MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
OBSERVATÓRIO NACIONAL

PORTARIA ON Nº 250, DE 11 DE FEVEREIRO DE 2025

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Observatório Nacional e estabelece suas atribuições.

O DIRETOR DO OBSERVATÓRIO NACIONAL, no uso de suas atribuições estabelecidas no Regimento Interno, aprovado pela Portaria MCTI nº 7.064, de 24 de maio de 2023, e tendo em vista o inciso VII do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018, e o art. 22 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, resolve:

Art. 1º Esta Portaria institui Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Observatório Nacional – ETIR/ON e estabelece suas atribuições.

Definições

Art. 2º Para os efeitos desta Portaria, ficam estabelecidos os seguintes termos e definições, conforme a Portaria GSI/PR nº 93, de 18 de outubro de 2021:

I - Agente Responsável: servidor público ocupante de cargo efetivo do ON, incumbido de chefiar e gerenciar a ETIR/ON;

II - comunidade: conjunto de pessoas, setores, órgãos ou entidades atendidas pela ETIR/ ON;

III - CTIR-GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Gabinete de Segurança Institucional da Presidência da República;

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

V - tratamento de incidente de segurança: conjunto de ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias; e

VI - vulnerabilidade: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

Competências

Art. 3º A ETIR/ON tem como missão planejar, coordenar e executar atividades de prevenção, tratamento e resposta a incidentes cibernéticos no âmbito do ON que afetem, direta ou indiretamente, sua rede computacional e a segurança de dados e de informações.

Art. 4º A ETIR/ON atenderá à seguinte comunidade:

I - todos os usuários de informação que exerçam suas atividades no âmbito da rede de computadores do ON;

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

III - a Rede Federal de Gestão de Incidentes Cibernéticos, instituída pelo Decreto nº 10.748, de 16 de julho de 2021; e IV – o CTIR-GOV.

Art. 5º Compete à ETIR/ON:

I - coordenar as atividades de tratamento e resposta a incidentes de segurança na rede computacional do ON;

II - agir de forma proativa com o objetivo de evitar que ocorram incidentes de segurança, sugerindo ao Diretor do ON a divulgação de práticas e recomendações de segurança da informação e avaliando as condições de segurança de rede por meio de verificações de conformidade;

III - promover a recuperação de serviços e sistemas de Tecnologia da Informação;

IV - realizar ações reativas que incluam recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

V - receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores do ON;

VI - executar as ações necessárias para tratar quebras de segurança;

VII - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes; e

VIII - cooperar com outras equipes de tratamento e resposta a incidentes.

§ 1º A ETIR/ON deverá manter um integrante de sobreaviso após o final do expediente e em dias sem expediente, ficando em condições de atuar na rede de computadores do ON, sempre que necessário.

§ 2º A escala de serviço da ETIR/ON ficará sob a responsabilidade do Agente Responsável.

Art. 6º Compete ao Agente Responsável da ETIR/ON:

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

II - realizar a interlocução entre o ON e o CTIR-GOV;

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

IV - enviar notificações de incidentes de segurança da informação; V – enviar ao Diretor

do ON, anualmente, o plano de capacitação e treinamento dos membros da ETIR/ON;

VI - apresentar relatório, sempre que necessário, ao Diretor do ON com as medidas adotadas no tratamento de incidentes de segurança da informação; e

VII - apresentar relatório, sempre que necessário, ao Diretor do ON com as sugestões de melhoria nas medidas de prevenção de incidentes na rede de computadores do ON.

Composição

Art. 7º A ETIR/ON estará constituída da seguinte forma:

I - o Gestor de Segurança da Informação do ON, atuando como Agente Responsável pela equipe;

II - o Chefe da Divisão de Tecnologia da Informação do ON;

III - no mínimo 3 (três) funcionários da Divisão de Tecnologia da Informação do ON, preferencialmente servidores efetivos.

§ 1º Em caso de eventual necessidade, o Agente Responsável poderá convidar outros servidores do ON para auxiliar a ETIR/ON no desenvolvimento de suas atividades.

§ 2º A Diretoria do ON prestará o apoio administrativo necessário para a execução dos trabalhos da ETIR/ON.

§ 3º A participação na ETIR/ON será considerada prestação de serviço público relevante, não remunerada.

Art. 8º Os membros da ETIR serão convocados pelo Agente Responsável, ao menos trimestralmente, para reunião ordinária, que deverá tratar sobre a atualização da estratégia de tratamento de incidentes.

§ 1º A ETIR reunir-se-á, extraordinariamente, todas as vezes que for convocada pelo Agente Responsável, em caso de necessidade, para proposição de ação de resposta a incidentes de segurança cibernética.

§ 2º O quórum de reunião e de deliberação da ETIR/ON é de maioria absoluta.

Art. 9º A ETIR/ON integrará a Rede Federal de Gestão de Incidentes Cibernéticos, coordenada pelo CTIR-GOV.

Modelo de atuação

Art. 10. A ETIR/ON deverá observar e adotar, pelo menos, os seguintes aspectos e procedimentos:

I - registro de incidentes de segurança em redes de computadores: todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades da equipe;

II - tratamento da informação: o tratamento da informação pela equipe deverá ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;

III - recursos disponíveis: a ETIR/ON deverá possuir os recursos materiais, tecnológicos

e humanos, suficientes para prestar os serviços oferecidos para sua comunidade;

IV - capacitação dos membros da ETIR/ON: os membros da equipe deverão estar capacitados para operar os recursos disponíveis para a condução dos serviços oferecidos para a sua comunidade;

V - durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, a ETIR/ON tem o dever de comunicar às autoridades competentes, para a adoção dos procedimentos legais julgados necessários; e

VI - observar os procedimentos para preservação das evidências; e VII – priorizar a continuidade dos serviços da equipe e da missão institucional do ON.

Art. 11. A ETIR/ON deverá ser comunicada sobre incidentes cibernéticos suspeitos ou confirmados com o envio de mensagem para o endereço eletrônico etir@on.br.

Art. 12. A ETIR/ON deverá comunicar imediatamente ao CTIR-GOV sobre a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados pelo ON.

Disposições finais

Art. 13. Os termos desta Portaria serão atualizados sempre que alterados os procedimentos de tratamento e resposta a incidentes cibernéticos definidos pela Rede Federal de Gestão de Incidentes Cibernéticos.

Art. 14. Esta Portaria entra em vigor nesta data e será publicada no Boletim de Comunicação Interna do ON.

JAILSON SOUZA DE ALCANIZ

Documento assinado eletronicamente por **Jailson Souza de Alcaniz**, **Diretor do Observatório Nacional**, em 17/02/2025, às 13:39 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **12615628** e o código CRC **41166A39**.