Conselho Federal de Biologia – CFBio

Política de Segurança da Informação - PSI

Brasília
2026

Política de Segurança da Informação - PSI

Diretoria

ALCIONE RIBEIRO DE AZEVEDO
Presidente

JOSÉ ROBERTO FEITOSA SILVA
Vice-Presidente

SANTIAGO VALENTIM DE SOUZA
Conselheiro Tesoureiro

ANDRÉA GRACIANO DOS SANTOS FIGUEIREDO
Conselheira Secretária

Elaboração

FREDSON DIAS DE ANDRADE
Chefe do Setor de Tecnologia da Informação

RUBEN ISAAC DIAS DA SILVA
Analista de Sistemas

Coordenação de Produção

ALEXANDRE SCHOLTZ
Chefe da Assessoria de Comunicação

ÉMERSON VINICIUS ALMEIDA SANTOS
Direção de arte e design

STEFANNY VIEIRA GALVÃO
YASMIM REGIS ALMEIDA SILVA SANTOS
Estagiárias de publicidade

Política de Segurança da Informação - PSI

Conselho Federal de Biologia

Sumário

Política de Segurança da Informação - PSI

1 - Introdução

A informação constitui ativo essencial ao funcionamento do Conselho Federal de Biologia - CFBio, sendo indispensável à execução de suas atividades institucionais e à prestação de serviços à sociedade.
As informações do CFBio encontram-se sujeitas a diversos riscos, tais como acessos indevidos, falhas técnicas, incidentes cibernéticos, erros operacionais, perda, destruição ou divulgação não autorizada, o que exige a adoção de medidas estruturadas de proteção.
A segurança da informação deve ser tratada como um processo contínuo, integrado à governança institucional, envolvendo aspectos tecnológicos, organizacionais e humanos.
Com a ampliação do uso de sistemas acessíveis via internet, serviços em nuvem e trabalho remoto, torna-se necessário estabelecer diretrizes que assegurem a proteção das informações em ambientes internos e externos.
Esta Política estabelece diretrizes para garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações, bem como a proteção de dados pessoais, em conformidade com a legislação vigente.
Aplica-se a todos os conselheiros, empregados, assessores, colaboradores, estagiários, prestadores de serviço e demais usuários que tenham acesso às informações e aos recursos de Tecnologia da Informação e Comunicação - TIC do CFBio.

2 - Definições

Para fins desta Política, aplicam-se as seguintes definições:

• **Segurança da Informação:** conjunto de ações e controles destinados a assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações.
• **Informação:** dados, processados ou não, que possuem valor para a organização e podem estar em qualquer meio ou formato.
• **Ativos de Informação:** todos os recursos que suportam a informação, incluindo sistemas, equipamentos, dados, documentos, serviços, infraestrutura e pessoas.
• **Confidencialidade:** garantia de que a informação seja acessada apenas por pessoas autorizadas.
• **Integridade:** garantia de que a informação não seja alterada ou destruída de forma indevida.
• **Disponibilidade:** garantia de que a informação esteja acessível quando necessária.
• **Autenticidade:** garantia da veracidade da origem e da autoria da informação.

• **Rastreabilidade:** capacidade de identificar e registrar ações realizadas sobre informações e sistemas.
• **Não repúdio:** impossibilidade de negar a autoria de uma ação realizada em ambiente computacional.
• **Usuário:** qualquer pessoa que tenha acesso aos ativos de informação do CFBio.
• **Credencial de acesso:** conjunto de informações utilizadas para autenticação do usuário, como login e senha.
• **Incidente de segurança da informação:** qualquer evento adverso, confirmado ou suspeito, que comprometa a segurança da informação.
• **Risco:** possibilidade de ocorrência de evento que cause impacto negativo aos ativos de informação.
• **Ameaça:** fator externo ou interno com potencial de causar dano à informação.
• **Vulnerabilidade:** fragilidade que pode ser explorada por uma ameaça.
• **Backup:** cópia de segurança de dados realizada para permitir sua recuperação em caso de perda ou incidente.
• **Computação em nuvem:** modelo de fornecimento de serviços de tecnologia da informação por meio da internet.
• **Dados pessoais:** informações relacionadas a pessoa natural identificada ou identificável.
• **Titular dos dados:** pessoa natural a quem se referem os dados pessoais.
• **Encarregado de Dados (DPO):** pessoa responsável por atuar como canal de comunicação entre o CFBio, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

3 - Princípios e Diretrizes de Segurança da Informação

A segurança da informação no CFBio observará os seguintes princípios:

• Confidencialidade: assegurar que a informação seja acessada apenas por pessoas autorizadas;
• Integridade: garantir a exatidão e completude da informação;
• Disponibilidade: assegurar o acesso à informação quando necessário;
• Autenticidade: garantir a identidade das partes envolvidas;
• Rastreabilidade: permitir o registro e auditoria das ações realizadas;
• Não repúdio: impedir a negação de autoria de ações realizadas;
• Privacidade: proteger dados pessoais conforme a LGPD;
• Transparência: observar a publicidade como regra e o sigilo como exceção, conforme a LAI;
• Proporcionalidade: aplicar controles de acordo com o nível de risco.

As ações de segurança devem ser contínuas, proporcionais aos riscos e alinhadas aos objetivos institucionais.

4 - Competência do Setor de Tecnologia e Segurança da Informação no Âmbito da Segurança da Informação

O Setor de Tecnologia e Segurança da Informação é responsável por coordenar a segurança da informação no CFBio, atuando como gestor de segurança da informação.

Compete ao Setor de Tecnologia e Segurança da Informação:

• planejar, implementar e manter controles de segurança;
• gerenciar acessos e identidades;
• monitorar redes, sistemas e serviços;
• implementar mecanismos de proteção contra incidentes;
• autorizar e controlar o uso de serviços em nuvem e acessos externos;
• apoiar o Encarregado de Dados (DPO);
• promover ações de capacitação;
• realizar auditorias técnicas;
• coordenar a resposta a incidentes.

5 - Gestão de Ativos e Classificação da Informação

As informações do CFBio devem ser classificadas de acordo com sua sensibilidade, criticidade e requisitos legais, de modo a garantir a aplicação de controles de segurança proporcionais ao seu valor e aos riscos envolvidos.

A classificação da informação tem como finalidade orientar seu tratamento ao longo de todo o seu ciclo de vida, incluindo acesso, armazenamento, compartilhamento, transmissão e descarte.

As informações deverão ser classificadas, no mínimo, nas seguintes categorias:

• **Pública**: informação cujo acesso é permitido ao público em geral, nos termos da legislação vigente, especialmente a Lei de Acesso à Informação (LAI);
• **Restrita**: informação cujo acesso deve ser limitado a usuários autorizados, em razão de seu caráter administrativo, operacional ou institucional;
• **Sigilosa**: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Informações que contenham dados pessoais ou dados pessoais sensíveis deverão ter acesso restrito aos usuários que necessitem tratá-las para finalidade institucional legítima, observadas as bases legais, os princípios e as medidas de segurança previstos na LGPD, sem prejuízo das hipóteses legais de sigilo ou restrição de acesso previstas na LAI e demais normas aplicáveis.

A definição da classificação da informação é de responsabilidade dos gestores das áreas que a produzem ou utilizam, devendo observar os critérios legais, institucionais e de segurança da informação aplicáveis.

A classificação deverá ser revista sempre que houver alteração no contexto, na sensibilidade da informação ou nos requisitos legais aplicáveis.

6 - Controle de Acesso

O acesso às informações e aos sistemas do CFBio deve observar os princípios do menor privilégio e da necessidade de conhecimento, sendo concedido apenas na medida necessária para o desempenho das atribuições do usuário.

As credenciais de acesso são individuais, pessoais e intransferíveis, sendo o usuário responsável por todas as ações realizadas com sua identificação. É vedado o compartilhamento de login e senha, bem como a utilização de credenciais de terceiros.

As senhas devem atender a requisitos mínimos de segurança, não podendo ser de fácil dedução, devendo conter combinação de caracteres e ser mantidas sob sigilo. Recomenda-se sua atualização periódica e imediata em caso de suspeita de comprometimento.

Deverá ser adotada autenticação multifator (MFA), sendo obrigatória para acessos administrativos, acessos remotos e sistemas críticos, e recomendada para os demais usuários, conforme diretrizes do Setor de Tecnologia e Segurança da Informação.

Os acessos aos sistemas e recursos de TIC devem ser concedidos mediante solicitação formal, devidamente autorizada pela chefia imediata ou responsável pela área, e configurados de acordo com o perfil de acesso necessário.

Os perfis de acesso devem ser revisados periodicamente e sempre que houver alteração de função, afastamento ou desligamento do usuário, devendo ser imediatamente revogados quando não mais necessários.

O Setor de Tecnologia e Segurança da Informação é responsável por implementar, controlar e monitorar os mecanismos de autenticação, autorização e registro de acessos, garantindo a rastreabilidade das ações realizadas nos sistemas institucionais.

O acesso aos recursos de Tecnologia da Informação e Comunicação do CFBio está condicionado à ciência e aceitação formal desta Política, mediante assinatura do Termo Individual de Responsabilidade.

7 - Uso dos Recursos de Tecnologia da Informação

Os recursos de TIC disponibilizados pelo CFBio devem ser utilizados exclusivamente para o desempenho das atividades institucionais, observando-se os princípios da legalidade, responsabilidade, ética e segurança da informação.

O uso desses recursos deve ocorrer de forma adequada, evitando riscos à segurança das informações, à integridade dos sistemas e à imagem institucional do CFBio.

É vedado aos usuários:

• instalar, executar ou utilizar softwares, aplicativos ou serviços não autorizados pelo Setor de Tecnologia e Segurança da Informação;
• utilizar os recursos de TIC para fins particulares, comerciais, ilícitos ou incompatíveis com as atividades institucionais;
• compartilhar credenciais de acesso ou permitir o uso de sua conta por terceiros;
• acessar, modificar, copiar ou divulgar informações sem autorização ou sem necessidade funcional;
• armazenar, transmitir ou compartilhar conteúdos que violem a legislação vigente, normas institucionais ou direitos de terceiros;
• utilizar dispositivos ou meios externos (como pendrives, HDs externos ou serviços em nuvem não autorizados) para armazenamento ou transferência de dados institucionais sem autorização;
• tentar burlar controles de segurança, explorar vulnerabilidades ou realizar qualquer ação que comprometa a integridade, confidencialidade ou disponibilidade dos sistemas e informações.

Os usuários são responsáveis pelo uso adequado dos recursos que lhes forem disponibilizados, devendo zelar pela sua conservação, segurança e correto funcionamento, bem como comunicar imediatamente ao Setor de Tecnologia e Segurança da Informação qualquer uso indevido, falha ou incidente identificado.

8 - Uso da Internet e Correio Eletrônico

O acesso à Internet e a utilização do correio eletrônico institucional devem ocorrer exclusivamente para fins relacionados às atividades do CFBio, observando conduta profissional, ética e alinhada às normas institucionais.

As comunicações realizadas por meio dos recursos institucionais, incluindo correio eletrônico e navegação na Internet, poderão ser monitoradas e auditadas pelo CFBio, respeitada a legislação vigente, com o objetivo de garantir a segurança da informação e a adequada utilização dos recursos.

Os usuários devem adotar boas práticas de segurança no uso da Internet e do correio eletrônico, especialmente quanto à identificação de mensagens suspeitas, tentativas de fraude (phishing), anexos desconhecidos e links potencialmente maliciosos.

É proibido:

• acessar, armazenar ou disseminar conteúdos ilícitos, impróprios ou incompatíveis com o ambiente institucional;
• utilizar o correio eletrônico institucional para fins particulares, comerciais ou não relacionados às atividades do CFBio;
• enviar ou encaminhar mensagens com conteúdo ofensivo, discriminatório, ilegal ou que possa comprometer a imagem institucional;
• abrir anexos ou acessar links de origem desconhecida ou suspeita, sem a devida verificação;
• compartilhar informações institucionais sem autorização ou em desacordo com sua classificação;
• utilizar contas de e-mail institucionais para cadastro em serviços não relacionados às atividades do CFBio, sem autorização.

Os usuários são responsáveis pelas mensagens enviadas a partir de suas contas institucionais, devendo zelar pelo uso adequado, pela veracidade das informações e pela proteção de dados e informações sob sua responsabilidade.

9 - Armazenamento de Informações e Uso de Nuvem

Os dados e informações institucionais do CFBio devem ser armazenados exclusivamente em ambientes corporativos autorizados, garantindo níveis adequados de segurança, controle de acesso, rastreabilidade e disponibilidade.

O armazenamento deve ocorrer, preferencialmente, em repositórios institucionais gerenciados pelo CFBio, incluindo servidores internos e plataformas oficiais em nuvem, como o Google Workspace ou outros serviços devidamente homologados pelo Setor de Tecnologia e Segurança da Informação.

É expressamente proibido o uso de contas pessoais, serviços não autorizados ou quaisquer meios externos não homologados para armazenamento, compartilhamento ou processamento de dados institucionais.

O uso de serviços em nuvem deve observar diretrizes de segurança da informação e proteção de dados, incluindo:

• controle de acesso adequado às informações, conforme sua classificação;
• restrição de compartilhamento com usuários externos, quando não autorizado;
• utilização de contas institucionais para acesso e armazenamento;
• monitoramento e rastreabilidade das ações realizadas;
• proteção contra acesso não autorizado, perda ou vazamento de informações.

O compartilhamento de arquivos e documentos por meio de plataformas em nuvem deve respeitar a classificação da informação, sendo vedada a disponibilização pública ou irrestrita de conteúdos institucionais sem autorização.

Os usuários são responsáveis por garantir o correto armazenamento das informações sob sua guarda, devendo evitar a duplicação desnecessária, o armazenamento local não protegido e a manutenção de dados fora dos ambientes institucionais.

O Setor de Tecnologia e Segurança da Informação poderá definir diretrizes complementares para uso seguro de serviços em nuvem, bem como monitorar sua utilização, com o objetivo de garantir a conformidade com esta Política.

10 - Acesso Remoto

O acesso remoto aos sistemas e recursos do CFBio deve ser realizado exclusivamente por meio de ferramentas e soluções previamente autorizadas pelo Setor de Tecnologia e Segurança da Informação, sendo vedado o uso de mecanismos não homologados.

O acesso remoto deverá observar requisitos mínimos de segurança, incluindo o uso de autenticação segura, preferencialmente com autenticação multifator (MFA), especialmente para acessos a sistemas críticos, administrativos ou que envolvam dados sensíveis.

Os usuários são responsáveis pela segurança do ambiente a partir do qual realizam o acesso remoto, devendo adotar medidas como:

• utilização de dispositivos confiáveis e atualizados;
• proteção contra acesso não autorizado (ex.: uso de senha no dispositivo e bloqueio de tela);
• uso de redes seguras, evitando conexões públicas ou não confiáveis;
• não compartilhamento do ambiente ou da sessão de acesso com terceiros.

O acesso remoto poderá ser monitorado pelo CFBio, com o objetivo de garantir a segurança das informações e a conformidade com esta Política.

O Setor de Tecnologia e Segurança da Informação poderá estabelecer diretrizes complementares, restringir acessos ou suspender permissões sempre que identificar riscos à segurança da informação.

11 - Gestão de Riscos em Segurança da Informação

A gestão de riscos em segurança da informação no âmbito do CFBio constitui um processo contínuo e estruturado, destinado a identificar, analisar, avaliar, tratar e monitorar os riscos que possam comprometer os ativos de informação e a continuidade das atividades institucionais.

Esse processo deve considerar, no mínimo:

• a identificação de ativos de informação relevantes;
• a identificação de ameaças e vulnerabilidades associadas;
• a análise dos impactos potenciais decorrentes de incidentes;
• a avaliação da probabilidade de ocorrência dos riscos;
• a definição e implementação de medidas de tratamento adequadas.

Os controles de segurança devem ser definidos e implementados de forma proporcional ao nível de risco identificado, à criticidade da informação e aos requisitos legais e institucionais aplicáveis.

A gestão de riscos deve estar integrada aos processos institucionais do CFBio, apoiando a tomada de decisão, a priorização de ações de segurança e a alocação eficiente de recursos.

Compete ao Setor de Tecnologia e Segurança da Informação coordenar as atividades relacionadas à gestão de riscos em segurança da informação, podendo estabelecer diretrizes, metodologias e instrumentos de apoio para sua implementação.

12 - Gestão de Incidentes de Segurança da Informação

Todo incidente de segurança da informação, confirmado ou suspeito, deve ser comunicado imediatamente ao Setor de Tecnologia e Segurança da Informação, para análise, registro e adoção das medidas necessárias à sua contenção, mitigação e tratamento.

Os incidentes devem ser formalmente registrados, classificados quanto à sua criticidade e acompanhados até sua completa resolução, incluindo a adoção de medidas corretivas e preventivas, com o objetivo de evitar recorrências.

Nos casos em que o incidente envolva ou possa envolver dados pessoais, o Encarregado de Dados (DPO) deverá ser acionado para avaliação dos impactos e das providências cabíveis.

A comunicação, análise e tratamento de incidentes de segurança envolvendo dados pessoais deverão observar as diretrizes, fluxos e prazos definidos pela Política de Comunicação de Incidente de Segurança com Dados Pessoais, instituída no âmbito do CFBio, em conformidade com a Lei Geral de Proteção de Dados e orientações da Autoridade Nacional de Proteção de Dados (ANPD).

O Setor de Tecnologia e Segurança da Informação atuará em conjunto com o Encarregado de Dados, fornecendo suporte técnico para análise do incidente, contenção, preservação de evidências e mitigação de riscos.

13 - Continuidade de Negócios e Backup

O CFBio deve adotar medidas que assegurem a continuidade de suas atividades institucionais e a disponibilidade dos serviços essenciais, mesmo diante de falhas, incidentes de segurança ou eventos adversos.

Devem ser implementadas rotinas de backup periódicas dos dados e sistemas institucionais, de acordo com sua criticidade, de modo a garantir sua recuperação em caso de perda, corrupção ou indisponibilidade.

Os backups devem ser protegidos contra acesso não autorizado, alteração indevida e perda, devendo, sempre que possível, ser armazenados em local seguro e distinto do ambiente principal.

Devem ser realizados testes periódicos de restauração, com o objetivo de verificar a integridade dos dados e a efetividade dos procedimentos de recuperação.
As ações de continuidade e recuperação devem considerar o impacto da indisponibilidade dos serviços, priorizando a restauração dos sistemas críticos e a manutenção das atividades essenciais do CFBio.

O Setor de Tecnologia e Segurança da Informação é responsável por definir, implementar e manter os procedimentos de backup e recuperação, podendo estabelecer diretrizes complementares conforme a criticidade dos serviços e a evolução dos riscos.

14 - Monitoramento e Auditoria

O CFBio realizará o monitoramento e a auditoria do uso dos recursos de Tecnologia da Informação e Comunicação, incluindo sistemas, redes, dispositivos e acessos, com a finalidade de garantir a segurança das informações, a integridade dos ambientes tecnológicos e o cumprimento desta Política.

O monitoramento poderá envolver o registro e a análise de eventos, acessos e operações realizadas nos sistemas institucionais, por meio de logs e trilhas de auditoria, respeitada a legislação vigente.

As informações coletadas poderão ser utilizadas para fins de investigação de incidentes, identificação de vulnerabilidades, prevenção de irregularidades e apoio a auditorias internas ou externas.

O Setor de Tecnologia e Segurança da Informação é responsável por implementar e manter mecanismos de monitoramento, bem como por apoiar processos de auditoria relacionados à segurança da informação.

Todos os usuários devem estar cientes de que os recursos institucionais não possuem caráter privado absoluto, podendo ser monitorados conforme previsto nesta Política e na legislação aplicável.

15 - Proteção de Dados Pessoais

O tratamento de dados pessoais no âmbito do CFBio deve observar a Lei Geral de Proteção de Dados (LGPD), bem como as normas institucionais relacionadas à privacidade e proteção de dados.

Devem ser adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, perda, alteração, destruição ou qualquer forma de tratamento inadequado ou ilícito.

Os incidentes de segurança que envolvam dados pessoais deverão ser tratados conforme diretrizes específicas estabelecidas na Política de Comunicação de Incidentes de Segurança com Dados Pessoais, garantindo a adequada avaliação de riscos, a adoção de medidas de mitigação e, quando aplicável, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares.

16 - Capacitação e Conscientização

O CFBio promoverá ações contínuas de capacitação e conscientização em segurança da informação e proteção de dados pessoais, com o objetivo de fortalecer a cultura organizacional e reduzir riscos decorrentes de falhas humanas.

As ações poderão incluir treinamentos, orientações, campanhas educativas, comunicados institucionais e outras iniciativas voltadas à disseminação de boas práticas no uso dos recursos de Tecnologia da Informação e Comunicação.

A capacitação deverá ser adequada aos diferentes perfis de usuários, considerando suas atribuições e níveis de acesso à informação.

Os usuários são responsáveis por participar das ações de capacitação promovidas e por aplicar, no exercício de suas atividades, as orientações e diretrizes estabelecidas nesta Política.

O Setor de Tecnologia e Segurança da Informação, em conjunto com as áreas competentes e com o Encarregado de Dados, poderá propor e coordenar iniciativas de capacitação e conscientização, especialmente nos temas relacionados à segurança da informação e à proteção de dados pessoais.

17 - Penalidades

O descumprimento das diretrizes estabelecidas nesta Política de Segurança da Informação poderá acarretar a aplicação de medidas administrativas, sem prejuízo das responsabilidades civis e penais cabíveis, conforme a legislação vigente e as normas internas do CFBio.

As sanções serão aplicadas de acordo com a gravidade da infração, os danos causados, a reincidência e as circunstâncias do caso concreto, assegurados o contraditório e a ampla defesa.

É vedado o uso de informações institucionais para obtenção de vantagem indevida, proveito próprio ou de terceiros, bem como sua utilização em desacordo com as finalidades institucionais. A violação dessa diretriz sujeitará o responsável às penalidades cabíveis.

Nos casos em que o descumprimento envolver tratamento inadequado de dados pessoais ou violação de segurança da informação, poderão ser adotadas medidas adicionais, inclusive aquelas relacionadas à legislação de proteção de dados e à comunicação às autoridades competentes, quando aplicável.

Os usuários respondem pelo uso indevido dos recursos de Tecnologia da Informação e Comunicação e das informações sob sua responsabilidade, nos termos da legislação vigente.

18 - Disposições Finais

Esta Política de Segurança da Informação deverá ser revisada periodicamente, de forma a garantir sua atualização frente a mudanças tecnológicas, organizacionais, legais e regulatórias, bem como em decorrência de recomendações de auditoria ou identificação de novos riscos.

A revisão poderá ser realizada sempre que necessário, sendo recomendada sua avaliação em intervalos regulares, a fim de assegurar sua aderência às boas práticas de segurança da informação e às diretrizes institucionais.

Normas complementares, procedimentos e orientações específicas poderão ser elaborados pelo CFBio para detalhar e operacionalizar as diretrizes estabelecidas nesta Política.

Todos os usuários deverão formalizar a ciência e concordância com esta Política por meio da assinatura do Termo Individual de Responsabilidade.

Os casos omissos ou situações excepcionais serão analisados pela Diretoria do CFBio, com apoio do Setor de Tecnologia e Segurança da Informação e, quando aplicável, do Encarregado de Dados, observada a legislação vigente e os princípios da Administração Pública.

19 - Vigência e Validade

Esta Política de Segurança da Informação entra em vigor na data de sua publicação, produzindo efeitos imediatos no âmbito do CFBio.

A partir de sua vigência, todos os usuários dos recursos de Tecnologia da Informação e Comunicação deverão observar integralmente as diretrizes aqui estabelecidas, sem prejuízo da adequação progressiva de procedimentos e controles internos, quando necessário.

20 - Referências

• Lei Federal nº 8.159 de 08 de janeiro de 1991 - Dispõem sobre a Política Nacional de Arquivos Públicos e Privados;
• Lei Federal nº 10.406 de 10 de janeiro de 2002 - Código Civil;
• Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI);
• Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
• Decreto nº 7.845, de 14 de novembro de 2012 — Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo;
• Decreto nº 12.572, de 4 de agosto de 2025 — Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da Administração Pública Federal;
• Acórdãos do Tribunal de Contas da União (TCU) relativos à governança e segurança da informação na Administração Pública;
• Normas Complementares do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) sobre Segurança da Informação;
• Norma ABNT/NBR ISO/IEC 27001 – Sistemas de Gestão de Segurança da Informação;
• Norma ABNT/NBR ISO/IEC 27002 – Código de Prática para Controles de Segurança da Informação;
• Norma ABNT/NBR ISO/IEC 27701 – Gestão de Privacidade da Informação;
• Política de Comunicação de Incidentes de Segurança com Dados Pessoais do CFBio;
• Resolução CD/ANPD nº 15, de 24 de abril de 2024 — Aprova o Regulamento de Comunicação de Incidente de Segurança.

CFBio