INSTITUTO BRASILEIRO DE MUSEUS

**RESOLUÇÃO NORMATIVA IBRAM Nº 4, DE 28 DE JUNHO DE 2021**

Regulamenta a Política de Segurança da Informação – POSIN do Instituto Brasileiro de Museus.

**O PRESIDENTE DO INSTITUTO BRASILEIRO DE MUSEUS,**no uso das atribuições que lhe confere o inciso IV do art. 20 do Anexo I doDecreto nº 6.845, de 07 de maio de 2009, e tendo em vista o Decreto nº 10.139, de 28 de novembro de 2019, a Instrução Normativa GSI/PR nº1, de 27 de maio de 2020, a Portaria GSI/PR nº 93, de 26 de setembro de 2019, Decreto nº 10.641, de 2 de março de 2021, na quinquagésima-oitava reunião realizada em 12 de julho de 2021, **resolve**:

Art. 1º Aprovar , na forma do Anexo a esta Portaria, a Política de Segurança da Informação do Instituto Brasileiro de Museus - POSIN/IBRAM, em consonância com a Instrução Normativa Nº 1, de 27 de maio de 2020 que dispõe sobre a estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.

Art. 2º Ficam revogados os seguintes atos normativos:

I - Portaria nº 171, de 26 de maio de 2017, publicada no Diário Oficial da União; e

II - Portaria n° 172, de 26 de maio de 2017, publicada no Boletim Administrativo Eletrônico 467, em 29 de maio de 2017.

Art. 3º A presente Portaria entra em vigor em 1º de setembro de 2021.

**Pedro Machado Mastrobuono**

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO BRASILEIRO DE MUSEUS

**CAPÍTULO I**

**DISPOSIÇÕES GERAIS**

**Seção I**

**Escopo**

Art. 1º Fica instituída a Política de Segurança da Informação - POSIN que objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações custodiadas e de propriedade do Instituto Brasileiro de Museus -Ibram, de modo a preservar os seus ativos e sua imagem institucional.

Art. 2º A POSIN trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do Ibram, em todo o seu ciclo de vida criação, manuseio, divulgação, armazenamento, transporte e descarte, visando a continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 3° Os objetivos e diretrizes estabelecidos nesta POSIN serão desenvolvidos para toda a organização - sede, escritórios de representação e unidades museológicas, devendo ser observados por todos os colaboradores, servidores, estagiários, terceirizados, prestadores de serviços, bolsistas, consultores e fornecedores, e se aplicam aos ambientes, sistemas, pessoas e processos, tanto em meio digital quanto nos meios analógicos de processamento, comunicação e armazenamento de informações.

Art. 4º A alta direção do Ibram deve manter postura exemplar em relação à segurança da informação e comunicação, bem como propiciar os recursos necessários para divulgações, capacitações, sensibilização e cumprimentos das normas e procedimentos.

Art. 5º São objetivos da Política de Segurança da Informação -POSIN do Ibram:

I - estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional;

II - apoiar a implantação das iniciativas relativas à Segurança da Informação e Comunicações; e

III - possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

Art. 6° Integram também a POSIN as normas, metodologias e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

**Seção II**

**Conceitos e definições**

Art. 7° Para os efeitos desta POSIN e, considerando o Glossário de Segurança da Informação, estabelecido pela Portaria GSI/PR nº 93, de 26 de setembro de 2019, entende-se por:

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

II - ativo – qualquer coisa que tenha valor para a organização;

III - 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;

IV - backup ou cópia de segurança – 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;

V - Comitê de Governança Digital - CGD - Comitê do tipo estratégico-executivo, de natureza Consultiva e deliberativa, com a finalidade de estabelecer políticas e diretrizes para a integração dos sistemas que compõem a plataforma operacional, assim como promover o alinhamento da área de negócio com a área de Tecnologia da Informação e Comunicações - TIC, em consonância com as ações do Poder Executivo Federal.

VI - Comitê Gestor de Segurança da Informação e Comunicação - CGSIC – grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

VII -computação em nuvem – modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços;

VIII - confidencialidade – propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

IX - credencial ( ou conta de acesso) – permissão, concedida por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha);

X - dado anonimizado – dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

XI - dado pessoal – informação relacionada a pessoa natural identificada ou identificável;

XII - dado pessoal 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;

XIII - dados processados – dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

XIV - 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;

XV - ETIR - acrônimo de Equipe de Tratamento de Incidentes de Rede, responsável pela prevenção, detecção e tratamento de incidentes de segurança, bem como pela criação e disseminação de práticas para uso seguro das Tecnologias de Informação e Comunicação.

XVI - gestão de continuidade – processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XVII - gestão de riscos – processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança quanto à realização de seus objetivos;

XVIII - gestão de segurança da informação – ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XIX - gestor de segurança da informação – responsável pelas ações de segurança da informação, no âmbito do órgão ou entidade da Administração Pública Federal;

XX - incidente – evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXI - incidente de segurança – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXII - informação – dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXIII - informação atualizada – informação que reúne os dados mais recentes sobre o tema, de acordo com sua natureza, com os prazos previstos em normas específicas ou conforme a periodicidade estabelecida nos sistemas informatizados que a organizam;

XXIV - informação classificada – informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

XXV - informação pessoal – informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

XXVI - informação sigilosa – informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo;

XXVII - integridade – propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVIII - metadados - representam "dados sobre dados" fornecendo os recursos necessários para entender os dados através do tempo, ou seja, são dados estruturados que fornecem uma descrição concisa a respeito dos dados armazenados e permitem encontrar, gerenciar, compreender ou preservar informações a respeito dos dados ao longo do tempo. Têm um papel importante na gestão de dados, pois a partir deles as informações são processadas, atualizadas e consultadas. As informações de como os dados foram criados/derivados, ambiente em que residem ou residiram, alterações realizadas, entre outras, são obtidas de metadados;

XXIX - perfil de acesso – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

plano de continuidade de negócios – documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

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

XXXI - plano de recuperação de negócios – documentação dos procedimentos e de informações necessárias para que o órgão ou entidade da Administração Pública Federal operacionalize o retorno das atividades críticas a normalidade;

XXXII - política de segurança – conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades;

XXXIII - política de segurança da informação -POSIN - documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação (Este termo substituiu o termo Política de Segurança da Informação e Comunicações);

XXXIV - plano de continuidade de negócios - PCN - documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

XXXV - plano de recuperação de negócios - PRN - documentação dos procedimentos e de informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade;

XXXVI - prestador de serviço – pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderá receber credencial especial de acesso;

XXXUII - programa de gestão de continuidade de negócios -PGCN - processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação

viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção;

XXXIV - quebra de segurança – ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

XL - risco (de segurança da informação) – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XLI - segurança cibernética – ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

XLII - Segurança da Informação -SI - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XLIII - segurança corporativa / orgânica – conjunto de medidas passivas com o objetivo de prevenir e até mesmo obstruir as ações que visem ao comprometimento ou à quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros;

XLIV - sensibilização – atividade que tem por objetivo atingir uma predisposição dos participantes para uma mudança de atitude sobre a segurança da informação, de tal forma que eles possam perceber em sua rotina pessoal e profissional ações que devem ser corrigidas. É uma etapa inicial da educação em segurança da informação;

XLV - serviços (conceito geral) – um meio de fornecer valor a clientes, facilitando a obtenção de resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XLVI - Serviços de Tecnologia da Informação – provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação;

XLVII - sistema de acesso – conjunto de ferramentas que se destina a controlar e a dar permissão de acesso a uma pessoa a um recurso;

XLVIII - sistema de informação – conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações em forma integrada;

XLIX - tecnologia da informação – ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

L - termo de responsabilidade e sigilo -TRS – 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;

LI - TIC – acrônimo de Tecnologia da Informação e Comunicações. Corresponde a um conjunto de recursos tecnológicos integrados entre si. Abrange todos os meios técnicos usados para tratar a informação e auxiliar na comunicação, o que inclui *hardware* e *software*.

LII - titular – pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

LIII - tratamento – toda operação realizada com dados pessoais, que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

LIV - 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;

LV - tratamento da informação classificada – conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo; e

LVI - usuário– pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade.

LVII - UORG - Unidade Organizacional, conforme Regimento do Ibram.

**Seção III**

**Princípios**

Art. 8° São princípios da Política de Segurança da Informação -POSIN do Ibram:

I- toda informação coletada, gerada, utilizada, em trânsito e armazenada por todos usuários deverá ser tratada como parte do patrimônio do Ibram, devendo ser assegurada sua confidencialidade, integridade e disponibilidade, bem como a proteção de dados pessoais e conformidade legal;

II-todos os recursos de informação do Ibram devem ser projetados para que seu uso seja consciente e responsável. Os recursos tecnológicos da instituição devem ser utilizados para a consecução de seus objetivos finalísticos;

III- deverão ser criados e instituídos controles apropriados, mapeamento de ativos, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que o Ibram julgar necessário, com vistas à redução dos riscos dos seus ativos de informação;

IV- os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades sob sua responsabilidade;

V- autorização definida pelos gestores: definir acessos e cancelar acessos aos recursos e aos locais restritos com base na solicitação do gestor de cada Unidade Organizacional - UORG, que também é responsável pelos ativos disponibilizados para uso;

VI- a segregação da administração e a execução de funções conflitantes ou áreas de responsabilidade críticas deverão ser implementadas para que ninguém detenha controle de um processo na sua totalidade, visando a reduzir os riscos de mau uso, acidental ou deliberado, dos ativos do Ibram, salvo em condições devidamente justificadas;

VII- todo o acesso a redes e sistemas do órgão deverá ser feito por meio de *credencial* de acesso único, pessoal e intransferível, qualificando o titular como responsável por todas as atividades desenvolvidas por meio dela, sendo pré-requisito o preenchimento do Termo de Responsabilidade e Sigilo – TRS;

VIII- o acesso e o uso dos ativos devem ser controlados e limitados de acordo com as funcionalidades necessárias para o cumprimento das atividades dos usuários, no estrito interesse institucional, para cumprimento de finalidades profissionais, lícitas, éticas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização do proprietário do ativo de informação;

IX- o Ibram pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocadas sob suas instalações;

X- cada usuário é responsável pela segurança das informações na instituição, principalmente das informações que estão sob sua responsabilidade;

XI- todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema e justificados, acordados, documentados, implantados e testados durante a fase de execução;

XII- a gestão da segurança da informação será realizada pelo Comitê de Governança Digital -CGD;

XIII- deverá constar em todos os contratos celebrados, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação, bem como o atendimento à Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018), a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no Ibram, inclusive provenientes de organismos internacionais;

XIV- nos contratos de prestação de serviços firmados pelo órgão deverá estar previsto que as empresas e profissionais prestadores de serviço devem entregar declaração expressa de compromisso em relação à confidencialidade e de termo de ciência das normas vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela instituição, devendo ser realizada revisão de procedimentos, implementação de soluções tecnológicas e atualização documental para atender aos requisitos de controle e governança previstos nos arts. 43 e 50 da LGPD ( gestão de riscos por contratos e códigos de conduta);

XV-somente será permitido o uso de ativos homologados e autorizados pelo Ibram, desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário responsável. Os ativos devem ter documentação atualizada, riscos mapeados, capacidade, manutenção e contingência adequadas e sua operação deve estar de acordo com essa Política de Segurança da Informação - POSIN , cláusulas contratuais e legislação em vigor;

XVI-os dados pessoais e a privacidade deverão ser protegidos de acessos não autorizados e de situações acidentais ou ilícitos de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequada ou ilícito que possa afetar a privacidade do titular;

XVII-toda a cadeia de suprimentos de TIC baseada em provedores de serviços no ambiente de computação em nuvem deverá ser avaliada por todos os aspectos da segurança, incluindo o cumprimento da legislação e regulamentação local e global, o gerenciamento de identidades, o monitoramento e auditoria regulares e as restrições de localização geográfica para proteger dados, metadados, informações e conhecimentos produzidos ou custodiados pelo Ibram;

XVIII -a conscientização contínua deverá ser promovida com o objetivo de instruir, informar e capacitar os usuários sobre questões relacionadas à segurança da informação na execução de suas atividades, bem como sobre o cumprimento de suas responsabilidades relacionadas aos ativos com o objetivo de minimizar riscos;

XIX- as diretrizes, normas e procedimento da POSIN deverão ser definidas, aprovadas pelo Comitê de Governança Digital, publicadas e comunicadas para todos os usuários e partes externas relevantes;

XX- a identificação de quebra ou fragilidade na segurança da informação deverá ser comunicada a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

XXI- a disponibilidade, o uso, o acesso e a proteção dos ativos que suportam os serviços e processos críticos deverão ser assegurados por meio de ações de administração de crise, prevenção e recuperação, com a implementação de estratégia de continuidade de negócios com o objetivo de mitigar possíveis interrupções causadas por desastres ou falhas; e

Parágrafo único. A Política de Segurança da Informação -POSIN, prevista nesta Resolução Normativa, será implementada por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

**CAPÍTULO II**

**DIRETRIZES GERAIS**

**Seção I**

**Do Tratamento da Informação**

Art. 9° O tratamento da informação no Ibram deverá observar diretrizes específicas e procedimentos próprios e deverão ser fixados em norma complementar, considerando como diretrizes gerais as normas de classificação de informações, o acesso à informação, o uso e descarte de ativos de informação, e o tratamento de dados pessoais, dentre outros temas afins, que serão fixados em estrita observância às leis e normas atinentes à Administração Pública Federal, considerando as competências regimentais.

**Seção II**

**Da Segurança Física e do Ambiente**

Art. 10. O Ibram deverá observar diretrizes específicas e procedimentos próprios de segurança física e do ambiente que deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I- o acesso físico ao ambiente deverá ser monitorado e controlado;

II- agentes públicos e prestadores de serviços deverão ser identificados por meio do uso de crachá.

III - o acesso de visitantes as dependências do órgão deverá ser autorizado por servidor;

IV- agentes públicos e prestadores de serviços desligados deverão ser excluídos da relação de pessoas autorizadas para acessar as dependências; e

V- os arquivos físicos, assim como os digitais, deverão ser protegidos e estabelecidos em locais de acesso restrito e devidamente trancados em sala ou armário específico com o controle de acesso sob responsabilidade do gestor responsável pelos ativos.

**Seção III**

**Da Gestão de Incidentes em Segurança da Informação**

Art. 11. No tratamento de incidentes em redes computacionais, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos -ETIR, responsável pelo tratamento e resposta aos incidentes, deverá considerar, na elaboração do Plano de Gerenciamento de Incidentes -PGI, no mínimo, as seguintes diretrizes:

I - todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;

II - o tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor;

III - a ocorrência de incidentes de segurança em redes de computadores do Ibram deverá ser comunicada ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, conforme procedimentos a serem definidos pelo próprio Centro, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública Federal , bem como a geração de estatísticas.

**Seção IV**

**Da Gestão de Ativos**

Art. 12. A gestão de ativos visa a estabelecer medidas de segurança pelo valor do ativo e em função dos riscos de impacto nos negócios, atividades e objetivos institucionais, com vistas à proteção de dados pessoais, à privacidade e à conformidade legal, implantando planos de contingência e de continuidade para os serviços e sistemas.

**Seção V**

**Da Gestão do Uso dos Recursos Operacionais e de Comunicações**

**Subseção I**

**Do Correio Eletrônico**

Art. 13. As diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico (e-mail) deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

I - o serviço de correio eletrônico será oferecido como um recurso institucional para apoiar os seus usuários no cumprimento das atividades; e

II - o correio eletrônico deverá ser utilizado somente para fins corporativos e relacionados às atividades do usuário no âmbito do Ibram, sendo vedado o uso para fins pessoais.

**Subseção II**

**Do Uso e Acesso à Internet**

Art. 14. As diretrizes específicas e procedimentos próprios de controles de uso e acesso à Internet serão fixadas em norma complementar, considerando as seguintes diretrizes gerais:

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

II - os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade do Ibram, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privativas da rede, visando a assegurar o cumprimento de sua Política de Segurança da Informação -POSIN.

**Subseção III**

**Do Serviço de Backup**

Art. 15. Os procedimentos próprios ao serviço de *backup* deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I- o serviço de *backup* deve ser automatizado por sistemas informacionais próprios, considerando, inclusive, a execução agendada fora do horário de expediente;

II- a solução de *backup* deverá ser mantida sempre atualizada, considerando suas diversas características tais como atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros;

III- a administração das mídias de *backup* deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter a sua segurança e integridade;

IV- as mídias de *backups* deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofres;

V- os *backup*s críticos exigem uma regra de retenção especial; e

VI- a execução de rotinas de *backup* e de recuperação deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

**Subseção IV**

**Do Uso Institucional das Redes Sociais**

Art. 16. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgar ou compartilhar informações do Ibram, será regida por normas internas especificas e deverá estar em consonância com esta POSIN e com os objetivos estratégicos do Ibram.

Art. 17. Os perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo.

**Subseção V**

**Da Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação**

Art. 18. As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação deverão observar os padrões, critérios e controles de segurança dispostos em normas e na legislação específica.

**Subseção VI**

**Do Uso de Computação em Nuvem**

Art. 19. O uso de recursos de computação em nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, será regido por normas e procedimentos específicos, que deverão ser instituídos pela unidade responsável pelos ativos de tecnologia e atenderão às determinações desta POSIN.

Art. 20. É vedado o uso de recurso de computação em nuvem não disponibilizado institucionalmente pelo Ibram, para o armazenamento de informação institucional ou custodiada.

**Subseção VII**

**Do Uso de Dispositivos Móveis**

Art. 21. A unidade responsável pelos ativos de tecnologia deverá instituir normas e procedimentos específicos para o uso de dispositivos móveis que acessarem aos ativos de tecnologia do Ibram, e atenderá às determinações desta POSIN.

**Subseção VIII**

**Dos Controles de Acesso**

Art. 22. Diretrizes específicas e procedimentos próprios de controles de acesso lógico e físico deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - os usuários terão identificação única, pessoal e intransferível;

II - o controle de acesso deverá considerar e respeitar o princípio do menor privilégio, pelo qual cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas atividades, para configurar as credenciais dos usuários aos ativos de informação do Ibram por meio de sistema de acesso;

III - a criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário;

IV - contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;

V- o acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma específica;

VI - as práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança; e

VII - o Ibram poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da POSIN ou das normas e procedimentos específicos dela decorrentes.

**Subseção IX**

**Da Gestão de Riscos**

Art. 23. A unidade responsável pelos ativos de tecnologia deverá implementar processo de Gestão de Riscos de Tecnologia da Informação, baseado na legislação própria, do qual deverá resultar na confecção de documento específico.

Art. 24. A Gestão de Riscos de Tecnologia da Informação será implementada com vistas a identificar os ativos de tecnologia relevantes e determinar ações de gestão apropriadas.

Art. 25. A Gestão de Riscos de Tecnologia da Informação deverá ser complementada pelo Plano de Continuidade de Tecnologia da Informação, visando a limitar os impactos de incidentes e a garantir que as informações requeridas para os processos de interesse institucional estejam prontamente disponíveis.

**Subseção X**

**Da Gestão de Continuidade**

Art. 26. O processo da Gestão de Continuidade deverá ser fixado pelo Programa de Gestão da Continuidade de Negócios - PGCN do Ibram, conforme legislação especifica, considerando os seguintes procedimentos:

I- desenvolver documento com as diretrizes do Programa de Continuidade;

II- definir as atividades críticas do Ibram;

III- avaliar os riscos a que estas atividades críticas estão expostas;

IV- definir as estratégias de continuidade para as atividades críticas; e

V- desenvolver e implementar, no mínimo, Planos de Gerenciamento de Incidentes (PGI), Plano de Continuidade de Negócios -PCN e Plano de Recuperação de Negócios -PRN.

Art. 27. O Programa de Gestão de Continuidade de Negócios (PGCN) deverá ser testado e revisado periodicamente, de forma a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Art. 28. Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios (PGCN) deverão ser executados em conformidade com os requisitos de segurança da informação e comunicações, necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, incluindo as pessoas, processos, infraestrutura e recursos de tecnologia da informação e comunicações.

**Subseção XI**

**Da Auditoria e Conformidade**

Art. 29. Para garantir a aplicação das diretrizes mencionadas nesta norma, além de fixar normas e procedimentos complementares sobre o tema, o Ibram poderá:

I- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou *wireless* (sem fio) e outros componentes da rede, de forma que a informação gerada por esses sistemas permitam a sua rastreabilidade, identificando usuários e respectivos acessos efetuados;

II- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gestor, seu superior ou por determinação do Comitê Gestor de Segurança da Informação e Comunicação -GSIC;

III - realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

IV- instalar sistemas de proteção, preventivos e/ou repressivos, para garantir segurança das informações e dos perímetros de acesso; e

V- desinstalar, a qualquer tempo, qualquer *software* ou sistema que represente risco ou esteja em desconformidade com as políticas, normas, procedimentos e princípios vigentes.

## CAPÍTULO III

## DA ESTRUTURA PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

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

I - o Gestor de Segurança da Informação;

II - o Comitê Gestor de Segurança da Informação e Comunicação - GSIC, com atuação por meio do Comitê de Governança Digital -CGD; e

III - uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos -ETIR.

§ 1º O gestor de segurança da informação será designado dentre os servidores públicos ocupantes de cargo efetivo e militares de carreira, com formação ou capacitação técnica compatível com a legislação vigente.

§ 2º. A coordenação do Comitê Gestor de Segurança da Informação e Comunicação - CGSIC ficará a cargo do Presidente do Comitê de Governança Digital -CGD.

§ 3º Caberá ainda ao Comitê Gestor de Segurança da Informação e Comunicação - CGSIC propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos, avaliar os incidentes de segurança, propor ações corretivas e definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação - POSIN e/ou das normas de segurança da informação complementares.

§ 4ºO funcionamento do Comitê Gestor de Segurança da Informação e Comunicação -CGSIC será definido por portaria específica.

§ 5ºDeverá ser elaborado documento de constituição da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, o qual designará suas atribuições e seu escopo de atuação.

§ 6º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos -ETIR será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe.

§ 7º A atuação da ETIR será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, sem prejuízo das demais metodologias e padrões conhecidos.

§ 8º As notificações enviadas pela ETIR ao Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo, bem como a troca de informações entre as Equipes existentes, devem seguir os formatos e os procedimentos que serão estabelecidos pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

### Seção I

### Das competências da Gestão de Segurança da Informação

Art. 31. Compete ao gestor de segurança da informação:

I - coordenar a elaboração da Política de Segurança da Informação - POSIN e das normas internas de segurança da informação do órgão;

II - assessorar a alta administração na implementação da Política de Segurança da Informação - POSIN;

III - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV - promover a divulgação da política e das normas internas de segurança da informação do Ibram a todos os servidores, usuários e prestadores de serviços que trabalham na autarquia;

V - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VI - propor recursos necessários às ações de segurança da informação;

VII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

VIII - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

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

X - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 32. São responsabilidades específicas do Comitê Gestor de Segurança da Informação e Comunicação - GSIC:

I - deliberar sobre a implementação das ações de segurança da informação e utilização dos recursos do Ibram;

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 -POSIN e das normas internas de segurança da informação;

IV - propor alterações e revisar periodicamente a Política de Segurança da Informação - POSIN do Ibram, em conformidade com a legislação existente sobre o tema;

V - propor, aprovar, alterar e revisar normas complementares e procedimentos internos de segurança da informação, em conformidade com a legislação existente sobre o tema; e

VI - indicar os integrantes da Equipe Técnica de Segurança da Informação e Comunicações.

Art. 33. São responsabilidades específicas da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

I - propor metodologias e processos específicos para a segurança da informação, como classificação da informação e avaliação de risco;

II - propor e apoiar iniciativas que visem à segurança dos ativos de informação do Ibram;

III - auxiliar na publicação e promoção da Política de Segurança da Informação - POSIN, das normas, e procedimentos específicos decorrentes, aprovados pelo Comitê Gestor de Segurança da Informação e Comunicação -GSIC;

IV - promover a conscientização dos usuários com relação à relevância da segurança da informação para o Ibram, mediante campanhas, palestras, treinamentos, dentre outros;

V - apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

VI - analisar, criticamente, incidentes em conjunto com o Comitê Gestor de Segurança da Informação e Comunicação - GSIC para encontrar oportunidades de melhoria e resolver possíveis inconformidades;

VII - manter comunicação efetiva com o Comitê Gestor de Segurança da Informação e Comunicação - GSIC sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o órgão; e

VIII - buscar alinhamento das práticas de segurança da informação com as diretrizes corporativas do Ibram e outras normas e boas práticas do mercado.

**Seção II**

**Das competências Gerais**

Art. 34. São responsabilidades de todos os usuários de serviços de rede, tais como internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do Ibram, com o objetivo de assegurar a segurança orgânica:

I- zelar pela segurança de suas credenciais de acesso aos serviços e espaços físicos e de seus respectivos dados;

II- seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do Ibram;

III- utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do Ibram;

IV -manter-se atualizado, em relação a esta e outras normas e procedimentos relacionados, buscando informações junto ao Gestor de Segurança da Informação e Comunicações -GSIC do Ibram sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações;

V-entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes; e

VI- ser responsável por todo prejuízo ou dano que vier a sofrer ou causar ao Ibram, em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação - POSIN e nas normas e procedimentos específicos dela decorrentes.

Art. 35. São responsabilidades específicas dos Gestores do Ibram:

I- tomar as ações necessárias para cumprir com suas atribuições, bem como dirimir eventuais dúvidas dos seus subordinados;

II-manter os processos de sua área aderentes às políticas, normas e procedimentos específicos de segurança da informação e comunicações do Ibram;

III-submeter ao Comitê Gestor de Segurança da Informação e Comunicação -GSIC o que for pertinente para o desenvolvimento de políticas específicas para o bom cumprimento da POSIN; e

IV- solicitar o bloqueio de acesso de usuário(s) por motivo de desligamento do Ibram, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos da autarquia.

Art. 36. São responsabilidades específicas da Coordenação de Tecnologia da Informação do Ibram:

I - zelar pela eficácia dos controles de segurança da snformação e comunicações utilizados e informar aos gestores e demais interessados dos riscos residuais;

II - configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para o cumprimento dos requisitos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação;

III- gerar e manter trilhas de auditoria com nível de detalhe para rastrear possíveis falhas e fraudes;

IV - prover segurança para sistemas com acesso público;

V - zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada usuário;

VI - administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o Ibram;

VII -definir as regras para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional e/ou dedicados à visitação externa, exigindo-se o seu cumprimento dentro do Ibram;

VIII- realizar, quando solicitado por chamado, o backup de ativo de TIC ,nos casos de movimentações internas, antes do ativo ser disponibilizado para outro usuário;

IX- planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão de forma segura;

X- atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, que será o encarregado pelo uso da conta, devendo ser observado que a responsabilidade pela gestão *das credenciais de usuários externos é do gestor do contrato de prestação de* serviços ou do gestor do setor em que o usuário externo desempenha suas atividades;

XI- proteger os ativos de informação do Ibram contra códigos maliciosos;

XII- garantir, quando demandado por solicitação dos gestores, via chamado, o bloqueio de acesso de usuários por motivo de desligamento do Ibram, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos do Ibram;

XIII- garantir que todos os servidores, estações de trabalho e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais do Governo Brasileiro; e

XIV- monitorar o ambiente de TIC, gerando dados indicadores e históricos de uso da capacidade da rede e de seus equipamentos, tais como: tempo de resposta no acesso à internet e aos sistemas críticos, períodos de indisponibilidade no acesso à internet e aos sistemas críticos, incidentes de segurança e atividade de todos os usuários durante os acessos às redes externas, inclusive internet, por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos.

## CAPÍTULO IV

## DAS PENALIDADES

Art. 37. As ações que violem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de segurança da informação serão devidamente apuradas, sendo cabíveis aos responsáveis as sanções administrativas, civis e penais.

## CAPÍTULO V

## ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 38. Os documentos que comporão a estrutura normativa de gestão de segurança da informação serão divididos em três categorias:

I - política (nível estratégico): trata-se de documento, que define as regras de alto nível que representam os princípios básicos que o Ibram decidiu incorporar à sua gestão de acordo com a visão estratégica da sua alta direção e serve como base para que as normas e os procedimentos sejam criados e detalhados;

II - normas (nível tático): especificam as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política; e

III - procedimentos (nível operacional): instrumentalizam o disposto nas normas e na política, permitindo sua direta aplicação nas atividades do dia a dia.

Art. 39. Os documentos integrantes da estrutura normativa de gestão de segurança da informação do Ibram deverão ser aprovados pelo Comitê Gestor de Segurança da Informação e Comunicação - GSIC.

## CAPÍTULO VIII

## DISPOSIÇÕES FINAIS

Art. 40. A política de segurança, as normas e os procedimentos complementares serão revisados periodicamente segundo os prazos estabelecidos pelo Comitê Gestor de Segurança da Informação e Comunicação - GSIC ou sempre que algum fato ou evento relevante acontecer, não excedendo a 4 (quatro) anos.

Art. 41. Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados para todos os servidores, colaboradores, estagiários, aprendizes e prestadores de serviços do Ibram quando de sua admissão, e também publicadas na Intranet corporativa, de maneira que seu conteúdo fique amplamente disponível a seus colaboradores a qualquer tempo.

Art. 42. Os casos omissos e as dúvidas na aplicação da Política de Segurança da Informação - POSIN e suas normas complementares serão resolvidas pelo Comitê Gestor de Segurança da Informação e Comunicação - GSIC.

Brasília, 29 de julho de 2021.

Este texto não substitui o publicado no DOU de 02 de agosto de 2021 (clique aqui).