INMETRO

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA

Boletim de SERVIÇO

EDIÇÃO ESPECIAL

Portaria Presi nº 288, de 11 de julho de 2022

Data de Publicação:

13 de julho de 2022

BOLETIM DE SERVIÇO

EDIÇÃO ESPECIAL

Marcos Heleno Guerson de Oliveira Junior
Presidente do INMETRO

Marcelo Petulante Fernandes
Diretor de Administração e Finanças, substituto

Marcelo Petulante Fernandes
Coordenador-Geral de Desenvolvimento e Gestão de Pessoas

Rio de Janeiro, 13 de julho de 2022.

Publicação eletrônica disponível na intranet produzida mensalmente pela COGEP – Coordenação-Geral de Desenvolvimento e Gestão de Pessoas.

As matérias aqui publicadas deverão ser do conhecimento de todos os servidores de cada unidade do Inmetro.

O Boletim de Serviço impresso encontra-se disponível para consulta no Serviço de Documentação e Informação – Sedin.

Este boletim contém a seguinte seção:
1. Atos do Presidente

Neste número, foram publicadas as matérias encaminhadas Coordenação-Geral de Desenvolvimento e Gestão de Pessoas - Cogep, até a data do fechamento do boletim.

SUMÁRIO

Serviço Público Federal

MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DE METROLOGIA , QUALIDADE E TECNOLOGIA - INMETRO

Portaria nº 288, de 11 de julho de 2022.

Institui e regulamenta o funcionamento da Equipe de Tratamento e Resposta a Incidentes Cibernéticos do Instituto Nacional de Metrologia, Qualidade e Tecnologia (ETIR-Inmetro).

O **PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO**, no exercício da competência que lhe foi outorgada pelo artigo 4º, § 2º, da Lei nº 5.966, de 11 de dezembro de 1973, combinado com o disposto nos artigos 18, inciso V, do Anexo I ao Decreto n.º 6.275, de 28 de novembro de 2007, e 105, inciso V, do Anexo à Portaria nº 2, de 4 de janeiro de 2017, do então Ministério da Indústria, Comércio Exterior e Serviços;

Considerando o disposto no Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernético;

Considerando o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação, alterado pelo Decreto n º 10.641, de 2 de março de 2021;

Considerando a Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

Considerando o disposto na Norma Complementar nº 05, de 17 de agosto de 2009, do Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes Cibernéticos - ETIR nos órgãos e entidades da Administração Pública Federal;

Considerando o disposto na Norma Complementar nº 08, de 24 agosto de 2010, do Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que estabelece as diretrizes para Gerenciamento de Incidentes Cibernéticos nos órgãos e entidades da Administração Pública Federal;

Considerando o que consta no Processo nº 52600.000683/2022-53;

Considerando a necessidade de tratamento e resposta a incidentes cibernéticos, em redes computacionais, bem como a obrigação de comunicá-los às autoridades competentes conforme as melhores práticas e diretrizes da Secretaria de Governo Digital do Ministério da Economia e do Gabinete de Segurança Institucional da Presidência da República; **resolve:**

Art. 1º Instituir a Equipe de Tratamento e Resposta a Incidentes Cibernéticos do Instituto Nacional de Metrologia, Qualidade e Tecnologia (ETIR-Inmetro), conforme disposto no ANEXO.

Art. 2º Esta Portaria entrará em vigor na data da sua publicação no Boletim de Serviço do Inmetro.

DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015 EM 13/07/2022, ÀS 15:36, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

MARCOS HELENO GUERSON DE OLIVEIRA JUNIOR
Presidente

A autenticidade deste documento pode ser conferida no site https://sei.inmetro.gov.br/sei/controlador_externo.php?

ANEXO

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR-INMETRO)

1. OBJETIVO

1.1 Instituir e regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes Cibernéticos do Instituto Nacional de Metrologia, Qualidade e Tecnologia (ETIR-Inmetro).

1.2 A ETIR-Inmetro comporá a rede de equipes dos órgãos e das entidades da Administração Pública Federal, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

2. MISSÃO

2.1 Planejar, coordenar e executar atividades de tratamento e resposta a incidentes cibernéticos, recebendo e notificando quaisquer eventos adversos, confirmados ou sob suspeita, relacionados à segurança cibernética, preservando os dados, as informações e a infraestrutura do Inmetro.

3. PÚBLICO ALVO

3.1 Usuários da rede corporativa de computadores, dos serviços e sistemas de TIC mantidos pelo Inmetro, que registrarem eventos identificados como incidentes de segurança cibernéticos.

4. MODELO DE IMPLEMENTAÇÃO

4.1 A ETIR adotará o Modelo 1 de implementação, "Utilizando a equipe de Tecnologia da Informação – TI", proposto pelo item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, e será formada por integrantes da Coordenação-Geral de TI (Ctinf), que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes cibernéticos.

5 CONCEITOS, DEFINIÇÕES E SIGLAS

5.1 Agente responsável - 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-Inmetro.

5.2 APF - Administração Pública Federal.

5.3 CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação - DSI do Gabinete de Segurança Institucional da Presidência da República – GSI/PR. É um Grupo de Resposta a Incidentes de Segurança, que tem por objetivo coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da APF, bem como: prevenir, monitorar, analisar e mitigar os incidentes de segurança da informação; promover o intercâmbio científico-tecnológico; participar da articulação para o estabelecimento de diretrizes sobre gestão de incidentes computacionais; e criar processo de inteligência de ameaças cibernéticas para subsidiar criação de políticas públicas e tomada de decisão.

5.4 ETIR-Inmetro - Equipe de Tratamento e Resposta a Incidentes Cibernéticos do Instituto Nacional de Metrologia, Qualidade e Tecnologia. Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes cibernéticos.

5.5 Incidente cibernético - Ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernético não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada.

5.6 Público Alvo - É o conjunto de pessoas, setores, órgãos ou entidades atendidas pela ETIR-Inmetro.

5.7 Rede corporativa de computadores - Conjunto de computadores corporativos, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação.

5.8 Segurança cibernética - Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

5.9 Segurança da Informação - Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

5.10 Serviço - É o conjunto de procedimentos, estruturados em um processo bem definido, oferecido ao Público Alvo pela ETIR-Inmetro.

5.11 TIC - Tecnologia da Informação e Comunicações.

5.12 Vulnerabilidade - Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

6. ESTRUTURA ORGANIZACIONAL

6.1 A ETIR-Inmetro será formada por integrantes da Coordenação-Geral de TI (Ctinf), sendo três (03) deles integrantes fixos e os demais alocados de forma dinâmica:

6.1.1 Titular - Chefe do Serviço de Infraestrutura de TI (SEINF), designado como Agente Responsável. Suplente: Chefe substituto do Serviço de Infraestrutura de TI (SEINF).

6.1.1.1 Além das atribuições definidas pela Norma Complementar nº 05/IN01/DSIC/GSIPR, o Agente Responsável deverá:

a) notificar o CTIR GOV, através do e-mail ctir@ctir.gov.br e/ou outros canais oficialmente definidos, quanto aos incidentes cibernéticos de maior impacto, com base nas informações obtidas através dos tratamentos de segurança realizados pela ETIR-Inmetro, conforme disposto no art. 12, VI, do Decreto nº 10.748, de 16 de julho de 2021;

b) interagir, quando requisitado e/ou aplicável, com as demais áreas do Inmetro, com o CTIR GOV, ou com outros Órgãos Públicos ou não, que necessitem de dados e/ou informações sobre o tratamento dos incidentes de segurança realizados pela ETIR-Inmetro;

c) criar os procedimentos internos, treinar os integrantes, gerenciar as atividades e distribuir tarefas para a equipe da ETIR-Inmetro; e

d) conduzir a coleta e preservação dos registros dos eventos de segurança cibernética conduzidos pela ETIR-Inmetro.

6.1.2 Titular - Chefe do Serviço de Sistemas (SESIS). Suplente: Chefe substituto do Serviço de Sistemas (SESIS).

6.1.3 Titular - Gestor de Segurança da Informação do Inmetro. Suplente: Chefe do Serviço de Infraestrutura de TI (SEINF), que estará acumulando as funções na ausência do Titular.

6.1.4 Integrantes alocados de forma dinâmica, com o perfil profissional adequado, que poderão ser alocados pelos integrantes fixos da ETIR-Inmetro, dependendo do serviço impactado e/ou da característica do incidente cibernético que deverá ser tratado. Estes integrantes estarão priorizando o atendimento dos incidentes cibernéticos selecionados, em tempo integral ou conforme acordado junto ao Agente Responsável.

6.1.5 A ETIR-Inmetro funcionará como um grupo de trabalho permanente, multidisciplinar, de atuação primordialmente reativa e não exclusiva. Entretanto, o Inmetro disponibilizará ferramental tecnológico para a monitoração dos ativos de TIC possibilitando, quando possível, a atuação preventiva e/ou pró-ativa, mitigando assim os riscos de segurança cibernética.

7. AUTONOMIA DA ETIR-INMETRO

7.1 A ETIR-Inmetro tem autonomia completa conforme definido no item 9.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, ou seja, ela poderá conduzir o seu Público Alvo para realizar ações ou as medidas necessárias para reforçar a resposta e/ou a postura da organização na recuperação de incidentes cibernéticos. Durante um incidente cibernético, se tal se justificar, a ETIR-Inmetro poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

8. CANAIS DE COMUNICAÇÃO

8.1 A comunicação e/ou identificação dos incidentes cibernéticos à ETIR-Inmetro poderá ocorrer através dos seguintes canais:

a) e-mail: abuse@inmetro.gov.br;

b) contato telefônico via central de suporte e atendimento técnico ao usuário;

c) notificações e alertas da Rede Nacional de Ensino e Pesquisa (RNP), através do seu Centro de Atendimento a Incidentes de Segurança (CAIS);

d) correspondências oficiais (cartas, ofícios);

e) notificações e alertas do CTIR Gov;

f) pessoalmente, em casos emergenciais; e

g) ferramental tecnológico - eventos detectados pelo monitoramento da ETIR-Inmetro.

9. SERVIÇOS E METODOLOGIA

9.1 A ETIR-Inmetro prestará os seguintes serviços:

9.1.1 Tratamento de Incidentes de Segurança Cibernética: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes cibernéticos, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

9.1.2 Tratamento de Vulnerabilidades: serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

9.1.3 Emissão de alertas e advertências: serviço que consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente cibernético, com o objetivo de advertir e/ou orientar os usuários do Inmetro sobre como agir diante deste tipo de evento.

9.1.4 A ETIR-Inmetro deverá buscar sanar, com prioridade e/ou urgência, os incidentes e as vulnerabilidades cibernéticas detectadas, em especial aquelas identificadas nos alertas e nas recomendações expedidos pelo CTIR GOV, ou que impactem os serviços críticos definidos pelo Inmetro.

10. VIGÊNCIA E REVISÕES

10.1 Este documento tem prazo indeterminado e deverá ser adequado caso seja necessário a alteração dos integrantes da ETIR-Inmetro e/ou para a manutenção da conformidade junto aos novos normativos legais e/ou para o atendimento as orientações e boas práticas do governo federal sobre o tema prevenção, tratamento e resposta a incidentes cibernéticos.

11. REFERÊNCIAS

11.1 Portaria GSI/PR nº 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação.

11.2 Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

11.3 Instrução Normativa nº 1 do GSI, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

11.4 Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

11.5 Política de Segurança da Informação e Comunicações do Inmetro. Declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação. Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro.

11.6 Norma complementar nº 05/IN01/DSIC/GSIPR, de 2009. Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

11.7 Norma Complementar nº 08/IN01/DSIC/GSIPR, de 2010. Estabelece as diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

11.8 Norma complementar nº 21/IN01/DSIC/GSIPR, de 2014. Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.