



POSIC

**POLÍTICA DE SEGURANÇA DA
INFORMAÇÃO E COMUNICAÇÃO**

2021 - 2022

BRASÍLIA, ABRIL DE 2021

MINISTÉRIO DAS
COMUNICAÇÕES



PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

Versão 1.1
Brasília – DF / 2021



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

EQUIPE DE ELABORAÇÃO DA POSIC

Secretário Executivo

Vitor Elísio Góes de Oliveira Menezes

Secretária-Executiva Adjunta

Flávia Duarte Nascimento

Subsecretária de Planejamento e Tecnologia da Informação

Wanessa Queiroz de Souza Oliveira

Coordenador-Geral

Daniel Miranda Pontes Rogério

Coordenador de Governança

Luiz Fernando Bastos Coura

Colaboradores

Daniele Meira Borges

Eder Beserra

Fábio Pontes

Filipe Carneiro Guimarães

Marcus Azevedo

Victor Taira

Wesin Ribeiro Alves

Willian da Silva Ferreira



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Responsável
07/01/2021	1.0	Elaboração da PoSIC	CGTI
20/04/2021	1.1	Inclusão de diretriz para Segurança Física do Ambiente. (Em atendimento ao parecer Jurídico n. 00133/2021/CONJUR-MCOM/CGU/AGU, item 59)	CGTI



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

SUMÁRIO

- I. APRESENTAÇÃO4
- II. INTRODUÇÃO4
- III. ESCOPO4
- IV. CONCEITOS E DEFINIÇÕES5
- V. PRINCÍPIOS5
- VI. DIRETRIZES GERAIS6
- VII. DIRETRIZES ESPECÍFICAS6
- VIII. COMPETÊNCIAS E RESPONSABILIDADES9
- IX. PENALIDADES10
- X. APROVAÇÃO E PUBLICAÇÃO11
- XI. POLÍTICA DE ATUALIZAÇÃO11
- XII. DISPOSIÇÕES FINAIS11



I. APRESENTAÇÃO

1. Este documento apresenta a Política de Segurança da Informação e Comunicações (PoSIC) do Ministério das Comunicações (MCOM), elaborado tendo como referência a ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, além de estar de acordo com o Decreto nº 9.637 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI) no âmbito da administração pública federal e a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, e outras leis vigentes.

II. INTRODUÇÃO

“Uma corrente é tão forte quanto seu elo mais fraco”.

2. A Segurança da Informação é um conjunto de ações de proteção aos ativos de informação contra todas as formas de agressões em seu ambiente físico, lógico e humano. Este documento estabelece princípios, diretrizes, competências, responsabilidades e objetivos para a Política de Segurança da Informação e Comunicação (PoSIC) do MCOM, a qual deverá ser adotada e cumprida por todos os servidores, estagiários, prestadores de serviços e demais usuários que utilizem suas informações. A Segurança da Informação é matéria atinente a todo o órgão, sejam atividades meio ou fim, devendo essa responsabilidade ser compartilhada por todas suas áreas, além de não estar apenas nos sistemas informatizados, mas também em papéis, documentos e pessoas. Sendo assim, para o sucesso desta PoSIC é necessário contar com o comprometimento de todos, independentemente do nível hierárquico, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação não autorizada. A PoSIC propõe uma gestão baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio e aplicar segurança a ele.
3. Diversas ações e outros normativos de Segurança da Informação serão implementados com o fim de padronizar e reger os processos institucionais do MCOM.
4. A ação “Elaborar e revisar a Política de Segurança da Informação” (prevista no PDTIC 2021 - 2022 do MCOM), é satisfeita com a instituição de PoSIC em atendimento a necessidade N4 - Prover segurança no armazenamento e disponibilidade da informação, que visa aprimorar os processos de segurança e controle no acesso, armazenamento e disponibilidade da informação e promover a conscientização e a educação dos usuários quanto à segurança da informação em meios tecnológicos.

III. ESCOPO

“A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados” (ABNT NBR ISO/IEC 17799:2005).



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

5. O objetivo desta política é instituir diretrizes e princípios de Segurança da Informação e Comunicação no âmbito do MCOM com o propósito de limitar a exposição ao risco a níveis aceitáveis e buscar continuamente a disponibilidade, a integridade, a confidencialidade, a autenticidade, a irretroatividade e o não repúdio das informações que suportam os objetivos estratégicos:
- estabelecer diretrizes, a serem seguidas pelo MCOM no que diz respeito à adoção de normas e procedimentos relacionados à segurança da informação e comunicações;
 - prover o MCOM de normas para a segurança da informação, estabelecendo responsabilidades e diretrizes, bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra a indisponibilidade, a divulgação, a modificação e o acesso não autorizado a dados e informações; e
 - definir um conjunto de instrumentos normativos e organizacionais que capacitem o MCOM a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e das informações.
6. Esta PoSIC aplica-se a todos os órgãos de assistência direta e imediata ao Ministro de Estado, aos órgãos específicos singulares e às unidades descentralizadas, não se aplicando às entidades vinculadas ao MCOM e deverá ser fielmente observada por todos os usuários: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade, conforme definição da Portaria GSI/PR nº 93, de 26 de setembro de 2019, sob pena de responsabilidade, na forma da lei.

IV. CONCEITOS E DEFINIÇÕES

7. Esta PoSIC utiliza-se do Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI/PR nº 93, de 26 de setembro de 2019.

V. PRINCÍPIOS

8. A Política de Segurança da Informação e Comunicações - PoSIC do MCOM está fundamentada nos seguintes princípios:
- autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
 - celeridade:** as ações de segurança da informação oferecem respostas rápidas a incidentes e falhas;
 - clareza:** as regras de segurança dos ativos de segurança da informação e comunicações são precisas, concisas e de fácil entendimento;
 - confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;
 - disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

- f. **equanimidade:** as normas e regras de segurança da informação são obedecidas por todos, sem distinção de cargo ou função;
- g. **ética:** os direitos dos agentes públicos são preservados sem comprometimento da segurança da informação e comunicações;
- h. **finalidade:** as normas e regras de segurança da informação consideram a finalidade dos ativos e das informações a que se referirem;
- i. **integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- j. **menor privilégio:** restringir o acesso às informações, ao estritamente necessário ao exercício das funções;
- k. **privacidade:** informação que fira o respeito, à intimidade, à integridade e a honra dos cidadãos não podem ser divulgadas;
- l. **publicidade:** dar transparência no trato das informações, observado os critérios legais. Divulgar a todos os agentes públicos do MCOM as diretrizes e a normas de segurança da informação; e
- m. **responsabilidade/obediência:** os agentes públicos têm o dever de conhecer e respeitar todas as normas de segurança da informação e comunicações do MCOM.

VI.DIRETRIZES GERAIS

- 9. É dever do agente público do MCOM conhecer e cumprir a PoSIC;
- 10. É condição para acesso aos ativos de informação do MCOM a adesão formal aos termos desta Política, mediante assinatura de Termo de Responsabilidade;
- 11. Todos os agentes públicos do MCOM são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: identificação de usuário da rede (login), crachá, carimbo, endereço de correio eletrônico ou qualquer forma de assinatura digital; e
- 12. Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo MCOM devem ser utilizados estritamente dentro do seu propósito.

VII.DIRETRIZES ESPECÍFICAS

- 13. Esta política aplica-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicação e armazenamento da informação e rege-se pelas seguintes diretrizes:

a. Propriedade da Informação:

- i. toda informação criada, armazenada, transportada ou descartada pelos agentes públicos do MCOM, no exercício de suas atividades, é de propriedade do órgão e é protegida segundo as diretrizes descritas na PoSIC e nas regulamentações em vigor;
- ii. na cessão de bases de dados nominais, informação custodiada ou de propriedade do MCOM a terceiros, o Gestor da Informação providenciará a documentação formal relativa à cessão ou autorização de acesso às informações antes da sua disponibilização, sobretudo para os dados aos quais se aplique a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Nº 13.709, de 14 de agosto de 2018; e
- iii. nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deverá, se necessário, providenciar junto à concedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

seu uso, sobretudo no caso de titulares de dados pessoais aos quais se aplique a Lei Nº 13.709/2018.

b. Segurança física do ambiente

- i. Deverão ser implementados controles de acesso físico para o acesso às dependências do Ministério das Comunicações, com a disponibilização de credenciais que permitam o acesso dos agentes públicos às instalações do órgão;
- ii. Deverão ser disponibilizadas credenciais de acesso físico também aos visitantes, que permitirão o acesso destes às instalações do Ministério, sempre mediante autorização de servidor da área visitada; e
- iii. Nos casos de invalidação temporária ou definitiva das credenciais de acesso de agentes públicos, o acesso aos ativos de informação do órgão dar-se-á mediante as condições estabelecidas para os visitantes.

c. Tratamento da Informação

- i. toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo MCOM é de sua responsabilidade e são classificadas e protegidas adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita conforme o Decreto nº 7.845, de 14 de novembro de 2012 e a Lei Nº 13.709, de 14 de agosto de 2018;
- ii. a classificação e reclassificação da informação é atribuição do Gestor da Informação, que é também responsável por conceder acesso a ela;
- iii. toda informação institucional, se eletrônica, estará armazenada nos servidores de arquivo e bases de dados sob gestão e administração da área de TIC e, se não eletrônica, mantida em local que a salvguarde adequadamente mediante comunicação a área de gestão documental do MCOM;
- iv. toda informação institucional, sob a forma eletrônica, estará salvguardada por meio de cópia de segurança sob administração da área de TIC e mantida em local que a proteja adequadamente e garanta sua recuperação em caso de perda da informação original;
- v. no descarte de informações institucionais são observadas as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação; e
- vi. as informações classificadas conforme a legislação vigente, produzida, armazenada e transportada em meios eletrônicos, utilizará criptografia compatível com o grau de sigilo, em especial as informações de autenticação dos usuários das aplicações.

d. Tratamento de Incidentes em Rede

- i. cabe a área de TIC a responsabilidade pela infraestrutura necessária para fins de registro e resposta aos incidentes de segurança da informação no âmbito da rede corporativa;
- ii. a Equipe de Tratamento de Incidentes de Rede (ETIR) será instituída na TIC; e
- iii. todo agente público do MCOM é responsável por notificar, imediatamente, incidentes que afetem a segurança da informação por meio de recursos de TIC ou o descumprimento da PoSIC à ETIR, para que as providências necessárias sejam adotadas a fim de sanar as causas.

e. Gestão de Ativos de Informação



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

- i.o MCOM deve manter um processo de Inventário e Mapeamento dos Ativos de Informação objetivando a Segurança das Infraestruturas Críticas que garantem suas Informações, as regras são definidas por norma específica, em conformidade com esta PoSIC e demais orientações e diretrizes de governo;
 - ii.o processo de Inventário e Mapeamento de Ativos de Informação subsidiará o conhecimento, valoração, proteção e a manutenção de seus ativos de informação, será dinâmico, periódico, e estruturado, para manter a Base de Dados de Ativos de Informação atualizada.
- f. Uso de correio eletrônico**
 - i.o correio eletrônico do MCOM tem seu uso exclusivo por agentes públicos no exercício de suas funções. As regras de acesso e utilização são definidas por norma específica, em conformidade com esta PoSIC e demais orientações e diretrizes de governo.
- g. Acesso à Internet**
 - i.o acesso à Internet no ambiente de trabalho do MCOM está condicionado às necessidades dos agentes públicos no exercício de suas atribuições e será regido por norma específica, em conformidade com esta PoSIC e demais orientações governamentais e legislação em vigor.
- h. Redes Sociais**
 - i.o uso institucional das redes sociais nos aspectos relacionados à Segurança da Informação e Comunicações será regido por norma específica que, além da segurança, abordará a estratégia de comunicação social, o processo de gestão de conteúdo e outros aspectos relevantes;
 - ii.a normatização interna de uso seguro das redes sociais deverá estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social a partir da infraestrutura das redes de computadores do MCOM; e
 - iii.perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por servidor, ou estar sob a coordenação e responsabilidade deste.
- i. Computação em Nuvem**
 - i.o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de segurança, estabelecidas pelo MCOM, e às legislações vigentes;
 - ii.o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço; e
 - iii.o armazenamento de informação em nuvem deverá estar respaldado por um contrato entre o MCOM e o provedor de serviço em nuvem, de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem.
- j. Controles de Acesso**



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

- i.o agente público do MCOM que utilizar os recursos de TIC terá uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em norma específica;
- ii.o gestor da informação é responsável pela concessão e revogação dos privilégios de acesso às informações, considerando sempre o princípio do menor privilégio; e
- iii.a identificação do agente público, qualquer que seja o meio e a forma, é pessoal e intransferível, e permite o reconhecimento de maneira inequívoca.

k. Gestão de Risco

- i.O MCOM deve manter Processo de Gestão de Riscos de Segurança da Informação e Comunicações (PGRSIC), com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações; e
- ii.o PGRSIC será regido por norma específica, em conformidade com esta PoSIC e demais orientações governamentais e legislação em vigor.

l. Gestão de Continuidade

- i.o MCOM deve manter Processo de Gestão de Continuidade de Negócio (PGCN) em segurança da informação e comunicações no âmbito do MCOM, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de TIC que suportam as operações do MCOM e assegurar a sua retomada em tempo hábil; e
- ii.o PGCN será regido por norma específica, em conformidade com esta PoSIC e demais orientações governamentais e legislação em vigor.

m. Auditoria e Conformidade

- i.o uso dos recursos de TIC disponibilizados pelo MCOM é passível de monitoramento e auditoria, com utilização, sempre que possível, de softwares utilitários específicos para monitoramento do uso dos sistemas, e serão implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso.

VIII.COMPETÊNCIAS E RESPONSABILIDADES

- 14. Compete à alta direção do MCOM prestar o suporte administrativo necessário à gestão da PoSIC;
- 15. Compete à área de TIC, conforme previsão no Decreto nº 10.462/2020 de 14 de agosto de 2020, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério das Comunicações, informar, orientar e supervisionar as unidades do Ministério quanto ao cumprimento das normas de segurança da informação aplicadas à tecnologia da informação e das normas técnicas de tecnologia da informação.
- 16. Compete ao Comitê de Segurança da Informação e Comunicações (CSIC), instituído pela Portaria nº 2.120-MCOM, de 4 de março de 2021, atuar em conformidade com as competências, responsabilidades e atribuições definidas em seu Regimento Interno (Anexo I da Portaria nº 2.120-MCOM/2021).
- 17. Compete ao Gestor de Segurança da Informação e Comunicações (GSIC), a ser designado pela alta administração:
 - a. Atuar em conformidade com as competências e responsabilidades definidas no Art. 2º da Portaria nº 67-MCOM, de 4 de março de 2021;



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

- b. Coordenar a elaboração e atualização da Política de Segurança da Informação e das normas internas de segurança da informação, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
 - c. Assessorar a alta administração na implementação da Política de Segurança da Informação; e
 - d. Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade.
18. Compete aos usuários:
- a. Acessar a rede de dados do MCOM somente após tomar ciência das normas de PoSIC e assinar o Termo de Responsabilidade;
 - b. Ao assinar o Termo de Responsabilidade, o usuário declara, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PoSIC; e
 - c. Tratar a informação digital como patrimônio do MCOM e como recurso que deva ter seu sigilo preservado;
 - d. Utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do MCOM exclusivamente para o interesse do serviço;
 - e. Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;
 - f. Não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;
 - g. No caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;
 - h. Não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional do MCOM para terceiros;
 - i. Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
 - j. Não transferir qualquer tipo de arquivo que pertença ao MCOM para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;
 - k. Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional do MCOM pode ser auditada;
 - l. Estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da administração central do Ministério das Comunicações deve obedecer a esse preceito;
 - m. Utilizar as credenciais de acesso (login e senha) e os recursos computacionais, em conformidade com a PoSIC do MCOM procedimentos estabelecidos em normas específicas do órgão.

IX. PENALIDADES

19. O desrespeito, descumprimento ou violação de um ou mais itens constantes nesta PoSIC caracteriza infração funcional passível de suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas administrativas, cíveis e penais cabíveis.



MINISTÉRIO DAS COMUNICAÇÕES

Secretaria Executiva

Subsecretaria de Planejamento e Tecnologia da Informação

Coordenação-Geral de Tecnologia da Informação

X. APROVAÇÃO E PUBLICAÇÃO

20. Conforme disposto nos Art. 9º e 10º da IN nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal, é obrigatório a todos os órgãos e as entidades da administração pública federal possuir uma Política de Segurança da Informação, implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, devendo ser elaborada sob a coordenação do Gestor de Segurança da Informação do MCOM com a participação do Comitê de Segurança da Informação.
21. Sua publicação deve ser oficializada por meio de Portaria assinada. Com intuito de dar transparência e publicidade, o documento é divulgado na área de publicações do sítio eletrônico do MCOM (<https://www.gov.br/mcom/pt-br>).

XI. POLÍTICA DE ATUALIZAÇÃO

22. Esta PoSIC deverá ser revisada e atualizada quando identificada necessidade, no limite de até 4 anos, a contar da data de sua publicação, observados os devidos procedimentos de aprovação.
23. Os instrumentos normativos gerados a partir desta PoSIC deverão ser revisados sempre que se fizer necessário.

XII. DISPOSIÇÕES FINAIS

24. Os casos omissos serão resolvidos pelo CSIC - Comitê de Segurança da Informação e Comunicação.
25. As propostas de alteração ou criação de normas internas sobre SIC deverão ser encaminhadas ao CSIC.
26. Esta Política Interna entrará em vigor a partir da data de sua publicação.