Tribunal Regional Eleitoral de Goiás

Secretaria Judiciária

Coordenadoria de Gestão da Informação

Seção de Legislação e Editoração

PORTARIA N° 309/2022 - PRES

Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e de Segurança Cibernética (ETIR) no âmbito do TRE/GO.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, no uso das atribuições que lhe são conferidas pelo artigo 15, inciso XXXVIII, da Resolução TRE/GO n° 298, de 18 de outubro de 2018 - Regimento Interno e,

CONSIDERANDO a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE), aprovada pela Resolução TSE nº 23.644, de 1º de julho de 2021, e adotada por este Tribunal através da Resolução TRE/GO nº 355, de 10 de novembro de 2021;

CONSIDERANDO a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSECPJ), instituída pela Resolução CNJ nº 396, de 07 de junho de 2021, que determina à alta administração dos órgãos do Poder Judiciário a instituição e implantação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e de Segurança Cibernética (ETIR);

CONSIDERANDO o disposto nos acórdãos n°s 866/2011, 594/2011, 7.312/2010 e 2.746/2010 do Plenário do Tribunal de Contas da União, que determinam a instituição de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas ISO NBR/IEC 27001:2013 e 27002:2013;

CONSIDERANDO a NC 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal, direta e indireta;

CONSIDERANDO a NC 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR) dos órgãos e entidades da Administração Pública Federal, direta e indireta,

RESOLVE:

Art. 1° INSTITUIR a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e de Segurança Cibernética (ETIR) no âmbito do Tribunal Regional Eleitoral de Goiás.

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 2° Para os efeitos desta Portaria e de suas regulamentações aplicam-se as seguintes definições:

I - agente responsável: servidor público, ocupante de cargo efetivo do TRE/GO, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou público alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

V - equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da ETIR;

VIII - tratamento de artefatos maliciosos: serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa;

IX - tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

X - tratamento de vulnerabilidades: serviço que consiste em receber informações

sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção;

XI - ameaças: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

XII - aquisição de evidência: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais;

XIII - coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente;

XIV - crise: um evento ou série de eventos danosos que apresenta propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram; e que apresenta implicações que afetam proporção considerável da organização e de seus constituintes;

XV - crise cibernética: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores. É decorrente de incidentes que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

XVI - evento: qualquer ocorrência observável em um sistema ou rede de uma organização;

XVII - evidência digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;

XVIII - evidência de auditoria: registros, declarações de fato ou outras informações verificáveis e relevantes para os critérios de auditoria;

XIX - gerenciamento de crise: decisões e atividades coordenadas que ocorrem em uma organização durante uma crise corporativa, incluindo crises cibernéticas;

XX - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXI - incidente de Segurança da Informação: evento que viola ou representa ameaça iminente de violação de política de segurança, de política de uso aceitável ou de prática de segurança padrão;

XXII - log: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXIII - plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado para ser usado quando ocorrer incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XXIV - preservação de evidência de incidentes em redes computacionais: processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que

os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações;

XXV - segurança cibernética: conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares. A Segurança Cibernética se aplica a uma parte da segurança da informação com foco na proteção digital, cuidando das ameaças às informações transportadas por meios cibernéticos. Já a Segurança da Informação tem um foco mais amplo, cuidando da redução de riscos no transporte de dados por qualquer meio, seja digital ou não.

CAPÍTULO II

DO OBJETIVO

Art. 3° A ETIR terá como objetivo garantir o cumprimento da missão institucional do Tribunal Regional Eleitoral de Goiás TRE/GO, por meio do tratamento e resposta a incidentes de segurança na rede interna de computadores e de segurança cibernética.

CAPÍTULO III

DO PÚBLICO ALVO

Art. 4° A ETIR atenderá, por meio do serviço de registro de chamados na Central de Serviços ou por e-mail, a todos os usuários da rede de computadores e de sistemas do TRE-GO, de outros Regionais e do TSE, que comunicarem eventos identificados como incidentes de segurança.

Parágrafo único. Após o registro do incidente, este será encaminhado ao agente responsável que tomará as medidas necessárias.

Art. 5° Externamente, poderá a ETIR interagir com outros órgãos da Administração Pública Federal, do Poder Legislativo, do Poder Judiciário e do Ministério Público que atuem no mesmo campo da ETIR, fornecendo informações acerca dos incidentes de segurança ocorridos na rede de computadores do TRE/GO, alimentando as suas bases de conhecimentos e fomentando a troca de tecnologias.

Parágrafo único. A comunicação dos incidentes de segurança, bem como o tratamento aplicado, será efetuada por meio de documento formal.

CAPÍTULO IV

DO MODELO DE IMPLEMENTAÇÃO

Art. 6° A ETIR será implementada segundo o Modelo 1, da NC 05/IN01/DSIC/GSIPR, devendo ser formada, preferencialmente, por servidores efetivos da Secretaria de Tecnologia da Informação que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais e cibernéticos.

CAPÍTULO V

DA AUTONOMIA

Art. 7° A ETIR seguirá o modelo "Autonomia Completa", descrito no subitem 9.1 da NC 05/IN01 /DSIC/GSIPR, que lhe permitirá conduzir o seu público alvo na realização de ações ou medidas necessárias para reforçar a resposta ou a postura da organização, na recuperação de incidentes de segurança.

Parágrafo único. Durante um incidente de segurança, a ETIR poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

CAPÍTULO VI

DA ESTRUTURA ORGANIZACIONAL

Art. 8° A ETIR estará vinculada à Secretaria de Tecnologia da Informação deste Tribunal e terá plena autonomia para desenvolver suas atividades.

Art. 9° A ETIR deverá apresentar ao Comitê Gestor de Segurança da Informação relatórios dos incidentes de segurança ocorridos, com os respectivos tratamentos adotados, com vistas à elaboração de estudos de melhoria dos mecanismos de segurança estabelecidos no Tribunal ou para fins de tomada de decisão estratégica relativa à Segurança da Informação junto à Administração.

Art. 10. A ETIR será formada, preferencialmente, por servidores públicos efetivos lotados na Secretaria de Tecnologia da Informação, nas áreas de Infraestrutura, de Sistemas e de Cibersegurança do Tribunal.

§ 1° Para cada integrante titular, será indicado o respectivo substituto.

§ 2° Seus integrantes, titulares e substitutos, serão indicados pelo Secretário de Tecnologia da Informação e designados por meio de Portaria da Presidência.

§ 3° Dentre os titulares, um deverá ser indicado como Agente Responsável.

Art. 11. A ETIR funcionará como um grupo de trabalho permanente, de atuação

primordialmente reativa e não exclusiva.

Parágrafo único. As atividades reativas da ETIR terão prioridade sobre aquelas designadas pelos chefes imediatos de seus respectivos integrantes.

CAPÍTULO VII

DOS SERVIÇOS E PROCEDIMENTOS

Art. 12. São serviços a serem desempenhados pela ETIR:

I - tratamento de incidentes de segurança em redes computacionais;

II - tratamento de vulnerabilidades;

III - tratamento de incidentes cibernéticos;

IV - comunicação dos incidentes de rede e cibernéticos;

V - identificação de incidentes que constituam Crise cibernética e comunicação ao Comitê de Crises;

VI - apoio técnico na Investigação de Ilícitos Cibernéticos;

VII - monitoramento de eventos, nos sistemas ou na rede de dados, com comportamento anômalo.

Art. 13. Para cada serviço elencado no artigo anterior, deverão ser utilizados procedimentos ou protocolos a serem observados pela ETIR, contendo os seguintes atributos:

I - objetivo;

II - funções básicas;

III - descrição das funções e procedimentos que compõem o serviço;

IV - competências de cada membro da equipe;

V - plano de comunicação.

Parágrafo único. Os documentos de que trata este artigo poderão ser elaborados pela ETIR ou adotados do CNJ, do TSE ou de qualquer outro órgão da Administração Pública Federal e atualizados sempre que possível e necessário.

CAPÍTULO VIII

DAS RESPONSABILIDADES

Art. 14. Caberá ao Agente Responsável:

I - definir, em conjunto com o Comitê Gestor de Segurança da Informação (CSI) do TRE-GO, quais os procedimentos a serem observados pela ETIR;

II - gerenciar as atividades desempenhadas pela ETIR;

III - distribuir, sempre que necessário, tarefas para a ETIR, inclusive as de caráter proativo;

IV - sugerir ao Secretário de Tecnologia da Informação, quando necessário, a convocação de representantes de outras unidades da respectiva Secretaria, para atuar no tratamento e resposta de determinado incidente de segurança;

V - propor treinamentos aos integrantes da equipe, para o fiel desempenho de suas atividades;

VI - assegurar que os usuários sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados;

VII - cuidar da capacitação dos membros da ETIR, fazendo constar do Plano Anual de Capacitação os eventos que entender relevantes ao bom desempenho dos trabalhos da equipe;

VIII - cuidar para que todos os materiais e informações coletados num processo de tratamento de incidentes sejam preservados e tratados como evidência de auditoria;

IX - participar do Comitê de Crises de Segurança, auxiliando a equipe no gerenciamento de crises cibernéticas identificadas pela ETIR.

Art. 15. Caberá à ETIR:

I - manter registro dos incidentes de segurança em redes de computadores notificados ou detectados, com o objetivo de assegurar registro histórico das atividades da ETIR;

II - recolher evidências imediatamente após a constatação de um incidente de segurança da informação na rede interna de computadores;

III - executar análise crítica sobre os registros de falhas para assegurar que as mesmas foram satisfatoriamente resolvidas;

IV - investigar as causas dos incidentes de segurança da informação na rede interna de computadores;

V - implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

VI - indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes;

VII - manter toda e qualquer evidência digital coletada armazenada para possíveis e futuras auditorias;

VIII - seguir o Plano de Gerenciamento de Incidentes definido e aprovado pela CSI.

Art. 16. Caberá ao Secretário de Tecnologia da Informação:

I - submeter ao Diretor-Geral a indicação do Agente Responsável, dos servidores titulares da ETIR e seus respectivos substitutos;

II - apoiar a ETIR, na execução de seu trabalho, viabilizando a disponibilização dos recursos materiais, tecnológicos e humanos necessários à prestação dos serviços oferecidos aos usuários.

CAPÍTULO IX

DAS DISPOSIÇÕES GERAIS

Art. 17. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo Comitê Gestor de Segurança da Informação deste Tribunal.

Art. 18. Este normativo deverá ser revisado periodicamente, em intervalos de, no máximo, três anos.

Art. 19. Esta Portaria entrará em vigor na data de sua publicação, revogando a Portaria nº 247/2018 - PRES e Portaria nº 170/2020 - PRES.

Desembargador ITANEY FRANCISCO CAMPOS

Presidente

ANEXO

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e de Segurança Cibernética - ETIR

Nome	Unidade	Função	E-mail
Marcílio Zaccarelli Bersaneti	CINF	Agente Responsável - titular	marcilio.bersaneti@tre-go.jus.br
Augusto César de Castro Ovelar	CESCO	Agente Resp. - substituto	augusto.ovelar@tre-go.jus.br
Marcos Rogério Santiago	SESRE	Rede - titular	marcos.santiago@tre-go.jus.br
Leandro Pires Rabelo	SESRE	Rede - substituto	leandro.rabelo@tre-go.jus.br
Roberto César Rodrigues	SEPRO	Produção - titutar	roberto.rodrigues@tre-go.jus.br
Aline Mikado	SEPRO	Produção - substituta	aline.mikado@tre-go.jus.br
Renato Oliveira da Silva	ACIBER	Assessoria de Cibersegurança	renato.oliveira@tre-go.jus.br

Brayton Marques Santana	SEDIS	Desenvolvimento - titular	brayton.santana@tre-go.jus.br
Chayner Cordeiro Barros	SEDIS	Desenvolvimento - substituto	chayner.cordeiro@tre-go.jus.br
Leonardo Antônio de Souza	SEAID	Banco de dados - titular	leonardo.souza@tre-go.jus.br
Luis Cláudio Fernandes	SEAID	Banco de dados - substitutol	luisclaudio.fernandes@tre-go.jus.br
Alexandre Einstein Barcelos Cunha	SESCO	Sistemas - titular	alexandre.einstein@tre-go.jus.br
Ramon de Freitas Elias Campos	ASPJE	Sistemas - substituto	ramon.campos@tre-go.jus.br
Roberto Lima Manoel da Costa	APGTI	Planejamento - titular	roberto.lima@tre-go.jus.br