Conselho Federal de Química

Plenário
Presidência
Gabinete

PORTARIA Nº 5, DE 19 DE JANEIRO DE 2024

Estabelece diretrizes de segurança da informação para a política de controle de acesso do Conselho Federal de Química.

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 ABNT NBR ISO/IEC 27002: 2013 que contém o código de Prática para controles de Segurança da Informação;

Considerando a Lei n° 13.709/2018 que dispõe sobre a Lei Geral de Proteção de Dados;

Considerando o CIS v8 - Center for Internet Security (CIS);

Considerando 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;

Considerando o Modelo para Política de Controle de Acesso elaborado pela Secretaria de Governo Digital do Ministério da gestão e da Inovação em Serviços Públicos;

Considerando a 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 Aprovar, no âmbito do Conselho Federal de Química - (CFQ), a Política para criação e administração de contas de acesso, em complemento às diretrizes estabelecidas na Seção VI da Política de Segurança da Informação, instituída pela Portaria CFQ nº 182, de 6 de outubro de 2022.

CAPÍTULO I

ACESSO LÓGICO

Art. 2º O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso, que será concedido e mantido pela Gerência de Tecnologia da Informação (GETIC), baseado nas responsabilidades e tarefas de cada usuário.

Art. 3° Os usuários de recursos de tecnologia da informação terão direito a acesso lógico aos recursos da rede local.

Parágrafo único. Para fins desta Portaria, consideram-se usuários de recursos de tecnologia da informação os Conselheiros, membros de colegiados, empregados e colaboradores, incluídos os funcionários de empresas prestadoras de serviços, estagiários e demais usuários

temporários em atividade no CFQ.

Art. 4° O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações e deve ser utilizado o MFA (autenticação multifator) para a autenticação de acesso remoto.

Parágrafo único. O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

Art. 5° A GETIC deve estabelecer e manter um inventário de todas as contas gerenciadas, com a relação de todas as contas de usuário, administrativas, testes e serviços.

§1° O inventário para as contas de serviço deverá conter no mínimo as informações de:

I -Departamento proprietário; e

II -Data de criação/última autorização de renovação de acesso.

§2° A GETIC deverá validar todas as contas ativas do CFQ, a cada 90 (noventa) dias.

Art. 6° Caberá a GETIC, quanto ao acesso lógico:

I- implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

II- estabelecer e manter um inventário dos sistemas de autenticação e autorização do CFQ, tal inventário deve ser revisado periodicamente.

III- definir e manter o controle de acesso dos usuários baseado em funções.

IV - elaborar a documentação dos direitos dos acessos para cada função dentro do CFQ.

Art. 7° A GETIC deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos no CFQ.

CAPÍTULO II

CONTA DE ACESSO LÓGICO E SENHA

Art. 8° Para utilização das estações de trabalho do CFQ, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pela GETIC, mediante solicitação formal da Gerência Estratégica de Gestão de Pessoas (GEPES), via abertura de chamado no GLPI.

§ 1º Os privilégios de acesso dos usuários à rede local devem ser definidos pela unidade de lotação ao qual o usuário será vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

§ 2º Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação formal, via GLPI, para a GETIC que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 9° O login e a senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela GETIC quando constatada qualquer irregularidade.

Parágrafo único. Havendo o bloqueio de login e senha, a retomada do acesso à rede, deverá ser formalizada à GETIC por nova requisição pelo titular da unidade do requisitante.

Art. 10. O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, "joao.silva".

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, a GETIC realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 11. O padrão adotado para o formato da senha é o definido pela GETIC, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

§ 1º A formação da senha da identificação (login) de acesso à rede local deve seguir as

regras de:

I -possuir tamanho mínimo de 8 (oito) caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 (quatorze) caracteres para contas que não utilizam MFA;

II -recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

III- não ser formada por sequência numérica (1,2,3...), alfabética (a,b,c...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

IV - não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou system;

V - não reutilizar as últimas cinco senhas.

§ 2º A GETIC fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à rede local.

Art. 12. As senhas de acesso serão renovadas a cada noventa dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à rede local até que a nova senha seja configurada.

CAPÍTULO III

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 13. A conta de acesso será bloqueada nos seguintes casos:

I- Após 20 (vinte) tentativas consecutivas de acesso errado;

II- Solicitação do superior imediato do usuário com a devida justificativa;

III- Quando da suspeita de mau uso dos serviços disponibilizados pelo CFQ ou descumprimento da Política de Segurança da Informação – POSIN e normas correlatas em vigência.

IV- Após número específico de 90 (noventa) dias consecutivos sem movimentação pelo usuário.

Art. 14. O desbloqueio da conta de acesso à rede local será realizado apenas após solicitação formal do superior imediato do usuário à GETIC.

Art. 15. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou da GEPES.

Art. 16. A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Art. 17. A GETIC deverá configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 18. A GETIC deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO IV

MOVIMENTAÇÃO INTERNA

Art. 19. Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à rede local devem ser revogados.

§ 1º A GEPES deverá realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

§ 2º Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou da GEPES.

CAPÍTULO V

CONTA DE ACESSO BIOMÉTRICO

Art. 20. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O CFQ deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI

ADMINISTRADORES

Art. 21. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

§ 1º Somente os colaboradores da GETIC, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

§ 2º Na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a GETIC, por meio da abertura de chamado técnico no GLPI, que poderá negar os casos em que entender desnecessária a utilização.

§ 3º Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da GETIC.

§ 4º Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

§ 5º Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do CFQ, não será concedida, para um mesmo usuário, identificação (*login*) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

§ 6º Excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do Gerente de Tecnologia da Informação por meio da GETIC.

§ 7º A GETIC deverá implementar o MFA para todas as contas de administrador.

§ 8º A GETIC deverá restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

CAPÍTULO VII
RESPONSABILIDADES

Art. 22. É de responsabilidade do superior imediato do usuário comunicar formalmente à GEPES e a GETIC o desligamento ou saída do usuário do CFQ para que as permissões de acesso à rede local sejam canceladas.

Art. 23. Caberá a GEPES a comunicação imediata a GETIC sobre desligamentos de funcionários para que seja efetuada a revogação definitiva da permissão de acesso aos recursos.

Art. 24. É responsabilidade da Gerência Administrativo-Financeira (GEAF) a comunicação imediata a GETIC sobre desligamentos de funcionários de empresas prestadoras de serviços, para que seja efetuada a revogação definitiva da permissão de acesso aos recursos.

Parágrafo único. Os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

Art. 25. O usuário é responsável por todos os acessos realizados através de sua conta de

acesso e por possíveis danos causados à rede local e a recursos de tecnologia custodiados ou de propriedade do CFQ.

§ 1º O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

§ 2º A utilização simultânea da conta de acesso à rede local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

§ 3º O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à rede local.

Art. 26. O usuário deve informar à GETIC qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 27. É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I- não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II- evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III- interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV- não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V- não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI- utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII-não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII- assinar o Termo de Responsabilidade (Modelo – Anexo Único) quanto a utilização da respectiva conta de acesso.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 28. Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários à GETIC, por meio da abertura de chamado, via GLPI.

Art. 29. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a ETIR-CFQ fará a investigação, podendo 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, para adoção de medidas cabíveis.

§ 2º Ações que violem a POSIN ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

§ 3º A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Governança Digital - CGD do CFQ.

Art. 30. 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. 31. Esta Portaria entra em vigor nesta data.

Dê-se ciência.

Publique-se.

Brasília, 19 de janeiro de 2024.

JOSÉ DE RIBAMAR OLIVEIRA FILHO

Presidente

ANEXO ÚNICO

Modelo de Termo de Responsabilidade Conselho Federal de Química.

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste Conselho , DECLARO , sob pena das sanções cabíveis nos termos da legislação vigente que assumo a responsabilidade por:

I. Tratar o(s) ativo(s) de informação como patrimônio do Conselho Federal de Química;

II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do Conselho Federal de Química;

III. Contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV. Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Conselho Federal de Química.;

V. Responder, perante o Conselho Federal de Química, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI. Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VII. Utilizar o correio eletrônico (e-mail) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X. Não me ausentar da estação de trabalho sem bloquear estação de trabalho garantindo assim a impossibilidade de acesso indevido por terceiros;

XI. Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII. Responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha

senha ou das transações a que tenha acesso.

Local, UF, _____de _____de _____.

_____

Assinatura
Nome do usuário e seu setor organizacional

Referência: Processo nº 2800.00.00233.2024

SEI nº 0045492

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