DIÁRIO OFICIAL DA UNIÃO

Publicado em: 18/02/2026 | Edição: 32 | Seção: 1 | Página: 266

Órgão: Entidades de Fiscalização do Exercício das Profissões Liberais/Conselho Federal de Fisioterapia e Terapia Ocupacional

RESOLUÇÃO-COFFITO Nº 648, DE 13 DE FEVEREIRO DE 2026

Aprova a Política de Segurança da Informação (PSI) do Conselho Federal de Fisioterapia e Terapia Ocupacional - COFFITO.

O PLENÁRIO DO CONSELHO FEDERAL DE FISIOTERAPIA E TERAPIA OCUPACIONAL - COFFITO, mediante atribuições que lhe são conferidas pela Lei nº 6.316, de 17 de dezembro de 1975, e conforme o deliberado na 41ª Reunião Plenária Ordinária, realizada no dia 17 de dezembro de 2025, na sede do COFFITO, situada no SIA, Trecho 17, Lote 810, Parque Ferroviário de Brasília, Brasília/DF, CEP: 71200-260;

Considerando o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), que estabelece a publicidade como preceito geral e o sigilo como exceção, impondo aos órgãos públicos o dever de assegurar a gestão, a proteção e o acesso adequado às informações sob sua responsabilidade;

Considerando o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), que disciplina o tratamento de dados pessoais com vistas a proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural;

Considerando o Decreto nº 12.572, de 4 de agosto de 2025, que instituiu a Política Nacional de Segurança da Informação, especialmente no que se refere à implementação de ações estruturadas de proteção da informação no âmbito da Administração Pública;

Considerando o Decreto nº 12.573, de 4 de agosto de 2025, que instituiu a Estratégia Nacional de Cibersegurança;

Considerando as Instruções Normativas GSI/PR nº 1/2020 e nº 3/2021, que estabelecem diretrizes, princípios e responsabilidades para a Gestão de Segurança da Informação no âmbito dos órgãos e entidades da Administração Pública Federal;

Considerando as boas práticas consagradas nas normas ABNT NBR ISO/IEC 27001:2022, 27002:2022 e demais normas da série 27000 aplicáveis, que orientam a implementação de sistemas de gestão de segurança da informação baseados em riscos e controles estruturados;

Considerando o Acórdão nº 1372/2025 - Plenário/TCU, que determinou aos Conselhos de Fiscalização Profissional a adoção de medidas formais de governança, gestão de riscos e segurança da informação, incluindo a instituição de Política de Segurança da Informação (PSI);

Considerando que o COFFITO recebe, produz, utiliza e armazena informações em formatos físicos e digitais, as quais devem permanecer íntegras, disponíveis, autênticas e, quando aplicável, sob regime de confidencialidade e sigilo, de modo a assegurar a continuidade das atividades institucionais;

Considerando que tais informações estão sujeitas a riscos decorrentes de incidentes naturais, falhas técnicas, vulnerabilidades cibernéticas, acessos indevidos, erros operacionais, extravio, perda, destruição ou divulgação não autorizada, exigindo a adoção de controles adequados de prevenção, detecção, resposta e recuperação;

Considerando o crescimento de incidentes cibernéticos em âmbito nacional e internacional, que demandam processos de trabalho estruturados e contínuos voltados à governança, à gestão de riscos e à proteção da informação;

Considerando a importância de estabelecer diretrizes, regras e responsabilidades internas relacionadas à segurança da informação, promovendo a cultura organizacional de proteção de dados e de uso seguro e responsável dos recursos tecnológicos;

Considerando a necessidade de estabelecer diretrizes e padrões que assegurem a proteção das informações do COFFITO, em meios digitais e físicos, de forma controlada, eficiente e segura, garantindo sua integridade, confidencialidade, disponibilidade, autenticidade e privacidade, em conformidade com as legislações vigentes, com as boas práticas de governança, gestão de riscos e segurança da informação, de modo a atender às demandas institucionais, aos profissionais de Fisioterapia e de Terapia Ocupacional e à sociedade;

Considerando a Portaria-COFFITO nº 303/2024, que instituiu a Comissão Gestora de Dados, definiu os agentes de tratamento de dados pessoais no âmbito do COFFITO e atribuiu ao Ouvidor a função de Encarregado pelo Tratamento de Dados Pessoais, com apoio do Departamento Jurídico; resolve:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO COFFITO

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

Do Escopo

Art. 1º Fica instituída a Política de Segurança da Informação (PSI), que tem por objetivo estabelecer princípios, diretrizes e responsabilidades para garantir a proteção das informações sob a custódia do Conselho Federal de Fisioterapia e Terapia Ocupacional (COFFITO).

Art. 2º Esta Política aplica-se a todos os processos, sistemas, serviços e ativos de informação do COFFITO, independentemente do meio ou forma de armazenamento.

Art. 3º O disposto neste instrumento aplicar-se-á a todos os conselheiros, empregados, assessores, estagiários, jovens aprendizes e, quando pertinente, a terceiros e a quaisquer outras pessoas que prestem serviços ao COFFITO e que tenham acesso a qualquer informação ou comunicação, 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.

§ 1º Os contratos, convênios e instrumentos congêneres conterão cláusulas específicas que imponham aos contratados e convenentes a obrigação de observarem o disposto nesta PSI, para o exercício de suas atividades no âmbito do COFFITO.

§ 2º Os termos aditivos dos contratos, convênios e instrumentos congêneres, celebrados após a aprovação desta PSI, deverão incluir cláusulas específicas que imponham aos contratados e convenentes a obrigação de observarem o disposto nesta Política.

Seção II

Dos Conceitos e Definições

Art. 4º Os conceitos e definições adotados nesta Política têm como referência prioritária o Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, podendo ser complementados por normas técnicas, guias oficiais e boas práticas reconhecidas, quando necessário à adequada compreensão do texto.

I - Segurança da Informação: ações que têm como objetivo viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

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

III - Ativos de Informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

IV - Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

V - Integridade: propriedade que assegura que a informação não seja modificada ou destruída de forma não autorizada ou acidental;

VI - Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados;

VII - Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

VIII - Termo de Responsabilidade: termo assinado pelo usuário, concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

IX - Risco: possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

X - Ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

XI - Vulnerabilidade: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha;

XII - Tratamento da Informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XIII - Gestão de Riscos em Segurança da Informação: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

XIV - Gestão de Incidentes Cibernéticos: processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação;

XV - Gestão de Segurança da Informação: processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

XVI - Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do COFFITO;

XVII - Comitê Interno de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do COFFITO;

XVIII - Gestão de Mudanças nos Aspectos Relativos à Segurança da Informação: processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;

XIX - Gestão de Continuidade em Segurança da Informação: processo que identifica ameaças potenciais para o COFFITO e os possíveis impactos nas funções e processos institucionais essenciais, caso essas ameaças se concretizem, fornecendo estrutura para o desenvolvimento da resiliência organizacional;

XX - Usuário de Informação: pessoa física autorizada pelo COFFITO a acessar seus ativos de informação, incluindo empregados públicos, conselheiros, membros de comissões, prestadores de serviços, estagiários ou quaisquer outros colaboradores, ainda que sem vínculo empregatício, sujeita às responsabilidades previstas nesta Política e nas normas internas aplicáveis;

XXI - Custodiante da Informação: pessoa física ou unidade organizacional que detenha responsabilidade formal por proteger a informação sob sua guarda e por aplicar controles de segurança, conforme as exigências comunicadas pelo proprietário da informação e pelas normas internas aplicáveis;

XXII - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

XXIII - Trilha de Auditoria: registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento;

XXIV - Dado Pessoal: informação relacionada à pessoa natural identificada ou identificável;

XXV - Titular do Dado: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XXVI - Criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

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

XXVIII - Direito de Acesso: privilégio associado a um cargo, pessoa ou processo, para ter acesso a um ativo;

XXIX - Backup: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

XXX - Dispositivos Móveis: equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: e-books, notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HD externo, e cartões de memória;

XXXI - Recurso Criptográfico: sistema, programa, processo, equipamento isolado ou em rede, que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXXII - Computação em Nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

XXXIII - Metadados: representam "dados sobre dados", fornecendo os elementos necessários para compreender as informações. São registros estruturados que oferecem uma descrição concisa do conteúdo armazenado, possibilitando sua localização, gerenciamento, interpretação e preservação ao longo do tempo. Desempenham papel fundamental na gestão da informação, pois viabilizam o processamento, a atualização e a consulta dos registros. Informações acerca da forma como foram criados ou derivados, do ambiente em que se encontram ou se encontravam, das modificações realizadas, entre outros aspectos, são obtidas por meio dos metadados;

XXXIV - Spam: prática, muitas vezes associada a atividades maliciosas como phishing e disseminação de malware. A ênfase é na natureza não solicitada e no potencial de risco à segurança;

XXXV - Phishing: é um tipo de fraude na qual o golpista tenta obter informações pessoais e financeiras do usuário, combinando meios técnicos e engenharia social. Do inglês "fishing", é uma analogia criada pelos golpistas, em que "iscas" (mensagens eletrônicas) são usadas para "pescar" informações de usuários;

XXXVI - Plano de Continuidade em Segurança da Informação: documento que estabelece diretrizes, procedimentos e informações necessárias para assegurar a continuidade das atividades institucionais críticas e a proteção dos ativos de informação essenciais do COFFITO, em nível previamente definido, em situações de incidentes ou interrupções relevantes;

XXXVII - Plano de Recuperação de Serviços Essenciais: documento que define os procedimentos e as informações necessárias para o restabelecimento controlado e progressivo dos serviços e das atividades institucionais críticas do COFFITO após a ocorrência de incidentes ou interrupções.

Seção III

Dos Objetivos

Art. 5º A Política de Segurança da Informação do COFFITO tem por objetivos específicos:

I - alinhar a gestão da segurança da informação às normas nacionais e internacionais aplicáveis, em especial à Política Nacional de Segurança da Informação (Decreto nº 12.572/2025), à Estratégia Nacional de Cibersegurança (Decreto nº 12.573/2025), às Instruções Normativas GSI/PR, à Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018), à Lei de Acesso à Informação - LAI (Lei nº 12.527/2011) e às normas ABNT NBR ISO/IEC 27001:2022 e 27002:2022;

II - apoiar a conformidade em auditorias internas e externas, em alinhamento com a Controladoria Interna do COFFITO, a Controladoria-Geral da União (CGU), o Tribunal de Contas da União (TCU) e a Autoridade Nacional de Proteção de Dados (ANPD);

III - proteger a imagem institucional e a confiança pública no COFFITO, prevenindo riscos reputacionais decorrentes de incidentes de segurança ou falhas de proteção da informação;

IV - promover a cultura de segurança da informação no âmbito do COFFITO, mediante capacitação contínua, campanhas de conscientização e disseminação de boas práticas de uso dos ativos de informação;

V - implementar e manter o processo de gestão de riscos de segurança da informação, abrangendo identificação, análise, avaliação, tratamento e monitoramento permanente de ameaças e vulnerabilidades;

VI - proteger as informações institucionais produzidas ou recebidas pelo COFFITO, em qualquer formato ou meio, assegurando sua confidencialidade, integridade, autenticidade e disponibilidade;

VII - disciplinar o tratamento e a resposta a incidentes de segurança, garantindo comunicação tempestiva, mitigação de impactos, investigação adequada e prevenção de recorrências;

VIII - assegurar interoperabilidade segura com os Conselhos Regionais de Fisioterapia e Terapia Ocupacional (CREFITOs) e com demais órgãos públicos, mediante padrões e controles de segurança consistentes;

IX - garantir a continuidade dos serviços críticos do COFFITO, por meio de estratégias, planos de contingência e exercícios periódicos de recuperação e resiliência;

X - assegurar a rastreabilidade e a auditoria das informações, garantindo registro, monitoramento e responsabilização pelos acessos e operações realizadas em sistemas, redes e documentos;

XI - garantir a inclusão de requisitos de segurança da informação em contratos, convênios e demais instrumentos firmados pelo COFFITO, de forma a estender a proteção também a fornecedores e terceiros que tratem informações da Autarquia;

XII - harmonizar a proteção de dados pessoais e o acesso à informação, assegurando o cumprimento da LGPD e da LAI de forma integrada, com a publicidade como regra e o sigilo como exceção, respeitada a devida classificação da informação;

XIII - fortalecer a governança institucional e a credibilidade pública do COFFITO, promovendo transparência, conformidade normativa e confiança dos profissionais e da sociedade.

Seção IV

Dos Princípios e Diretrizes

Art. 6º As ações de segurança da informação do COFFITO são norteadas pelos princípios constitucionais e administrativos que regem a Administração Pública, bem como pelos seguintes princípios:

I - Disponibilidade: assegurar que as informações, sistemas e serviços estejam acessíveis e utilizáveis quando necessários por usuários autorizados;

II - Integridade: preservar a exatidão, completude e confiabilidade das informações, prevenindo alterações, destruições ou perdas não autorizadas ou acidentais;

III - Confidencialidade: assegurar que a informação seja acessada apenas por usuários, sistemas ou entidades devidamente autorizados;

IV - Autenticidade: assegurar a comprovação da identidade, origem e autoria das informações, bem como de suas alterações;

V - Não Repúdio: impedir que autores de ações, comunicações ou transações neguem posteriormente sua participação;

VI - Privacidade e Sigilo: proteger dados pessoais e informações sensíveis, preservando os direitos fundamentais previstos na Constituição Federal, na Lei Geral de Proteção de Dados e nas demais legislações aplicáveis;

VII - Transparência: assegurar publicidade como regra, e sigilo como exceção, conforme a LAI e regulamentações internas;

VIII - Rastreabilidade: possibilitar a identificação e o registro de acessos, alterações e operações realizadas em informações e sistemas, de forma a permitir auditoria, responsabilização e controle;

IX - Proporcionalidade: adotar medidas de segurança de forma equilibrada, de modo a proteger as informações sem comprometer a eficiência administrativa ou criar restrições excessivas ao interesse público;

X - Economicidade: aplicar os recursos destinados à segurança da informação de forma eficiente, racional e alinhada aos objetivos institucionais;

XI - Educação e Comunicação: promover cultura permanente de segurança da informação por meio de capacitação, sensibilização e comunicação interna.

Art. 7º As ações de segurança da informação devem:

I - alinhar-se aos objetivos estratégicos e aos planos institucionais do COFFITO;

II - ser tratadas de forma integrada, respeitando as especificidades das unidades;

III - ser proporcionais aos riscos existentes, ao ambiente, ao valor e à criticidade da informação;

IV - priorizar a prevenção de incidentes e a mitigação de vulnerabilidades.

Art. 8º A gestão de segurança da informação deve ser contínua, dinâmica e alinhada à evolução tecnológica, considerando fatores internos e externos que possam impactar o alcance dos objetivos institucionais.

Art. 9º Os investimentos em segurança da informação devem ser dimensionados de acordo com o valor do ativo, a sensibilidade da informação envolvida e os riscos potenciais para o COFFITO.

Art. 10. Toda informação gerada, custodiada, manipulada, utilizada ou armazenada no COFFITO compõe seus ativos de informação e deve ser protegida conforme normas vigentes.

Parágrafo único. As informações que trafeguem pelo ambiente computacional do COFFITO estão sujeitas a monitoramento e auditoria, observados os limites legais.

Art. 11. Pessoas e sistemas devem operar com menor privilégio e mínimo acesso necessário ao desempenho de suas atividades.

Parágrafo único. O acesso aos recursos de tecnologia da informação exige assinatura de Termo de Responsabilidade, preferencialmente eletrônico, com ciência das obrigações e penalidades decorrentes.

Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do COFFITO, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Parágrafo único. Os usuários de informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a mitigar possíveis riscos à segurança da informação.

Art. 13. Os contratos de prestação de serviços, convênios e instrumentos congêneres firmados pelo COFFITO deverão incluir cláusulas específicas que assegurem a observância desta Política e das normas complementares de segurança da informação.

Parágrafo único. Quando houver tratamento de dados pessoais por terceiros em nome do COFFITO, estes atuarão como operadores, devendo observar integralmente esta Política, a LGPD e as orientações do COFFITO, na condição de controlador.

CAPÍTULO II

DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Seção I

Das Disposições Gerais

Art. 14. As informações produzidas, recebidas, armazenadas, tratadas ou custodiadas pelo COFFITO deverão ser classificadas de acordo com seu grau de sensibilidade, criticidade, valor institucional e requisitos legais, observadas as diretrizes desta Política e das normas complementares.

Art. 15. A classificação da informação tem por finalidade:

I - assegurar níveis adequados de proteção à confidencialidade, integridade, disponibilidade e autenticidade das informações;

II - orientar a aplicação proporcional de controles de segurança;

III - subsidiar decisões de acesso, armazenamento, compartilhamento, retenção e descarte;

IV - harmonizar a proteção da informação com a publicidade como regra e o sigilo como exceção, nos termos da LAI.

Seção II

Dos Níveis de Classificação da Informação

Art. 16. As informações do COFFITO deverão ser classificadas, no mínimo, nos seguintes níveis:

I - Informação Pública: informação cujo acesso é franqueado ao público em geral, nos termos da Lei nº 12.527/2011, ressalvadas as hipóteses legais de restrição;

II - Informação de Uso Interno: informação destinada ao uso exclusivo no âmbito interno do COFFITO, cujo acesso é restrito a usuários autorizados;

III - Informação Restrita ou Sigilosa: informação cujo acesso é limitado, em razão de seu conteúdo sensível, estratégico ou protegido por legislação específica, incluindo dados pessoais, dados sensíveis e informações protegidas por sigilo legal.

Parágrafo único. A classificação da informação deverá observar a legislação vigente, em especial a Lei de Acesso à Informação, a Lei Geral de Proteção de Dados Pessoais e demais normas aplicáveis.

Art. 17. A classificação da informação deverá considerar, no mínimo:

I - o impacto institucional em caso de acesso, alteração, perda ou divulgação indevida;

II - a presença de dados pessoais ou dados pessoais sensíveis, nos termos da LGPD;

III - requisitos legais, regulatórios ou contratuais aplicáveis;

IV - o valor estratégico, operacional ou histórico da informação.

Seção III

Da Responsabilidade pela Classificação

Art. 18. A responsabilidade pela classificação da informação compete:

I - ao gestor da unidade que produziu ou detém a informação;

II - ao custodiante da informação, no âmbito de suas atribuições;

III - ao Gestor de Segurança da Informação, quando necessário, para fins de orientação técnica.

Art. 19. Os níveis de classificação da informação, bem como os respectivos critérios, controles e responsabilidades, serão definidos em norma complementar específica, aprovada conforme a governança de segurança da informação do COFFITO.

Art. 20. A classificação da informação deverá ser registrada, sempre que aplicável, nos sistemas, documentos ou metadados correspondentes, de forma a permitir sua adequada identificação, tratamento e controle.

Parágrafo único. A responsabilidade pela correta classificação da informação é do gestor do processo ou do custodiante do ativo de informação, conforme definido nas normas internas.

Seção IV

Da Revisão e Reavaliação da Classificação

Art. 21. A classificação da informação deverá ser revisada periodicamente ou sempre que houver alteração relevante no contexto institucional, tecnológico ou legal.

Art. 22. A desclassificação ou reclassificação da informação deverá observar os mesmos critérios técnicos e legais adotados para a classificação inicial.

Seção V

Das Normas Complementares

Art. 23. Os critérios detalhados, procedimentos operacionais, fluxos e responsabilidades específicos relativos à classificação da informação serão disciplinados em normas complementares, manuais ou procedimentos internos, aprovados conforme a governança de segurança da informação do COFFITO.

Parágrafo único. As normas complementares deverão observar os princípios e diretrizes desta Política, podendo ser atualizadas sempre que necessário, sem prejuízo da validade desta PSI.

CAPÍTULO III

DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I

Da Estrutura de Governança de Segurança da Informação

Art. 24. A Gestão de Segurança da Informação no COFFITO é estruturada pelas seguintes instâncias e papéis:

I - Alta Administração;

II - Comitê Interno de Segurança da Informação;

III - Gestor de Segurança da Informação;

IV - Usuários de Informação.

Parágrafo único. Para fins desta Política, considera-se Alta Administração o conjunto formado pelo Plenário e pela Diretoria do COFFITO, nos termos da legislação e do Regimento Interno.

Seção II

Das Competências e Arranjos Operacionais

Art. 25. Compete à Alta Administração:

I - designar, dentre os empregados efetivos do COFFITO, o Gestor de Segurança da Informação, assegurando que a escolha recaia em profissional com perfil, competência técnica e autonomia compatíveis com a responsabilidade do cargo;

II - instituir o Comitê Interno de Segurança da Informação;

III - assegurar mecanismos adequados para a prevenção, o tratamento e a resposta a incidentes de segurança da informação e incidentes cibernéticos, observada a capacidade institucional do COFFITO e o disposto em normas complementares;

IV - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

V - patrocinar, priorizar e assegurar os recursos humanos, tecnológicos, financeiros e organizacionais necessários ao desenvolvimento, implementação, manutenção e melhoria contínua da Gestão de Segurança da Informação do COFFITO, garantindo que as ações e decisões relacionadas ao tema recebam o tratamento com a relevância e prioridade compatíveis com sua importância para a governança institucional e a credibilidade da Autarquia;

VI - aprovar a Política de Segurança da Informação do COFFITO, bem como suas alterações e atualizações, zelando pela sua conformidade com as legislações vigentes, com as recomendações dos órgãos de controle e com as melhores práticas nacionais e internacionais em segurança da informação;

VII - apoiar e promover a ampla divulgação da Política e das normas internas de segurança da informação, assegurando que tais instrumentos sejam disponibilizados de forma clara, acessível e tempestiva a todos os empregados, usuários, prestadores de serviço e demais partes interessadas, de modo a garantir o conhecimento, a adesão e a efetiva aplicação de suas diretrizes;

VIII - fomentar a cultura organizacional de segurança da informação, estimulando a conscientização, o engajamento e o compromisso de todos os níveis hierárquicos com a proteção das informações sob responsabilidade do COFFITO;

IX - supervisionar a execução da Política de Segurança da Informação, mediante análise de relatórios, auditorias, indicadores de desempenho e planos de ação;

X - garantir a integração da gestão de riscos de segurança da informação à governança de riscos institucional, assegurando planos de continuidade das atividades institucionais críticas e resposta a incidentes;

XI - apreciar e acompanhar os resultados dos trabalhos de auditoria relacionados à gestão de segurança da informação;

XII - determinar a adoção das medidas administrativas e corretivas cabíveis, nos casos de violação da segurança da informação, observadas a legislação vigente, as normas internas aplicáveis e o devido processo legal;

XIII - exercer outras competências relacionadas à segurança da informação e à proteção de dados pessoais que, por sua relevância institucional, lhe sejam atribuídas pela legislação, por esta Política ou por deliberação da própria Alta Administração.

Art. 26. O Comitê Interno de Segurança da Informação possui caráter consultivo, propositivo e estratégico, competindo-lhe:

I - assessorar a Alta Administração;

II - propor diretrizes, prioridades e planos de ação;

III - acompanhar resultados e indicadores;

IV - analisar e propor normas internas de segurança da informação, submetendo-as à aprovação da Alta Administração.

§ 1º O Comitê não executa atividades operacionais rotineiras.

§ 2º A composição, estrutura, recursos e funcionamento do Comitê Interno de Segurança da Informação será definido em ato administrativo próprio, de acordo com a legislação vigente.

§ 3º O Comitê Interno de Segurança da Informação deverá registrar atas de suas reuniões e manter arquivados planos de ação, pareceres e relatórios técnicos, observados os critérios de classificação da informação, assegurando a rastreabilidade, a transparência e a publicidade interna de suas deliberações.

Art. 27. Compete ao Gestor de Segurança da Informação coordenar, supervisionar e acompanhar a implementação da Política de Segurança da Informação, atuando como instância técnica de articulação entre as unidades, sem prejuízo das atribuições operacionais dos setores responsáveis.

Parágrafo único. As atividades operacionais, técnicas e executivas serão desempenhadas pelas unidades competentes, cabendo ao Gestor de Segurança da Informação o acompanhamento, a orientação técnica e a consolidação das informações necessárias à governança da segurança da informação.

Art. 28. A prevenção, o tratamento e a resposta a incidentes de segurança da informação serão realizados por meio de arranjos organizacionais flexíveis, observada a capacidade institucional do COFFITO e conforme definido em normas complementares.

§ 1º A constituição de equipe específica para o tratamento de incidentes poderá ocorrer por designação temporária, ato administrativo ou grupo de trabalho, dispensada a criação de estrutura permanente exclusiva.

§ 2º A forma de atuação, os fluxos de resposta e os níveis de escalonamento serão definidos em norma complementar, observada a capacidade institucional e o princípio da proporcionalidade.

Art. 29. Esta Política observa os princípios e diretrizes da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no que couber à proteção da informação e à segurança dos ativos informacionais, mantendo-se autônoma em relação à Política de Privacidade, a ser instituída em ato normativo próprio.

§ 1º As atribuições relacionadas ao tratamento de dados pessoais, à interação com titulares e à comunicação com a Autoridade Nacional de Proteção de Dados (ANPD) competem ao Encarregado de Dados, designado nos termos da Portaria-COFFITO nº 303/2024, com apoio da Comissão Gestora de Dados.

§ 2º Compete ao Gestor de Segurança da Informação atuar de forma colaborativa e técnica, fornecendo subsídios relacionados à segurança da informação, à prevenção de incidentes e à mitigação de riscos, sem prejuízo da autonomia e das atribuições próprias do Encarregado de Dados.

Art. 30. Compete aos Usuários de Informação:

I - conhecer e cumprir esta Política e as normas internas correlatas;

II - solicitar esclarecimentos ao Comitê Interno de Segurança da Informação em caso de dúvidas relacionadas à PSI;

III - utilizar ativos e recursos somente no interesse institucional;

IV - acessar a rede de dados do COFFITO somente após tomar ciência das normas de Segurança da Informação e assinar o Termo de Responsabilidade;

V - utilizar as informações arquivísticas digitais e impressas disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do COFFITO exclusivamente para o interesse do serviço;

VI - 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;

VII - não tentar obter acesso à informação cujo grau de sigilo não seja compatível com seu nível de acesso ou necessidade de conhecer;

VIII - não se fazer passar por outro usuário usando a identificação com login e senha de acesso;

IX - no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;

X - não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional do COFFITO por terceiros;

XI - responder perante o COFFITO pelo uso indevido das suas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a justiça, no âmbito penal e civil;

XII - não acessar, transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

XIII - não transferir qualquer tipo de arquivo que pertença ao COFFITO para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

XIV - utilizar as credenciais de acesso, login e senha, e os recursos computacionais, em conformidade com a PSI do COFFITO e procedimentos estabelecidos em normas específicas do Conselho;

XV - fazer uso da política 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.

CAPÍTULO IV

DOS PROCESSOS

Art. 31. A Gestão de Segurança da Informação no âmbito do COFFITO será composta, no mínimo, pelos seguintes processos:

I - tratamento da informação;

II - segurança física e do ambiente;

III - gestão de incidentes de segurança da informação;

IV - inventário, mapeamento e gestão de ativos de informação;

V - gestão do uso de recursos operacionais e de comunicações institucionais;

VI - controles de acesso;

VII - gestão de riscos de segurança da informação;

VIII - gestão de continuidade de negócios em segurança da informação;

IX - gestão de mudanças com impacto em segurança da informação;

X - avaliação de conformidade em segurança da informação.

§ 1º O Comitê Interno de Segurança da Informação poderá propor a criação de outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e diretrizes desta Política.

§ 2º Para cada processo previsto no caput deverão ser elaboradas normas, procedimentos, orientações ou manuais específicos, aprovados conforme a governança de segurança da informação do COFFITO, com vistas a disciplinar sua aplicação e padronizar condutas.

§ 3º As normas e instrumentos complementares integrarão a arquitetura de segurança da informação do COFFITO, devendo observar esta PSI e ser revisados periodicamente, quando necessário, em face da evolução de riscos, tecnologias e diretrizes institucionais.

Art. 32. As normas, procedimentos ou manuais complementares de que trata o § 2º do artigo anterior deverão contemplar, no mínimo:

I - requisitos de conformidade com a LGPD, LAI e demais normativos aplicáveis, inclusive orientações da ANPD;

II - critérios de classificação da informação e definição de controles proporcionais à sensibilidade, criticidade e riscos;

III - diretrizes de controle de acesso, credenciamento, segregação de funções, rastreabilidade e uso do princípio do menor privilégio;

IV - regras de uso aceitável de recursos institucionais de comunicação e tecnologia (e-mail, internet, mídias sociais, dispositivos móveis, nuvem e similares);

V - diretrizes e fluxos para gestão e resposta a incidentes, incluindo comunicação de incidentes relevantes aos titulares e à ANPD quando cabível;

VI - metodologia de gestão de riscos e continuidade de negócios aplicáveis aos ativos de informação;

VII - parâmetros de auditoria, monitoramento e avaliação de conformidade, incluindo registros e trilhas de auditoria.

§ 1º As unidades organizacionais deverão cooperar com verificações internas de conformidade em segurança da informação, quando demandadas pela governança de SI.

§ 2º Os processos, projetos, produtos e serviços do COFFITO deverão observar requisitos de segurança da informação e proteção de dados desde sua concepção, sempre que aplicável.

CAPÍTULO V

DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

Art. 33. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo COFFITO para acesso, guarda ou divulgação de conteúdo incompatível com o ambiente institucional, que viole direitos autorais ou infrinja a legislação vigente.

Art. 34. É proibido o uso ou a instalação de recursos de tecnologia da informação não homologados ou não autorizados pelo COFFITO.

Art. 35. É proibido compartilhar ou divulgar mecanismos de autenticação e autorização de uso pessoal e intransferível fornecidos pelo COFFITO.

Art. 36. É vedado explorar, testar, divulgar ou se aproveitar de falhas, vulnerabilidades ou fragilidades nos sistemas, redes ou ativos de informação do COFFITO. Qualquer vulnerabilidade identificada deverá ser comunicada imediatamente ao Setor de Tecnologia da Informação e ao Gestor de Segurança da Informação.

Art. 37. O COFFITO promoverá ações contínuas de conscientização e capacitação em segurança da informação e proteção de dados adequadas aos papéis e responsabilidades dos usuários.

Art. 38. Denúncias ou comunicações de violação a esta Política deverão ser direcionadas ao Gestor de Segurança da Informação, sem prejuízo dos canais institucionais cabíveis.

Art. 39. O cumprimento desta Política e de seus instrumentos complementares será acompanhado pelo Gestor de Segurança da Informação, com apoio do Setor de Tecnologia da Informação, por meio de avaliações de conformidade, monitoramento e relatórios periódicos ao Comitê Interno de Segurança da Informação, que poderá propor melhorias à Alta Administração.

Art. 40. A inobservância desta Política sujeita o infrator às sanções administrativas cabíveis, conforme legislação vigente, assegurados o contraditório e a ampla defesa, sem prejuízo de eventual responsabilização civil e penal.

Art. 41. Esta Política será revisada periodicamente, preferencialmente a cada 2 (dois) anos, e obrigatoriamente em até 4 (quatro) anos, ou sempre que ocorrerem alterações relevantes:

I - na legislação aplicável ou diretrizes governamentais;

II - no ambiente tecnológico, organizacional ou institucional;

III - por identificação de falhas, riscos ou não conformidades;

IV - por recomendações de órgãos de controle ou auditorias;

V - pela evolução das ameaças ou maturidade institucional.

Parágrafo único. A revisão será coordenada pelo Comitê Interno de Segurança da Informação, com apoio do Gestor de Segurança da Informação, e submetida à Alta Administração.

Art. 42. Casos omissos relacionados à segurança da informação, inclusive aqueles que envolvam dados pessoais, serão analisados à luz da legislação vigente.

Art. 43. Esta Resolução entra em vigor na data de sua publicação.

VINÍCIUS MENDONÇA ASSUNÇÃO
Diretor-Secretário

SANDROVAL FRANCISCO TORRES
Presidente do Conselho