TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Portaria Presidência Nº 527/2022 TRE/PRESI/DG/ASSDG, de 27 de julho de 2022

Institui o Comitê de Crises Cibernéticas no Tribunal Regional Eleitoral do Piauí.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DO PIAUÍ, no uso de suas atribuições legais e regimentais;

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma que ofereça as informações necessárias aos processos deste Tribunal;

CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação (TI), que visam garantir a disponibilidade e integridade dos ativos tecnológicos do Tribunal Regional Eleitoral do Piauí;

CONSIDERANDO a necessidade de agir de forma proativa e reativa a incidentes de segurança da informação;

CONSIDERANDO que a credibilidade da instituição na prestação jurisdicional deve ser preservada;

CONSIDERANDO as normas da Associação Brasileira de Normas Técnicas - ABNT NBR ISO IEC 27001:2013 e 27002:2013 que estabelecem, respectivamente, o sistema de gestão e o código de boas práticas em segurança da informação que recomendam o estabelecimento de regras para o uso aceitável dos ativos de informação; e

CONSIDERANDO o disposto na Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

RESOLVE:

Art. 1º Fica instituído o Comitê de Crises Cibernéticas no Tribunal Regional Eleitoral do Piauí.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Para os efeitos deste normativo, são estabelecidos os seguintes conceitos e definições:

I - ativo: qualquer coisa que represente valor para uma instituição, tal como a informação;

II - ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - atividades críticas: atividades que devem ser executadas para garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

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

V - crise cibernética: caracteriza-se quando o incidente: apresentar grave dano material ou de imagem; as ações de resposta ao incidente provavelmente persistirão por longo período; gerar impacto na atividade finalística ou serviço crítico mantido pelo Tribunal; ou quando o incidente atrair grande atenção da mídia e da população em geral;

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

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

VIII - 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;

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

X - incidente grave: evento que tenha causado dano, colocado em risco ativo de informação crítico ou interrompido a execução de atividade crítica por um período inferior ao tempo objetivo de recuperação; e

XI - 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.

CAPÍTULO II

DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 3º O gerenciamento de incidentes se refere às atividades que devem ser executadas na ocorrência de evento adverso de segurança da informação, para avaliar o problema e determinar a resposta inicial.

Art. 4º O gerenciamento de crise se inicia quando:

I - caracterizado grave dano material ou de imagem;

II - for evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

III - o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou

IV - o incidente atrair grande atenção da mídia e da população em geral.

CAPÍTULO III

DA COMPOSIÇÃO DO COMITÊ DE CRISES CIBERNÉTICAS

Art. 5º O Comitê de Crises Cibernéticas será formado pelos membros a seguir:

I - Presidente do TRE-PI ou representante por ela ou por ele designado;

II - Corregedora ou Corregedor Regional Eleitoral ou representante por ela ou por ele designado;

III - titular da Diretoria-Geral;

IV - titular da Secretaria Judiciária;

V - titular da Secretaria de Tecnologia da Informação;

VI - titular da Secretaria de Administração, Orçamento e Finanças;

VII - titular da Secretaria de Gestão de Pessoas;

VIII - Gestora ou Gestor de Segurança da Informação;

VIII - Encarregada ou Encarregado de Dados Pessoais;

IX - um representante da Comissão Permanente de Segurança;

X - titular ou o titular da área responsável pela Comunicação Institucional;

Parágrafo único. A coordenação do Comitê de Crises Cibernéticas ficará a cargo da Presidente ou do Presidente do TRE-PI ou da representante ou do representante por ela ou por ele designado.

CAPÍTULO IV

DURANTE A CRISE

Art. 6º O Comitê de Crises Cibernéticas deve coordenar ações para garantir que a comunicação entre as áreas envolvidas em crise seja tratada como fator crítico para uma organização responder a uma crise cibernética de longa duração ou de grande impacto.

Parágrafo único. Fica definido que a sala de situação, onde serão realizadas as reuniões do Comitê de Crises Cibernéticas, será, preferencialmente, na sala de reunião da Presidência ou em local a ser determinado pelo Presidente.

Art. 7º Assim que a ETIR identificar que um incidente constitui crise cibernética, deverá ser reunido imediatamente o Comitê de Crises Cibernéticas.

§ 1º O Comitê de Crises Cibernéticas deve reunir-se, presencialmente ou virtualmente, por meio de tecnologia oficial de videoconferência adotada no Tribunal, para deliberar se o incidente reportado pela ETIR constitui crise cibernética.

§ 2º Caso seja confirmada a crise cibernética, o Comitê de Crises Cibernéticas entrará em estado de convocação permanente, podendo reunir-se a qualquer horário para discutir, deliberar e agir no tratamento da crise em curso.

§ 3º O acesso às reuniões do Comitê de Crises Cibernéticas deve ser restrito aos membros deste Comitê e a atores eventualmente convidados a participar das reuniões.

§ 4º O Comitê de Crises Cibernéticas deve ter acesso ágil a meios que permitam fazer declarações públicas à imprensa.

§ 5º O Comitê de Crises Cibernéticas deve contar com equipe dedicada à execução de atividades administrativas necessárias durante o período de crise.

Art. 8º O Comitê de Crise Cibernéticas deverá coordenar esforços com equipes administrativas e técnicas do TRE-PI para:

I - entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;

II - levantar todas as informações relevantes, verificando fatos e descartando boatos;

III - levantar soluções alternativas para a crise, apreciando sua viabilidade e suas consequências;

IV - avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

V - centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

VI - realizar comunicação tempestiva e eficiente, que evidencie o trabalho diligente das equipes e enfraqueça boatos ou investigações paralelas que alimentem notícias falsas;

VII - definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

VIII - aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

IX - solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;

X - apoiar equipes de resposta e de recuperação com gerentes de crise experientes;

XI - avaliar a necessidade de recursos adicionais extraordinários para apoiar as equipes de resposta;

XII - fornecer aconselhamento sobre as prioridades e estratégias da organização para uma recuperação rápida e eficaz;

XIII - definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e

XIV - elaborar plano de retorno à normalidade.

Art. 9º As etapas e procedimentos de resposta são diferentes de acordo com o tipo de crise e são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

Art. 10. Os incidentes graves que ocasionam a deflagração de uma crise cibernética deverão ser comunicados ao Tribunal Superior Eleitoral e ao Conselho Nacional de Justiça.

CAPÍTULO V

DA FASE DE APRENDIZADO E REVISÃO (PÓS-CRISE)

Art. 11. Quando as operações retornarem à normalidade, o Comitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

Art. 12. Para a identificação das lições aprendidas e a elaboração de relatório final, deve ser objeto de avaliação:

I - a identificação e análise da causa do incidente;

II - a linha do tempo das ações realizadas;

III - a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;

IV - os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

V - o escalonamento da crise;

VI - a investigação e preservação de evidências;

VII - a efetividade das ações de contenção;

VIII - a coordenação da crise, liderança das equipes e gerenciamento de informações;

IX - a tomada de decisão e as estratégias de recuperação.

Art. 13. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta e a melhoria do processo de prevenção de crises cibernéticas.

Art. 14. Deve ser elaborado relatório contendo a descrição e detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

Art. 15. Os casos omissos serão resolvidos pela Presidência do TRE-PI.

Art. 16. Esta Portaria entra em vigor na data de sua publicação.

Desembargador ERIVAN LOPES

Presidente do TRE/PI

Documento assinado eletronicamente por **Erivan José da Silva Lopes**, **Presidente**, em 28/07/2022, às 10:01, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1595460** e o código CRC **270A5FEA**.
