Política de Segurança da Informação - PSI

CONSELHO FEDERAL DE BIOLOGIA

DIRETORIA

MARIA EDUARDA LACERDA DE LARRAZÁBAL DA SILVA

PRESIDENTE

ELIÉZER JOSÉ MARQUES

VICE-PRESIDENTE

ALCIONE RIBEIRO DE AZEVEDO

CONSELHEIRA TESOUREIRA

HELENA LÚCIA MENEZES FERREIRA

CONSELHEIRA SECRETÁRIA

CICLO DE APROVAÇÃO

Destacam-se as principais fases da **Politica de Segurança da Informação:**

Elaboração	**Data**
Fredson Dias de Andrade – Técnico em TI/CFBio	31/05/2021

Revisão e Aprovação	**Data**
Comissão de Avaliação de Documentos – CPAD/CFBio	09/07/2021

Aprovação Final	**Data**
Diretoria/CFBio	24/08/2021

Sumário

1 Introdução

A informação existe em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela esteja sempre adequadamente protegida.

A segurança da informação normalmente é obtida a partir da implementação de um conjunto de controles adequados, tomado preventivamente pela a administração, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos e a segurança da organização sejam atendidos.

Com o crescimento do uso de sistema para Internet cresceu proporcionalmente a preocupação com a segurança dos dados e informações que circulam por ela, fazendo-se necessário a criação de políticas de uso.

Como é sabido, tanto os sistemas de informação, quanto as redes de computadores das organizações, estão diuturnamente expostos a diversos tipos de ameaças à segurança da informação, dentre essas, destacam-se as fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio, etc. Danos causados por código malicioso, hackers e ataques de "*denial of service"* também estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os empregados da organização.

Assim é que compete a todos os membros da Administração Pública Federal (APF) elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI). Nesse sentido, este documento tem como objetivo, prever políticas que visem garantir a integridade, a confiabilidade e a transparência dos

dados e informações do Conselho Federal de Biologia (CFBio), definindo regras, normas e protocolos para o uso da rede interna e externa pelos seus colaboradores a fim de se evitar o uso indevido desses dados e informações, quer seja de forma intencional ou acidental.

Esta política se aplica a todas as informações que estejam sob a responsabilidade do CFBio, em quaisquer formas ou meios e que porventura sejam apresentadas ou compartilhadas. Deverão estar sempre protegidas adequadamente, de acordo com controles definidos nesta política.

Este documento se aplica a todos os colaboradores, incluindo empregados efetivos, de livre provimento e exoneração, assessores, estagiários, temporários, terceirizados, prestadores de serviço, consultores independentes ou quaisquer outros que tenham acesso a qualquer ativo de Tecnologia de Informação e Comunicação (TIC) do CFBio.

2 Competência do Setor de TI no Âmbito da Política de Segurança

Essa área será responsável pela gestão de todas as frentes de Segurança da informação do CFBio. Sua missão é estabelecer e utilizar uma metodologia para avaliar, implementar e monitorar as diretrizes de proteção dos bens de informações visando garantir a continuidade dos processos e serviços CFBio.

Compete ao Setor de TI:

2.1 A solicitação de recursos orçamentários para as ações de segurança da informação;

2.2 Promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

2.3 Instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

2.4 Coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

2.5 Consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação;

2.6 Recomendar a aplicação das ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação;

2.7 O credenciamento e descredenciamento de usuários;

2.7.1 O credenciamento será realizado mediante solicitação da chefia da área e o descredenciamento por solicitação do RH ou da chefia da área no caso de contratos;

2.8 A definição de perfis de usuários cujos privilégios sejam compatíveis com as atividades do usuário;

2.8.1 Após a definição do perfil do usuário caberá ao chefe da área indicar os usuáriosque possuirão direito de leitura e/ou gravação nas pastas compartilhadas de sua área;

2.8.2 Os usuários não terão contas com perfil administrador, nem contas do domínio com privilégio de administrador local da estação, exceto àquela cuja atividade funcional necessite de tal requisito.

2.9 A instalação de todos os softwares nos equipamentos do CFBio;

2.10 A desinstalação de quaisquer softwares considerados nocivos à integridade da rede;

2.11 A realização de auditoria (local ou remota);

2.12 A instalação de softwares de monitoramento;

2.13 A autorização para conexão a redes externas.

3 Direitos e deveres dos usuários

3.1 Os serviços de TIC deverão ser solicitados pelo canal estabelecido pelo Setor de TI.

3.2 Fica permanentemente proibida a instalação de quaisquer softwares sem a comunicação ao Setor de TI;

3.3 É permitida ao usuário final a atualização da versão do software que foi instalado pelo Setor de TI;

3.4 O Setor de TI poderá desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

3.5 É proibida a conexão a redes e computadores que não os previstos pelo Setor de TI, exceto à rede wireless de visitantes.

3.6 São de responsabilidade do usuário o acionamento e o desligamento dos equipamentos de informática, pertencentes à mesma, no início e término de cada expediente.

3.7 São vedados o remanejamento e a remoção de qualquer equipamento de informática sem aviso prévio a Chefia imediata e ao Setor de TI.

3.8 É vedada a manipulação dos equipamentos de rede (switches, hubs, fiação, cabeamento de rede, entre outros) sem a anuência do Setor de TI.

3.9 Nas aquisições referentes a software e/ou hardware, caberá ao gerente da área encaminhar um documento de oficialização de demanda para o Setor de TI, descrevendo a necessidade e os objetivos esperados com a aquisição.

3.10 É terminantemente proibido ao usuário o acesso ou manutenção no interior do gabinete do computador, assim como troca ou retirada de componentes do mesmo. Caso necessário deverá ser acionado o Setor de TI;

3.11 Todo usuário deverá comunicar imediatamente ao Setor de TI sobre a existência de vulnerabilidades ou incidentes de segurança , de que tenham conhecimento, que impactem ou possam impactar os serviços prestados ou contratados pelo CFBio;

3.12 É dever de todos os usuários 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.

4 Normas de uso e criação de chaves de acesso para Usuários

Esta norma tem como objetivo estabelecer os procedimentos adequados para a correta utilização das chaves de acesso no ambiente de Tecnologia da Informação do CFBio e será aplicada a todos os empregados que possuam chave de acesso aos sistemas.

4.1 O login de rede, quando aplicado, será criado preferencialmente com o formato "*nome.sobrenome*";

4.2 A identificação do empregado por senha ou outro meio é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo o usuário o responsável por guardá-la com segurança e sigilo;

4.3 Cada sistema possui sua regra de composição de senha, entretanto é obrigatório desde que o sistema permita, que as senhas contenham no mínimo 8 (oito) caracteres e seja utilizado no mínimo três dos tipos de caracteres abaixo:

4.3.1 Letras maiúsculas;

4.3.2 Letras minúsculas;

4.3.3 Números;

4.3.4 Caracteres especiais ("$", "%", "&","@").

4.3.5 Deverá ser evitada a composição de senhas contendo somente sequência numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento e outros);

4.4 Mesmo que não seja obrigatório, recomenda-se a troca trimestral da senha de acesso aos sistemas.

5 Normas quanto ao uso da Internet

Esta norma tem como objetivo estabelecer responsabilidade e requisitos básicos de utilização da Internet nos setores do CFBio. A Internet deve ser utilizada para fins de complemento às atividades do setor, para o enriquecimento intelectual de seus servidores e como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos. Com base nos procedimentos de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os empregados devem estar cientes da periculosidade da navegação na Internet, antes de acessá-la e de utilizar os seus recursos. Considerando que o uso da Internet é fundamental para as atividades desenvolvidas no CFBio e observando-a como ferramenta que possibilita ameaças às informações da Instituição, são de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

5.1 Todos os empregados 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;

5.2 O acesso à Internet por parte dos empregados utilizando equipamentos do CFBio deve ser feito exclusivamente por meio da única ligação existente entre a Internet e o Conselho, sendo vedado o acesso à Internet utilizando provedores de acesso privados para o acesso à rede mundial de computadores;

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

5.4 A infraestrutura do CFBio e os recursos de informática jamais devem ser utilizados para a realização de trabalhos de terceiros ou de atividades paralelas.

6 Normas para utilização do Correio Eletrônico

O objetivo desse capítulo é estabelecer responsabilidades e requisitos básicos de uso dos serviços de correio eletrônico, no ambiente de Tecnologia da Informação do Conselho Federal de Biologia. Os e-mails são uma excelente forma de comunicação, porém são fonte de vulnerabilidade para as informações organizacionais. Esta norma deverá ser aplicada aos ativos de informação e comunicação do CFBio.

6.1 Os e-mails corporativos serão criados preferencialmente no formato função@cfbio.gov.br;

6.2 O acesso às mensagens de correio eletrônico são de exclusividade do empregado detentor do endereço eletrônico, sendo garantida a inviolabilidade do conteúdo das mensagens eletrônicas, entretanto todas as mensagens podem ser monitoradas e passíveis de auditoria.

6.3 As auditorias poderão ser solicitadas, a qualquer momento, pela Diretoria do CFBio e realizadas pelo Setor de TI;

6.4 Os e-mails departamentais compartilhados serão criados quando solicitado pelo gestor da área e podem ser acessados por vários empregados;

6.5 O e-mail do CFBio deve ser utilizado apenas para assuntos referentes ao Conselho sendo vedado reenvio de mensagens que não estejam diretamente ligadas ao órgão;

6.6 É vedado o uso de e-mail para propaganda política, racial, financeira ou de qualquer outra natureza;

6.7 É vedado o uso de material pornográfico entre os e-mails da organização, tanto recebimento como envio;

6.8 É expressamente proibido sem o conhecimento prévio do Setor de TI a abertura de anexos com as extensões .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pelo Setor de TI;

6.9 Evitar enviar anexos com tamanho superior a 5MB.

7 Normas para Armazenamento de Arquivos

Regras e requisitos básicos aplicadas aos ativos de informação para armazenamento de arquivos no setor de Tecnologia da Informação do CFBio.

Os arquivos da rede do Conselho Federal de Biologia estão disponibilizados em unidades mapeadas na própria máquina do usuário, da maneira que se segue:

Servidor de arquivos: É um serviço disponibilizado pelo Departamento de TI para os empregados acessarem utilizando login da rede do CFBio, é uma área do disco rígido de um dos servidores, que disponibiliza para os usuários as pastas e documentos relativos ao setor onde trabalha.

Backup – é realizada cópia de segurança semanalmente dos arquivos, possibilitando ao usuário a recuperação dos mesmos em caso de perda acidental.

Armazenamento em nuvem- O armazenamento na nuvem é um modelo de computação que armazena dados na Internet por meio de um provedor de computação, que gerencia e opera o armazenamento físico de dados. É importante ressaltar que no armazenamento em nuvem é de responsabilidade do usuário realizar backup e controlar o acesso aos dados. São exemplos de provedores de armazenamento em nuvem:

- DropBox
- OneDrive
- Google Drive

8 Penalidades

8.1 O empregado que apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, arquivo ou programa de computador, de forma indevida ou não autorizada, fizer uso indevido dos equipamentos de informática, bem como praticar ato em desacordo com os termos da presente norma fica sujeito às punições cabíveis nos termos da lei.

8.2 O empregado infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu chefe imediato e a Diretoria do CFBio.

8.3 Todos os empregados ao tomarem conhecimento de qualquer incidente de segurança da

informação, devem informar o ocorrido, imediatamente, à administração.

9 Disposições Finais

9.1 O CFBio se reserva no direito de monitorar o tráfego através das suas redes de comunicação, incluindo o acesso à Internet.

9.2 A monitoração do cumprimento das normas de utilização da Internet será executada conforme os itens abaixo:

9.2.1 Técnicos do Setor de TI identificarão os usuários que descumprirem qualquer item desta norma de segurança.

9.3 Na primeira transgressão o empregado será notificado, sobre o item que transgrediu e orientado para não mais infringir, sob pena de sofrer outras sanções.

9.4 Na segunda transgressão o empregado será notificado novamente, mais com cópia para chefia imediata, do descumprimento das normas estabelecidas neste documento. Caso na infração cometida esteja caracterizando qualquer tipo de crime (acesso a sites de pedofilia, racismo, etc.), tomar-se-ão providências previstas em lei.

9.5 O CFBio se reserva no direito de verificar, sempre que julgar necessário, a obediência às normas ou procedimentos citados neste documento.

9.6 O uso indevido dos serviços de correio eletrônico, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente.

9.7 Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente norma, devendo também assinar o "Termo Individual de Responsabilidade" (ANEXO I).

9.8 Todos os equipamentos do CFBio devem ser mantidos em boas condições e possuir proteção de forma a preservar seus componentes internos.

9.9 O usuário arcará pelos danos causados pelo mau uso dos computadores e dos recursos do CFBio, mediante apuração cabível, nos termos da lei.

9.10 A saída de equipamentos do CFBio deve ser registrada utilizando documento de saída de equipamento assinada pelo superior imediato.

10 Vigência e Validade

A presente política passa a vigorar a partir da data de sua aprovação e publicação como Portaria do CFBio, sendo válida por tempo indeterminado.

11 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 (Institui o Código Civil).
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)
- Decreto nº 4.453, de 27 de dezembro de 2002 (Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal).
- Decreto n° 9.637, de 26 de dezembro de 2018 (Institui a Política Nacional de Segurança da Informação).
- Norma ABNT/NBR ISO 27.701/2019

12 Glossário

- Ativo - Tudo que tem valor para a organização.
- Arquivos infectados - Aqueles que sofreram a ação de vírus eletrônico.
- Caixa Postal / Correio eletrônico - Espaço em disco, onde são armazenadas as mensagensde correio eletrônico.
- Criptografia - Ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.
- Controle - forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de

gestão ou legal.

- Chave de Aceso - Código de aceso atribuído a cada usuário. Para cada chave de acesso é associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-o acessar os recursos disponíveis.
- Download - baixar um arquivo ou documento de outro computador, através da Internet.
- Ferramenta Tecnológica - Sistema (conjunto de programas) e/ou equipamento destinado a proteger, monitorar ou agregar valor aos ativos de informações.
- E-mail - Mensagem eletrônica.
- Política de Segurança da Informação - documentos que provêm uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
- Software - programa de computador.
- Spam - Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmo a tenha solicitado.

ANEXO I - Termo Individual de Responsabilidade

Eu,_____, matrícula _____ ,Identidade nº_____, expedida por_____, na qualidade de usuário dos recursos de Tecnologia de Informação disponibilizados pelo Conselho Federal de Biologia, 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 pelo Setor de TI, devidamente identificados.

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

Declaro estar ciente de que devo gravar os arquivos produzidos e manipulados por mim na rede de computadores do CFBio 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