ORIGEM

1. **Núcleo de Segurança da Informação e Comunicações do SISP.**

REFERÊNCIA NORMATIVA

2. **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 17799:2005 (27002). Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.**
3. **Constituição da República Federativa do Brasil de 1988.**
4. **Decreto nº 1.171, de 22 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.**
5. **Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.**
6. **Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.**
7. **Instrução Normativa GSI nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta e demais normas complementares.**
8. **Lei 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.**

CAMPO DE APLICAÇÃO

9. **Não se aplica.**

SUMÁRIO

INFORMAÇÕES ADICIONAIS

10. **Não há.**

1 OBJETIVO

11. Instituir diretrizes e princípios de Segurança da Informação e Comunicações (PoSIC) no âmbito do Ministério dos XXXXXXXXXX, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade (DICA) das informações que suportam os objetivos estratégicos deste Ministério.

2 ABRANGÊNCIA

12. Esta PoSIC e suas Normas Complementares aplicam-se a todas as unidades e entidades vinculadas ao Ministério dos XXXXXXXXXX, bem como aos servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem de alguma forma tenha acesso aos ativos da organização.

3 PRINCÍPIOS

13. O conjunto de documentos que compõe esta PoSIC deverá se guiar pelos seguintes princípios:
14. **Menor privilégio**: Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.
15. **Segregação de função**: Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.
16. **Auditabilidade**: Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial.
17. **Mínima dependência de segredos**: Os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam.
18. **Controles automáticos**: Sempre que possível, controles de segurança automáticos deverão ser utilizados, especialmente os controles que dependem da vigilância humana e do comportamento humano.
19. **Resiliência**: Os sistemas e processos devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre.
20. **Defesa em profundidade**: Controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança.
21. **Exceção aprovada**: Exceções à PoSIC deverão sempre ter aprovação superior.
22. **Substituição da segurança em situações de emergência**: Controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.
23. Esta PoSIC deve estar também em conformidade com os princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como aos demais dispositivos legais aplicáveis.

4 DIRETRIZES GERAIS

24. As diretrizes de Segurança da Informação e Comunicações (SIC) devem considerar, prioritariamente, os objetivos estratégicos, os requisitos legais a estrutura e finalidade do Ministério dos XXXXXXXXXX.
25. Os custos associados à Gestão da SIC deverão ser compatíveis com os custos dos ativos que

se deseja proteger.

26. A Gestão de SIC deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos do Ministério dos XXXXXXXXXXXX, assim como otimizar seus investimentos.
27. As normas e procedimento de SIC do Ministério dos XXXXXXXXXXXX, devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de SIC.

4.1 Gestão de Ativos

28. Os ativos da organização são elementos fundamentais para a consecução dos objetivos estratégicos, portanto ações de segurança específicas deverão garantir a proteção adequada dos mesmos. Os níveis de proteção deverão variar de acordo com a criticidade do ativo para o Ministério.
29. De forma a evitar incidentes de segurança que possam danificar a imagem da instituição e interromper suas operações, os ativos de informação devem ter controles de segurança implementados independentemente do meio em que se encontram e deverão ser protegidos contra divulgação não autorizada, modificações, remoção ou destruição.
30. De forma a garantir o entendimento e a prática efetiva da SIC, as pessoas, que de alguma forma tenham acesso aos ativos de informação da organização, devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação.
31. Os processos e atividades que sustentam os serviços críticos disponibilizados pelo Ministério dos XXXXXXXXXXX devem ser protegidos de forma a garantir a DICA das informações.

4.2 Gestão de Riscos

32. Com o objetivo de reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos da organização, deverá ser estabelecido processo que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

4.3 Gestão de operações e comunicações

33. Dada a importância estratégica que os recursos de processamento da informação têm para a consecução dos objetivos deste Ministério, ações de segurança deverão garantir a operação segura e correta desses recursos.
34. As interfaces com terceiros são importantes canais de informação que, sem um nível de segurança adequado, poderão levar a organização a uma elevada exposição a riscos. Com o objetivo de reduzir os riscos associados, o gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços.
35. A troca de informações, tanto internamente, quanto externamente, deverão ser reguladas de forma a manter o nível adequado da segurança.
36. Visando detectar o mais cedo possível atividades não autorizadas, as operações deverão ser adequadamente monitoradas.

4.4 Controle de Acessos

37. Com o objetivo de evitar a quebra de segurança, devem ser instituídas normas ou procedimentos que garantam o controle de acesso às informações e instalações.
38. É condição necessária para o acesso aos ativos deste Ministério, a concordância expressa e

por escrito aos preceitos desta PoSIC.

39. Considerando que ambientes de computação móvel e de trabalho remoto são necessários para a consecução das atividades do Ministério e que podem consistir em pontos fracos do sistema de gestão de segurança, devem ser instituídas normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto.

4.5 Gestão de Incidentes

40. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos do Ministério.

4.6 Gestão de Continuidade do Negócio

41. A interrupção das atividades deste Ministério leva à suspenção de serviços críticos prestados ao cidadão e poderá resultar em grave dano à imagem da organização. Portanto, deverão ser instituídas normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços do Ministério, além de recuperar perdas de ativos de informação a um nível estabelecido, por intermédio de ações de prevenção, resposta e recuperação.

5 CONFORMIDADE

42. O cumprimento desta política de segurança deverá ser avaliado periodicamente por meio de verificações de conformidade realizadas pela alta direção, que poderá solicitar o apoio de entidades externas e independentes.

43. Os controles de SIC devem ser analisados criticamente e verificados em períodos regulares, tendo por base as conformidades com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes.

44. Devem ser instituídos processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da APF, de forma a obter o absoluto cumprimento destes instrumentos legais e normativos.

6 RESPONSABILIDADES

45. É de responsabilidade da alta administração deste Ministério prover a orientação e o apoio necessários às ações de SIC, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

46. É de responsabilidade dos demais gestores zelar pelo cumprimento das diretrizes desta política no âmbito de suas áreas de atuação.

47. É de responsabilidade de todos que têm acesso aos ativos do Ministério dos XXXXXXXXXXX manter níveis de segurança da informação adequados, segundo preceitos desta política e de suas normas complementares.

6.1 Comitê de SIC

48. Deverá ser instituído, por portaria específica, o Comitê de Segurança da Informação e Comunicações do Ministério dos XXXXXXXXXX, constituído por representantes, titular e suplente, indicados pelas respectivas áreas. O Comitê se reunirá no mínimo duas vezes ao ano e ficará vinculada à Secretaria Executiva. Sempre que necessário, poderão ser convidadas outras instituições ou especialistas para a reunião do Comitê.

49. O Comitê terá como atribuições mínimas:

    49.1. assessorar na implementação das ações de SIC;

49.2. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre a SIC;

49.3. propor alterações na PoSIC; e

49.4. propor normas relativas à SIC.

50. O Comitê será a instância competente para dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIC deste Ministério.

51. Os membros do Comitê deverão receber regularmente capacitação especializada na disciplina de segurança da informação.

52. As Resoluções editadas pelo Comitê deverão ser cumpridas pelos servidores públicos, colaboradores e visitantes.

6.2 Gestor de Segurança da Informação e Comunicações

53. O Gestor de SIC será indicado e designado pela Secretaria Executiva do Ministério dos XXXXXXXXXX, dentre servidores de seu próprio quadro com conhecimento adequado em SIC, por meio de portaria e terá como atribuições mínimas:

53.1. promover a cultura de segurança da informação e comunicações;

53.2. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

53.3. propor recursos necessários às ações de segurança da informação e comunicações;

53.4. coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;

53.5. realizar e acompanhar estudos e novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

53.6. manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;

53.7. propor normas relativas à SIC;

53.8. coordenar a Gestão de Riscos de SIC;

53.9. coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

53.10. prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR; e

53.11. implementação dos procedimentos relativos ao uso dos recursos criptográficos, em conformidade com as orientações contidas na Norma Complementar 09/IN01/DSIC/GSIPR, de 22 de novembro de 2010.

6.3 Proprietário e Custodiantes dos Ativos de Informação

54. Os níveis adequados de segurança dos ativos de informação deverão ser garantidos pelos proprietários e custodiantes diretamente responsáveis pelos mesmos.

7 PENALIDADES

55. Ações que violem a PoSIC ou que quebrem os controles de segurança da informação e comunicações serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

56. Processo disciplinar específico deverá ser elaborado para apurar as ações que constituem em

quebra das diretrizes impostas por esta PoSIC.

8 ATUALIZAÇÃO

57. Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser revisados e atualizados anualmente, ou quando mudanças significativas ocorrerem.

9 VIGÊNCIA

58. Esta Política entra em vigor na data de sua publicação.

10 DISPOSIÇÕES GERAIS

59. Esta PoSIC, bem como as normas e procedimentos de SIC associados, deverão ter ampla divulgação, de forma a garantir que todos entendam suas responsabilidades e ajam de acordo com os preceitos desta Política.

11 CONCEITOS E DEFINIÇÕES

60. **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade [NC07/IN01/DSIC/GSIPR, 2010, p. 2].
61. **Ameaça:** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
62. **Ativo:** tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal;
63. **Ativos 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 têm acesso [NC04/IN01/DSIC/GSIPR, 2009, p. 2];
64. **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2];
65. **Capacitação em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na Organização como gestor de SIC. [DSIC/GSIPR]
66. **Capacitação:** visa a aquisição de conhecimentos, capacidades, atitudes e formas de comportamento exigidos para o exercício das funções;
67. **Comitê de Segurança da Informação e Comunicações**: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações. [NC03/IN01/DSIC/GSIPR]
68. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado [IN01/DSIC/GSIPR, 2008, p. 2];
69. **Conscientização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema. [DSIC/GSIPR]
70. **Continuidade de Negócios:** capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido [NC06/IN01/DSIC/GSIPR, 2009, p.

3];

71. **Controle de Acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso [NC07/DSIC/GSIPR, 2010, p. 3];
72. **Custodiante:** responsável por armazenar e preservar as informações que não lhe pertencem, mas que estão sob sua custódia;
73. **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2];
74. **Evento:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004]
75. **Gestão de Riscos de Segurança da Informação e Comunicações:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos [NC04/IN01/DSIC/GSIPR, 2009, p.2];
76. **Gestão de Segurança da Informação e Comunicações:** ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações [IN01/DSIC/GSIPR, 2008, p. 2];
77. **Gestor de Segurança da Informação e Comunicações:** é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF [IN01/DSIC/GSIPR, 2008, p. 2];
78. **Incidente de segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores [NC05/IN01/DSIC/GSIPR, 2009, p. 3];
79. **Informação Estratégica:** toda a informação corporativa relativa à administração, planejamento, estrutura, gestão, relações internas e externas, novos produtos e tecnologias, serviços e contratos;
80. **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental [IN01/DSIC/GSIPR, 2008, p. 2];
81. **Nível de Segurança Adequado:** será estabelecidos em documentos complementares a esta PoSIC.
82. **Política de Segurança da Informação e Comunicações (PoSIC):** documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações [NC03/IN01/DSIC/GSIPR, 2009, p. 2];
83. **Terceiro**: pessoa, não integrande do órgão ou entidade da APF, envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso [NC07/DSIC/GSIPR, 2010, p. 3].
84. **Proprietário da Informação:** pessoa ou setor que produz a informação;
85. **Quebra de Segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações [IN01/DSIC/GSIPR,

2008, p. 2];

86. **Riscos de Segurança da Informação e Comunicações:** potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização [NC04/IN01/DSIC/GSIPR, 2009, p.3];
87. **Segurança da Informação e Comunicações**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações [IN01/DSIC/GSIPR, 2008, p. 2];
88. **Segurança de Operações e Comunicações:** responsável pela manutenção do funcionamento de serviços, sistemas e da infraestrutura que os suporta.
89. **Sensibilização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional. [DSIC/GSIPR]
90. **Usuário:** servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade [NC07/DSIC/GSIPR, 2010, p. 3];
91. **Vulnerabilidade:** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação NC04/IN01/DSIC/GSIPR, 2009, p.3].