativos obsoletos, sem atualização recente ou com falhas de segurança. Após, atualização ou descontinuação do ativo	a serem levantados	a iniciar
	Implementação de solução para gestão de identidades	Garantir o adequado ciclo de vida de identidades digitais	CSI	Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados	dez/22	Levantar bases de usuários, interoperabilidade com serviço de SSO (Single-sign-on), adquirir ferramenta de IAM, caso necessário	a serem levantados	iniciado
	Implementação de solução para gestão de acesso privilegiado	Garantir o adequado monitoramento e controle dos acessos privilegiados a sistemas, computadores e bases de dados	CSI	Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados	dez/22	finalização da implementação da ferramenta guacamole, bem como adoção de novas ferramentas	a serem levantados	iniciado
	implentação de ferramentas de segurança, como IDS/IPS/GAT/SIEM/antivirus no proxy de navegação	Inserir niveis de segurança para prevenção de incidentes cibernéticos	CSI/STI	Gestores da área de infraestrutura	dez/22	Analisar e implementar ferramentas opensource e de mercado	a serem levantados	iniciado
	Reconfiguração de nossa infraestrutura de backup	Configuração de backups offline (fitas) , implementação de mecanismos de WORM	CSI/STI	Gestores da área de infraestrutura	dez/21	adquirir ativos necessários	já há processo SEI para essa finalidade	iniciado
	Atualização dos servidores de correio eletronico microsoft exchange 2013 e oracle	mitigar riscos de incidentes cibernéticos	STI/CIE	Gestores da área de infraestrutura	dez/21	adquirir os softwares necessários	a serem levantados	iniciado
	Confecção de um ambiente de contingência ativo-ativo, bem como resstruturação do datacenter principal	inserir niveis de resiliência a ataques cibernéticos	CSI/STI	Gestores da área de infraestrutura	dez/21	proceder a criação de um minidatacenter na CAE, extender o cluster principal para o datacenter citado	já há processo SEI para essa finalidade	a iniciar
	Realizar incrementos de segmentos de rede para proteger os ativos de informação mais criticos e as interfaces de gerenciamento	Inserir niveis de segurança para prevenção de incidentes cibernéticos	CSI/STI	Gestores da área de infraestrutura	abr/21	Analisar estratégias para incrementar redes isoladas	sem custos	iniciado
	Implementar Firewall de	Inferir mais um	CSI/STI	Gestores de	dez/21	Analisar	a serem	a iniciar

	Aplicações Web (WAF)	nível de segurança para aplicações Web externas e internas		áreas técnicas de infraestrutura e de sistemas		ferramentas de mercado e implementar o uso do firewall externo do TSE para aplicações acessíveis pela Internet	levantados	

Documento assinado eletronicamente por **LUCIR ROCIO VAZ**, **Analista Judiciário**, em 23/02/2021, às 11:37, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **KEITH WILIAN BANDEIRA MACEDO**, **Secretario(a)**, em 23/02/2021, às 11:51, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ALTAMIRO DANTAS CRUZ**, **Secretario(a)**, em 23/02/2021, às 12:03, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JONATHAS SANTOS ALMEIDA DE CARVALHO**, **Diretor Geral**, em 23/02/2021, às 13:19, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Denise Castelo Bonfim**, **Presidente**, em 23/02/2021, às 16:47, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DULCILEIDE REBOUÇAS DE MESQUITA DALACOSTA**, **Analista Judiciário**, em 23/02/2021, às 18:14, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-ac.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0408224** e o código CRC **CD706244**.

0000255-46.2021.6.01.8000 0408224v2