# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

# POSIC

MINISTÉRIO DOS DIREITOS HUMANOS

Ministro de Estado dos Direitos Humanos
Gustavo do Vale Rocha

**Secretário Executivo**
Marcelo Dias Varella

**Diretor de Tecnologia da Informação**
Davi Vernon Carlos de Oliveira

**Responsáveis pela Aprovação da POSIC**

Comitê de Segurança da Informação e Comunicação – CSIC/MDH

| Titulares | Suplentes |
|---|---|
| Davi Vernon Carlos de Oliveira | Danilo Silva Freitas Guimaraes |
| Laenny Christy Monteiro Pinto Rufino | Lorraine Alves dos Santos |
| Marcelo de Mello Benzi | Mayara Martins Sales de Araújo |
| Celiane Silva de Araújo | Bruno Bernardes Ferreira |
| Carlos Eduardo Bianchi Ferratoni | Eduardo Sousa dos Santos George |
| Caroline Dias dos Reis | Sérgio Paulo da Silveira Nascimento |
| Eli Ximenes da Silva | Iêda Maria de Miranda |
| Saulo Quadros Santiago | Rafaela Herrmann Gil |
| Thais Cristina Alves Passos | João Bosco de Melo Lima Júnior |
| Cecilia Maria de Souza Escobar | Renata de Brito Teles |
| Hélio Barbosa da Silva | Josiane Lima de Paiva |

Ministério dos Direitos Humanos
SEDE
Esplanada dos Ministérios, Bloco A, 5º e 9º andares
70.054-906 Brasília-DF

Art. 1º O presente documento tem por objetivo instituir a Política de Segurança da Informação e Comunicação - Posic no âmbito da Ministério dos Direitos Humanos - MDH.

## Capítulo I
## Do Escopo

Art. 2º A Política de Segurança da Informação e Comunicação - Posic tem como objetivo instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade e autenticidade - DICA - das informações custodiadas e de propriedade do MDH, de modo a preservar os seus ativos informação e sua imagem institucional.

Art. 3º A Posic trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do MDH, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e descarte, visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicação.

Art. 4º A Posic do MDH aplica-se aos servidores públicos, prestadores de serviço, fornecedores, estagiários, consultores externos e demais colaboradores que execute atividades vinculadas a todas as unidades da estrutura regimental deste Ministério

Art. 5º Esta política também se aplica, no que couber, ao relacionamento do MDH com outros órgãos e entidades públicos ou privados.

## Capítulo II
## Dos Conceitos e Definições

Art. 6º Para efeitos desta Posic, estabelece-se os significados dos seguintes termos e expressões:

I. Agente Público: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao MDH;

II. Ativo de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles tem acesso;

III. Autenticidade: propriedade que assegura que os dados ou informações são verdadeiros e fidedignos tanto na origem quanto no destino, permitindo, inclusive, a identificação do emissor e do equipamento utilizado, quando for o caso;

IV. Ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua confidencialidade, integridade, disponibilidade e autenticidade;

V. Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo, disponibilidade e integridade dado à informação, documento, material, área ou instalação;

VI. Comitê de Segurança da Informação e Comunicação: grupo de representantes de unidades do MDH com a responsabilidade deliberativa sobre as ações de segurança da informação e Comunicação;

VII. Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizadas não tenham conhecimento da informação, de forma proposital ou acidental;

VIII. Criticidade: grau de importância da informação para a continuidade das atividades e serviços do MDH;

IX. Custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

X. Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador e/ou armazenada em meio eletrônico;

XI. Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XII. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade autorizados;

XIII. Gestor da Informação: agente público do MDH responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;

XIV. Incidente: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XV. Informação Custodiada: informação sob a guarda e responsabilidade do MDH;

XVI. Integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;

XVII. Recursos computacionais e de comunicação: equipamentos utilizados para armazenamento, processamento e transmissão de dados ou voz;

XVIII. Rede corporativa: conjunto de todas as redes locais sob a gestão do MDH;

XIX. - Segurança da Informação e Comunicação – SIC - ações que objetivam viabilizar a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XX. Servidor público: pessoa que ocupa legalmente cargo ou função pública para prestar serviços à sociedade e ao Estado, visando ao interesse público e ao bem comum, exercendo as atribuições e responsabilidades previstas.

XXI. *Software*: programa de computador desenvolvido para executar um conjunto de ações previamente definidas; e

XXII. Usuário: agente público com acesso autorizado a sistemas, redes de dados ou informações do MDH.

## Capítulo III
## Das Referências Legais e Normativas

Art. 7º Esta Posic observa a legislação e normas específicas, destacando-se:

I. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos agentes públicos civis da União, das autarquias e das fundações públicas federais;
II. Lei nº 12.527, Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.;
III. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal e dá outras providências;
IV. Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil);
V. Lei nº 13.709, de 14 de agosto de 2018 que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
VI. 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 previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição.;
VII. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
VIII. Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores - Internet;
IX. Decreto nº 6.029, de 1º de fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

IX. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicação na Administração Pública Federal, direta e indireta, e dá outras providências e suas normas complementares;

X. Norma ABNT NBR ISO/IEC 27002:2013 – Técnicas de segurança - Código de práticas para a segurança da informação;

XI. Norma ABNT NBR ISO/IEC 27005:2011 - Técnicas de segurança - Gestão de riscos de segurança da informação; e

XII. E-PING – Padrões de interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2016.

## Capítulo IV
## Dos Princípios

Art. 8º Esta Posic observa os seguintes princípios, assim definidos:

I - Responsabilidade: os agentes públicos que prestam serviços ao MDH devem conhecer e respeitar esta Posic;

II - Ética: os direitos dos servidores públicos devem ser preservados, sem o comprometimento da segurança da informação e comunicação;

III - Celeridade: as ações de segurança da informação e comunicação devem oferecer respostas rápidas a incidentes e falhas de segurança;

IV - Clareza: as regras de segurança da informação e comunicação devem ser precisas, concisas e de fácil entendimento;

V - Privacidade: informação que diz respeito à intimidade e à honra dos cidadãos não pode ser divulgada;

VI - Publicidade: dar transparência no trato da informação, observados os critérios legais; e

VII - Serão observados ainda, sem prejuízo das demais, outros princípios constitucionais que regem a Administração Pública Federal – APF.

## Capítulo V
## Diretrizes Gerais

### Seção I
### Da Gestão da Segurança da Informação e Comunicação

Art. 9º A gestão da Segurança da Informação e Comunicação - SIC compreende a preservação dos ativos de informação do MDH quanto aos aspectos de confidencialidade, integridade, disponibilidade e autenticidade, independentemente do meio que se encontrem.

Art. 10 Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 11 Os sistemas de informação e as aplicações do MDH devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

### Seção II
### Da Gestão dos Ativos de Informação

Art. 12 Os ativos de informação devem:

I - ser inventariados e protegidos;

II - ter identificados os seus proprietários e custodiantes;

III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - ter a sua a entrada e saída nas dependências do MDH autorizadas e registradas por autoridade competente.

V - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

## Seção III
## Do Tratamento da Informação

Art. 13 Toda informação criada, adquirida ou custodiada pelo agente público, no exercício de suas atividades para o MDH, é considerada um bem e deve ser protegida pelo MDH de acordo com as regulamentações de SIC existentes.

Art. 14 As informações devem ser protegidas de acordo com as diretrizes descritas nesta Posic e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do MDH e preservar sua imagem.

Art. 15 As informações produzidas ou custodiadas pelo MDH devem ser descartadas conforme o seu nível de classificação.

## Seção IV
## Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 16. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 17. Os contratos, convênios, acordos e instrumentos congêneres podem incluir, quando necessário e justificado, autorização de acesso a outras pessoas, desde que expressamente autorizadas pelo MDH.

Art. 18. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta Posic.

Art. 19. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação, por escrito em cláusula específica, da outra parte se comprometer aos termos desta Posic e de suas normas complementares e divulgá-las aos seus empregados e prepostos envolvidos em atividades no MDH.

Art. 20. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

Art. 21. Deve ser definido um processo adequado e objetivo de gestão de mudanças, o qual será detalhado em norma específica.

## Seção V
## Da Classificação da Informação

Art. 22 As informações custodiadas ou de propriedade do MDH devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade de forma implícita ou explícita e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.

Art. 23 O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.

Art. 24 A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Art. 25 Todo agente público deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade do MDH e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

## Seção VI
## Da Sensibilização, Conscientização e Capacitação

Art. 26 O MDH desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos servidores públicos sobre os cuidados e deveres relacionados à SIC.

## Seção VII
## Da Gestão de Riscos

Art. 27 O MDH deve adotar processo contínuo de gestão de riscos, o qual será aplicado na implantação e operação da gestão de SIC.

## Seção VIII
## Da Gestão de Continuidade

Art. 28 O MDH deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

Art. 29 As ações de continuidade do MDH devem ser adotadas por todos os titulares de unidade administrativa, de forma a proteger a reputação e a imagem institucional.

Art. 30 As informações de propriedade ou custodiadas pelo MDH, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades do Ministério. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

## Seção IX
## Do Tratamento de Incidentes de Rede Computacional

Art. 31 A Diretoria de Tecnologia da Informação – DTI, manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

## Seção X
## Do Uso de Recursos Computacionais e Comunicação

Art. 32 O uso de recursos computacionais e comunicação do MDH pelos agentes públicos deve ser direcionado prioritariamente para realização das atividades profissionais desempenhadas para o Ministério nos limites dos princípios da ética, razoabilidade e legalidade.

Art. 33 O correio eletrônico corporativo é um serviço que pertence ao MDH, sendo um ativo de informação custodiado pelo agente público, e dessa forma, seu conteúdo pode ser monitorado em deferimento a ações judiciais e/ou administrativas sem aviso prévio, não cabendo ao usuário do serviço alegar ofensa ao sigilo das comunicações.

## Seção XI
## Da Auditoria, Inspeção e Conformidade

Art. 34 O MDH deve criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna do MDH.

Art. 35 O MDH, periodicamente e sem prévio aviso, poderá monitorar o conteúdo do tráfego de suas redes, mesmo o tráfego seguro, via mecanismos automático e sem inspeção humana, com a finalidade de proteger a sua rede e seus ativos computacionais de ameaças internas e externas de *softwares* maliciosos e afins.

Art. 36 Para garantir a aplicação das diretrizes mencionadas nesta Posic, além de fixar normas e procedimentos complementares sobre o tema, o MDH poderá:

I. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou *wireless* e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II. Realizar, a qualquer tempo e sem prévio aviso, inspeções físicas nos equipamentos e instalações de sua propriedade;

III. Desinstalar, a qualquer tempo e sem prévio aviso, qualquer *software* ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

Art. 37 O MDH deve, periodicamente, promover verificação de conformidade das práticas de SIC, suas normas e procedimentos, bem como com a legislação específica de SIC em vigor com esta Posic.

## Capítulo VI
## Das Competências e Responsabilidades

Art. 38 É dever do servidor público do MDH conhecer e zelar pelo cumprimento da Posic.

Art. 39 Os agentes públicos são responsáveis pela segurança dos ativos de informação e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como: crachá, login, senha eletrônica, certificado digital e endereço de correio eletrônico.

Parágrafo único. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

Art. 40 Compete aos coordenadores gerais do MDH dar o suporte administrativo necessário à gestão da Posic.

Art. 41 – Cabe ao Gestor de SIC:

I - promover cultura de segurança da informação e comunicação;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de SIC;

IV - presidir o Comitê de Segurança da Informação e comunicação -CSIC e a ETIR;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

VI - manter contato direto com o DSIC/GSI/PR para o trato de assuntos relativos à SIC; e

VII - propor normas relativas à SIC

Art. 42 Cabe à ETIR:

I - facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II - agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

III - promover a recuperação de sistemas;

IV – realizar as ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V - analisar os ataques e intrusões na rede do MDH;

VI – executar as ações necessárias para tratar quebras de SIC; e

VII - cooperar com outras Equipes de Tratamento e Resposta a Incidentes;

Art. 43 – Cabe ao Gestor do Ativo da Informação:

I - garantir a segurança dos ativos de informação sob sua responsabilidade;

II - definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta Posic;

III - conceder e revogar acessos aos ativos de informação;

IV – comunicar à ETIR a ocorrência de incidentes de segurança de informação e comunicação.

V - designar custodiante dos ativos de informação, quando aplicável.

VI - sempre que necessário, o gestor da informação do MDH providenciará autorização relativa à cessão de direitos sobre as informações de terceiros, antes de utilizá-las.

Parágrafo Único - A cessão de informações do MDH a terceiros, deverá ser submetida previamente, à autorização do gestor da informação.

Art. 44 - Cabe ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta Posic.

Art. 45 – Cabe ao titular da unidade administrativa:

I - corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;

II - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

III - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

IV - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

V - Independentemente da adoção de outras medidas, o titular da unidade administrativa deverá, de imediato, comunicar todo incidente de segurança que ocorra no âmbito de suas atividades ao gestor de SIC.

Art. 46 – Cabe aos usuários:

I - conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta Posic, bem como os demais normativos e resoluções relacionados à SIC;

II – obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

III - comunicar os incidentes que afetam a segurança dos ativos de informação e comunicação à ETIR.

## Capítulo VII
## Da Segurança Física e do Ambiente

Art. 47. O MDH deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

Art. 48 O acesso físico às instalações do MDH deverá ser regulamentado com o objetivo de garantir a segurança dos agentes públicos e a proteção dos seus ativos de informação.

## Capítulo VIII
## Dos Controles de Acessos

Art. 49 O MDH deve sistematizar a concessão de acesso como forma de evitar a quebra de SIC.

Art. 50. O controle de acesso deverá observar, na configuração das contas e concessão de credenciais de acesso o princípio do menor privilégio, que define que pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Art. 51 O acesso às informações custodiadas ou de propriedade do MDH pelos agentes públicos deve ser restrito ao necessário para desempenho de suas funções.

Art. 52. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 53. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 54. Os usuários do MDH são responsáveis por todos os atos praticados com suas identificações, notadamente, nome de usuário e senha, correio eletrônico e assinatura digital, garantindo o princípio de segurança de não-repudio.

Art. 55. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento

Art. 56. Todos os sistemas de informação do MDH, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

Art. 57. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, sendo cancelados em caso de desligamento do MDH.

Art. 58. A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

## Capítulo IX
## Da Propriedade Intelectual

Art. 59 As informações produzidas pelos agentes públicos, no exercício de suas funções, são patrimônio intelectual do MDH, não cabendo a seus criadores qualquer forma de direito autoral.

Art. 60. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do MDH em atividades ou projetos diversos dos estabelecidos, salvo autorização específica dos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Ministro de Estado, nos demais casos.

## Capítulo X
## Do Plano de Investimentos em SIC

Art. 61. Os investimentos em SIC serão realizados de forma planejada e consolidados no Plano Diretor de Tecnologia da Informação e Comunicação do MDH - PDTIC.

## Capítulo XI
## Das Penalidades

Art. 62. Ações que contrariem a Posic ou quaisquer de suas diretrizes, normas e procedimentos ou que violem os controles de SIC serão devidamente apuradas, sendo aplicadas as sanções penais, civis e administrativas cabíveis aos responsáveis.

## Capítulo XII
## Da Revisão da Posic

Art. 63 Esta Posic e/ou instrumentos normativos gerados a partir desta, devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 02 (dois) anos por deliberação do CSIC do MDH.

## Capítulo XIII
## Da Divulgação

Art. 64 Após a publicação desta Posic, deverá ser dada ampla divulgação a todos os agentes públicos, inclusive com publicação permanente na página da intranet do MDH.

Art. 65 Esta Portaria entra em vigor na data de sua publicação.