

Ministério da Cultura (MinC)

Norma Interna

de Segurança da Informação 04

(NISI 04)

Uso Aceitável de Internet e E-mail

Brasília, fevereiro de 2024

Escopo

Esta norma se aplica a serviço de Internet e E-mail Institucional em toda estrutura organizacional do Ministério da Cultura. De maneira que se aplica a todos os processos de negócios e dados, sistemas de informação e componentes, pessoal e áreas físicas do Ministério da Cultura.

Não inclui os serviços de internet utilizados pelos servidores/colaboradores no momento de sua atuação no serviço remoto.

Declarações da norma

Dos princípios gerais:

- I. A Norma de Uso Aceitável da Internet e E-mail tem por objetivo estabelecer responsabilidades e requisitos básicos de utilização da Internet e E-mail Institucional no âmbito do Ministério da Cultura em atenção ao disposto no Art. 26º da Política de Segurança da Informação (POSIN).
- II. A Norma de Uso Aceitável da Internet e E-mail deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
- III. Entende-se por acesso e uso da Internet os serviços oferecidos na Rede Mundial de Computadores.
- IV. Entende-se por E-mail Institucional o serviço de correio eletrônico disponibilizado e registrado sob o domínio do MinC.
- V. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso de acordo com a Norma Interna de Segurança da Informação (NISI 01) de Controle de Acesso;
- VI. As aplicações a serem disponibilizadas na Intranet devem ser previamente analisadas, homologadas e aprovadas pela Área de TI;
- VII. Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e E-mail, devem ser imediatamente comunicados à Área, para serem analisados e solucionados.
- VIII. As paralisações do serviço de Internet e E-mail, para manutenção preventiva, devem ser previamente divulgadas pela área de tecnologia.
- IX. Cabe aos gestores de setores, autarquias e escritórios descentralizados, em complementação às ações de divulgação do MinC relacionadas ao tema, orientar os usuários sob suas responsabilidades a respeito do uso adequado dos serviços de Internet e E-mail, conforme as regras estabelecidas na POSIN/MinC, informando à Área de TI do MinC ou ao CGDSI o seu descumprimento.

CAPÍTULO I

INTERNET

Art. 1º O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela área de Tecnologia da Informação (TI);

Art. 2º O acesso à internet é disponibilizado pelo MinC para uso nas atividades relacionadas ao trabalho, observado o disposto na Política de Segurança da Informação (POSIN).

Art. 3º É expressamente proibido:

- I. Utilização intencional de aplicações ou serviços para burlar as ferramentas de controle e segurança do MinC;
- II. Utilização de proxies externos ou similares, sem a autorização da Área de TI;
- III. Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*), exceto programas homologados pela Área de TI ou autorizados pelo Comitê de Governança de Dados e Segurança da Informação (CGDSI);
- IV. Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda que não estejam relacionados às atividades laborais, exceto programas homologados pela Área de TI ou autorizados pelo Comitê de Governança de Dados e Segurança da Informação;
- V. Acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do MinC;

- VI. As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela setor solicitante de acordo com a Norma Interna de Segurança da Informação (NISI 01) de Controle de Acesso;
- VII. Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo;
- VIII. A liberação de acesso a sítios e serviços bloqueados, quando necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, à Área de TI, que a submeterá, quando for o caso, ao CGDSI para deliberação;
- IX. Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais tais como: pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de software;
- X. Divulgação de informações confidenciais da instituição por meio de redes sociais, correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, ou ferramentas semelhantes;
- XI. Desvio na finalidade de qualquer software/sistema licenciado à Área de TI ou dados de propriedade deste órgão ou de seus usuários, salvo expressa e fundamentada autorização do responsável pela sua guarda.

Art. 4º Os softwares navegadores de Internet (browsers) utilizados no âmbito do MinC deverão ser homologados pela Área de TI, de acordo com a Norma Interna de Segurança da Informação (NISI 02) de Gestão de Ativos.

CAPÍTULO II

E-MAIL / CAIXAS POSTAIS DE CORREIO ELETRÔNICO

Art. 5º A criação, alteração e exclusão de contas acontecerá de acordo com a Norma Interna de Segurança da Informação (NISI 01) de Controle de Acesso.

- I. As caixas postais são identificadas unicamente por meio de seu endereço eletrônico.
- II. No âmbito deste MinC, o domínio do endereço eletrônico é "cultura.gov.br".
- III. A capacidade máxima de armazenamento padrão das caixas postais será definida pela Área de TI.
- IV. Somente será criada caixa postal institucional pessoal, caixa postal institucional da unidade ou caixa postal de sistema ou serviço.
- V. As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas à área de tecnologia.

Art. 6º O uso e-mail institucional restringe-se a mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário ou da unidade, sendo vedado o uso para fins particulares

Art. 7º O acesso ao correio eletrônico a partir de estações de trabalho fornecidas pelo MinC será feito a partir do navegador de internet ou utilização de software homologado, de acordo com a Norma Interna de Segurança da Informação (NISI 02) de Gestão de Ativos.

Art. 8º É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.

Art. 9º O tamanho máximo da mensagem eletrônica, incluindo os anexos, não pode exceder 35 megabytes (MB).

Art. 10º O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos - acima de 200(duzentos) destinos, é permitido em caráter excepcional ou a unidades administrativas, desde que autorizado pelas Secretarias ou Gabinete da Ministra.

Art. 11º É de responsabilidade do usuário de e-mail institucional:

- I. Eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;
- II. Manter exclusivo o acesso ao e-mail institucional pessoal, não compartilhando a respectiva senha e/ou delegando o acesso a terceiros.
- III. Informar à área de tecnologia da informação o recebimento de mensagem que contrarie o disposto na vedação a seguir.

Art. 12º É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:

- I. Informações privilegiadas, confidenciais e/ou de propriedade do MinC para destinatários não autorizados;
- II. Materiais obscenos, ilegais ou antiéticos;
- III. Materiais preconceituosos ou discriminatórios;
- IV. Materiais caluniosos ou difamatórios;
- V. Propaganda com objetivo comercial;
- VI. Listagem com endereços eletrônicos institucionais;

- VII. Malwares;
- VIII. Material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;
- IX. Material protegido por lei de propriedade intelectual;
- X. Entretenimentos e “correntes”;
- XI. Assuntos ofensivos;
- XII. Músicas, vídeos ou animações que não sejam de interesse específico do trabalho;
- XIII. *Spam, phishing e hoax*;
- XIV. Materiais criptografados, exceto nos casos em que as informações da mensagem necessitem proteção quanto ao sigilo.

Art. 13º A recuperação de mensagens de caixas postais institucionais de unidade poderá ser solicitada pelo respectivo responsável desde que justificado por meio de sistema de atendimento de TI ou outros canais disponibilizados para suporte aos usuários do MinC.

Art. 14º A Área de TI não garante a recuperação de mensagens de e-mails ou de caixas postais excluídos há mais de 20 dias.

Art. 15º Recuperada(s) a(s) mensagem(ns) de e-mail, a área de tecnologia da informação verificará com o solicitante a melhor forma de disponibilizá-la(s) novamente;

CAPÍTULO III

MONITORAMENTO E AUDITORIA

Art. 16º Por motivos de segurança, todo tráfego de internet será controlado, de forma automática, e poderá ser inspecionado por soluções de segurança implementadas pela Área de TI (filtros de conteúdo, proxy, DLP, etc.), configuradas de acordo com os limites estabelecidos na Política de Segurança da Informação do MinC, normas e legislação pertinentes ao tema.

Art. 17º O uso do e-mail será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam, hoax, phishing*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança da infraestrutura tecnológica do MinC ou que contenham conteúdo impróprio.

Art. 18º Os arquivos de registro de mensagens eletrônicas (logs) serão mantidos pelo prazo de 30 dias, exceto nos casos de auditoria ou notificação administrativa ou judicial, em que serão devidamente armazenados pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), a fim de salvaguardar os dados respectivos.

Art. 19º A Área de TI encaminhará, em dezembro de cada ano, um relatório às unidades e aos respectivos gestores, com o rol das listas de distribuição e caixas postais a elas vinculadas, bem como a lista de eventuais caixas postais de estagiários lotados na respectiva unidade.

Parágrafo Único. Cabe ao gestor conferir os dados do relatório e, no prazo de 10 (dez) dias úteis, solicitar os ajustes necessários a Área de TI.

Art. 20º Em caso de indícios de descumprimento das diretrizes previstas nesta norma, desde que devidamente apresentados os registros dos indícios, poderá ser solicitado por qualquer servidor ao CGDSI a realização de auditoria extraordinária;

Art. 21º Os relatórios decorrentes das auditorias ordinárias e extraordinárias serão encaminhados ao CGDSI, para os devidos fins;

Art. 22º Os registros de acessos dos usuários poderão ser analisados pela Área de TI para investigação de incidentes que comprometam a segurança das informações institucionais;

Art. 23º Os registros de acesso dos usuários poderão ser fornecidos aos órgãos de segurança para investigações quanto a incidentes de segurança;

Art. 24º Os registros de acesso poderão ser disponibilizados a outras instituições, desde que para atender a determinações judiciais.

CAPÍTULO IV

DISPOSIÇÕES GERAIS

Art. 25º Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação (POSIN) e Normas de Segurança da Informação (NISI) devem ser obrigatoriamente comunicados pelos usuários à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), através do e-mail <etir.minc@cultura.gov.br> ou outros meios disponíveis.

Art. 26º Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Subsecretaria de Tecnologia da Informação e Inovação fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

- I. Nos casos em que o ator da quebra de segurança for um usuário da Subsecretaria de Tecnologia da Informação e Inovação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.
- II. Ações que violem a POSIN ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.
- III. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela POSIN.
- IV. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Governança Digital e Segurança da Informação (CGDSI) do Ministério da Cultura.

Art. 27º Esta norma entra em vigor na data de sua publicação, observado o prazo de 180 (cento e oitenta) dias para adequação às disposições contidas neste documento.