



MINISTÉRIO DO DESENVOLVIMENTO REGIONAL - MDR
COMPANHIA DE DESENVOLVIMENTO DOS VALES
DO SÃO FRANCISCO E DO PARNAÍBA

REGIMENTO INTERNO DA EQUIPE DE PREVENÇÃO TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DA CODEVASF

RESOLUÇÃO Nº 498 de 3 de junho de 2022

2022

SUMÁRIO

CAPÍTULO I - DO OBJETIVO	3
CAPÍTULO II - DA MISSÃO	3
CAPÍTULO III - DO PÚBLICO ALVO.....	3
CAPÍTULO IV - DO MODELO DE IMPLEMENTAÇÃO.....	3
CAPÍTULO V - DA ESTRUTURA ORGANIZACIONAL	4
CAPÍTULO VI - DAS COMPETÊNCIAS	4
CAPÍTULO VII - DAS ATRIBUIÇÕES.....	5
Seção I - Do Agente Responsável pela ETIR.....	5
Seção II - Do Gestor de Segurança da Informação.....	5
CAPÍTULO VIII - DA AUTONOMIA	5
CAPÍTULO IX - DA ATUAÇÃO	6
CAPÍTULO X - DAS DISPOSIÇÕES GERAIS	7

CAPÍTULO I DO OBJETIVO

Art. 1º Este Regimento Interno tem como objetivo instituir a composição, organização e o funcionamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Codevasf – ETIR, em atendimento ao disposto no art. 9º da Política de Segurança da Informação da Codevasf - Posin.

CAPÍTULO II DA MISSÃO

Art. 2º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Codevasf - ETIR tem como missão prioritária identificar, proteger, detectar e responder a incidentes de segurança em redes computacionais e sistemas empregados na ambiência da Codevasf, bem como cooperar com outras equipes e participar em fóruns e seminários de redes nacionais e internacionais relacionados às ações da ETIR.

CAPÍTULO III DO PÚBLICO ALVO

Art. 3º O público alvo da ETIR abrange os ativos de informação disponibilizados pela Codevasf em sua rede de computadores e sistemas assim como seus respectivos usuários.

Art. 4º Externamente, a ETIR poderá se relacionar com as demais equipes de prevenção, tratamento e resposta a incidentes cibernéticos da Administração Pública Federal; com o Centro de Tratamento de Incidentes de Redes do Governo - CTIR Gov, ou equivalente; com os órgãos, entidades e empresas, públicas ou privadas, que tenham relacionamentos com a Codevasf para o intercâmbio de informações; e com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC.

CAPÍTULO IV DO MODELO DE IMPLEMENTAÇÃO

Art. 5º A ETIR da Codevasf será constituída por empregados efetivos da Gerência de Tecnologia da Informação – AE/GTI que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança em redes computacionais e sistemas, quando requisitados.

Art. 6º Os empregados que compõem a ETIR serão nomeados por meio de Determinação do titular da Área de Gestão Estratégica – AE, após indicação pelo titular da Gerência de Tecnologia de Informação – AE/GTI.

CAPÍTULO V DA ESTRUTURA ORGANIZACIONAL

Art. 7º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Codevasf - ETIR funcionará como um grupo de trabalho permanente, multidisciplinar, de atuação preventiva e reativa, sem dedicação exclusiva, chefiada e gerenciada pelo agente responsável pela ETIR e composta por no mínimo 2 (dois) empregados lotados na Gerência de Tecnologia da Informação – AE/GTI, indicados pelo titular desta Gerência.

§ 1º A ETIR poderá atuar proativamente a partir da identificação da causa do incidente.

§ 2º Para cada membro da ETIR será designado um membro suplente.

CAPÍTULO VI DAS COMPETÊNCIAS

Art. 8º Além das competências previstas na Política de Segurança da Informação da Codevasf – Posin, compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Codevasf - ETIR:

I - manter o registro dos incidentes de segurança a fim de assegurar o registro histórico das atividades da ETIR;

II - coletar evidências imediatamente após a constatação de um incidente de segurança de informação;

III - investigar os fatores de risco, as causas, vulnerabilidades e os possíveis atores responsáveis pelos incidentes de segurança da informação;

IV - coordenar, executar e acompanhar a análise de incidentes em segurança da informação, atuando e orientando para a recuperação dos ativos de informação e normalização das operações em estruturas ou ambientes comprometidos;

V - prestar, quando solicitada, assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação;

VI - emitir alertas e advertências com o objetivo de orientar a comunidade como agir diante do problema relacionados à segurança da informação;

VII - orientar os usuários, os colaboradores e o corpo técnico da Codevasf, para que estejam aptos a evitar possíveis riscos de segurança e formas de ataque cibernético adotando boas práticas de segurança da informação;

VIII - participar de cursos, palestras, seminários e treinamentos técnicos para o aperfeiçoamento contínuo, atualização quanto ao emprego de novas tecnologias e métodos assim como para com o aprimoramento dos procedimentos relacionados à segurança da informação; e

IX - executar outras atividades correlatas que lhe forem demandadas, desde que relacionadas à segurança da informação e ao cumprimento de sua missão.

CAPÍTULO VII DAS ATRIBUIÇÕES

Seção I Do Agente Responsável pela ETIR

Art. 9º Sem prejuízo das atribuições e responsabilidades estabelecidas na Política de Segurança da Informação da Codevasf – Posin, caberá ao agente responsável pela ETIR:

- I - coordenar a execução dos processos relacionados ao tratamento de incidentes;
- II - coordenar a divulgação do serviço de tratamento de incidentes para o público-alvo;
- III - assessorar a Gerência de Tecnologia da Informação e o gestor de segurança da informação nos assuntos relacionados ao tratamento de incidentes;
- IV - estabelecer contato e buscar cooperação com outras ETIR;
- V - assegurar que todos os envolvidos em um incidente sejam notificados;
- VI - propor a adoção de medidas e controles preventivos relacionados à segurança da informação; e
- VII - atuar juntamente com o gestor de segurança da informação na interlocução com instituições governamentais de atuação especializada em segurança da informação.

Seção II Do Gestor de Segurança da Informação

Art. 10. As atribuições do gestor de segurança da informação estão definidas na Política de Segurança da Informação da Codevasf – POSIN.

CAPÍTULO VIII DA AUTONOMIA

Art. 11. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Codevasf - ETIR seguirá o modelo de autonomia compartilhada, trabalhando em conjunto com a Gerência de Tecnologia da Informação – AE/GTI, Área de Gestão Estratégica - AE e as unidades orgânicas afetadas.

§ 1º A ETIR poderá recomendar os procedimentos a serem executados ou as medidas de recuperação a serem adotadas durante um ataque cibernético à rede computacional da Codevasf e discutirá as ações a serem adotadas pela AE/GTI, AE e demais unidades orgânicas afetadas.

§ 2º A ETIR documentará os incidentes, as causas e as soluções na base de conhecimento da TI para que sejam adotados os devidos procedimentos pelos empregados da GTI quando houver recorrência do incidente.

CAPÍTULO IX DA ATUAÇÃO

Art. 12. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Codevasf - ETIR poderá atuar por convocação da Gerência de Tecnologia da Informação – AE/GTI nas situações em que envolvam incidentes de segurança não solucionados pelas demais unidades orgânicas desta Gerência.

§ 1º Após convocada, caberá à ETIR identificar, analisar e apresentar a proposta de solução ou de contenção de incidentes de segurança.

§ 2º Os empregados da AE/GTI deverão fornecer informações qualitativas e quantitativas acerca dos incidentes para os quais a ETIR foi convocada.

Art. 13. A ETIR poderá acionar instituições governamentais de atuação especializada em segurança da informação para tratar de incidentes que tenham como origem outros órgãos da Administração Pública Federal ou de procedência estrangeira, mediante conhecimento prévio do gestor de segurança da informação e da Área de Gestão Estratégica.

Art. 14. A ETIR poderá propor a utilização de processos, ferramentas tecnológicas e recursos humanos capacitados para garantir a integridade, disponibilidade e o sigilo dos dados.

Art. 15. As ações preventivas, dentre outras, referem-se às atividades de proteção da informação de forma preventiva e planejada.

Art. 16. As ações reativas incluem o recebimento das notificações de incidentes, a orientação e atuação no reparo de dados e na análise de sistemas comprometidos buscando as causas, os danos e os respectivos responsáveis.

Parágrafo único. As atividades que envolvem as ações reativas da ETIR terão prioridades sobre aquelas designadas pela chefia imediata de seus integrantes.

Art. 17. As ações proativas incluem a identificação das vulnerabilidades, o monitoramento, a gestão e notificação de falhas.

Art. 18. A participação de empregados nas atividades da ETIR não ensejará remuneração de qualquer espécie, sendo considerada serviço público relevante.

Art. 19. Extraordinariamente, o agente responsável pela ETIR poderá convidar outros profissionais de TI para atuar em tratamento e resposta a determinado incidente de segurança.

CAPÍTULO X DAS DISPOSIÇÕES GERAIS

Art. 20. Este Regimento deverá ser revisado periodicamente, em intervalos de até 2 (dois) anos.

Art. 21. O canal de comunicação oficial com a ETIR é o endereço de correio eletrônico etir@codevasf.gov.br.

Art. 22. As dúvidas de interpretação deste Regimento serão dirimidas pela Gerência de Planejamento e Estudos Estratégicos - AE/GPE quanto ao teor redacional, pela Gerência de Tecnologia da Informação - AE/GTI quanto ao mérito técnico e operacional e pela Assessoria Jurídica quanto ao mérito jurídico.

Art. 23. Este Regimento entrará em vigor na data da sua publicação.