Conselho Federal de Química

Plenário
Presidência
Gabinete

PORTARIA Nº 6, DE 19 DE JANEIRO DE 2024

Estabelece diretrizes de segurança da informação para a política de gestão de incidentes de segurança da informação para o Conselho Federal de Química e protocolos a serem observados.

O PRESIDENTE DO CONSELHO FEDERAL DE QUÍMICA (CFQ), no uso das atribuições que lhe foram conferidas pelos incisos II e XXVI do art. 74 da Resolução Normativa CFQ Nº 307, de 22 de março de 2023;

Considerando a Instrução Normativa GSI/PR N° 01, 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;

Considerando a Portaria DSI/GSI/PR Nº 120 de 21 de dezembro de 2022 que aprova o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal – PLANGIC;

Considerando a Norma Complementar N° 08/IN01/DSIC/GSIPR que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

Considerando a Norma Complementar N° 21/IN01/DSIC/GSIPR que estabelece diretrizes para o registro, coleta e preservação de evidências de incidentes de segurança em redes computacionais dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF e a comunicação às autoridades competentes;

Considerando a Portaria CFQ Nº 190, de 9 de novembro de 2022 que institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do CFQ;

Resolve:

Art. 1º Instituir a Política de gestão dos incidentes de Segurança da Informação do Conselho Federal de Química.

Art. 2º A Política de gestão de incidentes de segurança da informação deve ser observada por todos os Conselheiros, membros de colegiados e empregados de todas as áreas de atuação do CFQ, nos níveis estratégico, tático e operacional.

CAPÍTULO I

DA ABRANGÊNCIA

Art 3º A Política de Incidentes de Segurança da Informação abrange todos os incidentes relacionados à Tecnologia da Informação, confirmados ou sob suspeita, que envolvam o nome ou a propriedade do Conselho Federal de Química, bem como qualquer Conselheiro, membro de colegiado ou empregado, no exercício de suas funções ou relação com o CFQ.

Art. 4° Estão abrangidos nesta Política todos os eventos contrários ao ordenamento

jurídico em vigor, bem como as normas constantes da política de segurança da organização, relativos à Segurança da Informação e Comunicações (SIC), como:

I- divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados do CFQ nos termos do art. 153, §1º-A do Código Penal;

II- invasão de dispositivo informático, nos termos do art. 154-A do Código Penal;

III- interrupção de serviço de TIC ou de informação de utilidade pública, previsto no §1º do art. 266 do Código Penal;

IV-inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados do CFQ nos termos do art. 313- A do Código Penal;

V- modificação ou alteração por agente público de sistema de informação ou programa de informática sem autorização, nos termos do art. 313-B do Código Penal;

VI- distribuição, armazenamento ou conduta vinculada a pornografia infantil, nos termos dos arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei nº 8069/90;

VII- interceptação de dados de forma clandestina, nos termos do art. 10 da Lei nº 9296/96;

VIII- quaisquer outros eventos que constituam violação de requisito de segurança estabelecido pela Política de Segurança da Informação do CFQ, tenham eles origem no próprio CFQ ou em grupos externos.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

Art. 5° Para efeitos desta Política, serão considerados os conceitos e as definições de segurança da informação estabelecidos pela Portaria GSI/PR N° 93, de 18 de outubro de 2021 , que aprova o Glossário de Segurança da Informação, destacando-se:

I - Atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços.

II - Atividade Crítica: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

III - Atividade Maliciosa: qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema, serviço ou rede.

IV - Auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

V - Evento de Segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas, ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança.

VI – ETIR - CFQ: Equipe de Tratamento e Respostas a Incidentes do Conselho Federal de Química, composta de integrantes com conhecimentos técnicos e habilitados designados pela Presidência do CFQ em portaria específica.

VII -Fluxo de Trabalho de Incidentes: predefinição de etapas que devem ser tomadas para lidar com um tipo particular de Incidente.

VIII - Gerenciamento de Incidentes: processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidente garante que a operação normal de um sistema, serviço ou rede seja restaurada tão rapidamente quando possível e que o impacto no negócio seja minimizado.

IX- Incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado,

interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

CAPÍTULO III

OBJETIVOS

Art. 6º São objetivos da Política de Incidentes de Segurança da Informação do CFQ:

I - Reduzir danos totais causados por incidentes que não puderam ser evitados, bem como a sua reincidência;

II- Formalizar o processo de gestão de incidentes do CFQ, adotando as fases de detecção, triagem, análise e resposta para o tratamento dos incidentes de segurança; e

III- Diminuir o número total de incidentes de segurança da informação envolvendo o CFQ, por meio de prevenção sistemática dos eventos e eliminação de situações que permitem a ocorrência desses incidentes.

Art. 7º A Política de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação do CFQ e visa orientar o funcionamento do processo de gestão de incidentes de segurança digital e não digital da informação, de forma que estes sejam tratados adequadamente, reduzindo ao máximo os impactos para as atividades do CFQ.

CAPÍTULO IV

DO PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 8º O processo de gestão de incidentes de segurança da informação inclui as seguintes fases:

I – Prevenção de incidentes cibernéticos: envolve as diretrizes para a comunicação, a identificação, a contenção, a erradicação, a recuperação, o encerramento e as lições aprendidas com os incidentes cibernéticos, no âmbito do CFQ;

II – Investigação de ilícitos cibernéticos: envolve as diretrizes para a coleta e a preservação das evidências dos incidentes relevantes, além da comunicação de ilícitos cibernéticos, no âmbito do CFQ; e

III – Gerenciamento de crises cibernéticas: envolve as diretrizes para o planejamento (pré-crise), a execução (durante a crise) e a melhoria contínua (pós-crise) do gerenciamento de crises cibernéticas no âmbito do CFQ.

Seção I

Da Prevenção de Incidentes Cibernéticos

Art. 9º O protocolo de prevenção de incidentes cibernéticos inclui as seguintes fases:

I – Identificação: envolve as diretrizes para a comunicação e a categorização dos eventos de segurança ou das vulnerabilidades, bem como o registro e a deliberação sobre o incidente cibernético;

II – Contenção: envolve as diretrizes para a definição do ponto de contato da ETIR-CFQ, o isolamento dos ativos comprometidos, a comunicação às áreas impactadas, a coleta das evidências e a execução de ações de contorno, caso necessário;

III – Erradicação: envolve as diretrizes para a investigação do incidente, a emissão do relatório de evidências, a comunicação com as áreas impactadas e a remoção das ameaças identificadas no incidente cibernético;

IV – Recuperação: envolve as diretrizes para a emissão e apreciação do plano de recuperação, o acionamento das áreas competentes para a execução do plano de recuperação, a análise detalhada do incidente cibernético, além de deliberações e demais providências, caso

necessário; e

V – Encerramento e registro das lições aprendidas: envolve as diretrizes para a emissão do relatório de encerramento de incidente, a atualização do banco de dados de incidentes conhecidos (BDIC), o encerramento formal do incidente cibernético, além da comunicação às áreas envolvidas sobre o fim do tratamento do incidente cibernético.

Subseção I

Da Identificação

Art. 10. Aos Conselheiros, membros de colegiados e empregados do CFQ caberão as responsabilidades de:

I — Reportar incidentes de segurança da informação identificados, quando for testemunhado, à ETIR- CFQ;

II — Notificar qualquer evento de segurança ou fragilidade observada que possa causar prejuízos, interrupções, mau funcionamento, imprecisão ou vazamento de informação nos sistemas, serviços ou redes do CFQ; e

III - Notificar as violações à política de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tornar conhecimento.

§ 1º Na apuração dos incidentes de segurança da informação, será considerada a vontade orientada à realização do incidente de segurança, ou seja, o elemento subjetivo que concretiza os requisitos de vulnerabilidade dos dados pessoais.

§ 2º Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos conselheiros, empregados e colaboradores, sob o risco de violar a política de segurança digital e não digital e da informação, bem como provocar danos aos sistemas, serviços ou recursos tecnológicos digitais ou não digitais.

Art. 11. A ETIR-CFQ viabilizará canais de comunicação para que os Conselheiros, membros de colegiados, empregados e colaboradores do CFQ possam comunicar os eventos ou indícios de incidente de segurança por meio de preenchimento do chamado “Incidente de Segurança da Informação”, pela abertura de chamado no GLPI.

Art. 12. Será disponibilizado no site do CFQ, em local específico, formulário para a comunicação de incidentes por parte de usuários externos, com o envio do comunicado do incidente para o e-mail getic@cfq.org.br.

Art. 13. Recebido o formulário, a ETIR-CFQ deverá apreciá-lo, observando o Plano de Gestão de Incidentes Cibernéticos para a categorização dos eventos, podendo:

I – Comunicar ao usuário requisitante o encerramento do tratamento do evento reportado, na hipótese de não se tratar de incidente de segurança tipificado no Plano de Gestão de Incidentes Cibernéticos; e

II – Registrá-lo no Registro de Incidente de Segurança e requerer informações adicionais ao usuário requisitante para nortear as deliberações, caso necessário, na hipótese do evento reportado se tratar de incidente de segurança tipificado no Plano de Gestão de Incidentes Cibernéticos.

Art. 14. Após o preenchimento do Registro de Incidente de Segurança, a ETIR-CFQ deliberará a respeito, observando:

I – Os protocolos previstos neste ato, na hipótese de se tratar de Incidente de Crise Cibernética;

II – O Protocolo para Investigação de Ilícitos Cibernéticos, na hipótese de se tratar de incidente de segurança cibernética penalmente relevante;

III – O protocolo previsto para contenção, dando-se ciência do incidente de segurança digital ao Comitê de Governança Digital, na hipótese de se tratar de incidentes de segurança cibernética, conforme os critérios de tipificação contidos no plano de gestão de incidentes cibernéticos e envolvendo do Encarregado de dados do CFQ, caso seja identificado o possível

vazamento de dados pessoais e dados pessoais sensíveis.

Subseção II

Da Contenção

Art. 15. A ETIR-CFQ deverá consultar a base de conhecimento sobre tratamento do incidente, bem como o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal - PLANGIC, para:

I – Identificar e definir equipe responsável, além do ponto de contato, pelo acompanhamento dos procedimentos de contenção, erradicação, recuperação e encerramento do incidente registrado;

II – Isolar os ativos de informação comprometidos no incidente registrado;

III – Comunicar às áreas responsáveis pelo serviço comprometido as ações a serem tomadas;

IV – Coletar as evidências do incidente, observando sua volatilidade; e

V – Adotar as ações de contorno, de acordo com os planos de continuidade e contingência.

Subseção III

Da Erradicação

Art. 16. A equipe responsável pelo incidente deverá investigá-lo detalhadamente e formular os quesitos necessários para esclarecer as possíveis causas, extensões e impactos, a fim de subsidiar as decisões e ações para sua contenção ou para seu encaminhamento.

Art. 17. Incumbe à equipe responsável pela investigação do incidente:

I – Elaborar relatório da análise de evidências;

II – Comunicar o incidente às áreas ou aos usuários afetados;

III – Remover as ameaças cibernéticas existentes nos ativos de informação comprometidos, garantindo que as operações essenciais sejam apoiadas, caso surjam desafios durante a etapa de restauração.

Subseção IV

Da Recuperação

Art. 18. A equipe responsável por investigar o incidente deverá elaborar plano de recuperação e executar as verificações ambientais e de segurança paralelas ao controle dos impactos de desempenho não intencionais da restauração.

Parágrafo único. O plano de recuperação deverá ser executado em fases para restauração de operações, com foco prioritário nos sistemas críticos ou na execução da operação, em modo analógico, até que haja confiança no desempenho do sistema.

Art. 19. A ETIR-CFQ possui autonomia completa e poderá conduzir o seu público alvo para realizar ações ou 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.

Art. 20. A ETIR-CFQ acionará as áreas competentes para apoiá-la na execução do Plano de Recuperação.

Art. 21. Após a execução do plano de recuperação, a ETIR-CFQ analisará detalhadamente o incidente para:

I – Certificar estar solucionado;

II – Verificar as ações e/ou providências adotadas até o momento, devendo elaborar Relatório de necessidades e soluções do incidente para conhecimento do CGD, caso necessário;

III – Elaborar novo plano de recuperação, na hipótese de o incidente de segurança não ter

sido solucionado;

IV – Encerrar e elaborar as lições aprendidas desta seção, conforme Subseção V, na hipótese de o incidente de segurança ter sido solucionado e não existir outras ações ou providências a serem tomadas.

Subseção V

Do Encerramento e das Lições Aprendidas

Art. 22. Solucionado o incidente, a ETIR-CFQ deverá:

I – Preencher o relatório de encerramento de incidente e registrá-lo em processo específico no Sistema Eletrônico de Informações - SEI;

II – Atualizar o indicador de desempenho dos incidentes de segurança, o Banco de Dados dos Incidentes Conhecidos (BDIC) e o Plano de Gestão de Incidentes de Segurança, caso necessário;

III – Encerrar o tratamento do Incidente de Segurança;

IV – Avaliar a necessidade de comunicar o CGD sobre o tratamento e o encerramento do incidente de segurança;

V – Comunicar ao usuário requisitante sobre o encerramento do incidente de segurança reportado.

Seção II

Da Investigação de Ilícitos Cibernéticos

Art. 23. O protocolo de investigação de ilícitos cibernéticos inclui as seguintes fases:

I – Coleta das evidências: envolve as diretrizes para a identificação dos ativos de informação e recursos de dados envolvidos, a solicitação de apoio das áreas para a coleta das evidências, a coleta dos dados voláteis e não-voláteis, a coleta e armazenamento de cópia dos arquivos afetados, e da elaboração da justificativa em caso de inviabilidade de preservação das evidências no Relatório de Comunicação de Incidente de Segurança Cibernética;

II – Preservação das evidências: envolve as diretrizes para a geração dos resumos criptográficos dos arquivos e da lista de resumos criptográficos, o lacre do material coletado e o preenchimento do Termo de Custódia dos Ativos de Informação; e

III – Comunicação do ilícito cibernético: envolve as diretrizes para a elaboração e apreciação do Relatório de Comunicação de Incidente de Segurança Cibernética e comunicação às autoridades responsáveis.

Art. 24. A execução da investigação de ilícitos cibernéticos será aplicada nos seguintes casos, entre outros:

I – Divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados do CFQ, nos termos do art. 153, §1.º-A, do Código Penal;

II – Invasão de dispositivo de TIC, nos termos dos arts. 154-A e 154-B do Código Penal;

III – Interrupção de serviço de TIC ou de informação de utilidade pública, previsto no art. 266, §1.º, do Código Penal;

IV – Inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados do CFQ, nos termos do art. 313-A do Código Penal;

V – Modificação ou alteração por agente público de sistema de informação ou programa de informática sem autorização, nos termos do art. 313-B do Código Penal;

VI – Distribuição, armazenamento ou conduta vinculada à pornografia infantil, nos termos dos arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei n.º 8.069/90;

VII – Interceptação de dados de forma clandestina, nos termos do art. 10 da Lei n.º 9.296/96.

Subseção I

Da Coleta de Evidências

Art. 25. Para fins de coleta de evidência, a ETIR-CFQ deverá seguir as disposições contidas nas diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes:

I – Identificar os ativos de informação envolvidos no incidente de segurança e quais serão os recursos de dados requeridos para a coleta das evidências;

II – Coletar as evidências, observando a ordem de volatilidade das evidências;

III – Avaliar a viabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou de suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado;

IV – Coletar e preservar, sem prejuízo de outras ações, os seguintes itens, quando possível:

a) dados voláteis armazenados nos dispositivos computacionais, tais como a memória principal (memória RAM, processos em execução, conexões de rede estabelecidas, tabela de rotas, dentre outros);

b) mídias de armazenamento dos dispositivos afetados ou imagens forenses; e

c) registros de eventos, coleta e preservação de evidências de incidentes de segurança em redes, devendo ser observado que devem ser armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

Subseção II

Da Preservação de Evidências

Art. 26. A ETIR-CFQ deverá, quando aplicável:

I – Gerar a lista dos resumos criptográficos (hashes) contendo a relação das evidências coletadas e armazená-la em arquivo no formato de texto puro (“.txt”);

II – Gravar os arquivos coletados (evidências) e o arquivo criado nos termos do inciso I;

III – Gerar hash do arquivo criado nos termos do inciso I;

IV – Lacrar o material coletado nos termos dos incisos I, II e III;

V – Preencher o Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante, contido na Norma Complementar N° 21/IN01/DSIC/GSIPR; e

VI – Armazenar os materiais lacrados em local seguro e de acesso restrito.

Subseção III

Da Comunicação de Ilícito Cibernético

Art. 27. A ETIR-CFQ elaborará o Relatório de Comunicação de Incidente Cibernético (RCIC-CFQ), que deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:

I – Nome do agente responsável pela ETIR-CFQ e informações de contato;

II – Nome do servidor da ETIR-CFQ responsável e informações de contato;

III – Órgão comunicante com sua localização e informações de contato;

IV – Número de controle da ocorrência;

V – Relato sobre o incidente, descrevendo como ocorreu o fato, como foi detectado, os dados coletados e preservados, bem como outros dados considerados relevantes;

VI – Descrição das atividades de tratamento e resposta ao incidente, bem como outras providências tomadas pela ETIR incluindo as ações de preservação, registrando-se a metodologia, caso aplicada, as ferramentas utilizadas e o local de armazenamento das informações preservadas;

VII – Resumo criptográfico dos arquivos coletados;

VIII – Termo de custódia dos ativos de informação relacionados ao incidente de

segurança;

IX – Número de lacre de material físico preservado, se houver; e

X – Justificativa sobre eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

Art. 28. A ETIR-CFQ acondicionará o RCIC-CFQ em envelope lacrado e rubricado pelo agente responsável pela ETIR-CFQ, além de protocolá-lo e encaminhá-lo formalmente à autoridade responsável pelo órgão ou entidade da APF.

Parágrafo único. Constará no documento formal de encaminhamento apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

Art. 29. Após receber a comunicação, a autoridade responsável pelo órgão ou entidade da APF deverá, de imediato, encaminhá-la formalmente à autoridade com atribuição para apurar os fatos. A comunicação deverá ser acompanhada de envelope lacrado contendo o RCIC-CFQ.

Art. 30. A preservação da privacidade e sigilo dos dados custodiados deverá ser observada durante todo o processo de coleta das evidências do incidente de segurança em redes computacionais, na elaboração do relatório, bem como, quando do seu envio às autoridades competentes, conforme legislação vigente.

Art. 31. O Relatório de Comunicação de Incidentes de Segurança em Redes Computacionais e o Termo de Custódia dos Ativos de Informação relacionados ao Incidente de Segurança contém informações sigilosas amparadas em hipóteses de sigilo previstas na legislação vigente.

Art. 32. O CFQ deverá adotar normas e procedimentos internos de tratamento das informações sigilosas que constam no Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, e no Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança.

Art. 33. A ETIR-CFQ deverá acionar os protocolos de Gerenciamento de Crises Cibernéticas.

Seção III

Do Gerenciamento de Crises Cibernéticas

Art. 34. O protocolo de gerenciamento de crises cibernéticas inclui as seguintes fases:

I – Planejamento do gerenciamento de crises cibernéticas (pré-crise): envolve as diretrizes do Comitê de Crise Cibernética, a execução do Programa de Gestão da Continuidade de Serviços e a avaliação do resultado das simulações dos planos e dos procedimentos produzidos;

II – Execução do gerenciamento de crises cibernéticas (durante a crise): envolve as diretrizes para o acionamento do Comitê de Crise Cibernética, a execução dos planos e procedimentos aplicáveis, o levantamento das informações e das soluções alternativas para a crise, a centralização da comunicação no porta-voz do Comitê de Crise Cibernética, o acionamento do protocolo de ilícitos cibernéticos, a orientação das prioridades e estratégias da organização para a recuperação, a definição dos procedimentos de compartilhamento de informações relevantes com outros órgãos, a elaboração, a apreciação e a execução do plano de retorno à normalidade; e

III – Melhoria contínua do gerenciamento de crises cibernéticas (pós-crise): envolve as diretrizes para identificar e registrar as lições aprendidas, a elaboração do relatório de encerramento do incidente de segurança, da necessidade de atualizar os procedimentos, o encerramento da crise e a comunicação do fim do tratamento da crise às partes interessadas.

Art. 35. O gerenciamento de crises cibernéticas será tratado em normativo específico.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 36. Diretrizes específicas poderão ser fixadas em procedimentos internos,

considerando esta Portaria e a Política de Segurança da Informação CFQ.

Art. 37. O Comitê de Governança Digital realizará a revisão deste ato normativo ordinariamente a cada dois anos.

Parágrafo único. A revisão poderá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem a gestão de incidentes de segurança da informação no CFQ.

Art. 38. Esta Portaria entra em vigor no dia 22 de janeiro de 2024.

Dê-se ciência.

Publique-se.

Brasília, 19 de janeiro de 2024.

JOSÉ DE RIBAMAR OLIVEIRA FILHO
Presidente

Referência: Processo nº 2800.00.00233.2024

SEI nº 0045494

SCS Quadra 09, Edifício Parque Cidade Corporate, Torre B, 9º andar
Brasília/DF, CEP 70.308-200
Telefone: (61) 2099-3300 - www.cfq.org.br