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. 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.

Ministério da Cultura (MinC)

Norma Interna de Segurança da Informação 02 (NISI 02)

Gestão de Ativos

Brasília, fevereiro de 2024

Escopo

Esta norma se aplica a todos os ativos de informação no Ministério da Cultura, incluindo ativos fora do órgão, de posse de colaboradores em trabalho remoto/híbrido e armazenados em um serviço de nuvem. 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.

Ativos de informação neste contexto, incluem documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos, guias, programas de computador, servidores, computadores, e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos.

Declarações da norma

Dos princípios gerais:

I. A Norma de Gestão de Ativos de informação regulamenta a gestão de Ativos de Informação no âmbito do Ministério da Cultura em atenção ao disposto nos Art. 21º e Art. 35º da Política de Segurança da Informação (POSIN).

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

III. O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

IV. As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.

V. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.

VI. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

VII. Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

   a. Ativos físicos;
   b. Bancos de dados;
   c. Dispositivos móveis;
   d. Hardwares;
   e. Mídias removíveis;
   f. Níveis de permissões;
   g. Serviços;
   h. Softwares;
   i. Servidores Virtuais;
   j. Unidade de Armazenamento Remotas.

VIII. Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.

IX. Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis.

CAPÍTULO I

ATIVOS DA INFORMAÇÃO

Art. 1º Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

I. A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização

II. A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.

III. A organização deve assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor.

Art. 2º A organização empregará o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.

Art. 3º A organização utilizará ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.

I. A organização utilizará controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado, sendo estes reavaliados semestralmente ou com mais frequência.

II. A organização utilizará controles técnicos para garantir que apenas bibliotecas e scripts autorizados, e assinados digitalmente tenham permissão para serem executados.

III. O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação.

Art. 4º A organização assegurará que exista um processo semanal para lidar com ativos não autorizados.

Art. 5º A organização utilizará ferramenta de gerenciamento de endereços IP, *Internet Protocol Address Management (IPAM)* ou similares, para atualizar o inventário de ativos da instituição.

Art. 6º As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação.

Art. 7º Cada ativo de informação (por exemplo, desktops, laptops, servidores, tablets), quando aplicável, deve ter uma etiqueta afixada ao dispositivo com esse identificador.

Art. 8º Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na Norma Interna de Segurança da Informação (NISI 01) de Gestão de Controle de Acesso e catalogadas no sistema de gestão de ativos.

Art. 9º Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.

Art. 10º Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

Art. 11º Registre o identificador de ativos da informação juntamente com outras informações relevantes no inventário de TI. Isso inclui:

- Identificador de ativos
- Data da compra
- Preço de compra
- Descrição do item
- Fabricante
- Número do modelo
- Número de série

- Nome do proprietário do ativo corporativo (por exemplo, administrador, usuário), função ou unidade de negócios, quando aplicável.
- Localização física do ativo da empresa, quando aplicável
- Endereço físico (controle de acesso à mídia (MAC))
- Endereço de Protocolo de Internet (IP)
- Data de validade da garantia/vida útil
- Qualquer informação de licenciamento relevante
- No caso de softwares instalados na organização deve ser registrado no inventário informações como:
    - Título do software;
    - Desenvolvedor ou editor de software;
    - Data de aquisição;
    - Data de instalação;
    - Duração do uso;
    - Finalidade comercial;
    - Lojas de aplicativos;
    - Versões;
    - Mecanismo de implantação;
    - Data de fim do suporte, se conhecida;
    - Qualquer informação de licenciamento relevante;
    - Data de descomissionamento.

CAPÍTULO II

CRITICIDADE DO ATIVO DE INFORMAÇÃO

Art. 12º A criticidade dos ativos de informação críticos da organização é determinada pelo:

a) Requisitos legais;
b) Pelo valor financeiro;
c) Pelo seu potencial de agregar valor ao negócio;
d) Por sua vida útil.

CAPÍTULO III

CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 13º Todos os ativos de informação devem ser classificados de acordo com sua criticidade.

Art. 14º As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do Ministério da Cultura devem ser classificados de acordo com a legislação pertinente (*vide* LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011), podendo ser classificado em uma das seguintes categorias:

a) **Ultrassecreta:** São passíveis de classificação como ultrassecretos, dentre outros, dados, informações ou documentos referentes à soberania e à integridade territorial nacionais, a planos e operações, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade ou do Estado.

b) **Secreta:** São passíveis de classificação como secretos, dentre outros, dados, informações ou documentos referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança do Ministério da Cultura, da sociedade ou do Estado.

c) **Reservada:** São passíveis de classificação como confidenciais, dentre outros, dados, informações ou documentos que, no interesse do Ministério da Cultura, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança do Ministério da Cultura, da sociedade ou do Estado.

Art. 15º Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de informações usados pela organização.

CAPÍTULO IV

MANIPULAÇÃO DE MÍDIA

Art. 16º A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.

Art. 17º A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.

Art. 18º A mídia contendo informações confidenciais e internas do Ministério da Cultura devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

CAPÍTULO V

SUPORTE TÉCNICO

Art. 19º Os procedimentos de instalação, configuração e manutenção de equipamentos e softwares serão realizados pela área de tecnologia da informação do Ministério ou por terceiros por ela autorizados, sob a supervisão do gestor da unidade, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade;

Art. 20º Não será fornecido suporte técnico a equipamentos particulares (Ex.: computadores, notebooks e tablets);

Art. 21º Quanto aos softwares e recursos disponibilizados pelo MinC que sejam autorizados para uso em equipamentos particulares, o suporte técnico se limitará a disponibilização de manuais e orientações aos usuários para que os mesmos efetuem os procedimentos em seus equipamentos (procedimentos de instalação de aplicativos de governo para smartphone e certificados digitais, por exemplo);

Art. 22º Os equipamentos institucionais, servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra malwares.

CAPÍTULO VI

EQUIPAMENTOS FORNECIDOS PELO MINC

Art. 23º O fornecimento de equipamentos a servidores e colaboradores, quando autorizado, está condicionado às necessidades de trabalho e à responsabilização destes;

Art. 24º Estação de Trabalho portátil (notebook, tablets e afins).

I. Os computadores portáteis serão fornecidos com instalação padrão desenvolvida pelo MinC, composta por softwares e aplicativos necessários ao desempenho das funções de trabalho, além de softwares para proteção, monitoramento e auditoria do equipamento;

II. Os problemas de software serão solucionados pela reinstalação padrão desenvolvida pelo MinC, que fica desobrigado de reinstalar e configurar programas que o usuário tenha instalado por iniciativa própria e isento da responsabilidade sobre eventual perda de dados;

III. Para a instalação de aplicativos e recursos, sempre que possível, o usuário deverá solicitar apoio da equipe de suporte técnico do MinC;

IV. A instalação, manutenção e suporte de qualquer software/sistema não fornecido pelo MinC, bem como o backup de dados locais não é responsabilidade da equipe de TI;

V. Em caso de falecimento, aposentadoria, exoneração, demissão, cedência, remoção, redistribuição, dispensa da função ou término de contrato, os equipamentos devem ser devolvidos ao MinC, com todos os acessórios que o acompanharam, no prazo de 20 dias, se outro prazo não houver sido estipulado em norma específica;

VI. Nos casos de perda, furto ou roubo do equipamento, bem como nas hipóteses de ausência de devolução ou verificação de existência de avarias no equipamento devolvido, a área de Tecnologia da Informação informará ao(s) setor(es) responsável(eis) a situação ocorrida, com a documentação respectiva, para as providências cabíveis.

CAPÍTULO VII

ESTAÇÃO DE TRABALHO DESKTOP

Art. 25º Os desktops serão fornecidos com instalação padrão desenvolvida pelo MinC, composta por softwares e aplicativos necessários ao desempenho das funções de trabalho, além de softwares para proteção, monitoramento e auditoria do equipamento;

Art. 26º Sempre que disponíveis pontos lógicos fisicamente, os desktops deverão ser conectados a rede cabeada e separados por VLAN criada especificamente para esta finalidade;

Art. 27º Toda aquisição de estações de trabalho com recursos do MinC deve ser realizada pela Área de TI;

Art. 28º Toda aquisição de estações de trabalho com recursos extraorçamentários deve ser submetida para análise prévia da Área de TI;

Art. 29º A troca de peças e componentes das estações de trabalho e demais equipamentos de TI, somente será efetuada pela Área de TI ou por profissional indicado por esta;

Art. 30º A Área de TI deverá disponibilizar equipamentos adequados às necessidades das áreas requisitantes, para tanto, caberá à coordenação:

I. Elaborar especificações técnicas padronizadas para atender as necessidades das atividades laborais dos servidores e colaboradores do MinC;

II. Disponibilizar modelos de estações de trabalho padronizadas classificando-as em pelo menos três modelos (exemplo: Desktop Básico, Desktop Intermediário e Desktop de Alto Desempenho);

III. Quando viável tecnicamente, efetuar o aproveitamento de peças e componentes disponíveis para a realização de upgrade de equipamentos para atender as necessidades das áreas requisitantes.

CAPÍTULO VIII

SERVIDORES

Art. 31º Todo equipamento servidor de rede deve estar, preferencialmente, instalado em salas a adequadas para este fim;

Art. 32º Somente os profissionais autorizados deverão ter acesso aos servidores;

Art. 33º O usuário somente terá acesso ao servidor de rede se atender aos seguintes requisitos:

I. Solicitação formal à área de tecnologia da informação com a justificativa e finalidade do acesso pretendido;

II. Avaliação e aprovação pela Área de Tecnologia;

Art. 34º Todos os servidores de rede devem utilizar os sistemas operacionais atualizados.

Art. 35º A atualização dos servidores de rede deverá ser realizada pelos profissionais autorizados.

CAPÍTULO IX

ARMAZENAMENTO DE DADOS

Art. 36º A área de tecnologia da informação do MinC deverá disponibilizar espaço de armazenamento em rede para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança;

Art. 37º Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas nesse item, cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais;

Art. 38º É proibido o armazenamento, em qualquer diretório na rede do MinC ou nas soluções baseadas em nuvem, de **arquivos não relacionados ao trabalho**, tais como:

I. fotos, músicas e filmes de qualquer formato;

II. programas não homologados ou não licenciados;

III. programas de conteúdo prejudicial à segurança do parque computacional do MinC.

Art. 35º O armazenamento de dados referente à cópia de segurança/backup deve atender à Norma Interna de Segurança da Informação (NISI 03) de Backup e Restauração de Dados.

CAPÍTULO X

LICENÇAS E SOFTWARES

Art. 36º As licenças de softwares, de qualquer natureza, contratadas ou adquiridas pelo MinC são de uso institucional;

Art. 37º É proibida a instalação de softwares não licenciados ou não homologados pela área de tecnologia da Informação nos equipamentos conectados à rede do Ministério;

Art. 38º A instalação de softwares não homologados poderá ser autorizada excepcionalmente pela área de tecnologia da informação, desde que demonstrada a necessidade de sua utilização para o desempenho das atribuições funcionais do usuário, observadas as condições de segurança computacionais disponibilizados pelo MinC;

Art. 39º As unidades organizacionais do MinC poderão encaminhar à Área de Tecnologia da Informação pedido de homologação de softwares, para o uso em suas atividades;

Art. 40º Homologado o uso, o software poderá integrar a formatação padrão utilizada na configuração dos novos equipamentos;

Art. 41º Toda aquisição de licença de software deve ser informada pelo gestor da unidade à Área de Tecnologia da Informação para documentação e atualização do inventário de softwares do MinC.

CAPÍTULO XI

REDE DE COMPUTADORES / REDE LOCAL

Art. 42º Todas as unidades do MinC devem, preferencialmente, dispor de Rede Local cabeada estruturada com capacidade para oferecer conexão individual para cada estação de trabalho;

Art. 43º A Rede Local deve, preferencialmente, dispor de dispositivo de comutação/concentrador gerenciável e Equipamento de Proteção (Firewall ou afins);

Art. 44º Todos os equipamentos e dispositivos conectados à Rede Local de dados do MinC terão seus acessos registrados e monitorados por questões de segurança e para fins de auditoria;

Art. 45º É proibida a conexão de qualquer dispositivo não fornecido pelo MinC na Rede Local cabeada do Ministério, sem a prévia anuência da Área de TI;

Art. 46º As intervenções no ambiente de rede somente serão permitidas mediante supervisão pelos profissionais autorizados pela Área de TI;

Art. 47º Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e configuração/uso devidamente documentado;

Art. 48º A Área de TI do MinC disponibilizará acesso à rede sem fio para usuários internos e externos;

Art. 49º A conexão para os usuários internos será feita por meio da credencial (nome de usuário e senha) utilizada para o acesso à rede, e para os usuários externos será feita mediante cadastramento prévio em sistema específico do MinC;

Art. 50º É permitida a conexão de dispositivos móveis particulares nas redes sem fio administradas pelo MinC;

Art. 51º O acesso à internet por meio das redes sem fio observará as regras dispostas na Norma de Segurança da Informação (NISI 04) de Uso Aceitável da Internet e E-mail;

Art. 52º Por questões de segurança tecnológica, regras específicas poderão ser implementadas no acesso à internet via rede sem fio;

Art. 53º Poderão ser bloqueados os acessos à rede sem fio, temporariamente ou por tempo indeterminado, de dispositivos móveis identificados, intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica;

Art. 54º A rede destinada a uso de visitantes deverá ser isolada da rede de usuários comuns.

CAPÍTULO XII

NUVEM CORPORATIVA

Art. 55º Os arquivos institucionais das unidades administrativas e finalísticas deverão ser armazenados, preferencialmente em espaço disponibilizados na nuvem corporativa do Ministério;

Art. 56º Os arquivos armazenados na nuvem corporativa deverão ser vinculados (ter como proprietário) à caixa postal institucional da unidade, quando fim.

CAPÍTULO XIII

DISPOSIÇÕES GERAIS

Art. 57º 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. 58º 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, esta 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. 59º 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.

Ministério da Cultura (MinC)

Norma Interna de Segurança da Informação 03 (NISI 03)

Backup e Restauração de Dados Digitais

Brasília, fevereiro de 2024

Escopo

- Esta norma se aplica a todos os dados no âmbito do Ministério da Cultura (MinC), incluindo dados fora deste, armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem e-mail; arquivos pessoais e compartilhados; bancos de dados; códigos fonte de aplicações; logs de auditoria e sistemas operacionais.

- Os serviços de Tecnologia da Informação (TI) críticos do Ministério da Cultura (MinC) devem ser formalmente elencados pelo Comitê de Governança Digital e Segurança da Informação (CGDSI), criado e nomeado por portaria específica do MinC.

- Já ficam previamente estabelecidos os seguintes sistemas críticos do Ministério da Cultura (MinC):

Sistema	**Área MinC**	**Grau de Criticidade**
Sistema Nacional de Cultura	SCDC	7
Sistema Salic	SEFIC	7
Vale Cultura	SEFIC	7
Sistema Eletrônico de Informações (SEI)	SPOA	7
Mapa da Cultura	VÁRIAS	6
Rede Cultura Viva	SCDC	5
Conselho Nacional de Política Cultural	SCC	5
Mapa das Bibliotecas SNBP	SEFLI	5
Portal de Dados da Cultura	SECULT (NECESSÁRIO NOVO INVENTÁRIO)	4
Acervo CTAv	SAV	4
Revista Filme Cultura	SAV	2

Fonte: PDTIC 2023-2027 v.1.0

- Esta norma se aplica a agentes públicos que podem ser criadores e/ou usuários de tais dados. A norma também se aplica a terceiros que acessam e usam no Ministério da Cultura (MinC) sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do Ministério da Cultura (MinC).

Declarações da norma

Dos princípios gerais

I. A Norma de Backup e Restauração de Dados regulamenta as ações referentes à Cópia de Segurança (backup) e Restauração de Dados do Ministério da Cultura em atenção ao disposto no Art. 29º da Política de Segurança da Informação (POSIN).
II. A Norma de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível ministerial.
III. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo (RTO) possível, principalmente quando da indisponibilidade de serviços de TI.
IV. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
V. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos do ministério.
VI. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede do ministério para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
VII. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
VIII. O responsável pelo produto, sistema ou serviço deve solicitar formalmente a área de Tecnologia da Informação a inserção de dados ao sistema de backup, previamente a entrada em operação de tais soluções.
IX. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.
X. A salvaguarda dos dados em formato digital pertencentes a serviços de TI do Ministério da Cultura (MinC) mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.
XI. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).
XII. Sob nenhuma hipótese uma mídia a ser descarta, antes da destruição física, pode ser doada ou armazenada com outros equipamentos do parque tecnológico.

CAPÍTULO I

DA FREQUÊNCIA, RETENÇÃO DOS DADOS E ESTRATÉGIA DE BACKUP

Art. 1º Os backups dos serviços de TI críticos do Ministério da Cultura devem ser realizados utilizando-se as seguintes frequências temporais:

I. Diária;
II. Semanal;
III. Mensal;
IV. Anual.

Art. 2º Os serviços de TI devem ser resguardados sob um padrão mínimo, o qual deve observar o estabelecido a seguir:

Criticidade do Serviço	Tipo	Frequência	Retenção	Janela de Backup	Local (is)

Críticos	Incremental /Diferencial	Diária	15 dias	Segunda à Quinta às 19:00	Storage/ Armazenamento primário
	Full/Completa	Semanal	30 dias	Sábado* às 00:10	Storage/ Armazenamento primário
	Full/Completa	Mensal	365 dias	Último domingo do Mês** por mês às 00:10	Storage/ Armazenamento primário Mídia Secundária/ Ambiente Externo
	Full/Completa	Anual	1825 dias	Último domingo do Ano** por mês às 00:10	Mídia Secundária/ Ambiente Externo
Não Críticos	Incremental /Diferencial	Diária	15 dias	Segunda à Quinta às 21:00	Storage/ Armazenamento primário
	Full/Completa	Mensal	60 dias	Domingo* às 00:10	Storage/ Armazenamento primário

* Exceto na sexta-feira que será realizada a cópia de segurança mensal

** Intervalo Mínimo de 25 dias entre as sextas-feiras que foram realizadas cópias mensais

Art. 3º Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 4º Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Art. 5º A solicitação de salvaguarda, por meio de um Plano de Backup e Restauração (ver ANEXO I), dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos é dever do Custodiante da Informação, cujo é responsável pelo produto, sistema ou serviço, com a anuência prévia e formal do Gestor de Tecnologia da Informação.

Art. 6º O Plano de Backup e Restauração deve refletir os requisitos de negócio do ministério, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I. Escopo (dados digitais a serem salvaguardados);
II. Tipo de backup (completo, incremental, diferencial);
III. Frequência temporal de realização do backup (diária, semanal, mensal, anual);
IV. Retenção;
V. *Recovery Point Objective* (RPO);
VI. *Recovery Time Objective* (RTO).

Art. 7º A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Custodiante da Informação. A aprovação para execução da alteração depende da anuência do Gestor de Tecnologia da Informação.

Art. 8º Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

CAPÍTULO II

DO USO DA REDE DE COMPUTADORES

Art. 9º A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 10º O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do Ministério da Cultura (MinC), garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI deste Ministério.

Art. 11º A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup. As “melhores práticas” apontam para realização do backup fora do horário de produção.

Art. 12º O período de janela de backup deve ser determinado pelo Administrador de Backup em conjunto com a área técnica responsável pela administração da rede de dados do Ministério da Cultura (MinC).

CAPÍTULO III

DO TRANSPORTE E ARMAZENAMENTO

Art. 13º As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I. A criticidade do dado salvaguardado;
II. O tempo de retenção do dado;
III. A probabilidade de necessidade de restauração;
IV. O tempo esperado para restauração;
V. O custo de aquisição da unidade de armazenamento de backup;
VI. A vida útil da unidade de armazenamento de backup.

Art. 14º O Administrador de Backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 15º Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

Art. 15º A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 17º No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo trinta (30) dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.

Art. 18º As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

CAPÍTULO IV

DA VERIFICAÇÃO DAS IMAGENS DE BACKUP E DOS TESTES DE RESTAURAÇÃO DE DADOS

Art. 18º Os backups serão verificados periodicamente:

I. Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
II. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
III. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta norma.
IV. Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

Art. 19º Os testes de restauração dos backups devem ser realizados, por amostragem uma vez por semana, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de

produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.

Art. 20º Verificar se foi atendido os níveis de serviço pactuados, tais como os *Recovery Time Objective* (RTOs).

Art. 21º Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 22º O Administrador de Backup deve ser capacitado para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Art. 23º São atribuições do Administrador de Backup:

I. Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
II. Definir a Janela de Backup em conjunto com a equipe de Infraestrutura Tecnológica;
III. Providenciar a criação e manutenção dos backups;
IV. Configurar as soluções de backup;
V. Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
VI. Definir os procedimentos de restauração e neles auxiliar;
VII. Solicitar o descarte de mídias de backup inservíveis ou inutilizáveis.

CAPÍTULO VI

DISPOSIÇÕES GERAIS

Art. 24º As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Governança Digital e Segurança da Informação (CGDSI) e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Parágrafo Único. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Governança Digital e Segurança da Informação.

Art. 25º O disposto na presente norma será atualizado sempre que alterados os procedimentos de backup, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação (POSIN) do Ministério da Cultura (MinC).

Art. 26º Quaisquer exceções à esta norma serão totalmente documentadas e aprovadas por Comitê de Governança Digital e Segurança da Informação (CGDSI).

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.

ANEXO I

Procedimentos Relevantes

1) **Procedimento para transporte e armazenamento das unidades de armazenamento de backup**
    i. A mídia será claramente identificada e armazenada em uma área segura acessível apenas para o Administrador de Backup ou pessoas por ele autorizadas. Caso exista um fornecedor de armazenamento seguro de mídia externo contratado usado pelo Ministério da Cultura, aquele comunicará seus colaboradores autorizados.
    ii. A mídia não será deixada sem supervisão durante o transporte.
    iii. As mídias de backup, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.
    iv. A movimentação de mídias de backup deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia e a data e a hora da movimentação

2) **Procedimento de restauração de backup**

O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

    i. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de controle de atendimentos;
    ii. O chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a data da versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s), se for o caso, e a justificativa para recuperação;
    iii. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.
    iv. O Administrador de Backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.
    v. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

3) **Do Descarte da Mídia**

A mídia de backup será retirada e descartada conforme descrito neste documento:

    i. A partir da solicitação do Administrador de Backup.
    ii. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.
    iii. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

ANEXO II
PLANO DE BACKUP E RESTAURAÇÃO

* Itens mínimos necessários

** Itens já definidos na Norma. Necessário caso os parâmetros precisem ser diferentes.

1. ESCOPO/ABRANGÊNCIA*

<quais arquivos de dados ou de sistemas, quais bases de dados, quais tabelas, quais diretórios>

2. FREQUÊNCIA DE REALIZAÇÃO*

<diário, semana, mensal, anual>

3. TIPO DE CÓPIA A SER REALIZADA*

<completa/full, incremental ou diferencial>

4. TEMPO DE RETENÇÃO*

<Observar a correlação frequência/retenção de dados declarados na Norma>

5. Recovery Point Objective (RPO)*

6. Recovery Time Objective (RTO)*

7. UNIDADE DE ARMAZENAMENTO**

<informar mídia de armazenamento em local seguro diferente do local primário>

8. JANELA DE BACKUP**

<Informar período no qual a execução das cópias de segurança deverá ocorrer preferencialmente>

9. ESTRATÉGIA DE BACKUP**

<Detalhar o esquema de realização das cópias de segurança; informar quais tecnologias e equipamentos serão utilizados nesta estratégia; informar a capacidade necessária para os dados a serem copiados/armazenados>

8. PERIODICIDADE DE TESTE DE RESTAURAÇÃO**

<informar período regular de teste de restauração/recuperação (*restore*) das cópias de segurança>

9. PROCEDIMENTO DE TESTE DE RESTAURAÇÃO**

<Detalhas quais os procedimentos de teste de restauração/recuperação (*restore*) das cópias de segurança>

10. PROCEDIMENTO DE RESTAURAÇÃO**

<Quais os procedimentos para realizar a restauração/recuperação (*restore*) das cópias de segurança quando necessário.>

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 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. 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.