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.