Conselho Federal de Química

Plenário
Presidência
Gabinete

PORTARIA Nº 21, DE 26 DE MARÇO DE 2025

Institui a Política de controle de acesso físico e de ambiente do Conselho Federal de Química.

O PRESIDENTE DO CONSELHO FEDERAL DE QUÍMICA—CFQ, no uso de suas atribuições, que lhe foram conferidas pelo art. 74, incisos II e XXVI, do Regimento Interno do CFQ, aprovado pela Resolução Normativa CFQ nº 307, de 22 de março de 2023; tendo em vista a Instrução Normativa GSI/PR Nº 01, de 27 de maio de 2020, a ABNT NBR ISO/IEC 27001: 2013, a ABNT NBR ISO/IEC 27002: 2013, a Lei nº 13.709/2018, que dispõe sobre a Lei Geral de Proteção de Dados, o Guia do Framework de Privacidade e Segurança da Informação elaborado pela Secretaria de Governo Digital do Ministério da gestão e da Inovação em Serviços Públicos; e o art. 9º da Portaria CFQ nº 182, de 6 de outubro de 2022, que dispõe sobre a institucionalização da Política de Segurança da Informação (POSIN) no âmbito do Conselho Federal de Química — CFQ e dá outras providências;

Resolve:

Art. 1º Instituir, no âmbito do Conselho Federal de Química—CFQ, a Política de Controle de Acesso Físico e de Ambiente, em complemento às diretrizes estabelecidas no Capítulo II, Seção II, da Política de Segurança da Informação, institucionalizada na Portaria nº 182, de 06 de outubro de 2022.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 2º Esta Política tem como objetivo estabelecer medidas para controlar o acesso físico aos ambientes do CFQ, a fim de mitigar danos e interferências nas informações e ativos de Tecnologia da Informação e Comunicação—TIC.

Art. 3º Devem ser utilizados perímetros físicos de segurança (barreiras) tais como paredes e portas de entrada com acesso controlado para proteger as áreas que contenham instalações de processamento, armazenamento e comutação de dados, além de controles para minimizar o risco de ameaças físicas potenciais, tais como: furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferências com o suprimento de energia elétrica, interferência nas comunicações, radiação eletromagnética e vandalismo.

Art. 4º Os perímetros de segurança devem ser claramente definidos e a sua localização e a sua capacidade de resistência devem estar associadas aos requisitos de segurança dos ativos existentes em seu interior.

Art. 5º A Gerência de Tecnologia da Informação e Comunicação — GETIC deverá avaliar e providenciar a melhoria dos recursos de segurança de seus centros de processamento, armazenamento e comutação de dados corporativos.

Seção I

Conceitos e definições

Art. 6º Para efeitos desta Política, serão considerados os conceitos e as definições de segurança da informação estabelecidos pela Portaria GSI/PR Nº 93, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação.

Seção II

Áreas de Processamento, armazenamento e comutação de dados

Art. 7º As instalações de data center devem atender às seguintes diretrizes:

I - paredes fisicamente sólidas, sem brechas nem pontos por onde possa ocorrer uma invasão;

II - portas externas adequadamente protegidas por mecanismos de controle contra acesso não autorizado, sem janelas ou, na impossibilidade, com janelas com proteção externa;

III - videomonitoramento de sua área interna e de seu perímetro;

IV - controle de acesso físico às áreas e às instalações, sob a responsabilidade da GETIC, com a utilização dos mecanismos necessários para o controle e registro de data e hora de todas as entradas e saídas de visitantes ou prestadores de serviço, permitindo-lhes o acesso, desde que previamente autorizados;

V - mecanismos de autenticação, para as instalações de processamento, armazenamento e comutação de dados, restritas ao pessoal autorizado;

VI - portas com sistema de alarme, monitoradas e que funcionem de acordo com os códigos locais, para minimizar os riscos de ameaças físicas potenciais;

VII - instalações de processamento e armazenamento das informações que sejam projetadas para minimizar os riscos de ameaças físicas potenciais;

VIII - edifícios que sejam dotados de proteção contra raios e que, em todas as linhas de entrada de força e de comunicações, tenham filtros de proteção contra raios;

IX - suplementação elétrica temporária;

X - iluminação de emergência; e

XI - sistema de controle de temperatura e umidade com recurso de emissão de alertas.

Art. 8º As áreas de processamento, armazenamento e comutação de dados devem ser rigorosamente protegidas por medidas de segurança e controles de acesso, com observância dos seguintes parâmetros:

I - o acesso às áreas de processamento, armazenamento e comutação de dados deve ser controlado por mecanismos apropriados, incluindo autenticação mínima de dois fatores, para validar e autorizar todos os acessos;

II - devem ser mantidos registros seguros de todos os acessos;

III - as permissões de acesso devem ser concedidas somente para finalidades específicas e com as devidas instruções sobre os requisitos de segurança da área e sobre os procedimentos de emergência;

IV - os direitos de acesso às áreas seguras devem ser revisados periodicamente e atualizados conforme necessário, com revogação imediata dos direitos quando não forem mais necessários;

V - o acesso de prestadores de serviços terceirizados que necessitem realizar suporte técnico nas áreas sensíveis será restrito, concedido apenas quando imprescindível, e será monitorado e autorizado previamente pela Gerência ou Coordenação da GETIC;

VI - as áreas de processamento, armazenamento e comutação de dados devem ser localizadas de forma discreta, sem identificação explícita de sua finalidade ou presença de letreiros evidentes;

VII - informações sobre a localização das instalações de processamento e armazenamento de dados sensíveis não devem ser facilmente acessíveis ao público;

VIII - equipamentos de contingência e mídias de backup devem ser armazenados em locais seguros e afastados das áreas principais, a fim de evitar danos decorrentes de desastres ou incidentes;

IX - não será permitido o uso de dispositivos de gravação, como câmeras fotográficas, gravadores de vídeo ou áudio, e outros dispositivos móveis, nas proximidades das instalações de processamento de dados, salvo autorização expressa da Gerência ou Coordenação da GETIC; e

X - é proibido realizar refeições nas proximidades das áreas de processamento, armazenamento e comutação de dados, assim como nas estações de trabalho e outros dispositivos de TIC.

Seção III

Dos equipamentos de processamento e armazenamento

Art. 9º Para evitar perdas, danos, furtos e o comprometimento de ativos e interrupção das operações da organização, devem ser observadas as seguintes diretrizes:

I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais e para evitar a retirada de equipamentos patrimoniados sem prévia autorização da Gerência Administrativa; e

II - utilizar, sempre que possível, racks que disponham de fechaduras com chave ou mecanismo semelhante, a fim de que apenas os membros da(s) equipe(s) responsável(eis) pelos ativos instalados nos racks possuam acesso físico.

Seção IV

Da segurança do cabeamento

Art. 10. O cabeamento de energia elétrica e de telecomunicações que transporta dados ou provê suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

I - as linhas de energia elétrica e de telecomunicações que chegam às instalações de processamento da informação devem ser subterrâneas, instaladas abaixo do piso, ou via eletrocalhas, sempre que possível, e devem atender aos requisitos mínimos de instalação e proteção, conforme padrões e normas vigentes; e

II - os cabos de energia elétrica devem ser segregados dos cabos de comunicação, para evitar interferências.

Seção V

Da manutenção técnica dos equipamentos

Art. 11. A manutenção dos equipamentos de processamento de informações deve seguir as seguintes diretrizes:

I - ser realizada exclusivamente por pessoal autorizado pela Gerência ou Coordenação da GETIC;

II - registrar todos os incidentes e operações de manutenção preventivas, preditivas, evolutivas e corretivas efetuadas via central de serviços;

III - eliminar, sempre que viável, informações sensíveis dos equipamentos ou tratar de forma alternativa os riscos associados à sua exposição; e

IV - realizar inspeções minuciosas para garantir o funcionamento adequado dos equipamentos após a conclusão da manutenção.

Seção VI

Da reutilização ou descarte seguro dos equipamentos ou dos equipamentos em prova de conceito

Art. 12. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização ou descarte, para assegurar que dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

Parágrafo único. As mídias que contenham informações com acesso restrito de propriedade intelectual devem ser destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

Seção VII

Da Política da mesa limpa e tela limpa

Art. 13. A informação com restrição de acesso não deve ser deixada à vista sobre mesas de trabalho ou em quaisquer outros suportes que não disponham de mecanismos de controle de acesso e deve ser destruída antes de ser descartada, seja em papel ou em formato digital.

Parágrafo único. A política de mesa limpa para papéis e mídias de armazenamento removíveis deve considerar a classificação da informação, requisitos contratuais e legais e o risco correspondente.

Art. 14. Os computadores pessoais e terminais de computador não devem apresentar senhas na tela e não devem permanecer logados caso o usuário esteja ausente.

Parágrafo único. A política de tela limpa para computadores e terminais deve ser aplicada por meio de bloqueio de tela por senha, token ou mecanismo de autenticação similar.

CAPÍTULO II

DO MONITORAMENTO

Art. 15. O acesso físico às dependências do CFQ será controlado e monitorado pela Gerência Administrativa, de acordo com as seguintes diretrizes:

I - a identificação de colaboradores, conselheiros e prestadores de serviços será feita, preferencialmente, por meio do uso de crachá, para permitir o controle e a segurança do ambiente;

II - o acesso de visitantes dependerá de autorização prévia por parte de empregado público, e o visitante terá o registro de entrada e saída, com data e hora, e deverá ser acompanhado durante toda a sua permanência no local; e

III - quando o acesso de visitantes ocorrer fora do horário regular de funcionamento, será necessário registrar o motivo do ingresso e as dependências de acesso.

Parágrafo único. A Gerência Administrativa deverá providenciar a remoção imediata de empregados, conselheiros e prestadores de serviços desligados da lista de pessoas autorizadas a acessar as dependências do CFQ, assim que solicitado.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 16. As responsabilidades pelo controle de acesso físico, para manter a segurança das informações, são compartilhadas entre diferentes unidades do CFQ, conforme as seguintes atribuições:

I - Comitê de Governança Digital (CGD): responsável por propor políticas e procedimentos necessários para o controle e a proteção dos dados, a fim de permitir a conformidade com as melhores práticas de segurança da informação;

II - Gerência de Tecnologia da Informação e Comunicação (GETIC): responsável pela implementação e execução das medidas de controle de acesso, de forma a assegurar a identificação e o registro dos acessos realizados por qualquer agente que tenha necessidade legítima de acessar as informações;

III - Gerência Estratégica de Gestão de Pessoas (GEPES): responsável pelo gerenciamento das solicitações de novas autorizações e pela revogação dos acessos, conforme as necessidades e mudanças na estrutura organizacional;

IV - Gerência Administrativa (GEAD): responsável pelo registro e pela manutenção dos registros de acesso físico dos visitantes, para permitir o monitoramento adequado das visitas; e

V - Colaboradores e Visitantes: responsáveis por utilizar os sistemas e serviços disponibilizados assim como seguir as regras e diretrizes estabelecidas nesta política de controle de acesso.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 17. Os incidentes que afetem a segurança das informações, assim como o descumprimento da Política de Segurança da Informação e demais normas de segurança devem ser obrigatoriamente comunicados pelos usuários à GETIC, por meio da abertura de chamado em Central de Serviços, sem prejuízo de outros procedimentos de comunicação estabelecidos.

Art. 18. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do CFQ - ETIR-CFQ fará a investigação, e poderá interromper temporariamente o serviço afetado, sem prévia autorização.

§ 1º Nos casos em que o ator da quebra de segurança for um usuário, a ETIR- CFQ comunicará os resultados ao superior imediato e ao Encarregado pelo Tratamento de Dados Pessoais, para adoção de medidas cabíveis.

§ 2º As ações que a Política de Controle de Acesso Físico e de Ambiente serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

Art. 19. 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.

Art. 20. O CFQ terá o prazo de até 18 meses para cumprir o disposto no inciso III do art. 7º desta Portaria.

Art. 21. A redação da epígrafe da Portaria nº 21, de 21 de março de 2025, passará a ser Portaria nº 20, de 21 de março de 2025.

Art. 22. Os casos omissos serão apreciados pelo Comitê de Governança Digital - CGD.

Dê-se ciência.

Publique-se.

Brasília, 26 de março de 2025.

JOSÉ DE RIBAMAR OLIVEIRA FILHO

Presidente

SCS Quadra 09, Edifício Parque Cidade Corporate, Torre B, 9º andar
Brasília/DF, CEP 70308-200
Telefone: (61) 2099-3300 - www.cfq.org.br