MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
OBSERVATÓRIO NACIONAL

PORTARIA ON/MCTI Nº 78, DE 10 DE MAIO DE 2021

Institui a Política de Segurança da Informação - POSIN do Observatório Nacional

O DIRETOR DO OBSERVATÓRIO NACIONAL, no uso das atribuições que lhe foram conferidas por meio da Portaria MCT nº 407, de 29 de junho de 2006, publicada no D.O.U. de 30 de junho de 2006, e de acordo com a Portaria MCTIC nº 1.511, de 16 de março de 2018, publicada no D.O.U. de 19 de março de 2018, e com o estabelecido no Regimento Interno aprovado pela Portaria MCTI nº 3.462 de 10 de setembro de 2020, publicada no D.O.U. de 11 de setembro de 2020, resolve:

Art. 1º Instituir a Política de Segurança da Informação - POSIN do Observatório Nacional, na forma do anexo a esta Portaria.

Art. 2º Esta Portaria entra em vigor em 1º de junho de 2021.

JOÃO CARLOS COSTA DOS ANJOS

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO OBSERVATÓRIO NACIONAL

CAPÍTULO I
ESCOPO

Art. 1º A Política de Segurança da Informação - POSIN objetiva garantir a disponibilidade, integridade, confidencialidade, autenticidade e não repúdio das informações produzidas ou residentes no Observatório Nacional - ON.

§ 1º A POSIN deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal (apêndice A).

§ 2º Integram também a POSIN as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização, já existentes no âmbito da administração pública federal ou a serem criadas em texto complementar.

Art. 2º O ON deve observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta POSIN.

§ 1º As diretrizes de Segurança da Informação - SI devem considerar, prioritariamente, missões institucionais, objetivos estratégicos, processos, requisitos legais e estrutura do ON.

§ 2º A Gestão de Segurança da Informação - GSI deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SI.

Art. 3º As diretrizes, normas complementares e manuais de procedimentos da POSIN do ON aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, bolsistas de iniciação ao trabalho, consultores externos e a quem, de alguma forma, execute atividades vinculadas a este órgão.

§ 1º Todos são solidariamente responsáveis e devem estar comprometidos com a segurança da informação.

§ 2º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo ON que envolvam Tecnologias da Informação - TI devem atender a esta POSIN.

§ 3º Esta política também se aplica, no que couber, ao relacionamento do ON com terceiros.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

Art. 4º No âmbito da POSIN considera-se:

I - agente responsável pela Equipe de Resposta a Incidentes de Segurança - ERIS: servidor público ocupante de cargo efetivo do ON incumbido de chefiar e gerenciar a ERIS;

II - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

III - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - 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;

V - capacitação em SI: saber o que é segurança da informação, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SI;

VI - classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

VII - Comitê de Segurança da Informação - CSI: colegiado de caráter deliberativo responsável pela normatização e supervisão da segurança da informação no âmbito do ON;

VIII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

IX - conscientização em SI: atividade que tem por finalidade orientar sobre o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XI - CTIR.GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação do Gabinete de Segurança Institucional da Presidência da República DSI/GSI/PR;

XII - custodiante do ativo de informação: é aquele usuário que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia, que consiste na responsabilidade de se guardar um ativo para terceiros:

a) a custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

XIII - disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados e no momento requerido;

XIV - Equipe de Resposta a Incidentes de Segurança - ERIS: colegiado com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do ON;

XV - especialização em SI: saber o que é segurança da informação, aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na organização como gestor de SI e tornando-se referência na pesquisa de novas soluções e modelos de SI;

XVI - estrutura de GSI: grupo responsável pela gestão e execução da SI;

XVII - gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XVIII - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem:

a) o processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XIX - gestão de operações e comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;

XX - gestão de riscos de segurança da informação - GRSI: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;

XXI - gestão de segurança da informação - GSI: 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, no âmbito da tecnologia da informação;

XXII - gestor dos ativos de informação: servidor público ocupante de cargo efetivo do ON responsável por gerenciar determinada unidade organizacional e todos os ativos relacionados;

XXIII - gestor de SI: servidor público ocupante de cargo efetivo do ON nomeado pelo Diretor da instituição como responsável pela gestão de segurança da informação no âmbito do órgão;

XXIV - incidente de SI: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXV - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XXVI - infraestrutura de TI: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e

armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XXVII - integridade: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental;

XXVIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXIX - recursos criptográficos: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXX - risco de SI: 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;

XXXI - segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXXII - sensibilização em SI: saber o que é segurança da informação aplicando em sua rotina pessoal e profissional;

XXXIII - sistema estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

XXXIV - terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao ON;

XXXV - tratamento de incidentes: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXVI - tratamento da informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

XXXVII - usuário: é aquele a quem foi dado acesso por um custodiante e faz uso do ativo de informação; e

XXXVIII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III
DIRETRIZES GERAIS

Art. 5º O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Segurança da Informação - CSI, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 6º Compete à Divisão de Tecnologia da Informação - DITIN, com o apoio do Serviço de Recursos Humanos - SERHU e demais unidades pertinentes, instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em SI, buscando parcerias com outros órgãos e entidades.

Art. 7º Fica instituída a Estrutura de GSI do ON, composta pelo Comitê de Segurança da Informação - CSI e pela Equipe de Resposta a Incidentes de Segurança - ERIS, os quais serão solidariamente responsáveis pelas seguintes atividades:

I - executar os processos de segurança da informação;

II - desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos do ON;

III - avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação e desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;

IV - fornecer subsídios visando à verificação de conformidade de segurança da informação; e

V - promover a melhoria contínua nos processos e controles de GSI.

§ 1º A Estrutura de GSI deve definir um Plano de SI para o ON.

§ 2º A Estrutura de GSI do ON deve possuir um sistema de registro de incidentes de SI.

§ 3º Os membros da Estrutura da GSI devem:

I - ser servidores públicos ocupantes de cargo efetivo do ON;

II - possuir formação ou cargo específico em TI, com ênfase em SI; e

III - receber regularmente capacitação especializada nas disciplinas relacionadas à SI de acordo com suas funções.

§ 4º A GSI do ON deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da instituição e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

§ 5º A Estrutura de GSI deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 8º Além das diretrizes estabelecidas nesta POSIN, o ON deve também se orientar pelas melhores práticas e procedimentos de SI recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 9º É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo ON.

Art. 10. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação e a não designação pressupõe que o gestor é o próprio custodiante.

Art 11. Os contratos firmados pelo ON devem conter cláusulas que determinem a observância da POSIN e seus respectivos documentos.

CAPÍTULO IV
DIRETRIZES ESPECÍFICAS

Art. 12. Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaboradas normas táticas específicas, manuais e procedimentos.

Seção I
Gestão de ativos da informação

Art. 13. Os ativos de informação definidos no inciso III do art. 4º devem:

I - ser inventariados e protegidos;

II - ter identificados os seus proprietários e custodiantes;

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

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

V - ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI - ser regulamentados por norma específica quanto a sua utilização; e

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

Art. 14. O ON deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 15. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como

perdas, danos, furtos, roubos e interrupções não programadas.

Art. 16. Os sistemas de informação e as aplicações do ON devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 17. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

Seção II
Gestão de riscos

Art. 18. O gestor dos ativos de informação deve estabelecer processos de Gestão de Riscos de Segurança da Informação - GRSI que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos nos ativos de informação, conforme definido no inciso XXX do art. 4º.

Art. 19. A GRSI é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação, levando em consideração o planejamento, execução, análise crítica e melhoria da SI no ON.

Seção III
Segurança física e do ambiente

Art. 20. A Estrutura de GSI deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

Parágrafo único. As proteções devem estar alinhadas aos riscos identificados.

Seção IV
Segurança em recursos humanos

Art. 21. Os usuários devem ter ciência:

I - das ameaças e preocupações relativas à SI; e

II - de suas responsabilidades e obrigações no âmbito desta POSIN.

§ 1º Todos os usuários devem difundir e exigir o cumprimento da POSIN, das normas de segurança e da legislação vigente acerca do tema.

§ 2º Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do ON, de acordo com suas competências funcionais.

§ 3º Os usuários devem ser sensibilizados e conscientizados para apoiar esta POSIN durante os seus trabalhos normais.

Art. 22. O controle de pessoal:

I - é de responsabilidade da chefia da Coordenação de Administração - COADM, juntamente com o Serviço de Recursos Humanos - SERHU; e

II - deve estabelecer controles de perfis, permissões e procedimentos necessários para a salvaguarda da SI.

Seção V
Gestão de operações e comunicações

Art. 23. A Estrutura de GSI deve estabelecer parâmetros adequados, relacionados à SI, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do ON.

Parágrafo único. Os acordos de nível de serviço devem ser compatíveis com padrões de mercado e requisitos de segurança.

Seção VI
Controles de acessos

Art. 24. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 25. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 26. Os usuários do ON são responsáveis por todos os atos praticados com suas identificações, tais como nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.

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

Art. 27. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.

Art. 28. Todos os sistemas de informação do ON, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

Art. 29. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do ON ou bloqueados em caso de afastamento.

Seção VII
Aquisição, desenvolvimento e manutenção de sistemas

Art. 30. A Estrutura de GSI deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Parágrafo único. O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Seção VIII
Tratamento de incidentes

Art. 31. A Estrutura de GSI deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo de órgãos gestores de TI superiores, como CTIR.GOV, CGI.BR, RNP, dentre outros.

Art. 32. Deve ser instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança.

Seção IX
Gestão de continuidade

Art. 33. A Estrutura de GSI deve instituir metodologias ou normas que estabeleçam a Gestão de Continuidade do Negócio.

Seção X
Conformidade

Art. 34. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SI do ON e de suas unidades organizacionais com esta POSIN e suas normas e procedimentos complementares, bem como com a legislação específica de SI.

§ 1º A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o ON.

§ 2º A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de GSI e aprovado pelo CSI.

§ 3º O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

§ 4º Nenhuma unidade organizacional poderá permanecer sem verificação de conformidade de suas práticas de SI por período superior a 2 (dois) anos.

§ 5º A execução da verificação de conformidade será realizada pela Estrutura de GSI, podendo, com a prévia aprovação do CSI, ser subcontratada no todo ou em parte.

§ 6º É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

§ 7º A verificação de conformidade poderá combinar ampla variedade

de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

§ 8º Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de SI ao Gestor da unidade organizacional verificada, para ciência e tomada das ações cabíveis.

Seção XI
Plano de investimentos em SI do ON

Art. 35. Os investimentos em SI serão realizados de forma planejada e consolidados em um plano de investimentos.

§ 1º O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

§ 2º O plano de investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo CSI, mediante recomendação elaborada pela Estrutura de GSI.

§ 3º Caso haja limitação na execução orçamentária, caberá ao CSI realizar a correspondente revisão do plano de investimentos.

Seção XII
Propriedade intelectual

Art. 36. As informações produzidas por usuários no exercício de suas funções são patrimônio intelectual do ON e não cabe a seus criadores qualquer forma de direito autoral.

Art. 37. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do ON em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica pelos titulares das unidades organizacionais, nos processos e documentos de sua competência, ou pelo Diretor, nos demais casos.

Seção XIII
Contratos, convênios, acordos e instrumentos congêneres

Art. 38. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 39. Os acordos com terceiros podem também envolver outras partes.

Parágrafo único. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pelo ON.

Art. 40. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIN e de suas normas complementares.

Parágrafo único. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta POSIN e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no ON.

Art. 41. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

Art. 42. Deve ser definido um processo adequado/objetivo de gestão de mudanças que será detalhado em norma específica.

CAPÍTULO V
PENALIDADES

Art. 43. Ações que violem a POSIN ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SI serão devidamente apuradas e aos responsáveis serão aplicadas as sanções em vigor, incluindo, mas não se restringindo a:

I - advertência formal;

II - suspensão;

III - rescisão do contrato de trabalho;

IV - ação disciplinar; e/ou

V - processo administrativo, civil ou penal.

Parágrafo único. Recomenda-se a assinatura de termo de responsabilidade associado ao grau de acesso ao equipamento (apêndice B).

CAPÍTULO VI
COMPETÊNCIAS E RESPONSABILIDADES

Art. 44. Compete à GSI:

I - promover cultura de segurança da informação;

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

III - propor recursos necessários às ações de SI;

IV - coordenar o CSI e a ERIS;

V - comunicar ao CSI os resultados e outras informações pertinentes;

VI - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI;

VII - manter contato direto com o DSI/GSI/PR para o trato de assuntos relativos à segurança da informação; e

VIII - propor normas relativas à SI.

Art. 45. Compete ao CSI:

I - normatizar e supervisionar a SI no âmbito do ON;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SI;

III - propor alterações na POSIN;

IV - solicitar apurações quando da suspeita de ocorrências de quebras de SI;

V - avaliar, revisar e analisar criticamente a POSIN e suas normas complementares, visando a sua aderência aos objetivos institucionais do ON e às legislações vigentes;

VI - dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIN do ON;

VII - constituir grupo de trabalho para realizar verificações de conformidade;

VIII - aprovar o plano de investimentos em SI do ON;

IX - monitorar e avaliar periodicamente o plano de SI, assim como determinar os ajustes cabíveis;

X - definir e atualizar seu Regimento Interno; e

XI - baixar normas e procedimentos complementares a esta POSIN.

Art. 46. Compete à ERIS:

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

II - promover a recuperação de sistemas;

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

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

V - analisar ataques e intrusões na rede do ON;

VI - executar as ações necessárias para tratar quebras de segurança;

VII - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

VIII - cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

IX - participar em fóruns, redes nacionais e internacionais relativos à SI.

Art. 47. Compete aos Gestores dos Ativos de Informação:

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

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

III - conceder e revogar acessos aos ativos de informação;

IV - comunicar à ERIS a ocorrência de incidentes de SI; e

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

VI - demandar de seus custodiantes e usuários a assinatura do termo de responsabilidade (apêndice B), quando cabível.

Art. 48. Compete ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta POSIN.

Art. 49. Compete ao Diretor, Coordenadores e Chefias de Divisão e Serviço:

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

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

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

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

V - informar à SERHU a movimentação de pessoal de sua unidade;

VI - realizar o tratamento e a classificação da informação;

VII - autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade organizacional;

VIII - assegurar que os recursos necessários para o GSI estejam disponíveis;

IX - comunicar à ERIS os casos de quebra de segurança; e

X - manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 50. Compete aos terceiros e fornecedores, conforme previsto em

contrato:

I - tomar conhecimento desta POSIN;

II - fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

III - fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 51. Compete aos usuários:

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

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

III - comunicar os incidentes que afetam a segurança dos ativos de informação à ERIS.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 52. Esta POSIN, bem como os documentos gerados a partir dela, deverão ser revisados anualmente, ou por deliberação do CSI.

Art. 53. O CSI formalizará a proposta de revisão da POSIN por meio de instrumento interno, o qual deve ser aprovado pelo Diretor do ON.

Art. 54. Casos omisos serão resolvidos pelo Diretor do ON, ouvidos os gestores e colegiados pertinentes.

APÊNDICE A
REFERÊNCIAS LEGAIS E NORMATIVAS

Leis, Decretos, Portarias, Instruções Normativas, dispositivos legais e legislação específica de caráter federal e normas técnicas relacionadas à Segurança da Informação: https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao

APÊNDICE B
TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em ____/____/_____, e lotado na unidade _____ do Observatório Nacional - ON, DECLARO, sob pena das sanções cabíveis nos termos da Legislação Vigente (*), que assumo a responsabilidade por:

1. tratar o(s) ativo(s) de informação como patrimônio do ON;

2. utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do ON;

3. contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

4. utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e as normas específicas do ON; e

5. responder, perante o ON, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Estou ciente que, caso o solicite, a senha de administrador será liberada para o meu uso, ficando a DTIN livre de responsabilidade por atualizações, instalações e suporte de programas na máquina em questão e reinstalação do Sistema Operacional.

Estou ciente também que a Lei nº 9.609/98 estabelece que a violação de direitos autorais de programas de computador é crime, punível com pena de detenção de 6 (seis) meses a 4 (quatro) anos e multa, além de ser passível de ação cível indenizatória.

Rio de Janeiro, RJ, _____ de _____ de _____ .

Nome do usuário: _____

Setor: _____

Assinatura: _____

Rio de Janeiro, RJ, _____ de _____ de _____ .

Nome do responsável: _____

Setor: _____

Assinatura: _____

_____

(*) Legislação Vigente:

Art. 6º da Lei nº 10.683, de 28 de maio de 2003;
Decreto nº 9.637, de 26 de Dezembro de 2018;
Decreto nº 10.641, de 2 de Março de 2021;
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008 e suas Normas Complementares;
NBR ISO/IEC 27001:2013 - Sistema de Gestão de Segurança da Informação;
NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação.
Política de Segurança da Informação - POSIN do ON/MCTI

Documento assinado eletronicamente por João Carlos Costa dos Anjos, Diretor do Observatório Nacional, em 10/05/2021, às 16:59 (horário oficial de Brasília), com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador 7271863 e o código CRC 556D6C33.