POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2022

INMETRO

Sumário

1. Introdução

1.1. A Política de Segurança da Informação (POSIN) é uma declaração formal acerca do compromisso com a proteção dos dados e informações de sua propriedade e/ou sob sua guarda no âmbito do Instituto Nacional de Metrologia Qualidade e Tecnologia – o Inmetro. Seu propósito é direcionar o Inmetro no que diz respeito à gestão dos riscos e dos incidentes de Segurança da Informação, por meio da adoção de procedimentos e mecanismos, que visam evitar possíveis modificações ou acessos não autorizados, bem como impactos que afetam a disponibilidade de recursos e sistemas críticos, buscando assim 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 Segurança da Informação.

1.2. A Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio. A Segurança da Informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, normas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.

1.3. Em particular, os controles de Segurança da Informação necessitam ser estabelecidos, implementados, monitorados, analisados e continuamente melhorados, objetivando assim viabilizar e assegurar o alinhamento junto aos objetivos de negócio do Inmetro.

2. Objetivo

2.1. De forma geral, esta POSIN objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando a mitigação dos riscos relacionados à Segurança da Informação, baseados na proteção da confidencialidade, integridade e disponibilidade (CID), dos dados corporativos ou pessoais, informações, recursos e sistemas informatizados mantidos pelo Inmetro, inclusive a sua imagem institucional.

2.2. Adicionalmente, objetiva também estabelecer o comprometimento da Alta Administração do Inmetro, com vistas a prover o apoio para a implementação desta POSIN e demais ações de Segurança da Informação, estabelecendo assim um ambiente tecnológico mais seguro, com uma melhor qualidade nos processos de gestão e dos controles de sistemas informatizados.

3. Abrangência e vigência

3.1. Esta POSIN se aplica a todos as unidades administrativas do Inmetro, incluindo os seus servidores públicos e colaboradores, prestadores de serviço 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. Esta POSIN entrará em vigor na data de sua publicação e permanecerá vigente até a sua atualização ou revogação formal.

4. Apresentação do INMETRO

4.1. O Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro - é uma autarquia federal, vinculada à Secretaria Especial de Produtividade, Emprego e Competitividade, do Ministério da Economia. O Instituto atua como Secretaria Executiva do Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro), colegiado interministerial, que é o órgão normativo do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (Sinmetro).

4.2. Objetivando integrar uma estrutura sistêmica articulada, o Sinmetro, o Conmetro e o Inmetro foram criados pela Lei nº 5.966, de 11 de dezembro de 1973, cabendo a este último substituir o então Instituto Nacional de Pesos e Medidas (INPM) e ampliar significativamente o seu raio de atuação a serviço da sociedade brasileira.

4.3. No âmbito de sua ampla missão institucional, o Inmetro objetiva fortalecer as empresas nacionais, aumentando sua produtividade por meio da adoção de mecanismos destinados à melhoria da qualidade e da segurança de produtos e serviços.

4.4. Missão do INMETRO

4.4.1. Viabilizar soluções de infraestrutura da qualidade que adicionem confiança, qualidade e competitividade aos produtos e serviços disponibilizados pelas organizações brasileiras, em prol da prosperidade econômica e bem-estar da nossa sociedade.

4.5. Visão de Futuro do INMETRO

4.5.1. Ser reconhecido pelo setor produtivo e mercado como uma caixa de ferramentas para superação dos desafios da sociedade 4.0.

4.6. Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2021-2023

4.6.1. O objetivo do PDTIC do Inmetro é atender às necessidades de informação da Instituição através de tecnologias que promovam a produtividade, agilidade, confiabilidade e inovação com colaboração, mobilidade e inteligência. Para tanto, seu conteúdo contempla diretrizes, metas, projetos e ações.

4.6.2. A Política de Segurança da Informação (POSIN) está alinhada com este documento e contém as diretrizes estratégicas para Segurança da Informação na Instituição.

5. Termos e Definições

5.1. Os conceitos e definições constantes neste item se aplicam de forma a auxiliar a interpretação desta POSIN e também no estabelecimento de futuras políticas e normas complementares.

5.2. Conforme a Instrução Normativa nº 1, de 27 de maio de 2020, em seu art 6º (IN 01/27-2020), os órgãos e as entidades da Administração Pública Federal deverão utilizar o Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI/PR nº 93, de 18 de outubro de 2021, disponível no momento da elaboração desta POSIN, como referência na elaboração de normativos internos afetos à Segurança da Informação e de trabalhos correlatos. Alguns termos e definições de Segurança da Informação foram transcritos desta portaria buscando atender as consultas e outros foram adequados e/ou obtidos em documentações correlatas e referenciadas.

5.3. A informação é um ativo essencial para os negócios do Inmetro e consequentemente necessita ter uma proteção adequada, em especial nos ambientes interconectados onde são crescentes os números e a variedades de ameaças e vulnerabilidades.

5.4. A estrutura normativa da Segurança da Informação do Inmetro é composta por um conjunto de documentos com dois níveis hierárquicos distintos, relacionados a seguir:

5.4.1. Política de Segurança da Informação (POSIN) - define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação.

5.4.2. Políticas e Normas internas - estabelecem responsabilidades e procedimentos definidos de acordo com as diretrizes da POSIN e tem como objetivos:

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

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

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

5.5. Para os fins desta POSIN, considera-se:

a) Ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização.

b) Ativo: tudo que tenha valor para a organização, material ou não.

c) 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.

d) Classificação da Informação: ato de se atribuir grau de sigilo a informação que requeira medidas especiais de salvaguarda e, por consequência, ao documento, material ou área que a contenha, utilize ou veicule.

e) Computação em Nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN).

f) Controle de Segurança da Informação: políticas, normas, processos, procedimentos, estruturas organizacionais e funções de hardware e software, cujo o principal objetivo é a proteção da confidencialidade, integridade e disponibilidade dos dados e informações do Inmetro.

g) Credencial de acesso: permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como por exemplo um crachá de identificação funcional), ou lógica (como por exemplo a identificação de usuário e senha).

h) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

i) Dispositivos móveis: equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USBdrives, HD externo, e cartões de memória.

j) Gestão de Segurança da Informação: processo que visa integrar 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 organizacional, aos processos institucionais estratégicos, táticos e operacionais, não se limitando, portanto, à tecnologia da informação.

k) Governança de TI: é de responsabilidade dos executivos e da Alta Administração, 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.

l) Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores do Inmetro.

m) Impacto: resultado de um evento de risco sobre os objetivos do processo.

n) Plano de continuidade de negócios: documentação dos procedimentos e das 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, em um nível previamente definido, em caso de incidente de segurança.

o) Redes ou mídias sociais: estruturas sociais digitais, compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

p) Resiliência: capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre, e retornar à normalidade das operações.

q) Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

r) Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

s) Tecnologia da Informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.

t) Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

u) Usuário: 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.

v) Vulnerabilidade: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

6. Princípios

As ações relacionadas com a Segurança da Informação no Inmetro são norteadas pelos seguintes princípios, assim definidos:

a) 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;

b) Celeridade: as ações de Segurança da Informação devem oferecer respostas rápidas a incidentes e falhas de segurança;

c) Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados pelo Inmetro;

d) Conhecimento: os usuários devem conhecer e respeitar a POSIN e as demais regulamentações sobre Segurança da Informação do Inmetro;

e) Clareza: as regras de Segurança da Informação, documentações e comunicações devem ser precisas, concisas e de fácil entendimento;

f) 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;

g) Ética: os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometimento da Segurança da Informação;

h) Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

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; e

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 gerais

7.1. Esta POSIN define as diretrizes para a Segurança da Informação 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 desta POSIN constituem os principais pilares da Gestão de Segurança da Informação, norteando a elaboração das políticas e normas internas.

7.3. 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 POSIN e demais regulamentações em vigor.

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

7.5. 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.

7.6. Os dados e informações confidenciais e/ou restritos do Inmetro não podem ser armazenados e/ou transportados em qualquer meio sem as devidas autorizações e proteções.

7.7. Assuntos confidenciais e/ou restritos de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas.

7.8. A credencial de acesso é pessoal, exclusiva e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o reconhecimento do envolvido.

7.9. Os planos, políticas e as normas de Segurança da Informação do Inmetro devem atender aos requisitos dispostos nas normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República, com especial atenção à Política Nacional de Segurança da Informação.

7.10. Qualquer tipo de dúvida sobre esta POSIN e políticas e normas internas de Segurança da Informação, assim como as demais regulamentações correlatas, deve ser encaminhada para a Coordenação-Geral de Tecnologia da Informação - CTINF.

8. Diretrizes Específicas

8.1. Da Gestão da Segurança da Informação

8.1.1. Os controles de Segurança da Informação devem ser mantidos, monitorados e avaliados, de forma contínua, com base em análise de riscos que possam impactar na confidencialidade, integridade, disponibilidade dos dados e informações corporativas e pessoais do Inmetro.

8.1.2. Requisitos de Segurança da Informação devem estar explicitamente citados em todos os termos de compromisso celebrados entre o Inmetro e terceiros.

8.2. Da Gestão de Ativos de TI

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

8.2.2. Os ativos de informação do Inmetro devem ser inventariados, atribuídos aos respectivos responsáveis, utilizados em conformidade com os padrões e normas operacionais de Segurança da Informação, e são destinados ao uso corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

8.2.3. É recomendável que todos os ativos sejam 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. Do Tratamento dos Dados e Informações Corporativas e Pessoais providos pela CTINF

8.3.1. Os dados e informações corporativas devem ser protegidos e, se requerido, classificados, de forma preventiva, de acordo com o seu valor, sigilo, sensibilidade e criticidade, contra ameaças e acessos não autorizados, acidentais ou não, com o objetivo de minimizar riscos de impactos às atividades de negócio do Inmetro.

8.3.2. Os dados e informações pessoais devem ser protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, buscando proteger os direitos fundamentais de privacidade, de acordo com a legislação vigente, em especial à Lei Geral de Proteção de Dados (LGPD).

8.3.3. A proteção dos dados e informações corporativas e pessoais devem observar os normativos e legislações específicas vigentes.

8.4. Do Material Impróprio

8.4.1. É expressamente proibido o acesso, uso, guarda e encaminhamento de material impróprio, como por exemplo, e não se limitando a: material ofensivo, de ódio, não ético, discriminatório, difamatório, ameaçador, malicioso, obsceno, pornográfico, sexualmente sugestivo, abusivo, ilegal, que infrinja a Lei nº 7.716, de 5 de janeiro de 1989, que infrinja as leis de propriedade intelectual/industrial ou que infrinja as leis de privacidade, por intermédio de quaisquer dos meios recursos de comunicações disponibilizados pelos serviços de TI do Inmetro.

8.5. Da Gestão de Tratamento de Incidentes de Segurança em Redes

8.5.1. A equipe de prevenção, tratamento e resposta a incidentes cibernéticos do Inmetro, ETIR-Inmetro, de forma geral, é responsável pelo recebimento, análise e resposta às notificações e atividades relacionadas aos incidentes de segurança na rede de computadores da Instituição. A ETIR-Inmetro compõe a rede de equipes dos órgãos e das entidades da administração pública federal, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

8.5.2. Os usuários devem registrar os incidentes de Segurança da Informação através dos canais de comunicação listados na Portaria Inmetro Presi nº 288, de 11 de julho de 2022, que instituiu a ETIR-Inmetro.

8.5.3. Demais diretrizes sobre a Gestão de Tratamento de Incidentes de Segurança em Redes nos órgãos e nas entidades da administração pública federal podem ser consultadas, por exemplo, nos Decretos nº 9.637, de 2018 e nº 10.748, de 16 de julho de 2021.

8.6. Gestão de Riscos de Segurança da Informação (GRSI)

8.6.1. A GRSI tem por objetivo direcionar e controlar o risco de Segurança da Informação, a fim de adequá-lo aos níveis aceitáveis para a Instituição. É composto por 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 serviços de TI do Inmetro providos pela CTINF. A GRSI é realizada de forma periódica e contínua.

8.6.2. A GRSI está alinhada ao modelo de gestão do Comitê de Riscos e Controles do Inmetro e as estratégias de continuidade para as atividades críticas da Instituição, visando assim limitar os impactos dos incidentes de Segurança da Informação e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

8.6.3. A GRSI busca identificar potenciais ameaças aos ativos de informação do Inmetro e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. O processo provê alternativas para desenvolver uma resiliência que seja capaz de responder efetivamente aos incidentes de Segurança da Informação e que minimize 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 da instituição e da sociedade.

8.6.4. Demais diretrizes sobre a Gestão de Riscos de Segurança da Informação nos órgãos e nas entidades da administração pública federal podem ser consultadas, por exemplo, na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021.

8.7. Da Auditoria e Conformidade

8.7.1. A CTINF mantém registros, como, por exemplo, trilhas de auditoria e relatórios técnicos, que apoiam na realização de análises de conformidade, através do rastreamento, acompanhamento, controle e verificação do uso e disponibilização dos sistemas, serviços e rede de computadores do Inmetro.

8.7.2. Da Auditoria

8.7.2.1. É uma atividade de avaliação independente, objetiva, sistemática e temporal, desenhada para fiscalizar a eficácia dos controles de Segurança da Informação.

8.7.3. Da Conformidade

8.7.3.1. É um conjunto de ações a fim de cumprir e se fazer cumprir os normativos legais, políticas, requisitos e diretrizes de Segurança da Informação estabelecidas para o negócio e para as atividades do Inmetro, bem como evitar, detectar, tratar e comunicar quaisquer desvios ou inconformidades relacionadas que possam ocorrer.

8.8. Do Controle de Acesso

8.8.1. As regras de controle de acesso a todos os sistemas e serviços de TI corporativos, a rede de computadores, acesso remoto, a intranet e internet, as informações, dados e às instalações físicas do Inmetro devem estar em conformidade com as leis, políticas e normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos do Inmetro.

8.8.2. Todas as credenciais de acesso aos ativos de informação e as instalações físicas do Inmetro devem ser, de forma imediata, revogadas ou suspensas, quando não mais necessárias, conforme normas e legislação específica em vigor.

8.8.3. 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. Quando cabível, deve ainda utilizar a legislação específica para a concessão de acesso às informações confidenciais e/ou restritas, 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 de TI do Inmetro.

8.9. Do Uso do Serviço de E-mail

8.9.1. O correio eletrônico é um recurso de comunicação corporativa do Inmetro. As regras de acesso e utilização do serviço de e-mail devem atender a todas as orientações desta POSIN, assim como as normas internas e demais diretrizes da APF.

8.10. Do Acesso à Internet

8.10.1. O acesso à rede mundial de computadores (Internet), no ambiente de trabalho, deve ser regido por normas internas, atendendo às determinações desta POSIN, assim como as normas internas e demais diretrizes da APF.

8.11. Do Uso das Mídias Sociais

8.11.1. O uso das Mídias Sociais disponíveis na rede mundial de computadores (Internet), com o objetivo de prestar atendimento e serviços púbicos, divulgando ou compartilhando informações do Inmetro, deve atender ao disposto na Instrução Normativa nº 6, de 23 de dezembro de 2021, que estabelece diretrizes de Segurança da Informação para o uso seguro de mídias sociais nos órgãos e nas entidades da APF, a esta POSIN, e demais normas internas e legislações em vigor.

8.11.2. Informações classificadas, confidenciais e/ou de acesso restrito não podem ser publicadas em Mídias Sociais.

8.11.3. A publicação de dados pessoais em Mídias Sociais deve observar o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e em normas correlatas.

8.11.4. É vedada a utilização de contas institucionais em mídias sociais para fazer recomendações profissionais ou que vise à promoção de produtos ou empresas não autorizadas pelo Inmetro.

8.12. Do Uso de Dispositivos Móveis

8.12.1. 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 POSIN e regidas por normas internas, a qual contemplará recomendações sobre o uso desses dispositivos.

8.13. Do Uso de Computação em Nuvem, Serviços e Recursos na Internet

8.13.1. 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, atendendo à determinações desta POSIN e demais orientações governamentais e legislação em vigor, como, por exemplo, a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, visando assim 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.

8.13.2. O tratamento de dados e informações, através do uso de serviços e/ou recursos disponibilizados na internet, buscando suprir demandas institucionais de transferência e armazenamento de documentos, processamento de dados, soluções, aplicações e/ou outras tecnologias da informação, deve atender às determinações desta POSIN e demais normativos legais, em especial a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021.

8.13.2.1. Dados e informações com grau de sigilo e, seus documentos preparatórios, não podem ser tratados em ambiente de computação em nuvem.

8.13.2.2. Podem ser exemplificados como serviços e/ou recursos disponibilizados na internet, mas não se limitando a: dropbox, google drive, onedrive, gmail, hotmail, outlook live, yahoo, icloud, whatsapp, facebook, linkedin, twitter, youtube, github, canva, wetransfer, slideshare, amazon web services, microsoft azure e teams, zoom, asana e google hangout.

8.14. Da Capacitação

8.14.1. O Inmetro deve promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à Segurança da Informação.

9. Competências e Responsabilidades

9.1. O Comitê de Segurança da Informação (CSI) do Inmetro tem como responsabilidade precípua o assessoramento para a implementação das ações de Segurança da Informação dispostos nesta POSIN.

9.2. O Gestor de Segurança da Informação do Inmetro tem a responsabilidade de promover a ampla e acessível divulgação desta POSIN e das normas internas de Segurança da Informação, assim como as demais atribuições constantes na Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional/PR, e nos diversos normativos legais correlatos e vigentes.

9.3. Compete a Coordenação-Geral de Tecnologia da Informação prover os recursos profissionais necessários e de TI para o estabelecimento, implementação, operacionalização, monitoração, análise e melhoria das ações, procedimentos, processos e controles de Segurança da Informação dentro do Inmetro.

9.4. Os usuários devem conhecer, observar e adotar as ações de Segurança da Informação estabelecidas nesta POSIN, sendo responsáveis pela segurança dos ativos e processos que estejam sob sua responsabilidade e por todos os atos executados com as suas credenciais de acesso.

9.4.1. Os usuários devem assinar Termo de Compromisso e Sigilo, concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e informações corporativas a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

9.5. Os casos omissos e as dúvidas surgidas na aplicação desta POSIN serão analisados, dirimidos ou solucionados pela CTINF.

10. Penalidades

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

10.1.1. O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar ao Inmetro.

10.2. Os usuários que tomarem conhecimento de práticas irregulares e/ou em não conformidade com esta POSIN devem levá-las ao conhecimento do superior imediato e/ou para as áreas competentes do Inmetro.

11. Principais Siglas

Sigla	Significado
ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CSI	Comitê da Segurança da Informação
CTINF	Coordenação-Geral de Tecnologia da Informação
DSIC	Departamento de Segurança da Informação e Comunicações da Presidência da
ETIR	Equipe de prevenção, tratamento e resposta a incidentes cibernéticos
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NBR	Norma Brasileira
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicações
POSIN	Política de Segurança da Informação
TI	Tecnologia da Informação

12. Principais referências legais e normativas

12.1. Plano Diretor de Tecnologia da Informação e Comunicações do Inmetro (PDTIC) 2021-2023. Este Plano Diretor de Tecnologia da Informação e Comunicação tem como objetivo organizar e apresentar o Planejamento de Tecnologia da Informação do Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro para o triênio 2021-2023.

12.2. Instrução Normativa GSI/PR nº 6, de 23 de dezembro de 2021. Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.

12.3. Portaria GSI/PR nº 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação.

12.4. Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

12.5. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Presidência da República.

12.6. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

12.7. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

12.8. Decreto nº 10.222, de 5 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética. E-Ciber. Orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área de segurança cibernética.

12.9. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24,caput,inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

12.10. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

12.11. ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls. 2a. Ed.

12.12. Norma complementar nº 18/IN01/DSIC/GSIPR de 2013. Diretrizes para as atividades de ensino em segurança da informação e comunicações nos Órgãos e entidades da administração pública federal. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional da Presidência da República.

12.13. Norma complementar nº 17/IN01/DSIC/GSIPR de 2013. Atuação e adequações para profissionais da área de segurança da informação e comunicações nos Órgãos e entidades da administração pública federal. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional da Presidência da República.

12.14. Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

12.15. ABNT NBR ISO/IEC 31010 de 2012. Gestão de riscos – Técnicas para o processo de avaliação de riscos.

12.16. Lei nº 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

12.17. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor.