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

ATA DA 5ª REUNIÃO CETIC – 17 de março de 2022

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
Iara Vilela	Gabinete | STIC

2. TÓPICOS DA REUNIÃO

TEMAS			
1	**ACOMPANHAMENTO DAS AÇÕES DELIBERADAS ANTERIORMENTE**		
ID	**DESCRIÇÃO**	**UNIDADE RESPONSÁVEL**	**PRAZO**
1	Atualizar o SEI nº 0001101-82.2022 com os itens de menu que o CETIC deliberou por manter ou não na **nova intranet (Plone)**	**Gabinete STIC**	17.fev.2022 **(concluída)**
2	Enviar e-mail aos servidores do 2º Grau, orientando a mudança para a versão PJe *Mobile*	**COSERV**	18.fev.2022 **(concluída)**
3	Registrar sugestão do CETIC de **inclusão** de rotatividade de servidores de TIC em relação a unidades **internas** do TRE-PE (excetuando a própria STIC)	**Gabinete STIC**	21.fev.2022 **(concluída)**
4	Realizar reunião semanal, inicialmente, com as unidades STIC, para a atualização dos SLAs	**COSERV**	21.fev.2022 **(concluída)**
5	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.2022 **Ação em andamento**
6	Publicar na *intranet* e noticiar aos usuários o **Plano de Continuidade dos Serviços Essenciais**, conforme anexo (doc. nº 1710015)	**COSERV**	28.fev.2022 **(concluída)**
7	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**
	Realizar reunião para definição do escopo da implantação da *TRIGGER*	**COSIS, COINF,**	15 mar 2022

8	no SGRH para inclusão/exclusão **automática** dos acessos aos sistemas.	**COSERV e COGGI-SESIN**	15.mar.2022 **(concluída)**
9	Minutar mensagem visando a orientar/esclarecer os usuários (servidores) quanto ao uso do *WhatsApp Web* e do *Telegram Web*, encaminhando-a ao **CGSI** para envio aos servidores.	**SESIN-COGGI**	24.mar.2022
10	Apresentar ao CETIC os **SLAs** das unidades da STIC para validação	**COSERV**	30.mar.2022
11	Conclusão dos bloqueios dos *applets*, com testes realizados pelos usuários.	**COSERV**	31.mar.2022
12	Realizar reuniões com unidades envolvidas nas ações do PDTIC	**SEPLAN-COGGI**	29.abr.2022

2 — ANÁLISE DE 2 DFEPs DO SIGEPE - SELOG

UNIDADE DEMANDANTE: COSIS

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: Para o **SIGEPE**, a **SELOG** apresentou 2 solicitações fora de escopo, que foram analisadas pelo CETIC:

- DFEP doc nº 1747968, SELOG: **Custo:** R$ 5.141,04 e **Tempo** (Recursos Humanos): 12d
- DFEP doc nº 1752886, SELOG: **Custo:** R$ 4.359,84 e **Tempo** (Recursos Humanos): 12d

Analisadas as solicitações e verificados os impactos, o CETIC deliberou por **pautar o COGEST**, para avaliação da solicitação e autorização de **priorização**, frente aos sistemas já priorizados (planilha atual: https://intranet.tre-pe.gov.br/publicanet/ServletBaixarAnexo.do?codObjetoAnexo=36156): SASS (item 11, da SGP) e Sistema para acompanhamento das Contratações (item 8, da SA).

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Pautar o COGEST, para deliberação sobre priorização dessas solicitações da SELOG (DFEP doc nº 1747968 e DFEP doc nº 1752886) frente às já ranqueadas	**Gabinete STIC**	18.mar.22

3 — VALIDAÇÃO DE FLUXO REFERENTE À INSTRUÇÃO NORMATIVA Nº 60/2021, QUE ESTABELECE A *POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NA JUSTIÇA ELEITORAL DE PERNAMBUCO*

UNIDADE DEMANDANTE: COGGI

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: **Saulo** apresentou para **registro da validação** pelo **CETIC**, o fluxo (documento: **Anexo Minuta-fluxo-IN-60-Processo-de-Incidentes-de-SI** (1784724), correspondente à **Instrução Normativa nº 60/2021**, que estabeleceu a **Política de Gestão de Incidentes de Segurança da Informação da Justiça Eleitoral de Pernambuco**, já objeto de análise prévia dos membros do CETIC.

Documento validado.

4 — ANÁLISE DE DFEP DO SISPEL - OUVIDORIA

UNIDADE DEMANDANTE: COSIS

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: Para o **SISPEL**, a **Ouvidoria** apresentou a solicitação fora de escopo, que foi analisada pelo CETIC:

- DFEP doc nº 1755937: **Custo:** R$ 6.993,60 e **Tempo** (Recursos Humanos): 15d

Analisada a solicitação e verificados os impactos, o CETIC deliberou por **pautar o COGEST**, para avaliação da solicitação e autorização de **priorização**, frente aos sistemas já priorizados (planilha atual: https://intranet.tre-pe.gov.br/publicanet/ServletBaixarAnexo.do?codObjetoAnexo=36156): SASS (item 11, da SGP) e Sistema para acompanhamento das Contratações (item 8, da SA).

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Pautar o COGEST, para deliberação para sobre priorização dessa solicitações da Ouvidoria (DFEP doc nº 1755937) frente às já ranqueadas	**Gabinete STIC**	18.mar.22

5 — EXTRA-PAUTA: INFRAESTRUTURA PARA A AVE (AUDITORIA DO VOTO ELETRÔNICO)

UNIDADE DEMANDANTE: COINF

ASSUNTO ANALISADO E DELIBERAÇÕES CETIC: **Júnior** trouxe o tema à análise do CETIC e deliberou-se por levar o questionamento ao COGEST, para deliberação:

- quais os parâmetros e que local será utilizado para a **cerimônia de Auditoria do Voto Eletrônico (AVE)** - de preferência para a próxima reunião do COGEST, para propiciar o devido planejamento de ações na STIC.

	AÇÃO	UNIDADE RESPONSÁVEL	PRAZO
PLANO DE AÇÃO	Pautar o COGEST, para deliberação sobre quais os parâmetros e que local será utilizado para a **cerimônia de Auditoria do Voto Eletrônico (AVE)** para propiciar o devido planejamento de ações	**Gabinete STIC**	18.mar.22

3. ASSINATURAS

Documento assinado eletronicamente por **GEORGE CAVALCANTI MACIEL FILHO**, **Secretário(a)**, em 24/03/2022, às 10:20, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IARA DE MORAIS ALVES VILELA DO NASCIMENTO**, **Assistente de Gabinete**, em 24/03/2022, às 12:04, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MLEXENER BEZERRA ROMEIRO**, **Coordenador(a)**, em 24/03/2022, às 15:06, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **SAULO DE CÁSSIO GOMES OLIVEIRA**, **Coordenador(a)**, em 25/03/2022, às 10:47, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **VALÉRIA FARIAS DE MIRANDA**, **Coordenador(a)**, em 25/03/2022, às 12:43, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOSÉ FERREIRA DE LIMA JÚNIOR**, **Coordenador(a)**, em 25/03/2022, às 13:42, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

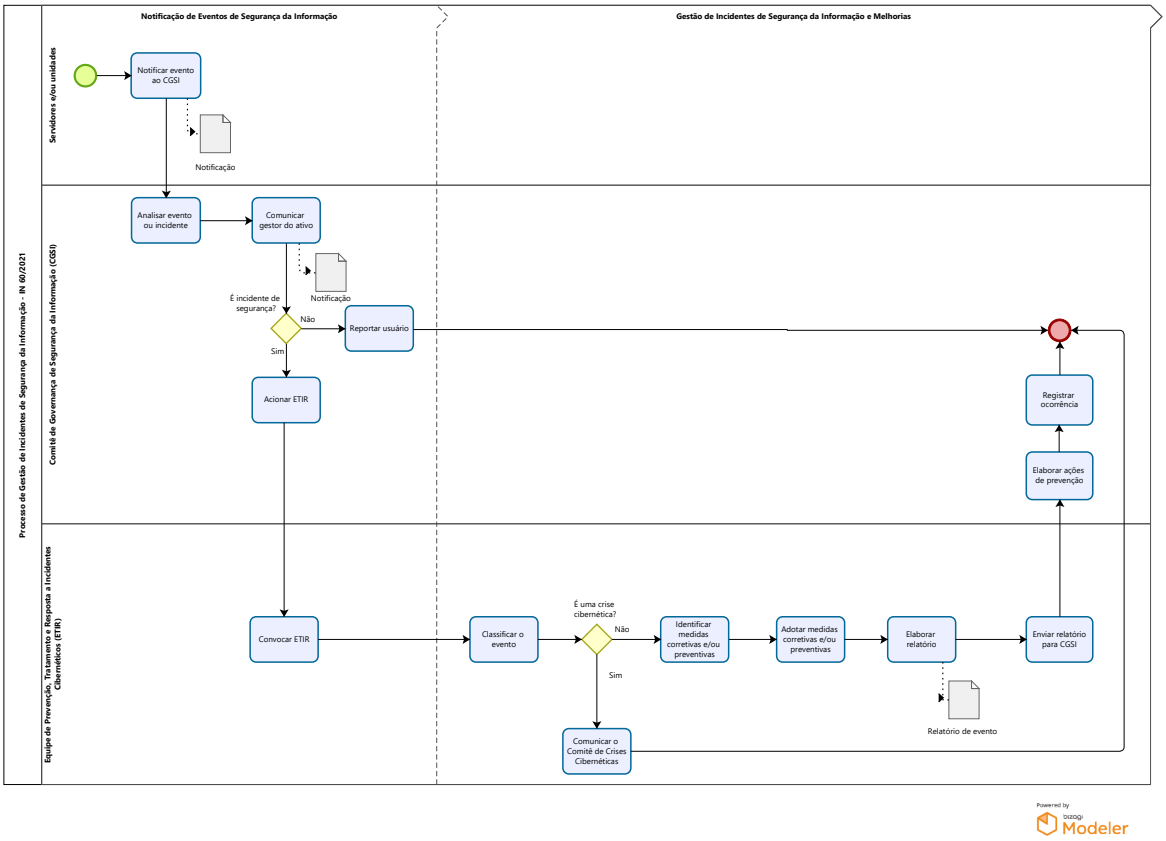
A autenticidade do documento pode ser conferida no site http://sei.tre-pe.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1784235** e o código CRC **3FF477D0**.

IN 60_2021 - Processo de incidentes de SI_atual

Bizagi Modeler

Índice

1 INSTRUÇÃO NORMATIVA Nº 60_2021



1.1 PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO - IN 60/2021

1.1.1 ELEMENTOS DO PROCESSO

1.1.1.1 Notificar evento ao CGSI

Descrição

Os servidores/unidades devem notificar ao CGSI os eventos de segurança da informação assim que identificá-los, art. 3º.

São exemplos de evento ou incidente de segurança da informação, art. 4º, I a VIII: perda de serviço, equipamento ou recursos; mau funcionamento ou sobrecarga de sistema; erros humanos; não conformidade com as políticas e diretrizes estabelecidas; violações de procedimentos de segurança física; mudanças descontroladas de sistemas, tais como realizadas sem monitoramento ou sem decorrência de invasão; mau funcionamento de software ou hardware; e violação de acesso a um sistema.

Observação:

- O(a) usuário(a) não deve realizar nenhuma ação por iniciativa própria nem, sob nenhuma circunstância, tentar averiguar uma fragilidade, para evitar o risco de causar danos ao sistema ou serviço de informação, art. 5º.

- A notificação deve ser realizada, preferencialmente, por meio de mensagem de correio eletrônico, art. 6º, parágrafo único.

1.1.1.2 Notificação

Descrição

A notificação deve conter relatos importantes, tais como o tipo de não conformidade, violação ou mau funcionamento, mensagem apresentada na tela ou comportamento considerado estranho, art. 3º, parágrafo único.

1.1.1.3 Analisar evento ou incidente

Descrição

O CGSI deve realizar, de forma prioritária, a análise das notificações de evento ou incidente de segurança da informação recebidas, art. 7º.

1.1.1.4 Comunicar gestor do ativo

Descrição

O CGSI deverá comunicar o(a) gestor(a) do ativo envolvido na notificação, art. 8º, § 2º.

1.1.1.5 Notificação

Descrição

A notificação deve conter relatos importantes, tais como o tipo de não conformidade, violação ou mau funcionamento, mensagem apresentada na tela ou comportamento considerado estranho, art. 3º, parágrafo único.

1.1.1.6 Reportar usuário

Descrição

Quando não se tratar de um incidente de segurança da informação, o CGSI deve prestar os devidos esclarecimentos ao(à) usuário(a) que apresentou a notificação, art. 8º, § 1º.

1.1.1.7 Acionar ETIR

Descrição

O CGSI deverá enviar a notificação, de imediato, à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), caso configurado um incidente de segurança cibernética, art. 8º.

1.1.1.8 Convocar ETIR

Descrição

O coordenador da ETIR convocará a equipe designada em portaria.

1.1.1.9 Classificar o evento

Descrição

A ETIR deverá analisar e classificar o evento, identificando se se configura como uma crise cibernética.

1.1.1.10 É uma crise cibernética?

Descrição

A crise cibernética se caracteriza por:

1) grave dano material ou de imagem;

2) restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

3) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou

4) o incidente atrair grande atenção da mídia e da população em geral.

Portões

Sim

Não

1.1.1.11 Comunicar o Comitê de Crises Cibernéticas

Descrição

No caso do incidente cibernético configurar uma crise cibernética, o Comitê de Crises Cibernéticas deve ser comunicado imediatamente. Devem ser observados o Plano de Gestão de Incidentes Cibernéticos, o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Poder Judiciário (PPINC-PJ), o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCRC-PJ) e o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário (PIILC-PJ), todos integrantes da Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), instituída pelo Conselho Nacional de Justiça (CNJ), art. 9º.

1.1.1.12 Identificar medidas corretivas e/ou preventivas

Descrição

A ETIR identificará as providências que deverão ser implementadas visando a solução do incidente, podendo convocar outras unidades caso necessário. Para tanto, deve ser considerado o Protocolo de Prevenção de Incidentes Cibernéticos (PPINC-PJ) e o Protocolo de Investigações para Ilícitos Cibernéticos (PIILC-PJ), ambos do Poder Judiciário (Portaria CNJ nº 162/2021), o Plano de Gestão de Incidentes Cibernéticos e o Plano de Continuidade dos Serviços Essenciais, dentre outros.

Para atendimento ao Protocolo de Investigações para Ilícitos Cibernéticos (PIILC-PJ), devem ser adotados procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

1.1.1.13 Adotar medidas corretivas e/ou preventivas

Descrição

Adotar as medidas necessárias à execução das ações corretivas e/ou preventivas.

A ETIR demandará tantas unidades quanto forem necessárias à adoção das medidas de prevenção, mitigação e correção.

1.1.1.14 Elaborar relatório

Descrição

A ETIR deverá elaborar relatório detalhado sobre incidente, as ações adotadas e as lições aprendidas.

1.1.1.15 Relatório de evento

Descrição

Relatório contendo as ações adotadas e as lições aprendidas.

1.1.1.16 Enviar relatório para CGSI

Descrição

A ETIR deverá enviar o relatório para conhecimento do CGSI.

1.1.1.17 Elaborar ações de prevenção

Descrição

O CGSI incluirá as orientações e lições aprendidas contidas no relatório da ETIR nas ações de conscientização e orientação quanto à segurança da informação.

1.1.1.18 Registrar ocorrência

Descrição

Os relatórios elaborados pela ETIR serão utilizados, junto com outros artefatos que se fizerem necessários, nas análises semestrais de incidentes de segurança cibernética para identificar eventos

recorrentes ou de alto impacto, que podem indicar a necessidade de outras melhorias ou controles adicionais para limitar a frequência, os danos e os custos.

1.1.1.19 Comitê de Governança de Segurança da Informação (CGSI)

Descrição

Comissão constituída pela Portaria TRE-PE nº 671/2021.

1.1.1.20 Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)

Descrição

Equipe constituída pela Portaria TRE-PE nº 604/2021.