

**INSTRUÇÃO NORMATIVA Nº 2, DE 29 DE JUNHO DE 2018**



Documento assinado eletronicamente por **Denio Menezes da Silva, Diretor(a) do Departamento de Planejamento e Gestão Interna**, em 29/06/2018, às 16:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [http://sei.museus.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](http://sei.museus.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0308766** e o código CRC **84A56C5A**.

**NORMA DE SEGURANÇA PARA USO DE INTERNET**

**1. OBJETIVO**

I. Esta norma tem como objetivo informar aos usuários da rede do Instituto Brasileiro de Museus quanto às regras de utilização do serviço de internet de forma a preservar a confidencialidade, integridade e disponibilidade das informações.

**2. APLICAÇÃO**

I. Esta norma se aplica ao Instituto Brasileiro de Museus (Sede, Museus e Representações).

**3. DOCUMENTOS DE REFERÊNCIAS**

- I. NBR ISO/IEC 17799:2005 – Código de Práticas para a Gestão de Segurança da Informação.
- II. ISO/IEC Guide 73:2002 – Gestão de Riscos/Vocabulário – Recomendações para uso em normas.
- III. Decreto nº. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- IV. Decreto nº. 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
- V. Política de Segurança da Informação do Instituto Brasileiro de Museus.
- VI. Cartilha de segurança para a Internet, versão 3.1 do cert.br – <http://cartilha.cert.br>.

**4. RESPONSABILIDADES**

Responsável	Atribuição
CTINF/DPGI	Aprovar e publicar este documento
Comitê de Segurança da Informação do Instituto Brasileiro de Museus	Revisar, monitorar e encaminhar este documento para aprovação

**5. PROCEDIMENTOS**

**5.1. Regras Gerais para Uso de Internet**

- I. O acesso à internet disponibilizado aos usuários da rede pelo Instituto Brasileiro de Museus - IBRAM deve ser realizado, prioritariamente, para os interesses de trabalho da Instituição.
- II. O uso da internet pelos Usuários da Rede deve observar aos princípios e limites da ética, bom senso e razoabilidade, bem como o acesso em ambientes que não contenham, recebam ou transmitam informações institucionais, sigilosas.
- III. É atribuição exclusiva da CTINF definir os softwares homologados para uso da internet no Instituto Brasileiro de Museus.
- IV. O acesso à internet por meio da rede local não pode ser realizado utilizando-se mais de um meio de comunicação simultaneamente.

**5.2. Permissão de Acesso à Internet**

I. A todo Usuário da Rede local do IBRAM é facultado o acesso internet em conformidade com os termos estabelecidos nesta norma.

**5.3. Cancelamento e Bloqueio do Acesso à Internet**

- I. O acesso à Internet pelo Usuário da Rede será obrigatoriamente cancelado quando do seu desligamento do Instituto, ao final do contrato ou de qualquer outro ato jurídico que mantém vínculo do mesmo com a Instituição.
- II. O cancelamento, bloqueio e desbloqueio do acesso à internet seguem as condições descritas na Norma de Criação e Manutenção de Contas e Senhas.

**5.4. Uso da Internet**

- I. O acesso à internet concedido ao Usuário da Rede do IBRAM é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados à Instituição por meio de seu uso.
- II. O acesso à internet quando realizado pela Rede Local disponibilizada pela CTINF por meio do browser homologado e disponibilizado nas estações de trabalho do IBRAM ou equipamentos portáteis, não poderá ser feito via proxies externos, que permitem burlar as regras de acesso estabelecidas.
- III. O Usuário da Rede deverá utilizar a Internet de forma a não causar tráfego desnecessário na Rede Local do IBRAM e demais redes de outras instituições.

IV. Todo serviço disponibilizado na Internet, antes de ser disponibilizado na rede local do IBRAM, deverá ser avaliado quanto a sua necessidade pelo Comitê de Segurança da Informação após a avaliação e emissão de relatório técnico fornecido pela CTINF, que deverá considerar os aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

#### 5.5. **Vedações na utilização da internet**

- I. Acesso a sites com códigos maliciosos e vírus de computador;
- II. Acesso a sites com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;
- III. Acesso a sites ou arquivos que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;
- IV. Acesso a sites ou arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares;
- V. Realizar download de arquivos que não estejam relacionados às necessidades de trabalho do IBRAM, em especial arquivos que contenham materiais ilegais ou que não respeitem os direitos autorais;
- VI. Realizar atividades relacionadas a jogos eletrônicos pela internet;
- VII. Assistir programas de TV, filmes e séries exceto nos casos em que tais ações sejam condizentes com atividades de trabalho do IBRAM; e
- VIII. Transferir e armazenar informações do IBRAM em sites com os quais não haja um contrato ou acordo de responsabilidade estabelecido com o IBRAM;

#### 5.6. **Outras vedações e/ou liberações**

- I. É de responsabilidade da CTINF garantir os serviços de transferência e compartilhamento de arquivos com informações do IBRAM na Internet de forma segura.
- II. O usuário sempre deverá certificar a procedência do site, verificando, quando cabível, o certificado digital do mesmo, principalmente para realizar transações eletrônicas via internet, digitando o endereço do site diretamente no browser da estação de trabalho, nunca clicando em um link existente em uma página ou em uma mensagem de correio eletrônico.
- III. A CTINF deverá homologar softwares ou serviços de mensagens instantâneas, de voz, de videoconferência e de transferência de arquivos via internet.
- IV. É vedado aos usuários disponibilizar informações de propriedade do IBRAM em sites da internet sem observar sua classificação e o público a que se destina.
- V. Só será permitida a utilização da rede local por máquinas que atendam a todos os requisitos de segurança da informação estabelecidos pelo IBRAM.
- VI. A utilização de equipamentos pessoais no ambiente do IBRAM, só será permitido desde que não acesse a rede local. Quando disponível será liberado o acesso à Internet por meio da rede sem fio (wireless), mediante concordância do usuário ao Termo de Responsabilidade.
- VII. Fica liberado o acesso a sítios (sites) de governo, de órgãos de ensino e pesquisa, de organismos internacionais, sites de pesquisa da Internet, jornais e revistas de cunho cultural e educativo, órgão técnico normativos e demais sites de interesse institucional.
- VIII. Para liberação de acesso a Redes Sociais e sítios (sites) de compartilhamento de vídeos será necessário requisição fundamentada para a CTINF, devendo ser assinada pelo dirigente da unidade - Chefe de Gabinete, Chefe da Auditoria, Chefe da Procuradoria, Coordenador do NRI, Diretor de Departamento, Coordenador Geral, Diretor de Museu e Chefe da Representação.
- IX. As solicitações de liberação a sítios (sites) bloqueados serão submetidas à CTINF que fará a análise técnica em relação à verificação do conteúdo e vulnerabilidades de segurança, emitindo seu parecer para deliberação no âmbito do Comitê de Segurança da Informação.

#### 6. **MONITORAMENTO**

- I. O acesso à internet pelos Usuários da Rede do IBRAM deverá ser monitorado pela CTINF para fins de verificação e controle do volume de dados trafegados;
- II. Como resultado do monitoramento a CETIF deverá produzir relatórios gerenciais com informações que possibilitem a tomada de decisão sobre o volume e demanda de uso da Internet no Instituto;
- III. As informações monitoradas têm relação com os endereços acessados, quantidade, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, devendo ser processadas com parâmetros gerais, não personalizados;
- IV. O superior imediato pode solicitar formalmente um relatório com as informações de acesso da internet de um de seus Usuários da Rede, para si ou para outro, nas seguintes situações:
  - Suspeita de infração à Política de Segurança da Informação em vigor e normas correlatas;
  - Necessidade de visualizar os sites acessados e o tempo gasto nos mesmos por seus Usuários de Rede.

#### 7. **DISPOSIÇÕES FINAIS**

- I. Os Usuários da Rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à área de gestão de incidentes.
- II. Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a área de gestão de incidentes deverá ser imediatamente acionada para tomar as providências necessárias para sanar as causas, podendo inclusive determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do Instituto Brasileiro de Museus.
- III. Os usuários da Rede que descumprirem as regras estabelecidas por esta Norma terão seu acesso à rede bloqueado até a apuração de responsabilidades.
- IV. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação.