POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS

Dezembro/2024 (versão 1)

SUMÁRIO

1. Propósito

Instituir a Política de Segurança da Informação (PSI), no âmbito da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Esta Política se aplica a todos os ativos de informação da FMIS, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações da FMIS. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela FMIS e entidades subsidiárias.

2. Termos e definições

Confidencialidade

O princípio da confidencialidade determina que certa informação, fonte ou sistema deve estar acessível apenas a pessoas autorizadas.

Integridade

O princípio da integridade estabelece que certa informação deve ser correta, confiável e sem alterações não autorizadas.

Disponibilidade

O princípio da disponibilidade determina que a informação deve estar sempre acessível para uso legítimo de pessoas autorizadas.

Autenticidade

O princípio da autenticidade se refere à garantia de que a informação é proveniente de uma fonte confiável e que não foi alterada por terceiros não autorizados.

Dado Pessoal

Informação relacionada a pessoa natural identificada ou identificável;

Dado Sensível

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Informação

Dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

3. Política de Segurança da Informação

I. Fica instituída a Política de Segurança da Informação da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

II. Esta Política de Segurança da Informação aplica-se a todas as unidades da FMIS, e deverá ser observada por todos os usuários de informação, seja servidor, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade da FMIS.

4. Objetivos

São objetivos da Política de Segurança da Informação:

I. Estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II. Estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III. Estabelecer competências e responsabilidades quanto à segurança da informação;

IV. Nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V. Promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da FMIS.

5. Princípios e Diretrizes

As ações de segurança da informação da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública, bem como pelos seguintes princípios:

I. Disponibilidade, integridade, confidencialidade e autenticidade das informações;

II. Continuidade dos processos e serviços essenciais para o funcionamento da FMIS.

III. Economicidade da proteção dos ativos de informação;

IV. Respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V. Observância da publicidade como preceito geral e do sigilo como exceção;

VI. Responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII. Alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico da FMIS, assim como demais normas específicas de segurança da informação;

VIII. Conformidade das normas e das ações de segurança da informação com a legislação, regulamentos aplicáveis; e

IX. Educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito da FMIS e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

As normas, procedimentos, manuais e metodologias de segurança da informação da FMIS devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

6. As ações de segurança da informação devem:

I. Considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da FMIS;

II. Ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da FMIS;

III. Ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

IV. Visar à prevenção da ocorrência de incidentes.

7. Disposições Gerais

I. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos a FMIS.

II. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada na FMIS compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

III. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma determinada tarefa.

IV. É condição para acesso aos recursos de tecnologia da informação da FMIS a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS.

V. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da FMIS, 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.

VI. 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 minimizar possíveis riscos à segurança da informação.

VII. Todos os contratos de prestação de serviços firmados pela FMIS conterão cláusula específica sobre a obrigatoriedade de atendimento à esta Política de Segurança da Informação, bem como de suas normas decorrentes.

8. Da Gestão de Segurança da Informação

A estrutura de Gestão de Segurança da Informação é composta por:

I. Alta Administração;

II. Gestor de Segurança da Informação;

III. Gestor de Tecnologia da Informação e Comunicação;

IV. Encarregado pelo Tratamento de Dados Pessoais; e

V. Usuários de Informação.

9. Compete à Alta Administração:

I. Fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da FMIS, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e

II. Formalizar e aprovar a Política de Segurança da Informação da FMIS, bem como suas alterações e atualizações.

10. Compete ao Comitê de Segurança da Informação:

I. Assessorar na implementação das ações de segurança da informação;

II. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV. Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V. Deliberar sobre normas internas de segurança da informação;

VI. Avaliar as ações propostas pelo gestor de segurança da informação.

11. Compete ao Gestor de Segurança da Informação:

I. Coordenar o Comitê de Segurança da Informação;

II. Coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

III. Assessorar a Alta Administração na implementação da Política de Segurança da Informação;

IV. Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V. Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI. Incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VII. Propor recursos necessários às ações de segurança da informação;

VIII. Acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX. Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

12 Compete ao Gestor de Tecnologia da Informação e Comunicação

I. Implementação eficaz de controles: Desenvolver e implantar mecanismos de proteção que cubram tanto os sistemas internos quanto os fornecedores e parceiros externos. Isso inclui autenticação, criptografia, gestão de acessos, e auditorias periódicas.

II. Gestão da cadeia de suprimentos: Avaliar e monitorar continuamente todos os envolvidos na cadeia de suprimentos, garantindo que fornecedores e parceiros cumpram os padrões de segurança e privacidade estabelecidos. Essa gestão requer uma análise contínua de riscos e a formalização de acordos que definam claramente as responsabilidades de segurança.

III. Realizar verificações de segurança em softwares e dispositivos da cadeia de suprimentos para identificar vulnerabilidades,

IV. Estabelecer um plano de resposta a incidentes, com equipes dedicadas e processos bem definidos para a investigação e resolução de incidentes de segurança. Incluir também um plano de recuperação de desastres para restaurar rapidamente os dados e sistemas críticos após um incidente.

V. Melhoria contínua: Monitorar, auditar e revisar regularmente os controles implementados para identificar e corrigir vulnerabilidades, adaptando-se às mudanças tecnológicas, regulatórias e de ameaças emergentes. A melhoria contínua permite que os controles se mantenham atualizados e eficazes diante de novos riscos.

13. Compete ao Encarregado pelo Tratamento dos Dados Pessoais

I. Dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

II. Planejamento estratégico: Identificar os requisitos de privacidade e segurança, alinhados às normas, regulamentações e melhores práticas, como ISO 27001,

GDPR e LGPD. Este planejamento visa garantir que os controles protejam todas as fases do ciclo de vida da informação, desde a coleta até o descarte.

14. Compete aos Usuários de Informação

I. Conhecer e cumprir esta Política e às demais normas específicas de segurança da informação da FMIS.

> *Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.*

15. Processos da Política de Segurança da Informação:

I. Tratamento da informação;

II. Segurança física e do ambiente;

III. Gestão de incidentes em segurança da informação;

IV. Gestão de ativos;

V. Gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI. Controles de acesso;

VII. Gestão de riscos;

VIII. Gestão de continuidade

> *O Comitê de Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.*

16. Procedimentos da Política de Segurança da Informação:

I. A conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

II. A classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III. A proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

IV. Ao uso aceitável da informação e a utilização de mídias de armazenamento;

V. A entrada e saída de ativos de informação das instalações da FMIS;

VI. Aos perímetros de segurança da FMIS;

VII. Aos controles de acesso baseados no princípio do menor privilégio;

VIII. As etapas de identificação, contenção, erradicação e recuperação e atividades pós incidente;

IX. Ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;

X. A Política de Gestão de Ativos da FMIS, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para a FMIS; a manutenção de inventario atualizado de ativos da FMIS, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

XI. A utilização adequada dos recursos operacionais e de comunicações fornecidos pela FMIS, a serem utilizados para fins profissionais, relacionados às atividades da FMIS, em conformidade com os princípios éticos e profissionais da FMIS, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS;

XII. Aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIII. O acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XIV. O uso de mídias sociais, a divulgação de informações nas mídias sociais, o uso de contas pessoais para fins profissionais e a interação com estranhos nas mídias sociais;

XV. As políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a conformidade com as leis e regulamentos aplicáveis;

XVI. As políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização, baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação da FMIS;

XVII. As políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente da FMIS, dos seus ativos de informação e das ameaças à segurança da informação; a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência; a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial

nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento;

XVIII. O tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos;

XIV. As políticas e procedimentos para Gestão de Continuidade de Negócios da FMIS, incluindo o Plano de Continuidade para garantir que a FMIS possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XX. Os procedimentos de backup e log são fundamentais para garantir a integridade e a disponibilidade das informações da FMIS. Realizar backups regulares, automáticos e monitorados, com armazenamento em locais seguros e redundantes, incluindo soluções em nuvem ou fora do ambiente principal. Os logs de acesso e atividades do sistema devem ser gerados automaticamente, protegidos contra alterações e armazenados por um período determinado em conformidade com normas legais e operacionais. Estes registros devem ser analisados regularmente para identificar acessos indevidos ou comportamentos anômalos, garantindo a rastreabilidade e o suporte a auditorias.

A FMIS mantém, monitora e analisa regularmente os logs gerados pelos ativos de software, hardware e rede dos servidores Windows Server, considerados críticos.

As unidades organizacionais da FMIS devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

Todas as ações, realizadas pelas unidades da FMIS, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis à esta temática.

As atividades, produtos e serviços desenvolvidos na FMIS devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes

17. Vedações e Disposições Finais

I. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela FMIS para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

II. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela FMIS.

III. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

IV. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

V. As unidades organizacionais da FMIS devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

VI. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais:

informatica@mis.rj.gov.br
web@mis.rj.gov.br

VII. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pela FMIS periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

VIII. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

IX. Esta Política será revisada periodicamente, pelo menos a cada dois anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente da FMIS, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

X. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidas ao Comitê de Segurança da Informação.

I. Comitê de Política de Segurança da Informação (CPSI)

Gestor de Segurança da Informação

Roberto Almeida Casimiro da Silva

Gestor de Tecnologia da Informação e Comunicação

André Luis Pereira Rodrigues

Representante da Alta Direção

Carlos Henrique Santos Viana

Encarregado pelo Tratamento de Dados Pessoais

Úrsula Resende

II. Metodologia

Informamos que o documento Política de Segurança da Informação - FMIS foi desenvolvido tomando como referência o documento INSTRUÇÃO NORMATIVA PRODERJ/PRE N. 02 DE 28 DE ABRIL DE 2022 e utilizamos a estrutura e alguns elementos do documento PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI) como base, ajustando o conteúdo conforme as especificidades e necessidades atuais. Esse processo visou garantir consistência com as diretrizes já estabelecidas, além de otimizar a criação de um material alinhado aos padrões de Política de Segurança da Informação.

O presente documento adota a metodologia PDCA (Planejar-Executar-Verificar-Agir) como base para a estruturação das etapas de desenvolvimento e melhoria contínua dos processos descritos.

Sobre o Modelo PDCA

O PDCA é um ciclo de quatro etapas que visa a implementação de melhorias gradativas, possibilitando um controle dos resultados e a adaptação de estratégias conforme necessário. Cada fase possui uma função específica:

Planejar (Plan): Nesta fase, são definidos os objetivos e metas, além de realizar uma análise do processo atual. A partir dessa análise, são identificadas oportunidades de aprimoramento e estabelecido um plano de ação com etapas específicas para alcançar os resultados esperados.

Executar (Do): Após o planejamento, o plano é colocado em prática em uma fase de execução inicial, geralmente em uma escala reduzida, para testar a viabilidade das ações propostas. Nessa etapa, são coletados dados e monitorados os processos para observar os primeiros resultados e ajustar rapidamente se necessário.

Verificar (Check): Com a execução em andamento, os dados coletados são analisados para verificar se os resultados estão alinhados com as metas estabelecidas. Esta fase permite identificar pontos de ajuste e validar a eficácia das mudanças propostas no plano inicial.

Agir (Act): Caso os resultados sejam satisfatórios, as mudanças são formalizadas e implementadas em maior escala, transformando o novo processo em um padrão. Caso contrário, os dados obtidos servem de base para um novo ciclo PDCA, promovendo uma melhoria contínua.

III. Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação— Requisitos. Rio de Janeiro, 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. Guia do Framework de Privacidade e Segurança da Informação. Março 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf . Acesso em: 23 set. 2024.

BRASIL. Presidência da República. Agência Nacional de Proteção de Dados - ANPD. Guia Orientativo - Tratamento de dados pessoais pelo Poder Público. Junho 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 16 out. 2024

ANEXO I

MODELO DE TERMO DE RESPONSABILIDADE

Referente ao Conhecimento e Compromisso com a Política de Segurança da Informação da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS

Eu, [Nome Completo], portador do documento de identidade [Número do RG/CPF], residente e domiciliado à [Endereço Completo], na qualidade de [Cargo/Função] da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS, declaro para os devidos fins que:

1. Declaração de Conhecimento

Confirmo que recebi, li e compreendi o conteúdo integral da Política de Segurança da Informação da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS, em vigor na presente data. Afirmo, ainda, que todas as minhas dúvidas sobre as diretrizes, normas e procedimentos estabelecidos foram devidamente esclarecidas.

2. Compromisso de Cumprimento

Comprometo-me a cumprir rigorosamente todos os requisitos e normas descritos na Política de Segurança da Informação, agindo sempre em conformidade com os procedimentos e controles de segurança previstos para a proteção de dados, informações e recursos da Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS.

3. Responsabilidade pela Confidencialidade e Integridade

Declaro ciência sobre a responsabilidade de preservar a confidencialidade, integridade e disponibilidade das informações às quais tenho acesso em razão do meu cargo. Reconheço que o uso não autorizado ou inadequado dessas

informações poderá resultar em sanções administrativas, disciplinares e legais, conforme o caso.

4. Conscientização sobre Consequências em Caso de Inobservância

Estou ciente de que a inobservância das normas da Política de Segurança da Informação poderá acarretar medidas disciplinares, que podem incluir advertências, suspensão, demissão por justa causa e, se aplicável, sanções civis e criminais.

5. Prazo de Vigência e Atualização

Este termo de responsabilidade permanece válido enquanto eu estiver vinculado a Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS, ou até que uma nova versão da política seja divulgada. Comprometo-me a me manter atualizado(a) sobre eventuais alterações na Política de Segurança da Informação e a adequar minhas ações a qualquer atualização realizada.

Por meio deste termo, reitero meu compromisso em colaborar para a segurança da informação na Fundação Museu da Imagem e do Som do Rio de Janeiro - FMIS e para o cumprimento dos padrões éticos e profissionais esperados.

[Localidade], [Data]

Assinatura: _____

Nome do Colaborador: _____

Cargo/Função: _____

Matrícula: _____