PORTARIA Nº 182 de 6 de outubro de 2022.

Dispõe sobre a institucionalização da Política de Segurança da Informação (POSIN) no âmbito do Conselho Federal de Química (CFQ) e dá outras providências.

O Presidente do Conselho Federal de Química, no uso de suas atribuições conferidas pelo art. 8º da Lei nº 2.800, de 18 de junho de 1956;

Considerando o Decreto n° 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

Considerando a Instrução Normativa n° 1-GSI/PR, de 27 de maio de 2020 que dispõe sobre a Estutura de Gestão de Seguraça da Informação nos órgãos e nas entidades da Administração Pública Federal;

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

Resolve:

Art. 1º Instituir no âmbito do Conselho Federal de Química (CFQ) a Política de Segurança da Informação (POSIN).

Art 2º Regular que a Política de Segurança da Informação (POSIN) aplica-se aos integrantes da Governança, colaboradores, estagiários, prestadores de serviços, e quando aplicável, a terceiros e quaisquer outras pessoas que prestem serviços ao CFQ.

Art 3º Definir que àqueles abrangidos pela POSIN devem zelar pelo cumprimento das diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Art. 4º Estabelecer a obrigatoriedade dos usuários de recursos de Tecnlogia da Informação e Comunicação (TIC) assinarem o Termo de Responsabilidade.

Art. 5º Revogar a Portaria n° 12, de 16 de abril de 2019.

Art. 6º Decretar que esta Portaria entra em vigor na data de sua assinatura.

Dê-se ciência.
Publique-se.

Brasília, 6 de outubro de 2022.

JOSÉ DE RIBAMAR OLIVEIRA FILHO
Presidente

Política de Segurança da Informação POSIN

CONSELHO FEDERAL DE QUÍMICA

JOSÉ DE RIBAMAR OLIVEIRA FILHO

PRESIDENTE

FUAD HADDAD

1º VICE-PRESIDENTE

ROBERTO LIMA SAMPAIO

2º VICE-PRESIDENTE

NEWTON MARIO BATTASTINI

1º TESOUREIRO

RENATA LILIAN RIBEIRO PORTUGAL FAGURY

2º TESOUREIRA

ANA MARIA BIRIBA DE ALMEIDA

1º SECRETÁRIA

ALI VEGGI ATALA

2º SECRETÁRIO

COORDENAÇÃO E ELABORAÇÃO
COMITÊ DE GOVERNANÇA DIGITAL

RENATO MELO
GERENTE EXECUTIVO
COORDENADOR

WEVERTON BORGES DO NASCIMENTO DE SOUSA
OUVIDOR GERAL
ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

BRUNO GOYTISOLO PIRES DA SILVA
GERENTE DE GESTÃO ESTRATÉGICA DE PESSOAS

CRISTIANO XAVIER LUCAS FERREIRA
GERENTE DE TECNOLOGIA DA INFORMAÇÃO

FAERISSON LIMA DE SOUZA
GERENTE DE OPERAÇÕES FINALÍSTICAS

SEBASTIÃO DIEGO DA CONCEIÇÃO SANTOS MEDEIROS
COORDENADOR ADMINISTRATIVO

JORDANA DE CASTRO SALDANHA
CHEFE DA ASSESSORIA DE COMUNICAÇÃO

LEONARDO NUNES FERREIRA
CHEFE DA CONTROLADORIA

ALINE ALVES DE MEDEIROS DE AZEVEDO
GESTORA DE SEGURANÇA DA INFORMAÇÃO

Controle de Versões

Versão	Atualização	Término da Modificação	Principais Alterações
Versão 1	0	22/08/2022	Primeira versão apresentada para avaliação Comitê de Governança Digital.
Versão 1	1	14/09/2022	Ajustes propostos na Reunião do Comitê de Governança Digital realizada em 13 de setembro de 2022.
Versão 2		29/09/2022	Ajustes do texto com a aplicação de alterações sugeridas pela AJUR.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

Escopo

Art. 1° A Política de Segurança da Informação – POSIN do Conselho Federal de Química objetiva instituir diretrizes estratégicas, responsabilidades e competências para assegurar a segurança das informações custodiadas e de propriedade do Conselho Federal de Química – CFQ, de modo a preservar seus ativos e sua imagem institucional.

Art. 2° A POSIN trata do uso e do compartilhamento do conteúdo de dados, informações e documentos no âmbito do CFQ, respeitando o seu ciclo de vida: criação, coleta, tratamento, divulgação, armazenamento, compartilhamento, medidas internas de segurança e descarte, em acordo com a continuidade de seus processos e com a legislação vigente, princípios de privacidade e proteção de dados, conforme o *privacy by design* e as melhores práticas de segurança da informação.

Art. 3° As diretrizes e objetivos desta Política se aplicam a todo o CFQ, devendo ser observados por todos os servidores, estagiários, conselheiros e diretores; e, quando aplicável, a terceiros e quaisquer outras pessoas que prestem serviços ao CFQ, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Parágrafo único. Os contratos, convênios, instrumentos congêneres e termos de aditivo conterão cláusulas específicas que imponham aos contratados e convenentes a obrigação de observarem o disposto nesta Política, para o exercício de suas atividades no âmbito do CFQ.

Art. 4° A diretoria do CFQ deverá se manter comprometida em relação à segurança da informação institucional, bem como garantir meios para a devida divulgação, capacitação, sensibilização e cumprimento das normas e procedimentos estabelecidos.

Art. 5° A Política de Segurança da Informação (POSIN) visa nortear a implementação de medidas de proteção que deverão ser aplicadas às informações que têm valor, independentemente, de seu suporte material ou tecnológico - ativo de informação, da reputação e imagem institucional do CFQ.

Art. 6° A POSIN tem por finalidade estabelecer normas, diretrizes e procedimentos para a segurança no uso, tratamento e controle, proteção dos dados, informações e conhecimentos produzidos ou transmitidos por qualquer meio de informação e comunicação.

Parágrafo Único: A POSIN está alinhada com a política de gestão de mudanças, com a gestão de riscos, plano de gerenciamento de incidentes e plano de recuperação de negócio.

Seção II

Conceitos e Definições

Art. 7° Para os efeitos desta POSIN, considera-se o Glossário de Segurança da Informação como conceitos básicos, estabelecido pela Portaria GSI/PR nº 93, de 26 de setembro de 2019 , e orienta-se os seguintes princípios:

I. Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta.

II. Ativo: qualquer coisa que tenha valor para a organização.

III. Ativo de Rede: equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

IV. Ativos de Informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos a que eles têm acesso.

V. Autenticidade: assegura que a informação foi produzida, expedida, modificada ou destruída e garante a identificação de pessoa física, sistema e entidade que assim o fez.

VI. Celeridade: garante respostas rápidas a incidentes e falhas de segurança.

VII. Clareza: define que as regras e a documentação sobre segurança da informação devam ser elaboradas de forma clara, precisa, concisa e de fácil entendimento.

VIII. Confidencialidade: garante que a informação não esteja disponível ou não seja revelada e/ou acessível a pessoas, a sistema e às entidades não autorizadas.

IX. Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

X. Criticidade: define a importância da informação para a continuidade da execução das finalidades institucionais.

XI. Disponibilidade: garante que a informação esteja sempre acessível e utilizada sob demanda para uso legítimo de pessoas físicas, sistemas, órgão ou entidades autorizadas.

XII. E-mail: acrônimo de *electronic mail* (correio eletrônico).

XIII. Ética: preserva o direito do empregado, colaborador, terceirizado, conselheiro, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação.

XIV. ETIR: acrônimo de Equipe de Tratamento de Incidentes de Rede.

XV. Incidente: evento, 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.

XVI. Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

XVII. Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

XVIII. Integridade: garante que a informação não foi modificada, esteja correta e confiável. Além disso, assegura que a informação não seja modificada, gravada ou excluída sem autorização ou acidentalmente.

XIX. Internet das coisas (IOT): sistema interrelacionado de dispositivos computacionais, equipamentos digitais e mecânicos, e objetos aos quais são vinculados UIDs e que possuem a habilidade de transferir dados pela rede sem a necessidade de interação do tipo pessoa-pessoa ou pessoa-computador.

XX. Proteção: assegura o direito individual e coletivo das pessoas à inviolabilidade da sua intimidade e ao sigilo da informação, nos termos previstos na Constituição Federal.

XXI. Legalidade: devem ser levadas em consideração as leis, as normas e as políticas organizacionais, administrativas, técnicas e operacionais vigentes.

XXII. Negação de Serviço (DoS): bloqueio de acesso devidamente autorizado a um recurso ou a geração de atraso nas operações e funções normais de um sistema, com a resultante perda da disponibilidade aos usuários autorizados. O objetivo do ataque DoS é interromper atividades legítimas de um computador ou de um sistema. Uma forma de provocar o ataque é aproveitando-se de falhas ou de vulnerabilidades presentes na máquina vítima, ou enviar um grande número de mensagens que esgotem algum dos recursos da vítima, como CPU, memória, banda, etc. Para isto, é necessária uma única máquina poderosa, com bom processamento e bastante banda

disponível, capaz de gerar o número de mensagens suficiente para causar a interrupção do serviço.

XXIII. Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes.

XXIV. Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

XXV. Plano de Recuperação de Negócios: documentação dos procedimentos e de informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade.

XXVI. POSIN: acrônimo de Política de Segurança da Informação.

XXVII. Prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderá receber credencial especial de acesso.

XXVIII. *Privacy by Design* – conceito que aplica a privacidade de dados desde a concepção dos serviços

XXIX. Privacidade: estabelece que o direito do cidadão de não ter registros pessoais e da vida privada divulgados sem sua prévia autorização deve ser assegurado.

XXX. Publicidade: determina que a divulgação das informações deve observar os critérios legais aplicáveis.

XXXI. Responsabilidade: define que os usuários são responsáveis pelo cumprimento desta POSIN e devem respeitar a legislação e normas pertinentes à Segurança da Informação vigentes.

XXXII. Tecnologia da Informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.

XXXIII. TIC: acrônimo de Tecnologia da Informação e Comunicações.

XXXIV. UID: acrônimo de Identificador Único (*Unique IDentifier*) em sistemas de computadores. Baseados nessa definição, há o GUID (Identificador Global Único -Global *Unique IDentifier*) e UUID (Identificador Universal Único - Universal *Unique IDentifier*). Ressalta-se que, no sistema UNIX, UID significa Identificador do Usuário (*User IDentifier*).

XXXV. Usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO II

DAS DIRETRIZES GERAIS

Seção I

Do Tratamento da Informação

Art. 8° Para o Tratamento da Informação será considerada nesta POSIN os seguintes requisitos:

I. Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade do CFQ e deve ser protegida segundo as diretrizes descritas nesta Política, com o objetivo de minimizar riscos às atividades e serviços institucionais e preservar sua imagem.

II. É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo CFQ.

Seção II

Da Segurança Física e do Ambiente

Art. 9°. As diretrizes específicas e procedimentos próprios de segurança física e do ambiente que deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I. O acesso físico ao ambiente deverá ser monitorado e controlado;

II. Agentes públicos e prestadores de serviços deverão ser identificados por meio do uso de crachá;

III. O acesso de visitantes às dependências do órgão deverá ser autorizado por empregado público;

IV. Os empregados e prestadores de serviços desligados deverão ser excluídos da relação de pessoas autorizadas; e

V. Os arquivos físicos e os centros de processamento de dados deverão ser protegidos e estabelecidos em locais de acesso restrito e devidamente trancados em sala ou armário específico com o controle de acesso, sob responsabilidade do gestor responsável pelos ativos e devem, ainda, dispor de normas específicas.

Seção III

Gestão de Incidentes em Segurança da Informação

Art. 10. A Gestão de incidentes de segurança da informação deverá ser realizada por meio de processo formalizado, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

Art. 11. Em resposta aos incidentes, deverá considerar a elaboração de uma Norma de Resposta a Incidentes Tecnológicos.

Art. 12. Deverá ser instituída Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR, responsável pelo tratamento e resposta aos incidentes, com a responsabilidade de receber, analisar e responder a notificações e a atividades relacionadas a incidentes de segurança em rede de computadores.

Art. 13. Sua criação, sua estrutura e seu modelo de implementação serão definidos em Portaria, que deverá estar em conformidade com as diretrizes desta POSIN.

Seção IV

GESTÃO DE ATIVOS

Art. 14. Os ativos de rede conectados fisicamente, virtualmente e remotamente à infraestrutura do CFQ, e aqueles em ambientes de nuvem, deverão ser inventariados, com o objetivo de fornecer subsídios para a gestão dos ativos.

Art. 15. Deverá ser instituída norma específica de Inventário e Mapeamento de Ativos de Informação que, no mínimo, devem englobar:

I. Inventário e controle de ativos corporativos;

II. Inventário e controle de ativos de software.

Seção V

GESTÃO DO USO DOS RECURSOS OPERACIONAIS E DE COMUNICAÇÃO

Subseção I

CORREIO ELETRÔNICO

Art. 16 O uso de e-mail no âmbito do CFQ deve ser definido em norma específica, em conformidade com as diretrizes desta POSIN, considerando e não se limitando a esses aspectos:

I. O serviço de correio eletrônico será oferecido como um recurso institucional para apoiar os seus usuários no cumprimento das atividades; e
II. O correio eletrônico deverá ser utilizado somente para fins corporativos e relacionados às atividades do usuário no âmbito do CFQ, sendo vedado o uso para fins pessoais.

Subseção II

DO USO E ACESSO À INTERNET

Art. 17 O acesso à rede mundial de computadores, no âmbito do CFQ, deve ser definido em norma específica, devendo ser utilizado estritamente para atividades laborais, em conformidade com as diretrizes desta POSIN, orientações governamentais e legislações específicas em vigor seguindo no mínimo as diretrizes gerais:

I. Toda informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, o CFQ, de acordo com norma legal vigente, reserva-se no direito de monitorar e registrar os acessos à rede mundial de computadores;

II. Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet podem ser analisados pelo CFQ. Se necessário, o CFQ pode bloquear qualquer arquivo, sítio, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privativas da rede, visando assegurar o cumprimento de sua POSIN;

III. Todos os usuários ao utilizarem esse serviço deverão fazê-lo no estrito interesse do órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público;

IV. O acesso à Internet, por parte dos colaboradores, utilizando equipamentos do CFQ, deve ser feito exclusivamente por meio do provedor contratado pelo Conselho, sendo vedado o acesso à Internet utilizando provedores de acesso privados, exceto quando autorizado pela Gerência de Tecnologia da Informação; e

V. É expressamente proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo.

Subseção III

DA RECUPERAÇÃO DE DADOS

Art. 18 Todo sistema ou informação relevante para a operação das finalidades institucionais do CFQ deverá possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou

minimizar os impactos nas operações da instituição, devendo a implementação dos procedimentos de *backup* ser definida em norma específica, em conformidade com esta POSIN.

Subseção IV

DO USO INSTITUICIONAL DAS REDES SOCIAIS

Art. 19 A utilização de perfis institucionais mantidos em redes sociais, com o objetivo de prestar atendimento e serviços públicos, divulgar ou compartilhar informações do CFQ, será regida por normas internas específicas e deverá estar em consonância com esta POSIN e com os objetivos estratégicos do CFQ.

Art. 20 Os perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por equipes coordenadas pela Assessoria de Comunicação do CFQ.

Subseção V

DO USO DE COMPUTAÇÃO EM NUVEM

Art. 21 O uso de recursos de computação em nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, será regido por normas e procedimentos específicos, que deverão ser instituídos pela unidade responsável pelos ativos de tecnologia e atenderão às determinações desta POSIN.

Subseção VI

DOS DISPOSITIVOS MÓVEIS

Art. 22 O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito do CFQ deverá ser definido em norma específica, em conformidade com as diretrizes desta POSIN, orientações governamentais e legislações específicas em vigor, seguindo, no mínimo, as diretrizes gerais:

I. Toda informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, o CFQ, de acordo com norma legal vigente, reserva-se no direito de monitorar e registrar os acessos na rede interna do CFQ e à rede mundial de computadores;
II. O CFQ pode analisar e, se necessário, bloquear qualquer sítio, correio eletrônico, domínio ou aplicação armazenados na internet, visando a assegurar o cumprimento de sua POSIN.

Seção VI

DO CONTROLE DE ACESSO

Art. 23 O controle de acesso, no âmbito do CFQ, deverá ser definido em norma específica, em conformidade com as diretrizes desta POSIN, orientações governamentais e legislações específicas em vigor, seguindo, no mínimo, as diretrizes gerais:

I. O controle de acesso aos sistemas internos e externos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico.

II. As medidas de proteção serão adotadas para evitar que usuários dos ativos de tecnologia da informação não tenham permissão para instalar, remover, modificar, criar ou desenvolver softwares sem devida autorização.

III. Os usuários terão identificação única, pessoal e intransferível.

IV. O controle de acesso deverá considerar e respeitar o princípio do menor privilégio, pelo qual cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas atividades.

V. O CFQ poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários.

Seção VII

DA GESTÃO DE RISCO

Art. 24 O processo de Gestão de Risco deve ser baseado nas diretrizes e normativos externos, a exemplo da Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016, e internos, tais como a Portaria CFQ nº 71, de 11 de agosto de 2020, a qual dispõe sobre a institucionalização das Linhas de Defesa na Gestão de Riscos e Controle Interno no âmbito do CFQ e pela Portaria CFQ nº 72, de 11 de agosto de 2020, que dispõe sobre a institucionalização da Política de Gestão de Riscos no âmbito do CFQ e manual de gestão de riscos, anexo da Portaria 114, de 3 de dezembro de 2020.

Art. 25 Os riscos devem ser continuamente identificados, avaliados, tratados e monitorados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos; e

Art. 26 Os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação, no âmbito do CFQ.

Seção VIII

DA GESTÃO DE CONTINUIDADE

Art. 27 O processo da Gestão de Continuidade será regido pelo Plano de Continuidade de Negócios, conforme legislação específica, obedecendo as boas práticas internacionais e considerando os seguintes procedimentos:

I. Definir um plano estruturado que abranja os ativos mais importantes para a continuidade dos serviços primordiais do CFQ.
II. Os responsáveis e suas devidas funções dentro do Plano.
III. Definir as estratégias de recuperação e continuidade do negócio; e
IV. Desenvolver e implementar, no mínimo, Plano de Gerenciamento de Incidentes (PGI), Plano de Continuidade de Negócio (PCN), Plano de Continuidade Operacional (PCO), Plano de Recuperação do Negócio (PRN).

Art. 28 Todas as normas, planos e diretrizes da Gestão de Continuidade deverão ser testados, quando possível, e revisados periodicamente, com vistas na confidencialidade, integridade e disponibilidade dos ativos e dados de informação.

Seção IX

DA AUDITORIA E CONFORMIDADE

Art. 29 Para garantia de aplicação das diretrizes dessa POSIN, além de fixar normas e procedimentos complementares, o CFQ poderá:

I. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou sem fio e outros componentes da rede, de forma que a informação gerada por esses sistemas permita a sua rastreabilidade, identificando usuários e respectivos acessos efetuados.

II. Inspecionar fisicamente, a qualquer tempo, os ativos de rede de sua propriedade.

III. Realizar as práticas de segurança, com periodicidade mínima anual, para a verificação de conformidade das práticas de Segurança da Informação.

IV. Instalar sistemas de proteção, anti negação de serviço, preventivos ou repressivos para garantir a segurança das informações e do perímetro de acesso; e

V. Desinstalar, a qualquer momento, qualquer *software* ou sistema potencialmente danoso ou comprovadamente inseguro dentro dos ativos da propriedade do CFQ.

VI. Impedir o acesso à rede no caso de detecção de comportamento inseguro por dispositivo pessoal. Quando possível e com autorização do proprietário serão realizados procedimentos para adequar o equipamento aos padrões de segurança preconizados nesta POSIN e normas específicas.

CAPÍTULO III

DA ESTRUTURA PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 30 De forma a estruturar a gestão da segurança da informação, o CFQ designará:

I. O Gestor de Segurança da Informação;

II. O Comitê de Governança Digital com atribuições de Segurança da Informação; e

III. A Equipe de Tratamento e Respostas a Incidentes Cibernéticos - ETIR.

Parágrafo Único: Os responsáveis pelas funções, suas responsabilidades, o funcionamento e o escopo de atuação do comitê e da equipe de tratamento e respostas a incidentes cibernéticos serão definidos em Portaria específica.

Seção II

DAS RESPONSABILIDADES

Subseção I

DA GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Art. 31 Caberá a GETIC:

I. O credenciamento e descredenciamento de usuários;

II. A instalação e remoção dos equipamentos de TI;

III. A instalação e desinstalação de todos os softwares nos equipamentos do CFQ;

IV. A realização de auditoria (local ou remota);

V. A instalação de softwares de monitoramento;

VI. A autorização para conexão a redes externas.

Subseção II

DOS USUÁRIOS

Art. 32 Para o Conselho Federal de Química, são considerados usuários todos os colaboradores, estagiários, prestadores de serviços, conselheiros, diretoria, grupos de trabalho e terceiros que tenham acesso ao ambiente de tecnologia da informação. Os mesmos possuem as seguintes responsabilidades:

I. Ter pleno conhecimento e cumprir fielmente a POSIN, as normas e os procedimentos de segurança da informação do CFQ.

II. Zelar pela segurança de suas credenciais de acesso aos serviços e espaços físicos.

III. Solicitar esclarecimentos ao Comitê de Governança Digital em caso de dúvidas relacionadas à POSIN.

IV. Solicitar os serviços de TIC utilizando os canais definidos pela Gerência de Tecnologia da Informação.

V. Gerenciar os ativos sob sua responsabilidade e garantir que os documentos e arquivos, impressos ou digitais, equipamentos e recursos tecnológicos à sua disposição sejam utilizados, exclusivamente, para uso a serviço do CFQ.

VI. Acessar a rede de dados do CFQ somente após tomar ciência das normas de Segurança da Informação e assinar o Termo de Responsabilidade.

VII. Não instalar, remanejar e a remover de qualquer equipamento de TI sem a comunicação a Gerência de Tecnologia da Informação.

VIII. Não instalar ou desinstalar de software sem a comunicação a Gerência de Tecnologia da Informação.

IX. Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las.

X. Não se fazer passar por outro usuário usando sua identificação com login e senha de acesso.

XI. Preservar o sigilo das informações que teve acesso no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento.

XII. Não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso e respectivas senhas utilizadas no ambiente computacional do CFQ e de terceiros.

XIII. Responder, perante o CFQ, pelo uso indevido das suas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil.

XIV. Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente.

XV. Não transferir qualquer tipo de arquivo que pertença ao CFQ para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente.

XVI. Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço não são permitidos na rede computacional do CFQ.

XVII. Assinar o Termo de Responsabilidade - Anexo I e declarar, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta POSIN.

XVIII. Fazer uso das diretrizes de mesa limpa e tela protegida para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho.

XIX. Devolver as informações ou documentos sigilosos que estejam em seu poder; e

XX. Excluir todos dados digitais que porventura foram armazenados em seus equipamentos eletrônicos e softwares de uso particular e e-mails pessoais.

Subseção III

DOS GESTORES DAS UNIDADES ORGANIZACIONAIS

Art. 33 Os Gestores do CFQ são responsáveis por:

I. Cumprir e fazer cumprir esta POSIN.

II. Ter postura exemplar em relação à segurança da informação para servir como modelo de conduta para os colaboradores sob sua gestão.

III. Exigir das entidades relacionadas, prestadores de serviços ou outras entidades externas, a assinatura do Termo de Confidencialidade ou Responsabilidade referente às informações as quais terão acesso; e

IV. Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade.

CAPÍTULO IV

DAS PENALIDADES

Art. 34 As pessoas submetidas a POSIN que apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, arquivo ou programa de computador ou, de forma indevida ou não autorizada, fizer uso dos equipamentos de informática, bem como praticar ato em desacordo com os termos da presente política, ficam sujeitas às punições cabíveis nos termos da lei.

Art. 35 O infrator deverá ser notificado e a ocorrência da transgressão deverá ser imediatamente comunicada ao seu chefe imediato, à gerência executiva, à Gestão Estratégica de Pessoas, caso seja servidor, e, não sendo, a comunicação deve ser diretamente à Presidência.

Art. 36 As pessoas submetidas a POSIN que tomarem conhecimento de qualquer incidente de segurança da informação, devem informar o ocorrido imediatamente à administração da rede, por meio da abertura de chamado ou qualquer outro meio disponível.

Seção I

DA VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 37 As ações que violem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de segurança da informação serão devidamente apuradas, sendo cabíveis aos responsáveis a comunicação de descumprimento conforme previsão do anterior.

Parágrafo único: O comunicado permanecerá arquivado junto à GEPES – Gestão Estratégica de Pessoas Departamento de Recursos Humanos, em se tratando de servidor.

Seção II

CAPÍTULO V

DA DIVULGAÇÃO E ATUALIZAÇÃO

Art. 38 Esta Política e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários e disponibilizadas no portal do CFQ, sendo consideradas um documento de relevante interesse público.

Art. 39 Esta Política de Segurança da Informação deverá ser revisada a cada 2 (dois) anos ou sempre que se fizer necessário, não excedendo ao período máximo de 4 (quatro) anos, a contar da data de sua publicação.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 40 Os casos omissos desta POSIN serão resolvidos pelo Comitê de Governança Digital do CFQ.

Art. 41 Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ter ampla divulgação a todos os colaboradores, estagiários, prestadores de serviço, conselheiros e diretoria do CFQ quando de sua admissão.

Art. 42 O Conselho Federal de Química tem o prazo de 24 (vinte e quatro) meses para implementação de todas as ações propostas por esta Política de Segurança da Informação.

ANEXO I - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CFQ

TERMO DE RESPONSABILIDADE

Eu, _____, CPF n° _____ na qualidade de usuário dos recursos de Tecnologia de Informação disponibilizados pelo Conselho Federal de Química, declaro estar ciente e concordar com a Política de Segurança da Informação.

Declaro assumir toda e qualquer responsabilidade de controle, guarda e conservação dos equipamentos relacionados nesta política, cuja responsabilidade tenha sido a mim atribuída. Tenho ciência de que a retirada de equipamentos para manutenção, bem como a instalação de qualquer software, deverá ser feita por

pessoas autorizadas pela Gerência de Tecnologia da Informação, devidamente identificados.

Declaro estar ciente de que os arquivos, documentos e e-mails que se encontram em computadores e/ou servidores de rede do CFQ são de propriedade do CFQ. Portanto, ao desligar-me do Conselho, não poderei fazer cópias de documentos, ou de softwares licenciados para o CFQ.

Declaro estar ciente de que devo gravar os arquivos produzidos e manipulados por mim na rede de computadores do CFQ e de que não existe rotina de backup para arquivos particulares nas estações de trabalho e no armazenamento em nuvem.

Declaro ainda reconhecer que é meu dever garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.

Brasília, ___de_____de_____

_____

Nome Completo

Política de Segurança da Informação