Ministério da Cultura (MinC)

Norma Interna de Segurança da Informação 01 (NISI 01)

Gestão de Controle de Acesso

Brasília, fevereiro de 2024

Escopo

Esta norma se aplica a todas as informações, cuja o Ministério da Cultura seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

Especificamente, inclui:

- Todos os funcionários, sejam servidores efetivos ou temporários, do Ministério da Cultura.
- Todos os contratados e terceiros que trabalham para o Ministério da Cultura.
- Todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do Ministério da Cultura

Declarações da norma

Dos princípios gerais:

I. A Norma de Gestão de Controle de Acesso regulamenta os acessos ao Sistemas e à Rede de Computadores do Ministério da Cultura em atenção ao disposto no Art. 21º da Política de Segurança da Informação (POSIN).

II. A Norma de Gestão de Controle de Acesso deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

CAPÍTULO I

ACESSO LÓGICO

Art. 1º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Coordenação de Suporte e Atendimento ao Usuário (COSAU), baseado nas responsabilidades e tarefas de cada usuário.

I. Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

II. Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no Ministério da Cultura.

Art. 2º A Coordenação de Suporte e Atendimento ao Usuário (COSAU), deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

a) Departamento proprietário.

b) Data de criação/última autorização de renovação de acesso;

c) A Coordenação de Suporte e Atendimento ao Usuário (COSAU) é responsável por validar todas as contas ativas do órgão a cada 90 (noventa) dias.

Art. 2º-A. Fica vedada a criação de contas de serviços destinadas ao recebimento de denúncias ou outras manifestações de que tratam a Lei nº 13.460, de 26 de junho de 2017, e a Portaria MinC nº 96, de 1º de dezembro de 2023.

Art. 3º A Coordenação de Suporte e Atendimento ao Usuário (COSAU) deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 4º A Coordenação de Suporte e Atendimento ao Usuário (COSAU) deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 5º A Coordenação de Suporte e Atendimento ao Usuário (COSAU) deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO.

Art. 6º A Coordenação de Suporte e Atendimento ao Usuário (COSAU) deve definir e manter o controle de acesso dos usuários baseado em funções.

I. Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

II. A Coordenação de Suporte e Atendimento ao Usuário (COSAU) deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

CAPÍTULO II

CONTA DE ACESSO LÓGICO E SENHA

Art. 7º Para utilização das estações de trabalho do Ministério da Cultura, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pela Coordenação de Suporte e Atendimento ao Usuário (COSAU), mediante solicitação formal pelo titular da unidade do requisitante.

I. O formulário de solicitação de acesso se encontra disponível para preenchimento na Intranet do Ministério da Cultura.

II. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III. Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a Coordenação de Suporte e Atendimento ao Usuário (COSAU) que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 8º O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela Coordenação de Suporte e Atendimento ao Usuário (COSAU) quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 9º O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, joão.silva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, A Coordenação de Suporte e Atendimento ao Usuário (COSAU) realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 10º O padrão adotado para o formato da senha é o definido pela Coordenação de Suporte e Atendimento ao Usuário (COSAU), que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha da identificação (*login*) de acesso à Rede Local deve seguir as regras de:

d) Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;

e) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

f) Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

g) Não utilizar termos óbvios, tais como: Brasil, senha, usuario, password ou system.

h) Não reutilizar as últimas 03 (três) senhas.

II. A Coordenação de Suporte e Atendimento ao Usuário (COSAU) fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 11º As senhas de acesso serão renovadas a cada 90 (noventa) dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

CAPÍTULO III

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 12º A conta de acesso será bloqueada nos seguintes casos:

I. Após 5 (cinco) tentativas consecutivas de acesso errado;

II. Solicitação do superior imediato do usuário com a devida justificativa;

III. Quando da suspeita de mau uso dos serviços disponibilizados pelo Ministério da Cultura ou descumprimento da Política de Segurança da Informação – POSIN e normas correlatas em vigência.

IV. Após 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário.

Art. 13º O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário à Coordenação de Suporte e Atendimento ao Usuário (COSAU).

Art. 14º Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou da Coordenação-Geral de Gestão de Pessoas.

Art. 15º A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Art. 16º A Coordenação de Infraestrutura Tecnológica (COINF), deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 17º A COINF deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO IV

MOVIMENTAÇÃO INTERNA

Art. 18º Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

I. O novo superior imediato ou a Coordenação-Geral de Gestão de Pessoas deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

II. Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou da Coordenação-Geral de Gestão de Pessoas.

CAPÍTULO V

AUTENTICAÇÃO MULTIFATORES

Art. 19º A fim de atender os conceitos da Autenticação de Multifatores (MFA), devem ser aplicadas soluções ao menos 02 tipos diferentes dentre os seguintes conceitos:

a) Algo que o usuário conhece. Podendo ser senhas ou frases de segurança;

b) Algo que o usuário possui. Podendo ser certificado digital, **tokens** ou códigos enviados por aplicativo específico;

c) Algo que o usuário é. Aferível por meios biométricos;

d) Onde o usuário está. Para acessos a partir da Rede Local do MinC

Parágrafo Único. Para autenticação de acesso remoto não poderá ser utilizado o tipo de MFA indicado no item “d”.

Art. 20º A Autenticação Multifatores é obrigatória nos seguintes casos.

I. Acesso remoto à Rede Local do MinC por meio de ferramenta específica baseada em abordagem Confiança Zero (ZeroTrust);
II. O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores;
III. Todas as contas de administrador.

Art. 21º A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da MFA.

Parágrafo Único. O Ministério da Cultura deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI

ADMINISTRADORES

Art. 22º A utilização de identificação (*login*) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Somente os técnicos da Coordenação de Infraestrutura Tecnológica (COINF), devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a Coordenação de Suporte e Atendimento ao Usuário (COSAU), que poderá negar os casos em que entender desnecessária a utilização.

III. Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da COINF.

IV. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

V. A identificação (*login*) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do superior imediato.

VI. Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

VII. Excepcionalmente, poderão ser concedidas identificações (*login*) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do Setor ou pessoa/função Responsável por meio da Coordenação de Suporte e Atendimento ao Usuário (COSAU).

VIII. A Coordenação de Suporte e Atendimento ao Usuário (COSAU) deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

CAPÍTULO VII

RESPONSABILIDADES

Art. 23º É de responsabilidade do superior imediato do usuário comunicar formalmente à Coordenação-Geral de Gestão de Pessoas e a Coordenação de Suporte e Atendimento ao Usuário (COSAU) o desligamento ou saída do usuário do Ministério da Cultura. para que as permissões de acesso à Rede Local sejam canceladas.

Art. 24º Caberá a Coordenação-Geral de Gestão de Pessoas do Ministério da Cultura a comunicação imediata à Coordenação de Suporte e Atendimento ao Usuário (COSAU) sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 25º É responsabilidade da Coordenação-Geral de Recursos Lógicos (CGRL) do Ministério da Cultura a comunicação imediata à Coordenação de Suporte e Atendimento ao Usuário (COSAU) da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

I. Os serviços serão filtrados por programas de *antivírus*, *anti-phishing* e *anti-spam* e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

II. Nenhum técnico do Ministério da Cultura terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores do Ministério da Cultura.

Art. 26º É de responsabilidade da Coordenação de Infraestrutura Tecnológica (COINF) o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do Ministério da Cultura.

Art. 27º O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do Ministério da Cultura.

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II. A utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 28º O usuário deve informar à Coordenação de Infraestrutura Tecnológica (COINF) qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 29º É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII. Assinar o Termo de Responsabilidade (Anexo II/POSIN) quanto a utilização da respectiva conta de acesso.

CAPÍTULO VIII

DISPOSIÇÕES GERAIS

Art. 30º Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança 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. 31º 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 (STII) 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 STII 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 sansões 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. 32º 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.