PRESIDENTE

ATO Nº 239, DE 28/06/2022

O DESEMBARGADOR JOSÉ PAULO CALMON NOGUEIRA DA GAMA, PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO, de acordo com os autos de protocolo 11.576/2013, Processo SEI nº 0002905-08.2020.6.08.8000, atendidas as exigências contidas na Lei nº 11.416/2006, alterada pela Lei nº 13.317/2016; na Resolução TSE nº 22.582/2007; e de acordo com o art. 3º da Resolução TRE/ES nº 87/2008, RESOLVE:

EFETUAR A PROMOÇÃO do servidor Diogo Damiani Mendes, Técnico Judiciário, da Classe B, Padrão 10, para a Classe C, Padrão 11, com efeitos financeiros a partir de 19/05/2022.

DES. JOSÉ PAULO CALMON NOGUEIRA DA GAMA

PRESIDENTE

PORTARIAS

PORTARIA Nº 236, DE 04/07/2022

INSTITUI O COMITÊ DE CRISES CIBERNÉTICAS NO TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO E DEFINE A SALA DE SITUAÇÃO.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO, no uso de suas atribuições legais e regimentais e

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 a integridade dos ativos tecnológicos do TRE-ES;

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

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

CONSIDERANDO o disposto na Portaria nº 162, de 10 de junho de 2021, que aprova Protocolos e Manuais criados pela Resolução CNJ no 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ),

RESOLVE:

Art. 1o. Instituir o Comitê de Crises Cibernéticas do Tribunal Regional Eleitoral do Espírito Santo, em consonância com a Portaria nº 162 do CNJ, de 10 de Junho de 2021, com a finalidade de promover o gerenciamento adequado de crises, por meio de resposta rápida e eficiente a incidentes em que os ativos de informação do Poder Judiciário tenham a sua integridade, confidencialidade ou disponibilidade comprometidas por longo período, ou quando tenha grande impacto, contribuindo assim para a resiliência corporativa.

CAPI TULO I

DISPOSIC O ES 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: 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: decorre de incidentes em dispositivos, serviços e redes de computadores, que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;
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. ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética, formalizado em ato próprio, responsável pelo gerenciamento e prevenção de incidentes de segurança da informação;
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.
XII. Gerenciamento de incidentes: atividades que devem ser executadas para avaliar o problema e determinar a resposta inicial diante da ocorrência de um evento adverso de segurança da informação.

CAPI TULO II

DA IDENTIFICAC A O DE CRISE CIBERNE TICA

Art. 3o. 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 pelo Tribunal; ou
IV. O incidente atrair grande atenção da mídia e da população em geral.

CAPI TULO III

DA COMPOSIC A O DO COMITE DE CRISES CIBERNE TICAS E DEFINIÇÃO DA SALA DE SITUAÇÃO

Art. 4o. O Comitê de Crises Cibernéticas será composto pelos titulares das seguintes unidades, sob a presidência do titular do primeiro:
I. Diretoria-geral;
II. Secretário de Administração e Orçamento;
III. Secretário de Tecnologia da Informação;
IV. Secretário de Judiciário;
V. Secretário de Gestão de Pessoas;
VI. Assessoria Jurídica da Presidência;
VII. Assessoria de Comunicação Institucional e Assessoria de Gestão Estratégica;
VIII. Coordenadoria de Análise e Desenvolvimento;
IX. Coordenadoria de Infraestrutura e Suporte;

X. Encarregado de Dados;
XI. Gestor de Segurança da Informação;
XII. Coordenadoria de Material e Patrimônio;
XIII. Coordenadoria de Serviços Gerais
XIV. Responsável pela ETIR.
XV. Assessoria técnica da Corregedoria.
Parágrafo único. Os membros a que se refere o caput deste artigo serão representados por seus substitutos eventuais, caso estejam impossibilitados de atuar ou participar de reuniões.
Art. 5o. Fica definida como Sala de Situação o gabinete da Diretoria-Geral deste Tribunal Regional.
CAPI TULO 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 fundamental para a organização responder a uma crise cibernética de longa duração ou de grande impacto.
Art. 7o. Assim que a ETIR identificar que um incidente constitui uma crise cibernética, devera comunicar imediatamente a situação ao Comitê de Crises Cibernéticas.
Art. 8o. O Comitê de Crises Cibernéticas reunir-se-á presencial ou virtualmente, para deliberar se o incidente reportado pela ETIR constitui de fato crise cibernética.
§ 1o. Caso a crise cibernética seja confirmada, o Comitê de Crises Cibernéticas entrara em estado de convocação permanente, podendo reunir-se a qualquer momento para discutir, deliberar e agir no tratamento da crise em curso.
§ 2o. O acesso às reuniões do Comitê de Crises Cibernéticas deve ser restrito aos membros desse Comitê e a outros entes eventualmente convidados a participar das reuniões.
§ 3o. O Comitê de Crises Cibernéticas deve contar com equipe dedicada a execução de atividades administrativas para o período de crise.
Art. 9o. O Comitê de Crises Cibernéticas devera coordenar esforços junto a equipes administrativas e técnicas do TRE-ES 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, avaliando 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, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer 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. Orientar 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 a normalidade.

Art. 10. O Comitê de Crises Cibernéticas deverá realizar reuniões regulares a fim de avaliar o progresso das ações implementadas para contornar a crise, até que seja possível retornar à condição de normalidade.
Art. 11. Os incidentes graves que ocasionam a deflagração de uma crise cibernética deverão ser comunicados ao Tribunal Superior Eleitoral e ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao CNJ.
CAPI TULO V
FASE DE APRENDIZADO E REVISA O (PO S-CRISE)
Art. 12. Após o retorno das operações a normalidade, o Comitê de Crises Cibernéticas devera realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.
Art. 13. Para a identificação das lições aprendidas e a elaboração de relatório final, devem 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; e
IX. A tomada de decisão e as estratégias de recuperação.
Art. 14. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta e para a melhoria do processo de preparação para crises cibernéticas.
Art. 15. O Comitê de Crises Cibernéticas deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética, contendo a descrição e o detalhamento da crise, bem como o plano de ac a o tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.
Art. 16. Os casos omissos serão resolvidos pelo Presidente do TRE-ES.
Art. 17. Esta Portaria entra em vigor na data de sua publicação.
Desembargador JOSÉ PAULO CALMON NOGUEIRA DA GAMA
Presidente

DOCUMENTOS DA DG

PORTARIAS

PORTARIA Nº 237, DE 05/07/2022

O DIRETOR GERAL DO TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO, NO USO DE SUAS ATRIBUIÇÕES,
RESOLVE,
CONCEDER ao servidor MAURÍCIO XAVIER DA COSTA Suprimento de Fundos na modalidade Cartão de Pagamento do Governo Federal no valor de R$ 17.600,00 (dezessete mil, seiscentos reais), sendo R$ 12.320,00 (doze mil, trezentos e vinte reais) para fatura e R$ 5.280,00 (cinco mil, duzentos e oitenta reais) para saque, para custeio de DESPESAS DE PEQUENO VULTO, na Ação Orçamentária 02.122.0570.20GP.0032 - Julgamento de Causas e Gestão Administrativa na Justiça Eleitoral, Natureza de Despesa 339030 - Material de Consumo e Plano Interno - ADM MATMAN,