TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - STIC
COMITÊ EXECUTIVO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - CETIC

ATA DA 32ª REUNIÃO CETIC – 7 de dezembro de 2021

1. PARTICIPANTES

George Maciel	Secretário de TI e Comunicação | STIC
Saulo de Cássio	Coordenador de Governança, Gestão e Segurança da Informação | COGGI
Valéria Miranda	Coordenadora de Serviços | COSERV
José Ferreira Júnior	Coordenador de Infraestrutura | COINF
Mlexener Romeiro	Coordenador de Sistemas | COSIS
Gilberto Martins	Chefe da Seção de Planejamento | SEPLAN-COGGI
Ricardo Baudel	Chefe da Seção de Segurança da Informação | SESIN-COGGI
Flávio Costa	Chefe da Seção de Atendimento ao Usuário | SEAU-COSERV

2. TÓPICOS DA REUNIÃO

TEMAS			
1	**ACOMPANHAMENTO DAS AÇÕES DELIBERADAS ANTERIORMENTE**		
ID	**DESCRIÇÃO**	**UNIDADE RESPONSÁVEL**	**PRAZO**
1	Pautar o **COGEST** para deliberar sobre as ações previstas no **Eixo 5** da Estratégia Nacional de Cibersegurança	**Gabinete STIC**	30.nov.21 **(concluída)**
2	Apresentar os valores estimados para as ferramentas sugeridas (Proteção de Infraestruturas Críticas de TIC) à COGGI	**COINF**	3.dez.21 **(concluída)**
3	Pautar o **COGEST** para deliberar sobre a possibilidade de manter e/ou ampliar o quantitativo usado para transmissão de resultados de eleição do 1º turno das Eleições 2020.	**Gabinete STIC**	30.nov.21 **(concluída)**

4	Minutar um questionamento ao TSE para encaminhamento pelo Gabinete da STIC, sobre alteração de metas do PDTIC e alguns esclarecimentos.	**COSIS** **Gabinete STIC**	19.nov.21 **(minuta concluída)** **Mudou-se o entendimento**, não sendo necessário o questionamento ao TSE.
5	O Secretário de TIC convocará uma reunião do grupo para avaliar a ação de definição de escopo e responsável (ref. conclusão do Plano de Ação e revisão do Cronograma para atendimento ao Protocolo de Ataques Cibernéticos).	**STIC**	**Ação parcialmente concluída**, conforme Proc. SEI nº 0013056-47.2021 **== Agendar 1ª Reunião ETIR em 2022 para 11.mar.22 ==**
6	Definir escopo e responsável pelo atendimento dos sistemas providos pelo TSE e externos (ref. conclusão do Plano de Ação e revisão do Cronograma para atendimento ao Protocolo de Ataques Cibernéticos).	**ETIR**	**Aguardar novo prazo que será definido pela ETIR**

2	**ANÁLISE DA DFEP DA SEBEN-SGP PARA REALIZAR O RECADASTRAMENTO ANUAL DE BENEFÍCIOS ATRAVÉS DO SISTEMA *SERVIDOR NA WEB***

UNIDADE DEMANDANTE: COSIS

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: Necessidade de inclusão de itens para marcação no Sistema de Gestão de Recursos Humanos - SGRH/**Servidor na Web** (aba Benefícios - Lista de Benefícios do servidor, com emissão de relatório de controle). SEI nº 0021914-67.2021.

Apresentada por **Mlexener** e avaliada a requisição, que foi **aprovada** pelo CETIC, tendo a previsão de liberação de nova versão estabelecida para **11.março.2022**.

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Solicitar pauta ao **COGEST** para análise dessa **DFEP** da **SEBEN**-SGP (SEI nº 0021914-67.2021)	**Gabinete STIC**	14.dez.21

3	**UTILIZAÇÃO DA 1TELECOM PARA ACESSO TEMPORÁRIO DA VPN**

UNIDADE DEMANDANTE: COINF

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: Considerando a conclusão do Pregão Eletrônico relativo à contratação dos novos *links* de comunicação de dados, com empresas vencedoras distintas das atualmente contratadas, **Júnior** informou que isso acarretará a alteração dos IPs dos *links* de comunicação para acesso à rede do TRE-PE por VPN.

Por consequência, para acesso à rede por VPN a partir do mês de **jan.2022**, os usuários de TIC terão que alterar a configuração de IP nos computadores pessoais. Assim, para facilitar a operação, a **COINF** elaborou uma rotina simplificada, não necessitando por parte do usuário realizar procedimentos técnicos complexos, para reconfiguração de IP.

Aprovado pelo CETIC o procedimento apresentado pela COINF, tendo deliberado que a **COSERV** providenciará comunicação aos usuários internos de VPN (que estiverem em regime de Teletrabalho) a necessidade de modificar o IP de acesso à VPN a partir de jan.2022, realizando o procedimento indicado pela COINF, devendo - para tanto - elaborar roteiro orientativo simplificado.

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO			

DE AÇÃO	Providenciar roteiro e comunicação aos usuários internos de VPN que estiverem em regime de Teletrabalho (para modificação do IP de acesso à VPN)	**COSERV**	17.dez.21

4	**ANÁLISE DA SOLICITAÇÃO DA COSIS REFERENTE À EXCLUSÃO DE DUAS AÇÕES CONSTANTES DO PLANO DE AÇÃO VINCULADO À PORTARIA CNJ Nº 290/2020 (ART. 8º)**

UNIDADE DEMANDANTE: COGGI

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: A **COSIS** solicitou a exclusão de 2 (duas) ações previstas no **Protocolo de Investigação para Ilícitos Cibernéticos** (identificadas no quadro do **Anexo I -** doc nº 1703914), argumentando que os registros de auditoria permitidos (IP, data/hora), visando ao disposto no artigo 8º, já são armazenados por ativos de infra como servidores de aplicação e *firewalls*.

Avaliada e discutida a proposta, o **CETIC** assim deliberou:

1 – A **COINF** realizará análise nos ativos de TIC identificados no **Anexo II** (doc. nº 1703919), quanto aos itens registrados com "**não**", para ratificar a argumentação da COSIS quanto à solicitação de exclusão de ações. Ratificada a premissa da COSIS, as ações "*Elaborar cronograma de atendimento*" e "*Executar cronograma visando o registro dos eventos relevantes*", para atendimento ao art. 8º, indicadas no **Anexo I** serão excluídas, anotando-se observação referenciando esta deliberação do CETIC;

2 – Em decorrência da proposta da **COSIS**, e para ficar consonante com a Portaria CNJ nº 162/2021 (que substituiu a Portaria CNJ nº 290/2020), a SESIN efetuará a revisão do **Protocolo de Investigação para Ilícitos Cibernéticos**;

3 – Que a **COGGI/SESIN** apresente na próxima reunião do **CETIC** proposta de cronograma de reuniões para realização de reuniões periódicas para acompanhamento de ações das coordenadorias, referentes à segurança da informação;

4 – Que as Coordenadorias que possuem ativos de informação sob controle (**COINF** e **COSERV**) procedam à identificação daqueles que não permitem o registro dos eventos indicados visando ao disposto no artigo 8º, devendo ser utilizado modelo da Planilha do **Anexo II**, elaborada pela COSIS;

5 – Tão logo concluída a ação indicada no item 2, a STIC providenciará a comunicação ao CNJ; e

6 – Fica ratificada a deliberação do **CETIC** aprovando a alteração do prazo da atividade "*Executar cronograma visando o registro dos eventos relevantes*", vinculada aos artigos 6º, 7º e 11, para **30.ago.2022**.

	AÇÃO	**UNIDADE RESPONSÁVEL**	**PRAZO**
PLANO DE AÇÃO	Revisar o **Protocolo de Investigação para Ilícitos Cibernéticos**	**COGGI-SESIN**	10.fev.22
	Realizar análise nos **ativos de TIC** identificados no **Anexo II**, quanto aos itens marcados com "**não**", os registros de auditoria permitidos (IP, data/hora), visando ao disposto no artigo 8º, já são armazenados por ativos de infra como servidores de aplicação e *firewalls*	**COINF**	28.fev.22

5	**ELABORAÇÃO DE TEXTO SOBRE O USO DE *PENDRIVES* E SEUS RISCOS E CUIDADOS**

UNIDADE DEMANDANTE: COGGI

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: Para concluir deliberação do CETIC disposta na Ata da **24ª Reunião**, ocorrida em 3 de agosto de 2021, foi apresentada proposta de texto a ser dirigido aos usuários de TIC internos, acerca do uso de dispositivos móveis de armazenamento (*pendrives*, HDs externos etc) nos equipamentos de propriedade do TRE-PE.

Lida a minuta apresentada, deliberou-se pela revisão do texto apresentado, no sentido de que a

comunicação seja sucinta e objetiva.

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Revisar e reapresentar a minuta de comunicação sobre o uso de dispositivos de armazenamento móveis nos computadores do TRE-PE.	**COGGI-SESIN**	Próxima reunião do CETIC

6	**APRESENTAÇÃO DE PROPOSTA DAS AQUISIÇÕES RELACIONADAS AO ORÇAMENTO DE SEGURANÇA, PARA O EXERCÍCIO 2022**

UNIDADE DEMANDANTE: COGGI

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: Para atender ao que exige a **Res. CNJ nº 396/2021** - Estratégia Nacional de Segurança Cibernética do Poder Judiciário (**ENSEC-PJ**), a **COGGI** apresentou proposta de orçamento para contratação de soluções de TIC, conforme documento **Anexo III** (doc. nº 1703926)

Analisada e discutida, a proposta foi **aprovada** conforme apresentada, para compor a proposta orçamentária 2022.

Também foi definida uma contratação que será indicada ao **TSE** (***Software* de Vulnerabilidade**) para compor o rol de contratações que podem vir a ser realizadas sob a forma de compra compartilhada (projeto piloto do TSE relacionado à Segurança Cibernética).

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Registrar no *ConnectJus* a indicação de possível compra compartilhada para 2022	**COGGI-SEGOR**	15.dez.21
	Solicitar inclusão das despesas relacionadas ao atendimento dos protocolos de Segurança Cibernética no PCI 2022	**COINF**	7.jan.2022

7	**CONFIGURAÇÃO DO SISTEMA ELO PARA USO POR SERVIDORES TERCEIRIZADOS NAS ZONAS ELEITORAIS E CENTRAIS DE ATENDIMENTOS AO ELEITOR (ACÓRDÃO TCU)**

UNIDADE DEMANDANTE: COSERV

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: Em decorrência do conhecimento do inteiro teor do **acórdão TCU** sobre o uso do **sistema ELO** por **terceirizados**, realizar a análise do trâmite do SEI nº 0022862-12.2017.6.17.8400, com relação à definição de quais funcionalidades devem ser atribuídas ao perfil de acesso ao sistema para esta finalidade.

Após contato com TSE, **Marcos Cerqueira (SEIPE-COSERV)** apresentou ao CETIC, na reunião de 23.jan.2021, as seguintes informações:

- que o perfil "Apoio Administrativo", no sistema ELO, para os usuários terceirizados que trabalham nos CZEs, Postos e Centrais de Atendimento ao Eleitor, será disponibilizado em março de 2020 na nova versão do ELO que funcionará em ambiente ODIN;
- que os perfis “Apoio Administrativo Zona” e “Apoio Administrativo Central” já estão disponíveis para uso no ELO para acesso via ODIN. As permissões estão compatíveis com as permissões definidas no Provimento nº 7 – CGE, constante do processo SEI nº 0022862-12.2017;
- que a migração para uso do acesso ao sistema ELO via ODIN, que estava prevista para acontecer em março de 2020, ficou prejudicada pelo estabelecimento do *home office* para os servidores do TRE, quando só foram configurados alguns acessos de forma provisória para os chefes de cartório e alguns servidores da CRE-PE; e
- que a continuidade das configurações de acessos para uso do sistema ELO via ODIN será continuada no retorno aos trabalhos presencias pelos cartórios, que também precisarão atualizar a aplicação ELO nas máquinas com SIS para passarem a usar a nova forma do

sistema, que permitirá a utilização dos perfis acima descritos.

Assim, restou deliberado pelo CETIC que a **COSERV** providenciará comunicação às zonas eleitorais no sentido de orientar a abertura de chamado, via **SAC**, para **requisição de concessão de acesso ao ELO** para os usuários terceirizados e correlatos (militares, estagiários etc).

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Providenciar comunicação às zonas eleitorais no sentido de orientar a abertura de chamado, via SAC, para requisição de concessão de acesso ao ELO para os usuários terceirizados e correlatos (militares, estagiários etc).	**COSERV**	12.jan.22

8	NOVO PROCEDIMENTO DE INCLUSÃO/EXCLUSÃO DE USUÁRIOS NESTE TRE-PE

UNIDADE DEMANDANTE: COSERV

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: A **COSERV** apresentou ao **CETIC**, para aprovação, o novo procedimento de inclusão/exclusão de usuários neste TRE-PE.

A COSIS sugeriu uma *TRIGGER* no SGRH para inclusão/exclusão **automática** dos acessos aos sistemas.

Por sua vez, a COSERV sugeriu um **cardápio básico** de acessos aos usuários (criação de usuário no AD, *e-mail*, SEI, pastas no *DAKAR*) e o chefe da unidade, se necessário, solicita outros acessos, via chamado SAC-STIC, realizando posteriormente, mapeamento de sistemas e acessos necessários para cada unidade.

Restou deliberado que COSIS, COINF, COSERV e COGGI/SESIN realizem reunião para definição do **escopo** desta ação.

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Realizar reunião para definição do escopo da implantação da *TRIGGER* no SGRH para inclusão/exclusão **automática** dos acessos aos sistemas.	**COSIS, COINF, COSERV e COGGI-SESIN**	28.fev.2022

9	TESTES PARA BLOQUEIO DA EXECUÇÃO DE *APPLETS* (CÓDIGOS DE TERCEIROS)

UNIDADE DEMANDANTE: COINF e COSERV

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: COINF e COSERV apresentaram a **necessidade** de realização de testes referentes ao bloqueio da execução de *applets* (códigos de terceiros) para o cumprimento da **IN nº 15**.

A **COSERV** realizou a identificação dos sistemas em uso pelas unidades do TRE e acredita que - em virtude de os servidores STIC não terem o perfil para fazer as operações realizadas pelos usuários - deva ser informado a cada área para que essas façam os testes após a implantação do bloqueio, sendo mais rápido esse procedimento na solução das falhas percebidas.

Qualquer problema percebido pelo usuário, deve ser aberto **chamado**, mantendo o ponto único de atendimento da STIC, via Central de Serviços.

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Apresentar minuta de mensagem e cronograma, ao CETIC, para viabilizar a realização dos testes de bloqueio da execução de *applets* (códigos de terceiros) pelos servidores.	**COSERV**	9.fev.2022

	Conclusão dos bloqueios dos *applets*, com testes realizados pelos usuários	**COSERV**	31.mar.2022

3. ASSINATURAS

Documento assinado eletronicamente por **GEORGE CAVALCANTI MACIEL FILHO**, **Secretário(a)**, em 25/02/2022, às 10:52, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **GILBERTO DA MOTA MARTINS**, **Chefe de Seção**, em 08/03/2022, às 13:39, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **VALÉRIA FARIAS DE MIRANDA**, **Coordenador(a)**, em 08/03/2022, às 14:35, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MLEXENER BEZERRA ROMEIRO**, **Coordenador(a)**, em 09/03/2022, às 07:54, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOSÉ FERREIRA DE LIMA JÚNIOR**, **Coordenador(a)**, em 09/03/2022, às 15:42, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **SAULO DE CÁSSIO GOMES OLIVEIRA**, **Coordenador(a)**, em 10/03/2022, às 08:53, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **FLÁVIO ROBERTO GOMES DA COSTA**, **Chefe de Seção**, em 11/03/2022, às 11:27, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RICARDO MACEDO BAUDEL**, **Chefe de Seção**, em 14/03/2022, às 16:35, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-pe.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1699243** e o código CRC **C6E74CE1**.

Anexo I

Resolução CNJ nº 362/2020
Regulamentada pela Portaria CNJ nº 291/2020)
- Protocolo de Investigação para Ilícitos Cibernéticos

Plano de Ação para adoção do Protocolo de Investigação para Ilícitos Cibernéticos, elencando sugestões de atividades a serem incluídas no plano

Dispositivo Legal (Portaria CNJ nº 291/2020)	**Atividades**	**Prazo**	**Responsável**	**Status**
Art. 5º O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).	• Verificar com equipe técnica do TSE se a sincronização de horário é efetuada segundo os padrões exigidos	30/04/21	STIC/COINF	
	• Ajustar/atualizar horários dos ativos internos conforme recomendação.	31/05/21	STIC/COINF	
Art. 6º Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), tais como: I – autenticação, tanto as bem-sucedidas quanto as malsucedidas; II – acesso a recursos e dados privilegiados; e III – acesso e alteração nos registros de auditoria.	• Definir o conjunto de ativos de infraestrutura a serem verificados	30/06/21	STIC/COINF	
	• Identificar os ativos de informação que não permitem o registro dos eventos indicados visando o disposto no artigo 8º.	31/08/21	STIC/COINF	
	• Efetuar ajustes nas configurações nos ativos de infraestrutura que possibilitem o registro dos itens solicitados	30/11/21	STIC/COINF	
Art. 7º Os registros dos eventos previstos no artigo anterior devem incluir as seguintes informações: I – identificação inequívoca do usuário que acessou o recurso; II – natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc; III – data, hora e fuso horário, observando o previsto no art. 5º; e IV – 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.	• Definir o conjunto de ativos de infraestrutura a serem verificados .	30/06/21	STIC/COINF	
	• Identificar os ativos de informação de infraestrutura que não permitem o registro dos eventos indicados visando o disposto no artigo 8º.	31/08/21	STIC/COINF	
	• Efetuar ajustes nas configurações nos ativos de infraestrutura que possibilitem o registro dos itens solicitados	30/11/21	STIC/COINF	
	• Definir escopo de ativos de informação para atendimento à recomendação.	31/05/21	STIC/COINF	
	• Identificar/listar ativos que não possam atender à recomendação	30/06/21	STIC/COINF	

Dispositivo Legal (Portaria CNJ nº 291/2020)	**Atividades**	**Prazo**	**Responsável**	**Status**
Art. 11. Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável.	• Realizar procedimentos e prospectar aquisições necessárias para atendimento à recomendação	30/11/21	STIC/COINF	
	• Definir eventos relevantes	31/03/21	CETIC	
	• Definir dados privilegiados	31/03/21	CETIC	
	• Identificar os ativos de informação sob responsabilidade da COSIS que permitem o registro dos eventos visando o disposto nos artigos 6º, 7º e 11º, analisando e definindo os requisitos para atendimento	31/05/21	STIC/COSIS	**Concluída**
	• Elaborar cronograma de atendimento	30/06/21	STIC/COSIS	**Concluída**
	• Executar cronograma visando o registro dos eventos relevantes	30/06/22 30/08/22	STIC/COSIS STIC/COINF STIC/COGGI	**Em andamento**
Art. 8º Os ativos de informação que não permitem os registros dos eventos acima listados devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.	• Elaborar documentação quanto ao tipo e formato de registros de auditoria permitidos e armazenados pelo ativo.	31/08/21	STIC/COINF	
	• Identificar os ativos de informação sob responsabilidade da COSIS que não permitem o registro dos eventos indicados nos artigos 6º, 7º, visando o disposto no artigo 8º	31/05/21	STIC/COSIS	**Concluída**
	• ~~Elaborar cronograma de atendimento~~	~~30/06/21~~	~~STIC/COSIS~~ (solicitação de exclusão)	**Concluída**
	• ~~Executar cronograma visando o registro dos eventos relevantes~~	~~30/06/22~~	~~STIC/COSIS~~ (solicitação de exclusão)	**Em andamento**
	• Definir escopo e responsável pelo atendimento dos sistemas providos pelo TSE e externos	31/05/21	CETIC	
Art. 9º Os sistemas e redes de comunicação de dados devem ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de	• Definir o conjunto de ativos de infraestrutura a serem verificados.	30/11/21	STIC/COINF	

Dispositivo Legal (Portaria CNJ nº 291/2020)	Atividades	Prazo	Responsável	Status
outros considerados relevantes: I – utilização de usuários, perfis e grupos privilegiados; II – inicialização, suspensão e reinicialização de serviços; III – acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis; IV – modificações da lista de membros de grupos privilegiados; V – modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, etc; VI – acesso ou modificação de arquivos ou sistemas considerados críticos; e VII – eventos obtidos por meio de quaisquer mecanismos de segurança existentes.	• Identificar os ativos de informação de infraestrutura que não permitem o registro dos eventos indicados visando o disposto no artigo 8º.	30/11/21	STIC/COINF	
	• Efetuar ajustes nas configurações nos ativos de infraestrutura que possibilitem o registro dos itens solicitados	29/04/22	STIC/COINF	
Art. 10. Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (logs) em formato que permita a completa identificação dos fluxos de dados. Parágrafo único. Os registros devem ser armazenados pelo período mínimo de seis meses, sem prejuízo de outros prazos previstos em normativos específicos.	• Revisar/Atualizar os procedimentos já utilizados para salvaguarda de logs em servidores web.	30/11/22	STIC/COINF	
Art. 12. A ETIR, sob a supervisão de seu responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar: I – as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses; II – os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e III – todos os registros de eventos citados no Capítulo IV.	• Realizar novos ajustes na minuta de revisão da portaria da ETIR para adequar às novas atribuições previstas nas Portarias CNJ nºs 290, 291 e 292/2020.	31/03/21	STIC/COGGI	**Concluída**
Art. 13. Nos casos de inviabilidade de preservação das mídias de armazenamento mencionadas no inciso I, do art. 12, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR, sob a supervisão	• Realizar novos ajustes na minuta de revisão da portaria da ETIR para adequar às novas atribuições previstas nas Portarias CNJ nºs 290, 291 e 292/2020.	31/03/21	STIC/COGGI	**Concluída**

Dispositivo Legal (Portaria CNJ nº 291/2020)	Atividades	Prazo	Responsável	Status
do seu responsável, deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os "metadados" desses arquivos, como data, hora de criação e permissões. Parágrafo único. O agente responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados. **Art. 14**. As ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências.				
Art. 15. Para a preservação dos arquivos coletados, deve-se: I – gerar arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados; II – gravar os arquivos coletados, acompanhado do arquivo com a lista dos resumos criptográficos descritos no inciso anterior; e III – gerar resumo criptográfico do arquivo a que se refere o inciso I.	• Realizar novos ajustes na minuta de revisão da portaria da ETIR para adequar às novas atribuições previstas nas portarias CNJ nºs 290, 291 e 292/2020.	31/03/21	STIC/COGGI	**Concluída**
Art. 16. Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação relacionados ao Incidente de Segurança penalmente relevante. Parágrafo único. O material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.	• Realizar novos ajustes na minuta de revisão da portaria da ETIR para adequar às novas atribuições previstas nas portarias CNJ nºs 290, 291 e 292/2020.	31/03/21	STIC/COGGI	**Concluída**
Art. 17. Assim que tomar conhecimento de Incidente de Segurança em Redes Computacionais penalmente relevante, deverá o responsável pelo órgão do Poder Judiciário afetado comunicá-lo de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos. Parágrafo Único. Considerado o incidente uma Crise Cibernética, o Comitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas.	• Incluir no normativo que irá adotar o Protocolo de Investigação para Ilícitos Cibernéticos do TRE-PE	31/05/21	COGEST	

Dispositivo Legal (Portaria CNJ nº 291/2020)	**Atividades**	**Prazo**	**Responsável**	**Status**
Art. 18. Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados.	• Realizar novos ajustes na minuta de revisão da portaria da ETIR para adequar às novas atribuições previstas nas portarias CNJ nºs 290, 291 e 292/2020.	31/03/21	STIC/COGGI	**Concluída**
Art. 19. Recebida a Comunicação de Incidente de Segurança em Redes Computacionais, a autoridade responsável pelo órgão do Poder Judiciário deverá encaminhá-la formalmente ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com o material a que se refere o art. 16, para fins de instrução da notícia crime.	• Realizar novos ajustes na minuta de revisão da portaria da ETIR para adequar às novas atribuições previstas nas portarias CNJ nºs 290, 291 e 292/2020.	31/03/21	STIC/COGGI	**Concluída**
Art. 20. Os órgãos do Poder Judiciário deverão elaborar e formalizar plano de ação, com vistas à construção de seu Protocolo de Investigação para Ilícitos Cibernéticos, no prazo máximo de sessenta dias e comunicar ao CNJ.	• Elaborar o plano de ação para construção do Protocolo de Investigação para Ilícitos Cibernéticos.	15/2/21	COGEST	

Anexo II

Cronograma de atendimento ao protocolo de ataques cibernéticos

Ativo	Permite registro	Observação	Prazo
Acesso Web (Sistema)	Sim		mar/22
Sistema de Gestão Orçamentária	Sim		mar/22
Sistema de Informações Gerais	Sim	Apenas para a parte administrativa	mar/22
Sistema de Envio de Ocorrências para o OcorreJE do TSE	Sim		mar/22
Sistema de Monitoramento de Ações	Sim		mar/22
Sistema de Suporte ao Processo Eleitoral	Sim		mar/22
Sistema de Suporte ao Processo Eleitoral - Versão 2	Sim		mar/22
Sistema de Transportes	Sim	Apenas para a parte administrativa	mar/22
Ouvidoria	Sim	Apenas para a parte administrativa	abr/22
Sistema de Atenção à Saúde do Servidor	Sim		abr/22
Sistema de Gerenciamento do Programa de Estágio	Sim		abr/22
Sistema de Questionários	Sim		abr/22
Portal do Servidor	Sim		mai/22
Sistema de Gerenciamento de Eventos	Sim		mai/22
Sistema de Logística	Sim		mai/22
Sistema de Pesquisa de Satisfação do Eleitor	Sim	Apenas para a parte administrativa	mai/22
Eleitor do Futuro	Sim		jun/22
Juntas Eleitorais	Sim		jun/22
Mesário Voluntário	Sim		jun/22
Sistema de Remoção	Sim	Apenas para a parte administrativa	jun/22
Sistema de Substituição	Sim		jun/22
Diárias	Sim		jul/22
Sistema de Controle de Documentação	Sim		jul/22
Sistema de Monitoramento do Plano de Ação da Biometria	Sim		jul/22
Sistema do Banco de Voluntariado	Sim	Apenas para a parte administrativa	jul/22
Sistema de Gerenciamento de Horas Extras	Sim		jul/22

Ativo	Permite registro	Observação	Prazo
Cadastra Digital	Sim	Sistema cliente/servidor feito com tecnologia antiga (Delphi 6.0), será necessária atualização em todas as máquinas que possuem o sistema instalado.	ago/22
EXPEDE	Sim	Sistema cliente/servidor feito com tecnologia antiga (Delphi 4.0), será necessária atualização em todas as máquinas que possuem o sistema instalado.	ago/22
Ponto Biométrico	Sim	Sistema cliente/servidor feito com tecnologia antiga (Delphi 6.0), será necessária atualização em todas as máquinas que possuem o sistema instalado.	ago/22
Sistema de Acompanhamento de Chamados da SA	Sim	Sistema cliente/servidor feito com tecnologia antiga (Delphi 5.0), será necessária atualização em todas as máquinas que possuem o sistema instalado.	ago/22
Acesso (Serviço)	Sim		Concluído
Portal do Servidor - Validação	Não	Sistema de consulta sem identificação do usuário	-
Legis	Sim		fev/22
Agenda	Sim		mar/22
Audioagenda	Sim		
Sigweb	Sim		mai/22
SRHWEB	Sim		
Busca servidor	Sim		jun/22
Agendabio	Sim		jul/22
SupreWS	Sim		ago/22
Publicanet	-	não se aplica (será substituído pelo Plone até a próxima eleição)	-
Eleições 1986 a 2004	-	não se aplica (migrando para páginas estáticas)	-
Eleições suplementares 2004	-	não se aplica (migrando para páginas estáticas)	-

Ativo	Permite registro	Observação	Prazo
Eleições 2006	-	não se aplica (migrando para páginas estáticas)	-
Eleições 2008	-	não se aplica (migrando para páginas estáticas)	-
Eleições 2010	-	não se aplica (migrando para páginas estáticas)	-
Eleições 2012	-	não se aplica (migrando para páginas estáticas)	-
APP local de votação (Gera JSON)	Não	Sistema de consulta sem identificação do usuário	-
WS-local-atendimento	Não	Webservice de consulta sem identificação do usuário	-
WS-local-votação	Não	Webservice de consulta sem identificação do usuário	-
WS-candidato	Não	Webservice de consulta sem identificação do usuário	-
WS-eleitor	Não	Webservice de consulta sem identificação do usuário	-
Infodip	Sim	Sistema desenvolvido majoritariamente pelo TRE-PR. Trata-se de um sistema web com dois módulos: Interno, que roda na intranet e é utilizado pelos servidores da JE, e Externo, que roda na internet e é utilizado pelos órgãos comunicantes (agentes externos à JE). Permite o registro de eventos de autenticação apenas pois podemos atuar na parte do software que cuida disso.	mar/22
iPleno	Não	Sistema web desenvolvido e mantido pelo TRE-SE	-
SEI	Não	Sistema web desenvolvido e mantido pelo TRF4.	-

Ativo	Permite registro	Observação	Prazo
SGRH	Não	Sistema *desktop* desenvolvido e mantido pelo TSE.	-
SIEL	Não	Sistema Web originalmente desenvolvido pelo TRE-RS e mantido, atualmente, pelo TSE.	-
Atena	Sim	Sistema desenvolvido colaborativamente entre vários regionais. Na arquitetura atual, existem dois módulos web: o primeiro é utilizado para a exibição e extração de resultados de metas e indicadores do CNJ e o segundo para tratamento e envio das informações processuais para a **Datajud**. Permite o registro de eventos de autenticação apenas pois podemos atuar na parte do software que cuida disso.	mar/22
Atualizador SGRH	Não	Sistema web com processamentos em *batch* disparados periodicamente. Originalmente desenvolvido por outro regional, mas atualmente customizado e mantido pelo TRE-PE.	-
Confirmação Mesários	Sim	Sistema com um módulo web que roda na internet e se comunica por web *service* com um módulo de serviço que roda na intranet no qual é feita a comunicação com o banco de dados.	jun/22
NEFT	Sim	Sistema web utilizado para controle da atribuição de matrículas para servidores.	mar/22
SAPE	Não	Sistema que permite o acompanhamento do processo eleitoral. Não possui registros de autenticação	-
SGPForms	Não	Sistema web que interage com o SEI via web *service* para geração de processos e documentos de finalidades específicas naquele sistema.	-

Ativo	Permite registro	Observação	Prazo
SIGMA	Sim	Sistema web. Realiza a gestão dos dados dos juízes e membros da justiça eleitoral.	abr/22
Transparência Dados Servidores	Não	Sistema web originalmente desenvolvido pelo TSE, mas atualmente customizado e mantido pelo TRE-PE.	-
AUDITSE	Não	Sistema web desenvolvido e mantido pelo TSE a partir de um projeto original do banco central.	-
SIJUREL	Não	Sistema web que interage com o SIGMA e com o SEI via web *service* para criação de processos referentes a solicitações de inscrições de juízes em rodízios eleitorais. Não permite registros de autenticação	-
SIS IMOVEIS	Sim	Sistema web originalmente desenvolvido pelo TRE-RS, mas atualmente customizado e mantido pelo TRE-PE.	nov/22
Estatísticas Biometria	Não	Sistema de consulta sem identificação do usuário	-

Anexo III

Proposta Aquisições 2022 - Orçamento de Segurança

Produto	Quantidade	Requisitos atendidos	Valor Estimado (R$)
Firewalls com *software* de análise de *log* e 5 anos de suporte/garantia	2	5.4 Implantar ferramentas de gerência de configuração de sistemas que automaticamente imponham e reapliquem opções de configuração sobre os sistemas em intervalos regulares agendados. 6.3 Habilitar o *log* dos sistemas de forma a incluir informações detalhadas, tais como origem do evento, data, usuário, horário, endereços de origem, endereços de destino e outros elementos úteis. 6.6 Implantar *Security Information and Event Management* (SIEM) ou ferramenta analítica de *logs* para correlação e análise de *logs*. 6.7 Em uma base regular, revisar os *logs* para identificar anomalias ou eventos anormais. 6.8 Em uma base regular, ajustar as configurações do SIEM de forma a melhor identificar eventos que requeiram ações e diminuir o ruído proveniente de eventos não importantes.	2 x 1.213.500,00 **Total** 2.427.000,00
Appliances de *backup* para salvaguarda de cópia de dados	2	9.3 Testar a integridade dos dados nas mídias das cópias de segurança de forma regular, por meio da realização de um processo de restauração dos dados, de forma a garantir que o processo de cópia de segurança (*backup*) esteja sendo executado de forma apropriada.	2 x 620.000,00 **Total** 1.240.000,00
Cofre de Senhas (solicitamos 313 licenças no máximo e há um valor também estimado para repasse de conhecimento e implantação na ata do TSE)	250 (*software*)	4.1 Utilizar ferramentas automatizadas para inventariar todas as contas administrativas, incluindo contas de domínio e contas locais, para garantir que apenas indivíduos autorizados tenham privilégios elevados. 4.4 Utilizar autenticação multifator e canais criptografados para todos os acessos de contas administrativas. 4.6 Limitar o acesso a ferramentas de *scripting* (tais como *Microsoft PowerShell and Python*) exclusivamente a usuários administrativos ou de desenvolvimento que necessitem acessar tais funcionalidades.	*Software*: 250 x 1.690,00 **Total** 422.500,00 Serviço: **Total** 150.000,00
Solução de Segurança para Servidores com XDR e *Sandbox*, com manutenção, garantia e suporte por 60 meses	100 (*software*)	8.8 Habilitar *log* de auditoria sobre ferramentas de linha de comando, tais como *Microsoft Powershell* e *Bash*.	*Software*: 100 x 605,00 **Total** 60.500,00

Produto	Quantidade	Requisitos atendidos	Valor Estimado (R$)
Software de Vulnerabilidade	500 IPs por 3 anos	3.1 Utilizar uma ferramenta atualizada e compatível com o SCAP para efetuar varreduras automatizadas em todos os ativos conectados à rede com frequência semanal ou inferior para identificar todas as vulnerabilidades potenciais nos sistemas da organização. 3.3 Utilizar uma conta dedicada para as varreduras por vulnerabilidades autenticadas, que não deve ser utilizada para quaisquer outras atividades administrativas e que deve ser vinculada a equipamentos específicos, em endereços IP específicos.	*Software*: 306.000,00 Serviço de Implantação e Treinamento: 50.000,00
Software de NAC	1.500 dispositivos	1.5 Garantir que ativos não autorizados sejam removidos da rede ou colocados em quarentena, ou que o inventário seja atualizado em tempo hábil.	*Software*: R$ 416.309,00 Serviço de implantação e suporte: 100.000,00
			TOTAL EQUIPAMENTOS/ *SOFTWARES*: 4.646.344,69 **TOTAL** SERVIÇOS: 300.000,00

OBS.: As estimativas foram realizadas com base em atas de registro de preços existentes, mas pode haver variação de preço por conta do dólar. A ARP do TRE-PB, que opinamos pela participação recentemente, já engloba também as *appliances*.