PORTARIA N° 172, DE 26 DE MAIO DE 2017.

O PRESIDENTE DO INSTITUTO BRASILEIRO DE MUSEUS - IBRAM, no uso das atribuições que lhe conferem o Art. 20, II e IV, do Anexo I, do Decreto n° 6.845, de 20 de janeiro de 2009, e considerando a necessidade de regulamentar a utilização dos recursos institucionais do IBRAM disponibilizados aos seus servidores, resolve:

Art. 1º Fica aprovada, na forma do Anexo a esta Portaria, a Política de Segurança da Informação e Comunicações do Instituto Brasileiro de Museus – IBRAM – POSIC/IBRAM, em consonância com o Parágrafo único do Art. 1º da Portaria nº 25, de 7 de abril de 2015, que institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura, com o inciso VII do Art. 5º da Instrução Normativa nº 01/2008 do gabinete de Segurança Institucional da Presidência da República e com os itens 6 e 7 de sua Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009.

Art. 2º Esta Portaria Normativa entra em vigor na data de sua publicação.

Marcelo Mattos Araujo
Presidente

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO BRASILEIRO DE MUSEUS – IBRAM – POSIC/IBRAM

1. ESCOPO

1.1. A Política de Segurança da Informação e Comunicações (PoSIC) objetiva instituir e implementar 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

1.2. A PoSIC 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.

1.3. Os objetivos e diretrizes estabelecidos nesta Política serão desenvolvidos para toda a organização, devendo ser observados por todos servidores, colaboradores, fornecedores e prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

1.4. Integram também a PoSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

2. CONCEITOS E DEFINIÇÕES

2.1. Para os efeitos desta Política entende-se por:

a) Agente Público: Aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao IBRAM;
b) Ativo: Aquilo que tem valor- tangível ou intangível – para o IBRAM (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional);

c) Autenticidade: Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada física, ou por um determinado sistema, órgão ou entidade;
d) *Backup*: Método de reprodução de dados em cópias de segurança, com o intuito de os preservar caso os originais se deteriorem ou sejam eliminados;
e) Colaborador eventual: Aquele profissional dotado de capacidade técnica específica, que recebe a incumbência da execução de determinada atividade sob a permanente fiscalização do delegante, sem qualquer caráter empregatício;
f) Comitê de Segurança da Informação e Comunicações: Grupo de representantes de unidades do IBRAM com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações;
g) Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
h) Credenciais: Autorização dada por alguém a uma outra pessoa, a fim de que possa tratar de certos assuntos de sua competência;
i) Disponibilidade: Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
j) Endomarketing: Conjunto de ações de marketing dirigidas ao público interno da organização;
k) Gestão de Continuidade: Conjunto de processos que buscam minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação;
l) Gestão de Riscos de Segurança da Informação e Comunicações: Conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.
m) Gestão de Segurança da Informação e Comunicações: Ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;
n) Incidente de segurança: Qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas de computação ou de rede de computadores;
o) Integridade: Estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada ou documentada;
p) *Login*: Significa ter acesso a uma conta de email, computador, celular ou outro serviço fornecido por um sistema informático;
q) Plano de Continuidade de Negócios: Documentação dos procedimentos e informações necessárias para que o IBRAM mantenha seus ativos de informação

críticos e a continuidade de suas atividades críticas em local alternativo, num nível previamente definido, em caso de incidentes.

r) Plano de Gerenciamento de Incidentes: Plano de ação claramente definido e documentado, a ser usado quando ocorrer um incidente, abrangendo as principais pessoas, recursos, serviços e ações necessárias para implementar o processo de gerenciamento de incidentes;
s) Plano de Recuperação de Negócios: Documentação dos procedimentos e informações necessárias para que o IBRAM operacionalize o retorno das atividades críticas à normalidade.
t) Política de Segurança da Informação e Comunicações: 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 e comunicações;
u) Preservação Digital: Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo acesso e interpretação dos documentos digitais pelo tempo que for necessário;
v) Quebra de Segurança: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
w) Segurança da Informação e Comunicações: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
x) *Restore*: Método de recuperação de dados através da utilização das mídias que contém o *backup*;
y) *Software*: programa de computador desenvolvido para executar um conjunto de ações previamente definidas;
z) Tratamento de Incidentes de Segurança em Redes Computacionais: Serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
aa) Usuário: Agente público com acesso autorizado a sistemas, redes de dados ou informações do IBRAM.

3. PRINCÍPIOS

3.1. São princípios da Política de Segurança da Informação e Comunicações do IBRAM:

a) Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, no âmbito do IBRAM. Possíveis exceções devem ser devidamente explícitas e formalizadas.

b) 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.
c) Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação.
d) 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.
e) Todo o acesso a redes e sistemas do órgão deverá ser feito, preferencialmente, por meio de *login* de acesso único, pessoal e intransferível.
f) 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.
g) Cada usuário é responsável pela segurança das informações dentro do IBRAM, principalmente das que estão sob sua responsabilidade.
h) Com o objetivo de reduzir o risco de descontinuidade das atividades do órgão e de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, deverão ser implantados planos de contingência e de continuidade para os principais serviços e sistemas.
i) 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.
j) A gestão da segurança da informação no IBRAM será realizada por comitê multidisciplinar, ora designado Comitê de Segurança da Informação e Comunicações (CSIC).
k) Deverá constar em todos os contratos do IBRAM, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no IBRAM, inclusive provenientes de organismos internacionais;
l) Deverá estar previsto em todos os contratos do IBRAM, quando o objeto for pertinente, 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;
m) Esta Política de Segurança da Informação e Comunicações será implementada no IBRAM 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.

4. OBJETIVOS

4.1. Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade, são objetivos da Política de Segurança da Informação e Comunicações do IBRAM:

a) 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.
b) Designar, definir ou alterar papéis e responsabilidades do Comitê de Segurança da Informação e Comunicações (CSIC).
c) Apoiar a implantação das iniciativas relativas à Segurança da Informação e Comunicações.
d) Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.
e) Preservação de longo prazo de materiais digitais, independentemente da área de aplicação.

5. SISTEMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

5.1. Papéis.

5.1.1. São papéis referentes à Política de Segurança da Informação e Comunicações do IBRAM – POSIC/IBRAM:

a) Usuários Internos: Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do IBRAM.
b) Usuário Externos: Prestadores de serviços contratados direta ou indiretamente pelo IBRAM e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
c) Gestores: Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
d) Área de Tecnologia da Informação (TI): Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custodiante da informação.
e) Gestor de Segurança da Informação e Comunicações (GSIC): Servidor responsável pela gestão da segurança da informação em todos os seus aspectos.
f) Equipe Técnica de Segurança da Informação e Comunicações: Servidores responsáveis por implementar e administrar as soluções de segurança da informação.
g) Comitê de Segurança da Informação e Comunicações (CSIC): Comitê Temático, vinculado ao Comitê Gestor de Tecnologia da Informação, responsável pelas decisões de alto nível relacionadas à gestão da segurança da informação.

5.2. Responsabilidades.

5.2.1. 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:

a) Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso.
b) Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do instituto.
c) Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do IBRAM.
d) Manter-se atualizado, em relação a esta e outras normas e procedimentos relacionados, buscando informações junto ao Gestor de Segurança da Informação e Comunicações da instituição sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.
e) Entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes.
f) 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 e Comunicações e nas normas e procedimentos específicos dela decorrentes.

5.2.2. O IBRAM poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da PoSIC ou das normas e procedimentos específicos dela decorrentes.

5.2.3. São responsabilidades específicas dos Gestores do IBRAM:

a) Tomar as ações necessárias para cumprir com suas atribuições, bem como dirimir eventuais dúvidas dos seus subordinados.
b) Manter os processos de sua área aderentes às políticas, normas e procedimentos específicos de segurança da informação e comunicações do IBRAM.
c) Submeter ao Comitê de Segurança da Informação e Comunicações o que for pertinente para o desenvolvimento de políticas específicas para o bom cumprimento da PoSIC.
d) 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 do instituto.

5.2.4. São responsabilidades específicas da área de Tecnologia da Informação do IBRAM:

a) Zelar pela eficácia dos controles de Segurança da Informação e Comunicações utilizados e informar aos gestores e demais interessados dos riscos residuais.
b) Negociar e acordar com os gestores níveis de serviço relacionados a Segurança da Informação e Comunicações, incluindo os procedimentos de resposta a incidentes.
c) 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.
d) Gerar e manter trilhas de auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
e) Garantir a segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
f) Zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de casos em que possam os funcionários ocultar ou dificultar o acesso às suas próprias ações.
g) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o IBRAM.
h) Informar previamente o Gestor de Segurança da Informação e Comunicações sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo antes que a informação seja definitivamente descartada pelo custodiante.
i) Nas movimentações internas dos ativos de Tecnologia da Informação, assegurar-se de que as informações de determinado usuário não sejam removidas de forma irrecuperável antes que seja disponibilizado o ativo para outro usuário.
j) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas internas da organização.
k) 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 (a responsabilidade pela gestão dos "*logins*" 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).
l) Proteger continuamente todos os ativos de informação do instituto contra códigos maliciosos, garantindo que todos os novos ativos só entrem para o ambiente de produção após estarem livres de possíveis ameaças.
m) Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades em nenhum dos ambientes operacionais do IBRAM, seja de desenvolvimento, teste, homologação ou produção (quando tais ambientes forem acessados por terceiros,

a responsabilização deve ser explicitada nas cláusulas dos instrumentos contratuais).

n) Definir as regras formais 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 da instituição.
o) Responsabilizar-se pela gestão, manuseio ou guarda de assinatura de certificados digitais corporativos.
p) Garantir, da forma mais rápida possível, com recebimento de solicitação formal dos gestores, 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 instituto.
q) 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.
r) Monitorar o ambiente de TI, 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). Esses dados servirão para posteriores melhorias e ajustes da capacidade institucional.

5.2.5. São responsabilidades específicas do Comitê de Segurança da Informação e Comunicações do IBRAM:

a) Assessorar o IBRAM na implementação das ações de segurança da informação.
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação.
c) Propor alterações e revisar periodicamente a Política de Segurança da Informação e Comunicações do IBRAM, em conformidade com a legislação existente sobre o tema.
d) Propor, aprovar, alterar e revisar normas complementares e procedimentos internos de segurança da informação, em conformidade com a legislação existente sobre o tema.
e) Subsidiar o Comitê Gestor de Tecnologia da Informação do IBRAM nas decisões relativas à segurança da informação.
f) Indicar os integrantes da Equipe Técnica de Segurança da Informação e Comunicações.

5.2.6. A coordenação do Comitê de Segurança da Informação e Comunicações ficará a cargo do Gestor de Segurança da Informação e Comunicações, servidor público designado pelo Presidente do IBRAM;

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

5.2.8. O Comitê de Segurança da Informação e Comunicações deverá ser formalmente instituído pelo Comitê Gestor de Tecnologia da Informação do IBRAM, como Comitê Temático (segundo art. 4°, inc. I da Portaria IBRAM n° 235, de 20/07/2010) e integrado por gestores com nível hierárquico gerencial – nomeados formalmente pelo Presidente do IBRAM para participar do grupo. Sua composição deve incluir representante de cada uma das seguintes áreas: Presidência, Auditoria Interna, Procuradoria, Departamento de Planejamento e Gestão Interna (DPGI), Departamento de Difusão, Fomento e Economia dos Museus (DDFEM), Departamento de Processos Museais (DPMUS), Coordenação Geral de Sistemas de Informações Museais (CGSIM).

5.2.9. O funcionamento do Comitê de Segurança da Informação e Comunicações será definido por portaria específica.

5.2.10. São responsabilidades específicas do Gestor de Segurança da Informação e Comunicações do IBRAM:

a) Examinar, formular, promover e coordenar as ações de Segurança da Informação e Comunicação do IBRAM.
b) Acompanhar investigações e avaliações de danos decorrentes de quebras de segurança.
c) Propor às autoridades competentes os recursos necessários às ações de Segurança da Informação e Comunicações no IBRAM.
d) Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe Técnica de Segurança da Informação e Comunicações do IBRAM.
e) Divulgar e supervisionar o cumprimento da Política de Segurança da Informação e Comunicações e suas normas complementares.
f) Propor normas e procedimentos relativos à Segurança da Informação e Comunicações no âmbito do IBRAM.
g) Resolver os casos omissos e as dúvidas surgidas na aplicação da Política de Segurança da Informação e Comunicações e suas normas complementares.

5.2.11. São responsabilidades específicas da Equipe Técnica de Segurança da Informação e Comunicações:

a) Propor metodologias e processos específicos para a segurança da informação, como classificação da informação e avaliação de risco.

b) Propor e apoiar iniciativas que visem à segurança dos ativos de informação do IBRAM.
c) Auxiliar na publicação e promoção da Política de Segurança da Informação, das normas, e procedimentos específicos decorrentes, aprovados pelo Comitê de Segurança da Informação e Comunicações.
d) Promover a conscientização dos usuários com relação à relevância da segurança da informação para o IBRAM, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
e) Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
f) Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação e Comunicações para encontrar oportunidades de melhoria e resolver possíveis inconformidades.
g) Manter comunicação efetiva com o Comitê de Segurança da Informação e Comunicações sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o órgão.
h) Buscar alinhamento das práticas de segurança da informação com as diretrizes corporativas da instituição e outras normas e boas práticas do mercado.
i) Atuar, quando necessário e no que couber, com atribuições de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), da qual trata a Norma Complementar 05 IN01/DASIC/GSI/PR.

6. DAS DIRETRIZES GERAIS

6.1. Tratamento da Informação

6.1.1. Diretrizes específicas e procedimentos próprios de tratamento da informação corporativa deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

a) Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de *backup* e poderão ser perdidos caso ocorra uma falha na máquina, sendo, portanto, de responsabilidade do próprio usuário.
b) Arquivos pessoais e/ou não pertinentes às atividades institucionais do IBRAM (fotos, músicas, vídeos, etc.) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar os dispositivos de armazenamento nos servidores. Caso identificados, tais arquivos poderão ser excluídos definitivamente sem a necessidade de comunicação prévia ao usuário.

c) Normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas em estrita aderência às leis e normas atinentes à Administração Pública Federal – considerando as competências regimentais.

6.2. Controles de Acesso

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

a) O controle de acesso deverá considerar e respeitar o princípio do menor privilégio, o qual cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas atividades, para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação do IBRAM.
b) A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário.
c) Para o usuário que não exerce funções de administração de rede será criada uma única conta institucional de acesso, pessoal e intransferível.
d) Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.
e) 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.
f) As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.

6.3. Correio Eletrônico

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

a) O correio eletrônico é uma ferramenta disponível e obrigatória para todos os usuários do IBRAM, independentemente de seu vínculo funcional.
b) O correio eletrônico do IBRAM deverá ser utilizado somente para fins corporativos e relacionados às atividades do usuário no âmbito da autarquia.
c) O uso do correio eletrônico do IBRAM não poderá ser utilizado para tratar de assuntos de cunho pessoal.

6.4. Uso e acesso à Internet

6.4.1. Diretrizes específicas e procedimentos próprios de controles de uso e acesso à Internet deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

a) Todas as regras corporativas sobre uso de Internet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de obtenção de benefícios, a proteção dos ativos de informação do IBRAM deverá sempre ser privilegiada.
b) Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente do órgão.
c) Em conformidade com a Norma Complementar n° 17/IN01/GSI/PR, é vedada a terceirização completa da administração e da gestão de perfis de órgãos e entidades da Administração Pública Federal nas redes sociais, assim entendida a terceirização que viole o disposto no item "B".
d) Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, o IBRAM, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores.
e) 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 e Comunicações.

6.5. Serviço de Backup

6.5.1. Os procedimentos próprios ao serviço de *backup* (cópia de segurança) deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

a) O serviço de *backup* deve ser automatizado por sistemas informacionais próprios, considerando, inclusive, a execução agendada fora do horário de expediente normal do órgão, nas chamadas "janelas de *backup*" – períodos em que não há nenhum ou pouco fluxo de dados nos sistemas de informática.

b) A solução de *backup* deverá ser mantida sempre atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros).
c) A administração das mídias de *backup* deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter a sua segurança e integridade.
d) Deverá ser mantido no IBRAM estoque de mídias de *backup* para uso emergencial.
e) As mídias de *backups* históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofres.
f) Os *backups* críticos para o bom funcionamento dos serviços do IBRAM exigem uma regra de retenção especial.
g) A execução de rotinas de *backup* e de *restore* deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

6.6. Data Center

6.6.1. Os procedimentos para administração do centro de processamento de dados (data center) deverão ser fixados em norma própria, considerando as seguintes diretrizes gerais:

a) A administração de dados e de serviços de data center é tarefa tecnicamente complexa e sua realização deve balizar-se nas melhores práticas de mercado e na alocação de profissionais com perfil técnico adequado.
b) O acesso físico ao data center deverá ser realizado mediante a concessão da chave do ambiente juntamente com a autorização de um servidor qualificado para tal.
c) O acesso ao data center por visitantes ou terceiros somente poderá ser realizado com acompanhamento ou autorização de um servidor qualificado, que deverá preencher solicitação de acesso prevista em norma própria, bem como assinar Termo de Responsabilidade.
d) No caso de desligamento de usuários que possuam acesso ao data center, imediatamente após a formalização do procedimento deverá ser providenciada a sua exclusão da relação de pessoas autorizadas para realizarem o acesso às suas instalações.
e) A função de administrador do datacenter deverá ser atribuída exclusivamente a servidor público efetivo, preferencialmente vinculado à área de infraestrutura de TI.

6.7. Monitoramento e Auditoria do Ambiente

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

a) Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de forma que a informação gerada por esses sistemas permitam a sua rastreabilidade, identificando usuários e respectivos acessos efetuados.
b) Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação.
c) Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade.
d) Instalar sistemas de proteção, preventivos e/ou repressivos, para garantir segurança das informações e dos perímetros de acesso.
e) Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos e princípios vigentes.

6.8. Gestão de Riscos

6.8.1. Diretrizes específicas e procedimentos próprios ao processo de Gestão de Riscos de Segurança da Informação e Comunicações deverão ser fixadas no Plano de Tratamento de Riscos, considerando as seguintes diretrizes gerais:

n) Alinhamento aos objetivos estratégicos, à estrutura organizacional, aos processos de trabalho e requisitos legais do IBRAM.
o) Alinhamento a esta Política de Segurança da Informação e Comunicações.
p) Aplicado às contratações de soluções de Tecnologia da Informação.

6.9. Gestão de Continuidade

6.9.1. O processo da Gestão de Continuidade deverá ser fixado pelo Programa de Gestão da Continuidade de Negócios (PGCN) do IBRAM, conforme Norma Complementar nº 06/IN01/DSIC/GSIPR, considerando os seguintes procedimentos:

a) Desenvolver documento com as diretrizes do Programa de Continuidade.
b) Definir as atividades críticas do IBRAM.
c) Avaliar os riscos a que estas atividades críticas estão expostas.
d) Definir as estratégias de continuidade para as atividades críticas.
e) Desenvolver e implementar, no mínimo, Planos de Gerenciamento de Incidentes (PGI), Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Negócios (PRN).

6.9.2. 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.

6.9.3. 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.

6.10. Tratamento de Incidentes em Redes Computacionais

6.10.3. No Tratamento de Incidentes em Redes Computacionais, a Equipe Técnica de Segurança da Informação e Comunicações, responsável pelo tratamento e resposta aos incidentes, deverá considerar, na elaboração do Plano de Gerenciamento de Incidentes (PGI), no mínimo, as seguintes diretrizes:

a) Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas.
b) 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, naquilo que diz respeito ao estabelecimento de graus de sigilo.
c) No caso de incidentes notificados terem indícios de ilícitos criminais, o Gestor de Segurança da Informação ou membros da Equipe Técnica de Segurança da Informação e Comunicações terão como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços do IBRAM.
d) A ocorrência de incidentes de segurança em redes de computadores do IBRAM deverá ser comunicada ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR), conforme procedimentos a serem definidos pelo próprio centro, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública Federal (APF), bem como a geração de estatísticas.

7. PENALIDADES

7.1. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, sobre às quais o IBRAM aplicará todas as medidas cabíveis nos âmbitos administrativo, civil e judicial.

8. ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

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

a) Política (nível estratégico): Trata-se deste 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 alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados.
b) Normas (nível tático): Especificam as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política.
c) Procedimentos (nível operacional): Instrumentalizam o disposto nas normas e na política, permitindo sua direta aplicação nas atividades do dia-a-dia.

8.2. Os documentos integrantes da estrutura normativa de gestão de segurança da informação do IBRAM deverão ser aprovados segundo as seguintes instâncias:

a) POLÍTICA: Comitê Gestor de Tecnologia da Informação.
b) NORMA COMPLEMENTAR: Comitê de Segurança da Informação e das Comunicações.
c) PROCEDIMENTO: Coordenação Geral de Tecnologia da Informação.

8.3. A política de segurança, as normas e os procedimentos complementares serão revisados periodicamente segundo os prazos estabelecidos pelo Comitê de Segurança da Informação ou sempre que algum fato ou evento relevante acontecer.

8.4. 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.

9. DISPOSIÇÕES FINAIS

9.1. Para a uniformização da informação organizacional, esta Política de Segurança da Informação e Comunicações deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço do IBRAM, a fim de que seja conhecida e cumprida dentro e fora da autarquia.

9.2. O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas cabíveis nos âmbitos administrativo, civil e judicial.