MINISTÉRIO DA CULTURA

RESPONSABILIDADES DOS USUÁRIOS

ORIGEM

Ministério da Cultura – MinC.

REFERÊNCIAS LEGAIS E NORMATIVAS

Portaria nº 327/2014/MinC - Aprova, no âmbito do Ministério da Cultura, norma de Segurança que estabelece as Diretrizes de Segurança da Informação e Comunicações.

Portaria nº 119/2011/MinC - Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações e dá outras providências.

Portaria nº 40/2013/MinC – Aprova o Regimento Interno do Ministério da Cultura.

ABNT ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO 31000:2009 – Gestão de Riscos - Princípios e diretrizes.

ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação.

Norma Complementar nº 02/IN01/DSIC/GSIPR – Metodologia de Gestão de Segurança da Informação e Comunicações.

Instrução Normativa IN 01/2008 GSI - Disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal – APF direta e indireta, e dá outras providências.

Norma Complementar nº 14/IN01/DSIC/GSIPR – Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da APF, direta e indireta.

Lei nº 12.527, de 18 de novembro de 2011 - Regula o acesso a informações.

Decreto nº 7.724, de 16 de maio de 2012 - Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Ministério da Cultura – MinC.

SUMÁRIO

APROVAÇÃO

Comitê de Segurança da Informação e Comunicações - CSIC

1. OBJETIVO

1.1 Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.

2. ESCOPO

2.1 Estabelecer regras de segurança no que tange ao uso de recursos e ao compartilhamento de informações no âmbito do Ministério da Cultura – MinC.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores do Ministério da Cultura, sendo responsabilidade de cada um o seu cumprimento.

4. CONCEITOS E DEFINIÇÕES

4.1 Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações estão conceituados no Dicionário de Referência.

5. PRINCÍPIOS

5.1 Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, integridade, confidencialidade e autenticidade, visando à proteção e à preservação das informações necessárias às atividades da instituição.

6. ADMINISTRAÇÃO

6.1 Os chefes imediatos ou superiores devem garantir que seus subordinados tenham conhecimento da Política de Segurança da Informação – POSIC e normas correlatas.

6.2 Qualquer solicitação de suporte aos recursos computacionais deve ser encaminhada formalmente à área responsável pela administração dos recursos de tecnologia da informação.

7. USUÁRIOS

7.1 Os usuários devem utilizar obrigatoriamente, de maneira visível, os crachás institucionais nas instalações do MinC de maneira que os identifique e comprove sua identidade.

7.2 Os usuários não podem compartilhar contas de usuários e recursos de autenticação e identificação.

7.3 Os usuários devem proteger as informações relevantes do MinC contra acesso, destruição, alteração e divulgação não autorizadas.

7.4 O padrão de segurança para criação e manutenção das senhas é regulamentado pela área responsável pela administração dos recursos de tecnologia da informação na norma Gerenciamento de Acesso do Usuário.

7.5 Fica vedada a utilização de tecnologia de computação em nuvem (a exemplo de skydrive, dropbox, google drive, entre outros) para armazenamento, cópia de segurança, transferência, etc., de informações institucionais. Tal vedação encontra justificativa técnica no fato dos dados se encontrarem fora do País, situação essa não recomendada dada à fragilidade na segurança e na situação legal de propriedade dos dados.

8. CONTROLE DE ACESSO

8.1 As instalações do MinC que contiverem informações críticas só devem ser acessadas por pessoas devidamente autorizadas.

8.2 Os visitantes, prestadores de serviços ou terceirizados somente terão acesso às instalações do MinC após terem sido identificados e autorizados nos pontos de entrada e saída do Ministério.

8.3 Para transitarem nas instalações do MinC, as pessoas autorizadas devem portar de maneira visível a identificação que lhes for concedida nos pontos de entrada e saída.

8.4 Os visitantes e colaboradores autorizados a transitarem pelas instalações do MinC devem ter acesso somente aos locais que lhes são permitidos, estando sempre acompanhado por servidor do Ministério.

9. CLASSIFICAÇÃO DA INFORMAÇÃO

9.1 As informações do Ministério da Cultura devem ser classificadas pelas respectivas Autoridades Classificadoras, conforme níveis de classificação definidos no Ministério.

9.1.1 Os usuários devem tratar os documentos e as informações a que tenham acesso respeitando os níveis de classificação.

9.1.2 Os usuários devem guardar em locais apropriados os documentos que contiverem informações críticas, de forma a preservar a confidencialidade, integridade, disponibilidade e autenticidade da informação.

9.2 As informações de natureza pessoal, independente de classificação de sigilo, terão seus acesso restrito pelo prazo máximo de 100 (cem) anos a contar da sua data de produção. (Lei nº 12.527, de 18 de novembro de 2011).

10. EQUIPAMENTO DE USUÁRIO SEM MONITORAÇÃO

10.1 Equipamentos instalados em áreas de trabalho comuns, por exemplo, estações de trabalho ou servidores de arquivos, possuem informações sensíveis ao negócio da instituição. Com isso, necessitam de proteção específica contra acesso não autorizado quando deixados sem monitoração por certo período de tempo.

10.2 Os usuários devem estar cientes dos procedimentos para proteger equipamentos desacompanhados, bem como de suas responsabilidades na execução das medidas de proteção correspondentes, atendendo minimamente aos seguintes requisitos e procedimentos:

a) bloquear, imediatamente, a sessão de trabalho ao afastar-se dos dispositivos, a fim de evitar que outras pessoas tenham acesso às informações armazenadas.;
b) desconectar dos servidores quando a sessão de trabalho for finalizada (utilizar procedimento para desconexão (*logoff*)).

11. POLÍTICA DE MESA LIMPA E TELA LIMPA

11.1 A política de "mesa limpa" para informações deixadas nas mesas de trabalho (papéis, mídias magnéticas, etc.) deve considerar a classificação das informações e os riscos, contendo regras que incluam os seguintes pontos:

a) papeis e mídias de computador devem ser guardados, quando não estiverem sendo utilizados, em lugares adequados, com fechaduras ou outras formas seguras de mobiliário, especialmente fora do horário normal de trabalho;
b) informações consideradas críticas, devem ser guardadas em local seguro que garanta a proteção da informação;
c) pontos de recepção e envio de correspondências e máquinas de fax não assistidas devem ser protegidos;
d) equipamentos de reprodução (fotocopiadoras, *scanners* e máquinas fotográficas digitais) devem ser travados ou de alguma forma protegidos contra o uso não autorizado fora do horário de trabalho;
e) informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora e fax.

11.2 A política de "tela limpa" para recursos de tecnologia da informação deve considerar a classificação das informações e os riscos, contendo regras que incluam os seguintes pontos:

a) computadores pessoais, estações de trabalho, terminais de computador e impressoras devem ser posicionados de forma a evitar que estranhos consigam visualizar as informações manuseadas nos mesmos;

b) computadores pessoais, estações de trabalho e terminais de computador devem conter mecanismo de travamento de tela e teclado controlados por senhas, chaves ou ferramentas de autenticação, quando não estiverem em uso;
c) computadores pessoais, estações de trabalho, terminais de computador e impressoras devem ser desligados ao término do trabalho.

12. RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

12.1 Recursos Físicos

12.1.1 Todos os recursos de tecnologia da informação do MinC são inventariados e identificados como patrimônio do Ministério, e devem ter seu acesso e utilização controlados;

12.1.2 Os recursos de tecnologia da informação e os dispositivos móveis devem ser posicionados de forma a ficarem livres de ameaças ambientais;

12.1.3 Os recursos de tecnologia da informação e os dispositivos móveis do MinC devem possuir um mecanismo de controle antifurto de componentes e dos equipamentos;

12.1.4 A alteração, troca, substituição e remoção física dos recursos de tecnologia da informação do MinC, quaisquer que sejam, somente deve ser realizada pela área responsável pela administração dos recursos de tecnologia da informação, sob pena do agente não autorizado assumir o dolo e a eventual restituição de valor caso ocorra dano. Ao agente causador acarretará apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização administrativa, penal e civil;

12.1.5 O transporte dos dispositivos móveis do MinC deve ser realizado nos compartimentos (maleta) disponibilizados pelo MinC juntamente com o equipamento;

12.1.6 Os dispositivos móveis que entrarem e saírem das instalações do MinC devem ser identificados, registrando-se, no mínimo, os seguintes dados:

a) fabricante;
b) marca;
c) modelo;
d) nº de Série;
e) nome do responsável;
f) CPF do responsável;
g) data de entrada e saída; e
h) local no Ministério a ser visitado.

12.2 Recursos Lógicos

12.2.1 O acesso lógico aos recursos de tecnologia da informação e dispositivos móveis do MinC somente será permitido aos usuários por meio de autenticação de conta e senha.

12.2.2 Os recursos de tecnologia da informação do MinC devem ter identificação única na rede corporativa de forma a facilitar a localização.

12.2.3 Os usuários não estão autorizados a alterar as configurações de hardware e software dos recursos computacionais ou praticar qualquer outra ação que possa indisponibilizar o equipamento. Qualquer necessidade de modificação deve ser solicitada formalmente à área responsável pela administração dos recursos de tecnologia da informação, considerando que:

a) as solicitações de alteração de hardware e software devem ser precedidas de parecer técnico da área responsável pela administração dos recursos de tecnologia da informação quanto a disponibilidade e viabilidade, sendo atendidas de acordo com a disponibilidade do recurso solicitado; e
b) softwares proprietários não licenciados ou que não foram homologados, serão removidos pela área responsável pela administração dos recursos de tecnologia da informação.

12.2.4 Os usuários devem utilizar o software de proteção em todas as mídias removíveis como CDs, DVDs *e pen-drives*.

13. PROTEÇÃO DE INFORMAÇÕES

13.1 O usuário deve tratar as informações a ele fornecidas como patrimônio do MinC e, portanto, zelar por sua proteção, de acordo com a legislação vigente.

13.2 O usuário deve preservar o conteúdo das informações a ele fornecidas e pelo seu sigilo.

13.3 O usuário não deve copiar ou reproduzir, por qualquer meio ou modo, informações a ele fornecidas, exceto mediante autorização prévia e expressa da autoridade competente.

13.4 O usuário é responsável pelo mau uso e pelo descarte incorreto que fizer de mídias removíveis, tais como CDs, DVDs, pen-drives, quando este resultar em vazamento de informações.

13.5 Documentos e informações institucionais relacionados deverão ser salvos em drives de rede (Servidor de Arquivos). Tais arquivos, se gravados nas estações de trabalho, não terão garantia de backup, sendo, portanto, de responsabilidade do usuário.

13.6 É vedado o armazenamento de arquivos pessoais e/ou não pertinentes às atividades institucionais do MinC (fotos, músicas, vídeos, etc.) nos drives de rede (Servidor de Arquivos).

13.7 Caso sejam identificados arquivos pessoais e/ou não pertinentes às atividades institucionais nos servidores de rede, os arquivos serão excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

14. SEGURANÇA PARA USO DA INTERNET

14.1 O acesso à internet disponibilizado pelo MinC aos usuários deve ser realizado a fim de apoiar a atividade diretamente relacionada ao trabalho.

14.2 O usuário é responsável por todas as ações e os acessos realizados por meio do seu perfil funcional e esta sujeito à apuração de responsabilidades em caso de uso indevido de sua conta.

14.3 O acesso à internet somente deve ser feito por meio do browser e ferramentas disponíveis pelo MinC.

14.4 O acesso será protegido por infraestrutura de segurança adequada como firewalls, antivírus e demais recursos que se façam necessários para a proteção da rede.

14.5 É proibida a instalação e utilização de acessos alternativos às redes externas, tais como modems e provedores de internet locais sem o prévio conhecimento e aprovação da área responsável pela administração dos recursos de tecnologia da informação.

14.6 O uso da internet deve ser feito de forma a não causar tráfegos desnecessários na rede corporativa do MinC.

14.7 É vedado o uso da internet para:

a) transmitir para si ou para terceiros softwares, arquivos ou informações custodiadas ou de propriedade do MinC, sem prévia autorização;
b) realizar download, transferência e compartilhamento de arquivos não afins às atividades de interesse do MinC;
c) realizar download, transferência e compartilhamento de arquivos executáveis ou que sejam considerados como possíveis portadores de códigos maliciosos;
d) executar atividades relacionadas a jogos eletrônicos, conteúdo multimídia, bate-papos ou ferramentas de relacionamento similares, exceto nos casos em que tais ações sejam condizentes com as atividades de trabalho realizadas;
e) acessar sites de pornografia, pedofilia, que façam incitação à violência e outros contrários à legislação e regulamentação em vigor, mesmo que alguns desses sítios não estejam bloqueados pelos mecanismos de segurança implementados na rede corporativa;
f) acessar sites com materiais atentatórios à moral e aos bons costumes, ofensivos ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;

g) acesso a serviços de streaming de áudio e/ou vídeo (NetFlix, Youtube, etc.), salvo quando de interesse das atividades relacionadas à execução do trabalho no MinC;
h) armazenar informações relativas à instituição e às atividades funcionais em tecnologia de computação em nuvem;
i) qualquer uso que atrapalhe a condução e continuidade das atividades de interesse do MinC.

14.8 O usuário poderá solicitar liberação de acesso a sítios de internet, mediante solicitação formal devidamente justificada pela chefia imediata. A solicitação será avaliada pela área responsável pela administração dos recursos de tecnologia da informação, podendo ser negada em caso de risco ou vulnerabilidade à segurança e à integridade da rede do MinC.

14.9 Criação, bloqueio, desbloqueio e cancelamento do acesso à internet

14.9.1 A utilização da internet é uma concessão do MinC, não um direito do usuário;

14.9.2 Para cada usuário é concedida apenas uma única conta de acesso à rede corporativa para acesso à internet, conforme definições descritas na norma de Gerenciamento de Acesso do Usuário;

14.9.3 Comprovada a utilização irregular, o usuário envolvido poderá ter seu acesso à internet bloqueado pela área responsável pela administração dos recursos de tecnologia da informação, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

14.10 Monitoramento da internet

14.10.1 O acesso à internet deve ser monitorado pela área responsável pela administração dos recursos de tecnologia da informação, quanto ao endereço de destino, quantidade de acessos, horário, tempo de permanência em sítios;

14.10.2 O chefe imediato ou superior do usuário pode solicitar formalmente um relatório com as informações de acesso à internet de seus subordinados, caso:

a) haja suspeita de infração à Política de Segurança da Informação e Comunicações;
b) necessite visualizar os sítios acessados e o tempo gasto com acessos.

14.11 Uso de internet sem fio

14.11.1 Qualquer equipamento que utilize a rede sem fio do MinC deve respeitar as regras estabelecidas neste termo, inclusive os equipamentos particulares;

14.11.2 O MinC não presta suporte nas configurações dos dispositivos de rede sem fio dos equipamentos de terceiros;

14.11.3 O MinC não se responsabiliza por danos de software ou hardware causados em qualquer equipamento que utiliza o serviço de rede sem fio, nem em casos de perda de dados, roubo de informações, violação de acesso, problemas em software, sistema operacional, e entre outros fatores que possam impossibilitar o uso parcial ou total do equipamento em uso.

15. USO DO CORREIO ELETRÔNICO

15.1 O uso do e-mail funcional é obrigatório a todos os usuários do Ministério da Cultura. O cadastramento em sistemas de informação corporativos somente será feito mediante e-mail funcional ou institucional.

15.2 O uso do correio eletrônico funcional ou institucional somente deve ser realizado pelo software de correio disponibilizado pelo MinC ou por meio de browser de internet.

15.3 Mensagens recebidas por remetentes desconhecidos, estranhos ou suspeitos não devem ser lidas e nem respondidas. Em caso de ocorrência, o usuário deve reportar, imediatamente, o incidente à área responsável pela administração dos recursos de tecnologia da informação.

15.4 O uso do correio eletrônico particular é de inteira responsabilidade do usuário e não receberá suporte técnico da área responsável pela administração dos recursos de tecnologia da informação, além de estar sujeito ao monitoramento e à Política de Prevenção de Perda de Dados com possível bloqueio no envio de anexos ou conteúdo classificado.

15.5 O acesso ao correio eletrônico particular somente deve ser feito por meio do browser disponível nos recursos computacionais cedidos ao usuário.

15.6 O usuário deve utilizar os serviços de correio eletrônico, tanto funcional, institucional, quanto particular, de forma a não prejudicar o trabalho de terceiros, causar tráfego desnecessário na rede local ou sobrecarregar os sistemas do MinC.

15.7 O usuário deve realizar manutenção periódica em sua caixa de correio eletrônico funcional de forma a garantir que o limite de tamanho não seja ultrapassado e manter o serviço sempre disponível.

15.8 Uma assinatura padrão deve ser colocada no final de cada mensagem e deve ser usada somente para identificar seu remetente, conforme o modelo do (Anexo II).

15.9 A senha padrão do correio eletrônico funcional deve ser trocada no primeiro acesso do usuário.

15.10 As orientações para formação da senha estão descritas na norma de Gerenciamento de Acesso do Usuário.

15.11 Mensagens de correio eletrônico que contenham informações classificadas devem, sempre que possível, ser criptografadas antes do envio de forma a preservar o seu sigilo e integridade.

15.12 A utilização do serviço de correio eletrônico funcional e institucional do MinC deve ser feita de forma a preservar o bom funcionamento e para isso o usuário deve:

a) evitar o acesso a links de internet que tenham origem desconhecida a fim de eliminar a possibilidade de instalação de softwares que contenham códigos maliciosos;
b) não executar arquivos anexados às mensagens recebidas pelo correio eletrônico funcional e institucional de remetentes desconhecidos;
c) não divulgar o endereço do correio funcional e institucional em sites ou listas de discussão na internet;
d) evitar anexar arquivos às mensagens a serem enviadas por correio eletrônico funcional, priorizando disponibilizar o caminho para localização do arquivo na rede corporativa.

15.13 O acesso ao correio eletrônico funcional e institucional não pode ser realizado utilizando-se mais de um recurso computacional simultaneamente.

15.14 As listas de discussões do MinC só podem ser utilizadas mediante acesso por correio eletrônico funcional.

15.15 É vedada a utilização do serviço de correio eletrônico funcional e institucional para receber, armazenar e enviar/encaminhar mensagens contendo:

e) códigos maliciosos (vírus, Cavalos de Tróia, entre outros);
f) materiais com conteúdo pornográfico, erótico, atentatórios à moral e aos bons costumes, ofensivos ou que incentivem a violência ou discriminação de raça ou credo;
g) conteúdo criminoso ou ilegal ou que façam sua apologia;
h) conteúdo que não respeite os direitos autorais;
i) mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens;
j) transmissão de conteúdo potencialmente perigoso, tais como arquivos executáveis ou outros que possam conter vírus ou outras ameaças;
k) grande quantidade de mensagens de correio eletrônico (junk mail ou spam, incluindo qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos ou propaganda política) que afete a capacidade da rede corporativa.

15.16 Criação, bloqueio, desbloqueio e cancelamento da conta de correio eletrônico

15.16.1 A utilização do correio eletrônico funcional e institucional é uma concessão do MinC.

15.16.2 Para cada usuário é concedida apenas uma única conta de correio eletrônico corporativo, conforme definições descritas na norma de Gerenciamento de Acesso do Usuário.

15.17 Monitoramento do correio eletrônico

15.17.1 O correio eletrônico funcional deve ser monitorado pela área responsável pela administração dos recursos de tecnologia da informação no que tange à origem e destino da mensagem, quantidade, tipo de conteúdo, tipo de anexo e volume das informações;

15.17.2 As contas de correio eletrônico funcional, bem como as mensagens enviadas e recebidas, seu conteúdo e seus anexos são instrumentos de trabalho, e, por isso, são tratadas como patrimônio do MinC.

15.17.3 Todas as mensagens enviadas e recebidas devem ser mantidas em ambiente de resguardo (sistemas de backup) pela área responsável pela administração dos recursos de tecnologia da informação.

15.17.4 A solicitação de cópia backup pelo exonerado deverá ser motivada pela chefia imediata.

15.17.5 Nos casos de suspeita de infração à Política de Segurança da Informação e Comunicações em vigor e suas normas correlatas, a área responsável poderá acessar a caixa postal funcional do usuário, sem prévio consentimento.

15.17.6 O chefe imediato ou superior do usuário pode solicitar formalmente à área responsável pela administração dos recursos de tecnologia da informação acesso à caixa postal funcional de seus subordinados, caso haja:

a) desligamento do usuário;
b) término do contrato;
c) afastamentos do usuário por motivos de licenças;
d) falecimento do usuário; e
e) suspeita de infração à Política de Segurança da Informação e Comunicações.

16. USO DE SENHAS

16.1 O uso de senhas deve ser baseado minimamente nos seguintes cuidados:

a) NÃO digitar a senha quando alguém estiver observando;
b) NÃO compartilhar a senha ou utilizar a senha de outro usuário;
c) NÃO escolher nome, sobrenome, username, nomes de parentes (esposa, filhos, etc.), número de telefones, datas importantes (aniversário, casamento, etc.) ou qualquer variação (por exemplo, de trás para frente). Todas são alternativas fáceis de serem deduzidas na tentativa de apropriação indevida de senhas dos usuários;
d) NÃO escolher nenhuma das opções acima seguidas ou antecedidas de números ou caracteres especiais. Estas combinações também são testadas pelos programas de quebra de senha disponíveis na internet, e
e) NÃO permanecer com a mesma senha por longos períodos, trocando-a quando:

   – fizer o primeiro acesso (para trocar a senha padrão - fácil de ser descoberta);

- o sistema solicitar uma nova senha;
- notar que a senha pode ter sido descoberta, e
- se a senha não tiver sido alterada nos últimos 90 dias.

16.2 Usuários que necessitam de múltiplas senhas para acesso a diferentes serviços, sistemas ou plataformas devem usar uma única senha forte para todos eles.

17. PENALIDADES

17.1 Todos os servidores e colaboradores estão sujeitos às regras da Política de Segurança da Informação e Comunicações e devem observar integralmente o que dispõe este documento. A inobservância dessas regras acarretará em apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização administrativa, civil e penal.

18. COMPETÊNCIAS E RESPONSABILIDADES

18.1 Os servidores e os colaboradores devem ter conhecimento da Política de Segurança da Informação e Comunicações, tendo a obrigação de seguir rigorosamente o disposto nas normas de segurança.

19. DISPOSIÇÕES GERAIS

19.1 Qualquer dúvida ou sugestões sobre a Política de Segurança da Informação e Comunicações e suas orientações devem ser imediatamente encaminhadas à área responsável por Segurança da Informação para análise e/ou esclarecimento.

20. ATUALIZAÇÃO

20.1 Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação e Comunicações, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

21. VIGÊNCIA

21.1 Esta norma entra em vigor na data de sua publicação.

22. ANEXOS

Anexo I – Termo de Responsabilidade do Usuário da Rede MinC
Anexo II – Modelo de Assinatura de Correio Eletrônico