Política de Segurança da Informação e Comunicações

- 2015 –

INMETRO

1. Apresentação do INMETRO

O Instituto Nacional de Metrologia, Qualidade e Tecnologia é uma autarquia do governo federal que atua em várias frentes que envolvem proteção ao cidadão nas relações de consumo, estímulo à competitividade da empresa brasileira, qualidade, inovação e ampliação de conhecimento em ciência e tecnologia e como regulamentador de produtos e serviços com foco em segurança, saúde e meio ambiente.

2. Missão do INMETRO

Prover confiança à sociedade brasileira nas medições e nos produtos, por meio da metrologia e da avaliação da conformidade, promovendo a harmonização das relações de consumo, a inovação e a competitividade do país.

3. Visão de Futuro do INMETRO

Órgão de Estado fundamental e estratégico ao desenvolvimento socioeconômico do Brasil, pela relevância e qualidade de seus serviços, pelo apoio à inovação, por sua excelência técnica, científica e de gestão, com amplo reconhecimento nacional e internacional.

4. Plano Diretor de Tecnologia da Informação 2015-2016 e Política de Segurança da Informação e Comunicações (PoSIC)

O Plano Diretor de Tecnologia da Informação (PDTI) do INMETRO é um instrumento base de planejamento estratégico o INMETRO. Ele direciona a equipe de TI nas suas rotinas e projetos e também norteia os investimentos e orçamento para infraestrutura de TI da instituição, alinhando-os continuamente com os objetivos de negócio. Além disso, é uma ferramenta de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação para atender às necessidades de informação do INMETRO realizadas através da área de TI e auxiliá-la no alcance dos seus objetivos e metas institucionais.

A Política de Segurança da Informação e Comunicações (PoSIC) está alinhada com este documento e contém as diretrizes estratégicas para segurança da informação e comunicações na Instituição.

ANEXO I

Política de Segurança da Informação e Comunicações - PoSIC

Sumário

1. Escopo

1.1. A Política de Segurança da Informação e Comunicações (PoSIC) é uma declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda. Seu propósito é direcionar o INMETRO no que diz respeito à gestão dos riscos e do tratamento dos incidentes de Segurança da Informação e Comunicações (SIC), por meio da adoção de procedimentos e mecanismos, que visam a eliminação ou redução de ocorrência de modificações não autorizadas (confidencialidade, integridade e autenticidade), bem como a disponibilidade de recursos e sistemas críticos para garantir a continuidade dos negócios do INMETRO, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de SIC.

2. Objetivo

2.1. A PoSIC objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, documentos e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio dos sistemas de informação do INMETRO, contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, inclusive sua imagem institucional.

2.2. Além disso, objetiva estabelecer o comprometimento da alta direção organizacional do INMETRO, com vistas a prover apoio para implementação da Gestão de Segurança da Informação e Comunicações (GESIC), e estabelecer um ambiente seguro, proporcionando melhor qualidade nos processos de gestão e controle dos sistemas de informação e informática.

3. Abrangência e vigência

3.1. A Política de Segurança da Informação e Comunicações (PoSIC) se aplica a todos as unidades administrativas, servidores, funcionários e colaboradores externos que prestam serviço em razão de contratos administrativos firmados na forma da Lei e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação de qualquer tipo, convênios e termos congêneres.

3.2. A PoSIC tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

4. Conceitos e Definições

Os conceitos e definições constantes deste item se aplicam de forma a auxiliar a interpretação da Política de Segurança da Informação e das Comunicações do INMETRO e também no estabelecimento de futuras normas complementares.

4.1. A informação é um ativo essencial para os negócios do INMETRO e consequentemente necessita ter uma proteção adequada, em especial nos ambientes interconectados onde é crescente o número e a variedade de ameaças e vulnerabilidades.

4.2. A estrutura normativa da SIC do INMETRO será composta por um conjunto de documentos com dois níveis hierárquicos distintos, relacionados a seguir:

4.2.1. **Política de Segurança da Informação e Comunicações (PoSIC)**: Define a estrutura, as diretrizes e as obrigações referentes à SIC.

4.2.2. **Normas Internas (NIs)**: Estabelece responsabilidades e procedimentos definidos de acordo com as diretrizes da PoSIC. Tem como objetivos:

4.2.2.1. Definir regras e instrumentos de controle para assegurar a conformidade de processos, produtos ou serviços;

4.2.2.2. Proporcionar meios mais eficientes na troca de informações, melhorando a confiabilidade das atividades públicas e dos serviços prestados pelo INMETRO;

4.2.2.3. Evitar a existência de regulamentos conflitantes sobre processos, produtos ou serviços.

4.3. Para os fins desta Política, considera-se:

a) **Ameaça**: Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para o INMETRO.

b) **Ativos de informação**: Os meios de armazenamento, transmissão e processamento de informação, os sistemas de informação, bem como os locais onde se encontram esses meios, as pessoas que a eles têm acesso, a imagem institucional, os serviços e tudo aquilo que tem valor para o INMETRO e que esteja relacionado com a informação e comunicações.

c) **Contas de acesso**: Permissões concedidas por autoridade competente do INMETRO após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão, token, selo ou lógica para identificação de usuários.

d) **Governança de TI**: É de responsabilidade dos executivos e da alta direção, consistindo em aspectos de

liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização. (IT Governance Institute - ITGI, 2007, p. 7)

e) **Incidente de segurança**: Qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a disponibilidade, a integridade, confidencialidade ou a autenticidade de qualquer ativo de informação do INMETRO.

f) **Plano de Continuidade de Negócios**: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.

g) **Plano de Gerenciamento de Incidentes**: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

h) **Plano de Recuperação de Desastres**: documentação dos procedimentos e informações necessárias para que o órgão ou entidade da Administração Pública Federal operacionalize o retorno das atividades críticas a normalidade.

i) **Quebra de segurança**: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC do INMETRO.

j) **Resiliência**: Poder de recuperação ou capacidade de enfrentamento ágil de situações inesperadas e de superação das adversidades para restabelecer processo de normalidade do INMETRO e resistir aos efeitos de um incidente.

k) **Segurança da Informação e Comunicações (SIC)**: Ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações, abrangendo não só aspectos tecnológicos, mas também recursos humanos e processos.

l) **Tecnologia da Informação (TI):** Conjunto de todas as atividades e soluções providas por recursos de computação. Serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação.

Este termo é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como o modo como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas.

m) **Usuário(s):** Servidores, agentes públicos, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada de acesso aos Ativos de Informação do INMETRO, formalizada por meio da assinatura de um Termo de Responsabilidade.

n) **Vulnerabilidade:** Qualquer fragilidade dos sistemas computacionais e redes de computadores que permita a exploração maliciosa e acessos indesejáveis ou não autorizados. Também definida como conjunto de fatores internos ou causa potencial de um incidente indesejado, que pode resultar em risco para um ativo ou sistema e pode ser evitado por uma ação interna de SIC.

o) **Dispositivos móveis**: Consiste em equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória.

p) **Computação em Nuvem**: Modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, processamento, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

q) **Redes Sociais**: Estruturas sociais, disponíveis na rede mundial de computadores (Internet), compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

5. Referências Legais e Normativas

As ações de SIC do INMETRO deverão observar os seguintes requisitos legais e normativos:

5.1. Lei nº 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.

5.2. 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.

5.3. Lei n° 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública.

5.4. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse de segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

5.5. 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).

5.6. Norma ABNT NBR/ISO/IEC 27002:2005, que institui o código de melhores práticas para

Gestão de Segurança da Informação e Comunicações.

5.7. Norma ABNT NBR/ISO/IEC 27001:2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações.

5.8. Portaria Interministerial MCT/MPOG nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores (Internet) e dá outras providências.

5.9. Norma ABNT NBR/ISO/IEC 15999:2007, que institui o código de melhores práticas para Gestão de continuidade de negócios.

5.10. 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.

5.11. Norma ABNT NBR ISO/IEC 27005:2008, que fornece as diretrizes para a Gestão de Riscos de Segurança da Informação e Comunicações.

5.12. Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

5.13. Norma Complementar nº 01/IN01/DSIC/GSI/PR, de 13 de outubro de 2008, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

5.14. Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008, que define a metodologia de Gestão de Segurança da Informação e Comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

5.15. Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (PoSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta.

5.16. Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal, direta e indireta.

5.17. Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009, que estabelece

diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

5.19. Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 19 de agosto de 2010, que Estabelece as Diretrizes para Gestão de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

5.20. Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF, publicada no DOU Nº 30 - Seção 1, de 10 de fevereiro de 2012. (Republicada por ter saído com omissão do Anexo no DOU, de 9 de fevereiro de 2012, Seção 1).

5.21. Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF, publicada no DOU Nº 30 - Seção 1, de 10 de fevereiro de 2012. (Republicada por ter saído com omissão do Anexo no DOU, de 9 de fevereiro de 2012, Seção 1).

5.22. Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta, publicada no DOU Nº 30 - Seção 1, de 10 de fevereiro de 2012. (Republicada por ter saído com omissão do Anexo no DOU, de 9 de fevereiro de 2012, Seção 1).

5.23. Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF), publicada no DOU Nº 30 - Seção 1, de 10 de fevereiro de 2012. (Republicada por ter saído com omissão do Anexo no DOU, de 9 de fevereiro de 2012, Seção 1).

5.24. 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 Administração Pública Federal

(APF), direta e indireta, publicada no DOU Nº 30 - Seção 1, de 10 de fevereiro de 2012. (Republicada por ter saído com omissão do Anexo no DOU, de 9 de fevereiro de 2012, Seção 1).

5.25. Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 119, de 21 Jun 2012 - Seção 1).

5.26. Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 224, de 21 Nov 2012 - Seção 1).

5.27. Norma Complementar nº 17/IN01/DSIC/GSIPR, Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 Abr 2013 - Seção 1).

5.28. Norma Complementar nº 18/IN01/DSIC/GSIPR, Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 Abril 2013 - Seção 1).

5.29. Norma Complementar nº 19/IN01/DSIC/GSIPR, Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1).

5.30. Norma Complementar nº 21/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 196, de 10 Out 2014 - Seção 1).

5.31. Instrução Normativa GSI Nº 2, de 5 de fevereiro de 2013 - Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 32, de 18 Fev 2013- Seção 1).

5.32. Instrução Normativa GSI Nº 3, de 6 de março de 2013 - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para

criptografia da informação classificada no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 50, de 14 Mar 2013- Seção 1).

5.33. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011 - de acesso a informações.

5.34. Decreto Nº 7.845, de 14 de novembro de 2012 - os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

6. Princípios

As ações relacionadas com a SIC no INMETRO são norteadas pelos seguintes princípios, assim definidos:

a) **Autenticidade**: Garantia de que a informação foi produzida, expedida, modificada ou destruída dentro de preceitos legais e normativos, por pessoa física, ou por sistema, órgão ou entidade vinculado ao INMETRO.

b) **Celeridade**: As ações de SIC devem oferecer respostas rápidas a incidentes e falhas de segurança.

c) **Confidencialidade**: Garantia de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada pelo INMETRO.

d) **Conhecimento**: Os usuários devem conhecer e respeitar a PoSIC, NIs e demais regulamentações sobre SIC do INMETRO.

e) **Clareza**: As regras de SIC, documentação e comunicações devem ser precisas, concisas e de fácil entendimento.

f) **Disponibilidade**: Garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade vinculada ao INMETRO.

g) **Ética**: Os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometimento da SIC.

h) **Integridade**: Garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino.

i) **Legalidade**: As ações de segurança devem levar em consideração as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do INMETRO.

j) **Privacidade**: Garantia ao direito pessoal e coletivo, à intimidade e ao sigilo da correspondência e das comunicações individuais.

k) **Publicidade**: Transparência no trato da informação, observados os critérios legais.

l) **Responsabilidade**: As responsabilidades primárias e finais pela segurança dos ativos do INMETRO e pelo cumprimento de processos de segurança devem ser claramente definidas

7. Diretrizes de Segurança

7.1. Esta PoSIC define as diretrizes para a SIC do INMETRO e descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

7.2. As diretrizes da PoSIC constituem os principais pilares da Gestão de Segurança da Informação, norteando a elaboração das Normas Internas (NIs):

7.3. Deverão mantidos Plano de Gerenciamento de Incidentes e Plano de Recuperação de Desastres formais e periodicamente testados, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade.

7.4. Os sistemas, as informações e os serviços do INMETRO utilizados pelos usuários, no exercício de suas atividades, são de exclusiva propriedade do INMETRO, não podendo ser interpretados como de uso pessoal e devem ser protegidos, segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

7.5. Todos os ativos de informação estão sujeitos a monitoração e auditora, e que os registros assim obtidos poderão ser utilizados para detecção de violações da PoSIC e demais regulamentações em vigor.

7.6. Os recursos de tecnologia da informação de propriedade do INMETRO são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração. É considerada imprópria a utilização desses recursos para propósitos não profissionais ou não autorizados. Os usuários e visitantes que tomarem conhecimento dessa prática devem levá-la ao conhecimento do superior imediato para que sejam aplicadas as ações disciplinares cabíveis.

7.7. Informações confidenciais do INMETRO não podem ser transportadas em qualquer meio sem as devidas autorizações e proteções.

7.8. Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas.

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

7.10. Qualquer tipo de dúvida sobre a PoSIC, as Normas Internas (NIs) e demais regulamentações de SIC deve ser imediatamente esclarecido com a área de Gestão de Segurança da Informação.

8. Diretrizes Específicas

8.1. Gestão da Segurança da Informação e Comunicações (GESIC)

8.1.1. Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade do negócio (regular exercício das funções institucionais).

8.1.2. As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido.

8.1.3. Os requisitos de SIC do INMETRO devem estar explicitamente citados em todos os termos de compromisso celebrados entre o INMETRO e terceiros.

8.2. Gestão de Ativos

8.2.1. A gestão dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

8.2.2. Os ativos de informação do INMETRO deverão ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas operacionais de SIC e são destinados ao uso corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

8.2.3. Todos os ativos deverão ser classificados em termos de valor, requisitos legais, sensibilidade e criticidade para a Instituição.

8.2.4. O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação.

8.3. Tratamento da Informação

8.3.1. A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do INMETRO.

8.3.2. Os dados, as informações e os sistemas de informação do INMETRO devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

8.3.3. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade, elaborando-se, para tanto, sistema de classificação da informação.

8.4. Da Classificação da Informação

8.4.1. As informações criadas, armazenadas, manuseadas, transportadas ou descartadas no INMETRO deverão ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas e legislação específica em vigor.

8.4.2. Todo usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pelo INMETRO e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

8.5. Do Material Impróprio

8.5.1. É expressamente proibido o acesso, uso, guarda e encaminhamento de material não ético, discriminatório, malicioso, obsceno ou ilegal, por intermédio de quaisquer dos meios recursos de comunicações disponibilizados pelo INMETRO.

8.6. Gestão de Tratamento de Incidentes de Segurança em Redes (GETIR)

8.6.1. A área de Tecnologia da informação deverá criar e manter Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), instituída pelo Comitê da Segurança da Informação e Comunicações (COSIC), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas à incidentes de segurança em rede de computadores.

8.6.2. Os eventos e incidentes de SIC devem ser tratados de acordo com um Plano de Gerenciamento de Incidentes específico, comunicados e registrados.

8.7. Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)

8.7.1. A GRSIC é um 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.

8.7.2. As áreas responsáveis por ativos de informação deverão implementar processo contínuo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIC.

8.7.3. A GRSIC deve ser realizada no âmbito do INMETRO, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizada periodicamente, no mínimo

01 (uma) vez por ano, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades. Trata-se de um instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Negócio e um Plano de Gerenciamento de Incidentes.

8.7.4. O Plano de Continuidade de Negócio deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

8.7.5. O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SIC.

8.8. Gestão de Continuidade de Negócios (GECON)

8.8.1. A GECON é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação do INMETRO e possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes de SIC e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do INMETRO, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, objetivando salvaguardar os interesses do INMETRO e da sociedade.

8.8.2. As áreas do INMETRO deverão manter processo de gestão de continuidade de negócios, visando não permitir que os negócios baseados em Tecnologia da Informação sejam interrompidos e, também, assegurar a sua retomada em tempo hábil, quando for o caso.

8.8.3. A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática pró-ativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional do INMETRO.

8.8.4. A área de Tecnologia da Informação do INMETRO, responsável pela GECON, deverá criar um Plano de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros e estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

8.8.5. As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar a disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante do acontecimento de

situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

8.9. Auditoria e Conformidade

8.9.1. A área de Tecnologia da Informação deverá manter registros e procedimentos, como trilhas de auditoria e outros que assegurem a conformidade através do rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos e rede interna do INMETRO.

8.10. Auditoria

8.10.1. Auditar conformidades significa aferir a compreensão da cultura de conformidade e o grau de comprometimento dos profissionais.

8.10.2. É uma atividade independente, de avaliação objetiva e de consultoria, destinada a acrescentar valor e melhorar as operações do INMETRO. Além disso, assiste ao INMETRO na consecução dos seus objetivos por meio de abordagem sistemática e disciplinada, na avaliação da eficácia da gestão de riscos, do controle e dos processos de Governança de TI.

8.10.3. A auditoria efetua verificação de forma aleatória e temporal por meio de amostragens para certificar-se do cumprimento das normas e processos instituídos pela alta administração.

8.11. Conformidade

8.11.1. A conformidade é o conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as diretrizes, as PoSIC, as NIs e os procedimentos estabelecidos para o negócio e para as atividades do INMETRO, bem como para evitar, detectar e tratar qualquer desvio ou não conformidade que possa ocorrer, objetivando:

a) Evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações contratuais e de quaisquer requisitos de SIC;

b) executar atividades de verificações de forma rotineira e permanente, monitorando-as para assegurar, de maneira corporativa, que os departamentos e unidades estejam respeitando as regras aplicáveis a cada negócio, ou seja, cumprindo as normas e processos internos para a prevenção e controle dos riscos envolvidos em cada atividade;

c) ser tão independente quanto à auditoria, reportando-se à alta administração para informá-la de eventos que representem riscos que possam afetar a reputação do INMETRO;

d) englobar o acompanhamento dos pontos falhos identificados pela auditoria até que sejam regularizados, configurando interseção das duas áreas;

e) auxiliar os usuários na resolução de situações não cobertas pela legislação.

8.11.2. Metodologias voltadas à boa conduta e de conformidade devem estar integradas, pois se baseiam em valores e responsabilidade morais, bem como no cumprimento e conformidade das leis e políticas internas.

8.12. Controle de Acesso

8.12.1. As regras de controle de acesso a todo sistema corporativo, Intranet, Internet, informações, dados e às instalações físicas do INMETRO deverão ser definidas e regulamentadas, através de Normas Internas (NIs), com o objetivo de garantir a segurança dos usuários e a proteção dos ativos do INMETRO.

8.12.2. Todas as contas de acesso aos ativos de informação e as instalações físicas do INMETRO deverão ser revogadas ou suspensas quando não mais necessárias, conforme normas e legislação específica em vigor.

8.12.3. Todo acesso às informações e aos ambientes lógicos do INMETRO deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação contemplando:

a) **Controle de Acesso Lógico**: Permite que os sistemas de TI verifiquem a identidade dos usuários que tentam utilizar seus serviços. Deve ainda utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.

b) **Controle de Acesso Físico**: Por questão de segurança, é obrigatório o uso de identificação física em todos os ambientes e instalações do INMETRO.

8.13. Uso de e-mail

8.13.1. O correio eletrônico é um recurso de comunicação corporativa do INMETRO. As regras de acesso e utilização de e-mail devem atender a todas as orientações desta PoSIC e das Normas Internas (NIs) específicas, além das demais diretrizes do Governo.

8.14. Acesso a Internet

8.14.1. O acesso à rede mundial de computadores (Internet), no ambiente de trabalho, deve ser regido por Normas Internas (NIs) específicas, atendendo às determinações desta PoSIC, e demais orientações governamentais e legislação em vigor.

8.15. Uso das Redes Sociais

8.15.1. O uso das Redes Sociais disponíveis na rede mundial de computadores (Internet), com o objetivo de prestar atendimento e serviços púbicos, divulgando ou compartilhando informações do INMETRO, deve ser regido por Normas Internas (NIs) específicas, atendendo às determinações desta PoSIC, e demais orientações governamentais e legislação em vigor.

8.16. Uso de Dispositivos Móveis

8.16.1. As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail do INMETRO, devem considerar, prioritariamente, os requisitos legais e a estrutura da Instituição, atendendo a esta Política de Segurança da Informação e Comunicações e regidas por Normas Internas (NIs) específicas, a qual contemplará recomendações sobre o uso desses dispositivos.

8.17. Uso de Computação em Nuvem

8.17.1. O uso de recursos de Computação em Nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por Normas Internas (NIs) específicas, atendendo à determinações desta PoSIC e demais orientações governamentais e legislação em vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

9. Penalidades

9.1. O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e Comunicações (PoSIC) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

9.2. O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar ao INMETRO, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

10. Competências e Responsabilidades

10.1. O INMETRO deverá criar e manter um Comitê de Segurança da Informação e Comunicações (COSIC) competente para:

a) Assessorar na implementação das ações de SIC;

b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

c) Instituir Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas à incidentes de segurança em rede de computadores;

d) Propor alterações na PoSIC;

e) Propor Normas Internas (NIs).

10.2. No âmbito do INMETRO, o Gestor da Política de Segurança da Informação e Comunicações deverá:

a) Promover cultura de SIC;

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) Propor recursos necessários às ações de SIC;

d) Coordenar o COSIC e a ETIR

e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

f) Manter contato direto com o DSIC para o trato de assuntos relativos à SIC;

g) Propor Normas Internas (NIs);

h) Fornecer o suporte administrativo necessário à gestão da PoSIC.

10.3. O usuário é responsável pela segurança dos ativos e processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, tais como: crachá, token, login, senha eletrônica, certificado digital e endereço de correio eletrônico.

10.4. Independentemente da adoção de outras medidas, o titular da unidade administrativa deverá, de imediato, comunicar todo incidente de SIC que ocorra no âmbito de suas atividades ao COSIC, mediante o envio de relatório circunstanciado.

10.5. No caso de incidente de SIC, o comunicado deve ser feito à ETIR do INMETRO.

10.6. É dever do usuário do INMETRO conhecer e zelar pelo cumprimento desta Política de Segurança da Informação e Comunicações.

10.7. Quando for o caso, o titular da unidade administrativa do INMETRO providenciará autorização relativa à concessão de acessos sobre as informações de terceiros.

10.8. Para a cessão de informação do INMETRO a terceiros, o titular da unidade administrativa, ouvida a área jurídica do INMETRO, providenciará a documentação formal relativa a essa cessão.

10.9. Todos os usuários do INMETRO são responsáveis pelas ações de SIC, observando de forma específica as atribuições pertinentes a cada cargo e /ou função.

10.10. Os casos omissos e as dúvidas surgidas na aplicação desta PoSIC serão analisados, dirimidos ou solucionados pelo COSIC.

11. Divulgação e Conscientização

11.1. A divulgação das regras e orientações de segurança aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança dentro do INMETRO.

11.2. Cabe ao Gestor de Segurança da Informação e Comunicações providenciar a divulgação interna desta PoSIC e das Normas Internas (NIs), inclusive com publicação permanente na página da intranet do INMETRO, para que seu conteúdo possa ser consultado a qualquer momento e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SIC.

12. Atualização

12.1. A SIC, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

12.2. Os instrumentos normativos gerados a partir desta PoSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal, ou conforme os seguintes critérios:

12.2.1. Política de Segurança da Informação e Comunicações (PoSIC):

a) Nível de Aprovação: Secretaria Executiva (SE)

b) Periodicidade de Revisão: Anual

12.2.2. Normas Internas (NIs):

a) Nível de Aprovação: Comitê de Segurança da Informação e Comunicações (COSIC)

b) Periodicidade de Revisão: anual

12.3. As unidades do INMETRO terão prazo de 90 (noventa) dias, a contar da publicação desta PoSIC, para submeterem ao Comitê de Segurança da Informação e Comunicações (COSIC), proposta de atualização desta PoSIC.

13. Principais Siglas

Sigla Significado

ABNT Associação Brasileira de Normas Técnicas

COSIC Comitê da Segurança da Informação e Comunicações

DSIC Departamento de Segurança da Informação e Comunicações da Presidência da República

ETIR Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

GECON Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações

GESIC Gestão de Segurança da Informação e Comunicações

GETIR Gestão de Tratamento de Incidentes de Segurança em Redes de Computadores

GRSIC Gestão de Riscos de Segurança da Informação e Comunicações

GSI/PR Gabinete de Segurança Institucional da Presidência da República

IEC International Electrotechnical Commission

ISO International Organization for Standardization

NBR Norma Brasileira

NIG Norma Interna Geral

PoSIC Política de Segurança da Informação e Comunicações

SIC Segurança da Informação e Comunicações

SISP Sistema de Administração dos Recursos de Informação e Informática

TI Tecnologia da Informação