PORTARIA Nº 190, de 9 de novembro de 2022.

Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do CFQ.

O Presidente do Conselho Federal de Química, no uso das atribuições que lhe foram conferidas pelo art. 11 da Lei nº 2.800, de 18 de junho de 1956, e pelas alíneas b e z da Resolução Normativa nº 55, de 27 de março de 1981,

Considerando o disposto na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Considerando a Portaria GSI/PR n° 38, de 14 de agosto de 2009 que homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR a qual disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

Considerando a Portaria GSI/PR n° 57, de 23 de agosto de 2010 que homologa a Norma Complementar nº 08/IN01/DSIC/GSIPR a qual estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais - Gestão de ETIR, nos órgãos e entidades da Administração Pública Federal.

Considerando a Portaria GSI/PR n° 93, de 26 de setembro de 2019 que aprova o Glossário de Segurança da Informação.

Considerando a Instrução Normativa GSI/PR n° 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, resolve:

Art. 1º Instituir e implementar, na forma do Anexo a esta Portaria, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos do Conselho Federal de Química – ETIR CFQ.

Art. 2º Esta portaria entra em vigor em 9 de novembro de 2022.

Dê-se ciência.

Publique-se.

Brasília, 9 de novembro de 2022.

JOSÉ DE RIBAMAR OLIVEIRA FILHO
Presidente

ANEXO I

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS DO CONSELHO FEDERAL DE QUÍMICA – ETIR CFQ

CAPÍTULO I
DISPOSIÇÕES GERAIS

Seção I
Do Escopo, missão e objetivos

Art. 1º Em alinhamento com a Política de Segurança da Informação do Conselho Federal de Química, fica instituída a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Conselho Federal de Química - ETIR CFQ.

Art. 2º A missão da ETIR é facilitar, coordenar e executar as atividades de tratamento e resposta a incidentes em redes computacionais no ambiente do Conselho Federal de Química, de modo a promover a segurança dos dados, das informações e da infra estrutura tecnológica do Conselho.

Art. 3º São objetivos da ETIR CFQ:

I. Monitorar as redes computacionais;
II. Detectar e analisar ataques e intrusões;
III. Tratar incidentes de segurança da informação;
IV. Identificar vulnerabilidades e artefatos maliciosos;
V. Recuperar sistemas de informação; e
VI. Promover a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais relativos à Segurança da Informação e Comunicações.

Seção II
Conceitos e Definições

Art.4º Para os efeitos desta ETIR, considera-se o Glossário de Segurança da Informação, estabelecido pela Portaria GSI/PR nº 93, de 26 de setembro de 2019:

I. **Agente responsável**: Empregado Público ocupante de cargo efetivo incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
II. **Artefato malicioso**: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores;
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 da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República – GSI;
IV. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais**: 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. **ETIR**: acrônimo de Equipe de Tratamento de Incidentes de Rede;
VI. **Incidente de segurança**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
VII. **Público Alvo da ETIR**: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Também chamado de Comunidade ETIR;
VIII. **Tratamento de Incidentes de Segurança em Redes Computacionais**: serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar análises dos incidentes de segurança, procurando extrair informações que permitam impedir a

continuidade da ação maliciosa e também a identificação de tendências;

IX. **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.

Seção III
Do público-alvo e Modelo de implementação

Art.5º O público-alvo da ETIR CFQ são todos os usuários dos serviços de Tecnologia da Informação e Comunicação - TIC.

Art.6º O Modelo de implementação da ETIR CFQ a ser utilizado tem como base o Modelo I – estampado no item 7.1 da Norma Complementar 05/IN01/DSIC/GSIPR de agosto de 2009 – "utilizando a equipe de Tecnologia da Informação e Comunicação – TIC" e deverá seguir as seguintes diretrizes:

I. Não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de rede;

II. A equipe desempenhará as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais;

III. As funções e serviços de tratamento de incidente deverão ser realizadas por empregados do Conselho;

IV. A equipe desempenhará suas atividades, via de regra, de forma reativa; e

V. O Agente Responsável pela ETIR CFQ atribuirá, sempre que necessário, responsabilidades para que os seus membros exerçam atividades proativas.

Seção IV
Da Autonomia

Art. 7º A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR CFQ terá autonomia completa e poderá conduzir o seu público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

Seção V
Das Atribuições

Art. 8º O Gestor de Segurança da Informação e Comunicação é responsável por coordenar a instituição, implementação e manutenção da infraestrutura necessária à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008.

Art. 9º Caberá aos membros titulares da ETIR CFQ e, na ausência desses aos respectivos suplentes, prevenir, detectar, tratar e responder aos incidentes de segurança da informação, de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e a autenticidade das informações custodiadas e de propriedade do CFQ, de modo a preservar os seus ativos e sua imagem institucional.

Art. 10. O Agente Responsável pela ETIR CFQ será designado dentre os analistas de infraestrutura da Gerência de Tecnologia da Informação e, em sua ausência, o seu suplente.

Parágrafo Único. O Agente Responsável atuará como a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV e será o responsável por criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a ETIR.

Art. 11. A participação na ETIR CFQ será considerada prestação de serviço público relevante e não ensejará remuneração adicional àquela recebida pelo agente público.

Seção VI
Do Funcionamento

Art. 12. Caberá ao Agente Responsável acionar, via e-mail, os membros da ETIR CFQ sempre que observar indícios de incidentes de segurança da informação acometendo ativos do CFQ, devendo registrar a ocorrência na ferramenta de abertura de chamados.

Art. 13 Caso o agente responsável verifique a ocorrência de incidente que comprometa a imagem do CFQ, é seu dever convocar uma reunião extraordinária com os membros da ETIR CFQ, assim que detectado o incidente.

Art. 14. A ETIR CFQ reunir-se-á, por convocação do seu Coordenador:
I. Ordinariamente, trimestralmente; e
II. Extraordinariamente, sempre que necessário, por convocação do seu Coordenador ou da maioria dos seus membros.
Parágrafo único. O quórum deliberativo será de metade mais um dos seus membros.

Seção VII
Da Estrutura Organizacional

Art. 15. A ETIR CFQ é vinculada à Gerência de Tecnologia da Informação do CFQ.

Art. 16. A ETIR CFQ é composta de 5 (cinco) membros titulares representantes das seguintes funções:
I. Aline Alves de Medeiros de Azevedo, Gestora de Segurança da Informação.
II. Henrique Selvero Menezes Cardoso, Agente Responsável pela ETIR CFQ.
III. Ermerson Ferreira da Silva, integrante ETIR CFQ.
IV. Leonardo Rodrigues Peixoto, integrante ETIR CFQ.

§ 1º Os membros do CGD serão substituídos em seus afastamentos ou impedimentos legais pelo seu substituto nomeado em portaria.

§ 2º A ETIR CFQ poderá ser estendida com a inclusão dos seguintes membros: representantes legais de áreas específicas da organização, advogados, estatísticos, recursos humanos, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outro que a organização entenda ser adequado.

§ 3º A ETIR CFQ poderá ser estendida caso a complexidade dos incidentes de segurança da informação exija conhecimentos e capacidades técnicas além das disponíveis pela ETIR CFQ.

§ 4º A coordenação da ETIR CFQ será exercida pelo Agente Responsável.

§ 5º A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV.

§ 6º A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

Seção VIII
Dos Serviços

Art. 17. A ETIR CFQ poderá trabalhar em acordo com outros setores da instituição no processo de tomada de decisão sobre as medidas que serão adotadas em caso de incidente de segurança da informação.

Art. 18. A ETIR CFQ prestará os seguintes serviços:

I. Tratamento de incidentes de segurança em redes computacionais;

II. Emissão de alertas e advertências;

III. Tratamento de vulnerabilidades; e

IV. Criação e disseminação de práticas para uso seguro das Tecnologias de Informação e Comunicação.

Seção IX
Das Disposições Finais

Art. 19. Os casos omissos desta portaria serão resolvidos pelo Comitê de Governança Digital do CFQ.

Art. 20. Esta Portaria entrará em vigor em 9 de novembro de 2022.