Enap Escola Nacional de Administração Pública

Boletim de Serviço Eletrônico em 29/12/2021

RESOLUÇÃO Nº 28

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) no âmbito da Fundação Escola Nacional de Administração Pública (Enap).

O COMITÊ DE GOVERNANÇA DIGITAL DA FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP, no uso da atribuição que lhe confere a Portaria Enap nº 556, de 19 de setembro de 2019, e tendo em visto o disposto na Lei nº 12.527, de 18 de novembro de 2011, na Lei nº 13.709, de 14 de agosto de 2018, no Decreto Nº 9.637, de 26 de dezembro de 2018, no Decreto nº 10.222, de 5 de fevereiro de 2020, no Decreto nº 10.748, de 16 de julho de 2021, na Portaria Enap nº 556, de 19 de setembro de 2019, nas normas do Gabinete de Segurança Institucional da Presidência da República que dispõem sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, e conforme a deliberação ocorrida na reunião realizada em 20 de dezembro de 2021, e o constante dos autos do processo n° 04600.002238/2021-02, resolve:

Art. 1º Fica instituída a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) no âmbito da Fundação Escola Nacional de Administração Pública (Enap) nos termos do Anexo a esta Resolução.

Art. 2º Esta Resolução entrará em vigor em 4 de janeiro de 2022.

BRUNA SILVA DOS SANTOS
Presidente Substituta

ANEXO

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Fundação Escola Nacional de Administração Pública (ETIR/Enap)

Art. 1º A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Fundação Escola Nacional de Administração Pública (ETIR/Enap) fica instituída com o objetivo de promover a gestão centralizada em atividades de tratamento e resposta a incidentes em redes computacionais da Enap.

Art. 2º A ETIR/Enap tem como missão:

I - estar alinhada à Política de Segurança da Informação da Enap (POSIN/Enap);

II - facilitar e coordenar as atividades de prevenção, tratamento e resposta a incidentes em redes computacionais da Enap;

III - receber e notificar qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, a fim de contribuir para a adequada prestação dos serviços da Enap;

V - analisar ataques e intrusões nos sistemas e redes de computadores;

VI - cooperar com outras equipes que tratam de incidentes de segurança da informação, bem como outros assuntos relacionados a segurança da informação; e

VII - participar em fóruns e redes nacionais e internacionais.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos desta Resolução são estabelecidos os seguintes conceitos e definições:

I - agente responsável da ETIR: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a ETIR;

II - comunidade ou público alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR;

III - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI;

IV - equipe de prevenção, tratamento e resposta a incidentes em cibernéticos - 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 - tratamento de incidentes de segurança em redes computacionais: é o 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.

CAPÍTULO III
DA COMUNIDADE OU PÚBLICO ALVO

Art. 4º O público-alvo das atividades pertinentes à ETIR/Enap inclui:

I - todos os servidores e colaboradores que exercem suas atividades no âmbito da Enap;

II - demais equipes de respostas a incidentes de segurança da informação da Administração Pública Federal;

III - centro de tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal - CTIR GOV;

IV - órgãos, entidades, empresas, públicas e privadas, que tenham contratos, acordos ou convênios com a Enap para o intercâmbio de informações;

V - titular de dados, pessoa natural a quem se referem os dados pessoais que são objeto de tratamento pela Enap.

CAPÍTULO IV
DA COMPOSIÇÃO

Art. 5º A ETIR/Enap fará parte, automaticamente, da Rede Federal de Gestão de Incidentes Cibernéticos, instituída pelo Decreto nº 10.748, de 16 de julho de 2021.

Art. 6º A ETIR/Enap será formada por integrantes da Coordenação-Geral de Tecnologia da Informação da Diretoria de Gestão Interna, sendo um deles designado Agente Responsável da ETIR.

§ 1º A ETIR será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo, com capacidade técnica compatível com as atividades dessa equipe.

§ 2º Os membros da ETIR deverão ser selecionados, sempre que possível, dentre o pessoal existente, com perfil técnico adequado às funções de tratamento de incidentes de rede.

§ 3º Neste modelo as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

§ 4º A ETIR será composta por 02 (dois) integrantes da Coordenação-Geral de Tecnologia da Informação, 02 (dois) integrantes da Coordenação de Automação Sistêmica, Dados, BI e Design de Interfaces (COSIS), todos os integrantes da Coordenação de Infraestrutura, Cibersegurança e Serviços de TI (COINF) e o Agente Responsável da ETIR.

§ 5º Seus integrantes serão indicados pelo Comitê de Governança Digital da Enap - CGD/Enap e designados por meio de portaria do Presidente da Enap.

§ 6º Para cada membro titular da ETIR, deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da equipe.

§ 7º Os servidores integrantes da ETIR passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais e segurança cibernética, além de suas funções regulares na Enap.

Art. 7º As atividades da ETIR/Enap deverão ser desempenhadas de forma proativa e reativa, sendo o Agente Responsável da ETIR quem irá atribuir as responsabilidades.

CAPÍTULO V
DA ESTRUTURA E DO FUNCIONAMENTO

Art. 8º O Gestor de Segurança da Informação da Enap, designado pelo CGD/Enap, nos termos do art. 2º, inciso III, alínea "a" da Portaria Enap nº 556, de 19 de setembro de 2019, é o responsável por coordenar a implantação e manutenção da infraestrutura necessária à ETIR e por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe, bem como prover a infraestrutura necessária.

Art. 9º O Agente Responsável da ETIR/Enap possui as seguintes competências:

I - coordenar e orientar os membros da ETIR na gestão de incidentes em redes de computadores;

II - ser a interface com o CTIR GOV;

III - gerenciar as atividades, os procedimentos internos e distribuir tarefas para os integrantes da ETIR;

IV - enviar notificações de incidentes de segurança da informação;

V - ser interface com o Gestor de Segurança da Informação no processo de capacitação e treinamento dos membros da ETIR; e

VI - representar a ETIR junto ao CGD/Enap quanto às medidas no tratamento de incidentes de segurança da informação.

Art. 10. A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes ao CTIR GOV, sobre a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados.

Parágrafo único. As notificações enviadas ao CTIR GOV, bem como a troca de informações entre as equipes existentes, devem seguir os formatos e os procedimentos estabelecidos pelo próprio CTIR GOV, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

Art. 11. A ETIR poderá realizar ações ou medidas necessárias para reforçar a resposta ou a postura da Enap na recuperação de incidentes de segurança, durante os quais a equipe somente executará as medidas de recuperação após a aprovação de níveis superiores de gestão.

Art. 12. São atividades típicas da ETIR:

I - apoiar a definição de Políticas e Normas de Segurança da Informação na Enap;

II - implementar, no mínimo, o tratamento de incidentes de segurança em redes computacionais, contemplando o tratamento de artefatos maliciosos;

III - propor soluções para os incidentes de segurança da informação da Enap;

IV - implementar tratamento de vulnerabilidades;

V - disseminar a cultura de segurança da informação;

VI - emitir alertas e advertências;

VII - prospectar novas ferramentas e tecnologias na área de segurança da informação e comunicações;

VIII - implantar mecanismos de detecção de intrusão;

IX - promover a disseminação de informações relacionadas à segurança;

X - criar planos de resposta a incidentes e remediação com fluxos definidos;

XI - atuar de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio da organização;

XII - cooperar com outras equipes de segurança da informação;

XIII - receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação e comunicações na rede e em sistemas computacionais da Enap;

XIV - atuar conforme os padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança da informação, orientados pelo CTIR GOV;

XV - atuar conforme a Norma Complementar do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

CAPÍTULO VI
DA AUTONOMIA

Art. 13. A ETIR/Enap adotará o modelo de Autonomia Compartilhada, trabalhando em acordo com as deliberações do CGD/Enap, a fim de subsidiar o processo de tomada de decisão do colegiado sobre quais medidas deverão ser adotadas.

Art. 14. A participação da ETIR/Enap no processo decisório do CGD/Enap, por meio da representação do Agente Responsável, consiste na apresentação de recomendações dos procedimentos a serem executados ou das medidas de recuperação durante um ataque, além das discussões das ações a serem tomadas ou das repercussões se as recomendações não forem seguidas.

CAPÍTULO VII
DAS DISPOSIÇÕES GERAIS

Art. 15. A ETIR/Enap deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo CTIR GOV.

Art. 16. A ETIR/Enap poderá usar as melhores práticas de mercado, em gestão de segurança da informação, bem como no tratamento de incidentes de segurança da informação.

Referência: Processo nº 04600.002238/2021-02 SEI nº 0534860