POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (Posin) 2024-2028

CENTRO DE TECNOLOGIA, INOVAÇÃO E CIÊNCIA DE DADOS
CETIC

INEP MINISTÉRIO DA EDUCAÇÃO

REPÚBLICA FEDERATIVA DO BRASIL

MINISTÉRIO DA EDUCAÇÃO | **MEC**

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS
EDUCACIONAIS ANÍSIO TEIXEIRA | **INEP**

CENTRO DE TECNOLOGIA, INOVAÇÃO
E CIÊNCIA DE DADOS | **CETIC**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIN)

2024-2028

Brasília-DF
Inep/MEC
2025

CENTRO DE TECNOLOGIA, INOVAÇÃO E CIÊNCIA DE DADOS (CETIC)

GESTÃO
Fernando Szimanski (Chefe do Centro)

COORDENAÇÃO-GERAL DE INFRAESTRUTURA TECNOLÓGICA E SEGURANÇA CIBERNÉTICA (CGITS)
Welber Antonio Luchine (Coordenador-Geral)

COORDENAÇÃO-GERAL DE GOVERNANÇA (CGGOV)
Marco Túlio de Vasconcelos (Coordenador-Geral)

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (CSIC)
I - Gestor de Segurança da Informação:
Titular: Welber Antonio Luchine (CETIC)
Substituto: Fernando Szimanski (CETIC)

II - Gabinete da Presidência do Inep (GAB):
Titular: Tânia Carolina Nunes Machado Gonçalves
Suplente: Webster Spiguel Cassiano

III - Diretoria de Avaliação da Educação Básica (DAEB):
Titular: Giordano Alan Barbosa Sereno
Suplente: Marcos de Carvalho Mazzoni Filho

IV - Diretoria de Estatísticas Educacionais (DEED):
Titular: Clodoaldo de Oliveira Lemes
Suplente: Fábio Pereira Bravin

V - Diretoria de Estudos Educacionais (DIRED):
Titular: Marco César Araújo Pereira
Suplente: Isabella Maia Fernandes

VI - Diretoria de Gestão e Planejamento (DGP):
Titular: Leonardo Ferreira da Silva
Suplente: Thiago Gondim Ribeiro

VII - Diretoria de Avaliação da Educação Superior (DAES):
Titular: Priscilla Bessa Castilho
Suplente: Marco Aurélio Khoury Porto
Suplente: Marcus Vinicius Soares de Brito

VIII - Centro de Tecnologia, Inovação e Ciência de Dados (CETIC):
Titular: Emerson Vieira dos Santos
Suplente: Carlos Marinho de Souza

EQUIPE TÈCNICA
Welber Antônio Luchine
Ana Carolina Neves dos Santos
Rafael Barbosa da Silva

DIRETORIA DE ESTUDOS EDUCACIONAIS (DIRED)

COORDENAÇÃO-GERAL DE EDITORAÇÃO E PUBLICAÇÕES (CGEP)
Priscila Pereira Santos

DIVISÃO DE PERIÓDICOS (DPE)
Roshni Mariana de Mateus

DIVISÃO DE PRODUÇÃO EDITORIAL (DPR)
Ricardo Cézar Blezer

APOIO EDITORIAL
Janaína da Costa Santos

PROJETO GRÁFICO CAPA/MIOLO
Marcos Hartwich/Raphael C. Freitas

REVISÃO GRÁFICA
Érika Janaína de Oliveira Saraiva

PROJETO GRÁFICO CAPA/MIOLO
Marcos Hartwich/Raphael C. Freitas

DIAGRAMAÇÃO E ARTE-FINAL
Raphael C. Freitas

Esta publicação deverá ser citada da seguinte forma:

BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep). *Política de Segurança da Informação (Posin) 2024-2028*. Brasília, DF: Inep, 2025.

SUMÁRIO

ESTA PUBLICAÇÃO POSSUI SUMÁRIO INTERATIVO
PARA RETORNAR AO SUMÁRIO, CLIQUE NO NÚMERO DA PÁGINA EM CADA SEÇÃO

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA

PORTARIA Nº 26, DE 14 DE JANEIRO DE 2025

Institui a Política de Segurança da Informação - Posin, no âmbito do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira - Inep.

O PRESIDENTE DO INSTITUTO NACIONAL DE ESTUDOS E PESQUISASEDUCACIONAIS ANÍSIO TEIXEIRA, no uso das atribuições que lhe confere o Decreto nº 11.204, de 21 de setembro de 2022, e considerando o disposto na Instrução Normativa PR/GSI nº 1, de 27 de maio de 2020, resolve:

Art. 1º Fica instituída a Política de Segurança da Informação - Posin no âmbito do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira - Inep, na forma do Anexo à presente Portaria.

Art. 2º Fica revogada a Portaria nº 211, de 24 de maio de 2021.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

MANUEL FERNANDO PALACIOS DA CUNHA E MELO

Documento assinado eletronicamente por **Manuel Fernando Palacios da Cunha e Melo**, **Presidente**, em 31/01/2025, às 19:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.inep.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1618410** e o código CRC **0EDCB02F**.

CAPÍTULO I
DO ESCOPO

SEÇÃO I
DO OBJETIVO

Art. 1º A Política de Segurança da Informação (Posin) do Inep tem por objetivo estabelecer diretrizes, responsabilidades, competências e subsídios para a institucionalização e fortalecimento da gestão de segurança da informação no âmbito do Inep, visando:

I. garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas ou custodiadas pelo Inep;

II. garantir a proteção dos dados e dos ativos de informação;

III. alinhar as ações de segurança da informação com a natureza, a finalidade e o planejamento estratégico do Inep;

IV. orientar a implantação das iniciativas relativas à Segurança da Informação;

V. apoiar e orientar a tomada das decisões institucionais quanto a otimização de investimentos em segurança da informação que visem à eficiência, à eficácia e à efetividade das atividades organizacionais; e

VI. garantir a ampla divulgação dessa Política e normas correlatas.

Art. 2º Esta Política de Segurança da Informação será composta por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

SEÇÃO II
DA ABRANGÊNCIA

Art. 3º A Posin se aplica a toda a organização e deve ser cumprida por todos os seus servidores, colaboradores, estagiários, fornecedores, prestadores de serviços, consultores externos e a quem, de alguma forma, execute atividades para o Inep.

Art. 4º Esta Posin também se aplica, no que couber, ao relacionamento do Inep com terceiros.

Art. 5º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Inep devem atender a esta Posin.

Art. 6º Deverá constar em todos os contratos do Inep, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no Inep, inclusive provenientes de organismos internacionais. Deverá estar prevista, por parte das empresas e profissionais prestadores de serviço, entrega de declaração expressa de compromisso em relação à confidencialidade e de termo de ciência das normas vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela instituição.

Art. 7º Esta Política, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

Art. 8º Cada usuário é responsável pela segurança das informações dentro do Inep, principalmente daquelas que estão sob sua responsabilidade.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 9º Esta Posin considerou os seguintes conceitos e definições, em consonância com a Portaria GSI/PR Nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação:

I. **ativo**: qualquer coisa que tenha valor para a organização;

II. **agente responsável pela equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR)**: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal incumbido de chefiar e gerenciar a ETIR;

III. **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;

IV. **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;

V. **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;

VI. **capacitação em segurança da informação**: 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 Segurança da Informação;

VII. **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;

VIII. **colaborador**: todas as pessoas envolvidas com o desenvolvimento de atividades na organização, de caráter permanente, continuado ou eventual, incluindo prestadores de serviços, bolsistas, consultores e estagiários;

IX. **comitê de segurança da informação e comunicação (CSIC)**: colegiado de caráter deliberativo responsável pela normatização e supervisão da Segurança da Informação no âmbito do Inep;

X. **confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados;

XI. **conscientização em segurança da informação**: saber o que é Segurança da Informação aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

XII. **controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XIII. **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 e Comunicações do Gabinete de Segurança Institucional da Presidência da República DSIC/GSI/PR;

XIV. **custodiante do ativo de informação**: é aquele 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;

XV. **dado**: qualquer elemento identificado em sua forma bruta, que por si só, não conduz a uma compreensão de determinado fato ou situação;

XVI. **disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;

XVII. **equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR)**: 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 Inep;

XVIII. **especialização em segurança da informação**: 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 Segurança da Informação e tornando-se referência na pesquisa de novas soluções e modelos de segurança da informação;

XIX. **estrutura de GSI**: grupo responsável pela gestão e execução da segurança da informação;

XX. **gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XXI. **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. Esse 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;

XXII. **gerenciamento de operações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;

XXIII. **gestão de riscos de segurança da informação**: 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;

XXIV. **gestão de segurança da informação**: 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 e comunicações;

XXV. **gestor de segurança da informação**: servidor nomeado pelo Presidente do Inep como responsável pela gestão de Segurança da Informação no âmbito do órgão;

XXVI. **incidente de segurança da informação**: 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 inferior ao tempo objetivo de recuperação;

XXVII. **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;

XXVIII. **infraestrutura de tecnologia da informação**: 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;

XXIX. **integridade**: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental;

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

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

XXXII. **risco de segurança da informação**: 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;

XXXIII. **servidor**: pessoa legalmente investida em cargo público;

XXXIV. **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;

XXXV. **sensibilização em segurança da informação**: saber o que é segurança da informação aplicando em sua rotina pessoal e profissional;

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

XXXVII. **terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao Inep;

XXXVIII. **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 a identificação de tendências;

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

XL. **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 (APF), formalizada por meio da assinatura do Termo de Responsabilidade; e

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

CAPÍTULO III
DOS PRINCÍPIOS

Art. 10 A Política de Segurança da Informação do Inep será norteada pelos seguintes princípios:

I. disponibilidade;

II. integridade;

III. confidencialidade; e

IV. autenticidade.

Art. 11 A Posin deve obedecer também aos princípios constitucionais, administrativos e ao arcabouço normativo vigente que rege a segurança da informação no âmbito da Administração Pública Federal (APF).

CAPÍTULO IV
DA ESTRUTURA DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 12 A estrutura de gestão da Segurança da Informação do Inep será composta:

I. pelo Comitê de Segurança da Informação de Comunicação (CSIC);

II. pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR); e

III. pelo Gestor de Segurança da Informação (GSI).

Art. 13 O Inep deverá instituir formalmente o Comitê de Segurança da Informação de Comunicação (CSIC) com objetivo de assessorar a implementação das ações de segurança da informação no âmbito do Inep.

Art. 14 O Inep deverá instituir formalmente a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas aos incidentes na rede computacional do Inep que afetem a segurança da informação.

Art. 15 O Gestor de Segurança da Informação coordenará o Comitê de Segurança da Informação de Comunicação (CSIC) e acompanhará os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Art. 16 A estrutura de gestão de Segurança da Informação deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 17 A estrutura de gestão de Segurança da Informação do Inep 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.

Art. 18 Os servidores representantes da estrutura da gestão de Segurança da Informação devem receber regularmente capacitação especializada nas disciplinas relacionadas à segurança da informação de acordo com suas funções.

Art. 19 O CSIC e a ETIR devem elaborar políticas, normas, planos de ação e procedimentos quando couber e no limite de sua atuação, observando as necessidades específicas do Inep e todos os normativos da Administração Pública Federal sobre essa temática.

CAPÍTULO V
DOS PAPÉIS E DAS RESPONSABILIDADES

SEÇÃO I
DOS PAPÉIS

Art. 20 A Posin define os seguintes papéis e perfis para os usuários internos e externos:

USUÁRIOS INTERNOS		
PAPEL	**PERFIL**	**DESCRIÇÃO**
USUÁRIOS INTERNOS	Servidores públicos, servidores sem vínculo e colaboradores terceirizados.	Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas, consultores e colaboradores terceirizados, que fazem uso dos recursos informacionais e computacionais do Inep.
GESTORES	Presidente, Diretores, Chefe de Gabinete, Coordenadores Gerais, Coordenadores, Chefes de Divisão e Chefes de Serviço.	Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
ÁREA DE TECNOLOGIA DA INFORMAÇÃO	Chefe do Centro de TIC, Coordenadores Gerais, Chefes de Divisão e Chefes de Serviço.	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e Custodiante da informação.
GESTOR DE SEGURANÇA DA INFORMAÇÃO (GSI)	Gestão técnica	Responsável pelas ações de Segurança da Informação no âmbito do órgão ou entidade da Administração Pública Federal (APF).
EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR)	Equipe técnica	Grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores.
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (CSIC)	Alta Administração	Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de Segurança da Informação no âmbito do órgão ou entidade da Administração Pública Federal (APF).
USUÁRIO EXTERNO		
PAPEL	**PERFIL**	**DESCRIÇÃO**
USUÁRIOS EXTERNOS	Prestadores de serviço e demais colaboradores externos.	Prestadores de serviços contratados direta ou indiretamente pelo Inep e demais colaboradores externos (clientes dos serviços do Inep) que fazem uso de seus recursos informacionais e computacionais.

SEÇÃO II
DAS RESPONSABILIDADES GERAIS

Art. 21 São responsabilidades gerais e comuns a todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação do Inep:

I. conhecer e cumprir todos os princípios, diretrizes e responsabilidades estabelecidos nesta Posin, bem como os demais normativos e resoluções relacionados à segurança da informação, apreciados e aprovados pelo CSIC;

II. respeitar a propriedade intelectual, não copiando, modificando, usando ou divulgando, no todo ou em parte, textos, artigos, programas ou qualquer outro material, sem a permissão expressa, por escrito, do detentor deste direito;

III. zelar pelos equipamentos de TI que utiliza, não sendo permitida qualquer remoção, movimentação, desconexão de partes, substituição ou qualquer alteração em suas características físicas ou técnicas;

IV. zelar pela segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso;

V. não executar programas, instalar equipamentos ou executar ações que tenham como finalidade a decodificação de senhas, a monitoração da rede do Inep, a leitura de dados de terceiros, a facilitação do acesso à rede do Inep de usuários não autorizados, a propagação de vírus de computador, enganar programas e sistemas de segurança, a destruição parcial ou total de arquivos ou causar a indisponibilidade de serviços;

VI. não utilizar os direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função que tenha exercido no Inep;

VII. não utilizar a rede do Inep ou permissões de acesso concedidas para divulgar informações a terceiros que são sigilosas ou de interesse apenas do Inep;

VIII. não compartilhar credenciais de acesso e conexões com outras pessoas;

IX. manter a confidencialidade, memorizar e não registrar a senha em lugar algum;

X. alterar a senha sempre que existir qualquer suspeita do seu comprometimento;

XI. comunicar imediatamente à área de tecnologia da informação suspeita de comprometimento de senha;

XII. seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos corporativos de informação e comunicação utilizando-os sempre de forma ética, legal e consciente;

XIII. manter-se atualizado em relação a esta Posin e às suas normas complementares e procedimentos relacionados, buscando informação junto ao Gestor de Segurança da Informação sempre que não estiver absolutamente seguro quanto à obtenção, tratamento, uso e/ou descarte de informações; e

XIV. os bancos de dados sob responsabilidade das diretorias devem possuir procedimentos próprios de segurança, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD) de n° 13.709/2018.

SEÇÃO III
DAS RESPONSABILIDADES ESPECÍFICAS DOS USUÁRIOS INTERNOS E EXTERNOS

Art. 22 É responsabilidade dos usuários internos e externos cumprir as seguintes normas:

I. obedecer aos requisitos de controle de acesso físicos e lógicos especificados pelos gestores e custodiantes da informação;

II. comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à ETIR;

III. não permitir ou colaborar com o acesso aos recursos computacionais por parte de pessoas não autorizadas. Os usuários são responsáveis por qualquer atividade desenvolvida através de suas contas e pelos eventuais custos dela decorrentes em atividades não autorizadas;

IV. controlar o acesso físico aos equipamentos sob sua responsabilidade; e

V. cooperar no cumprimento desta Norma.

Parágrafo único. O desconhecimento das regras contidas nesta Posin é inescusável, ou seja, a alegação de seu desconhecimento não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade.

DOS GESTORES (TITULAR OU SUBSTITUTO DA UNIDADE ADMINISTRATIVA)

Art. 23 É responsabilidade dos Gestores (titular ou substituto da unidade administrativa) cumprir as seguintes normas:

I. corresponsabilizar-se 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 Segurança da Informação;

III. incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à Segurança da Informação;

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

V. informar à área de recursos humanos a movimentação de pessoal de sua unidade;

VI. autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

VII. comunicar à ETIR os casos de quebra de segurança; e

VIII. defender os direitos autorais (copyright), as leis que regulamentam o acesso e o uso das informações, e as regras e normas específicas de uso de recursos de TI.

DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Art. 24 É responsabilidade da Área de Tecnologia da Informação cumprir as seguintes normas:

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

II. definir e gerir os requisitos de segurança para os ativos de informação, em conformidade com esta Posin;

III. manter os recursos de TI do Data Center do Inep sob sua gestão;

IV. preservar a disponibilidade, integridade e confidencialidade dos dados e informações sob sua custódia;

V. configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de Segurança da Informação;

VI. gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes; para as trilhas geradas e/ou mantidas em meio eletrônico, devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas como evidências;

VII. garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

VIII. zelar pela segregação de funções gerenciais e operacionais, de modo a restringir os privilégios de cada indivíduo ao mínimo necessário, bem como descredenciar o acesso de pessoas que possam excluir registros de logs e trilhas de auditoria referentes às próprias ações;

IX. administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o Inep;

X. implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

XI. informar previamente o Gestor de SI sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante;

XII. nas movimentações internas dos ativos de TI, assegurar-se de que as informações de determinado usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

XIII. gerir a capacidade de armazenamento, processamento e transmissão de dados de forma a garantir os níveis de segurança requeridos;

XIV. atribuir cada conta de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta;

XV. proteger continuamente todos os ativos de informação contra ameaças de segurança, buscando assegurar que novos ativos apenas sejam integrados ao ambiente de produção após cumprirem os requisitos de segurança da informação definidos;

XVI. zelar pela não introdução de vulnerabilidades ou fragilidades indesejadas nos ativos de informação ou nos ambientes informacionais do Inep durante sua operação ou durante eventos de mudança de ambiente (de desenvolvimento para teste, homologação ou produção, por exemplo);

XVII. definir regras para instalação de softwares e hardwares no ambiente corporativo e demais ambientes vinculados;

XVIII. definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos;

XIX. responsabilizar-se pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos, aqueles instalados nos servidores de rede;

XX. garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento do Inep, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos da instituição;

XXI. garantir que todos os servidores, estações de trabalho e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais do Governo Brasileiro;

XXII. monitorar o ambiente de TI, gerando indicadores e históricos de uso da capacidade instalada da rede e dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos; períodos de indisponibilidade no acesso à internet e aos sistemas críticos; incidentes de segurança; e atividade de todos os usuários durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos); e

XXIII. suspender preventivamente ou parcialmente o direito de acesso aos recursos de TI do Inep de determinado usuário por razões ligadas à segurança, considerando que:

a) o fato deverá ser comunicado imediatamente ao titular da unidade administrativa do Inep a qual o usuário esteja lotado, explicitando o motivo para o bloqueio;

b) o acesso será restabelecido quando a segurança e o bem-estar puderem ser restabelecidos e assegurados; e

c) comunicar à ETIR a ocorrência de incidentes de Segurança da Informação.

DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 25 É responsabilidade do Gestor de Segurança da Informação (GSI) cumprir as seguintes normas:

I. promover a cultura de Segurança da Informação e Comunicação;

II. coordenar o Comitê de Segurança da Informação e Comunicação;

III. convocar e coordenar as reuniões do CSIC;

IV. coordenar a elaboração da política de segurança da informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

V. assessorar a alta administração na implementação da Política de Segurança da Informação e Comunicações - Posin;

VI. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

VII. promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VIII. oferecer orientação e treinamento sobre a Posin e assuntos relacionados à Segurança da Informação e Comunicações a todos os servidores e colaboradores do Inep, quando necessário;

IX. incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

X. propor projetos e iniciativas relacionados ao aperfeiçoamento da Segurança da Informação e Comunicações do Inep, mantendo-a atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;

XI. acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes em Redes computacionais, relacionados à Segurança da Informação;

XII. realizar trabalhos de análise de vulnerabilidade com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações do Inep;

XIII. requisitar informações às demais áreas do Inep (diretorias, coordenações etc.), realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Posin e das Normas de Segurança da Informação e Comunicações;

XIV. estabelecer mecanismo de registro e controle de não-conformidade à Posin e às Normas de Segurança da Informação e Comunicações, sempre comunicando o CSIC;

XV. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

XVI. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XVII. manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

DA EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR)

Art. 26 É responsabilidade da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) cumprir as seguintes normas:

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 Inep;

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 relativas à Segurança da Informação.

DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (CSIC)

Art. 27 É responsabilidade do Comitê de Segurança da Informação e Comunicação (CSIC) cumprir as seguintes normas:

I. assessorar a implementação das ações de segurança da informação;

II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV. propor ajustes, aprimoramentos e modificações das diretrizes constantes na Política de Segurança da Informação (Posin);

V. deliberar sobre normas internas de segurança da informação;

VI. analisar os casos de violação da Posin, das Normas e da Legislação referente à Segurança da Informação e Comunicações, encaminhando-os à Alta Administração do Instituto, quando for o caso;

VII. propor projetos e iniciativas relacionados à melhoria da Segurança da Informação do Inep;

VIII. propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à Segurança da Informação e Comunicações do Inep;

IX. determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de Segurança da Informação e à tomada de decisão;

X. acompanhar o andamento dos principais projetos e iniciativas relacionados à Segurança da Informação e Comunicações; e

XI. elaborar o Plano de Capacitação em Gestão de Segurança da Informação do Inep.

CAPÍTULO VI
DAS DIRETRIZES

SEÇÃO I
DAS DIRETRIZES GERAIS

Art. 28 O Inep, além das diretrizes estabelecidas nesta Posin, deve também se orientar pelas melhores práticas e procedimentos de segurança da informação recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 29 É vedado comprometer a disponibilidade, integridade, confidencialidade, autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Inep.

Art. 30 O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

SEÇÃO II
DAS DIRETRIZES ESPECÍFICAS

Art. 31 Para cada uma das diretrizes estabelecidas nesta seção, deverão ser elaboradas políticas e procedimentos específicos, que serão implementados conforme a disponibilidade, considerando as peculiaridades operacionais do Inep e em conformidade com os normativos da Administração Pública Federal (APF), a legislação nacional aplicável, como a Lei Geral de Proteção de Dados (LGPD) de n° 13.709/2018 e o Marco Civil da Internet da lei nº 12.965/2014, além de normas internacionais, como a ISO/IEC 27001.

Art. 32 Esses procedimentos devem seguir as melhores práticas de mercado e segurança da informação, assegurando a proteção integral dos ativos e dados sob a responsabilidade do Inep.

Art. 33 Essas diretrizes abrangem:

I. tratamento da informação;

II. segurança física e do ambiente;

III. gestão de incidentes em segurança da informação;

IV. gestão de ativos;

V. serviço de cópia e restauração (Backup/Restore);

VI. controle de acesso;

VII. gestão de registros (logs) de auditoria;

VIII. gestão de provedores de serviços;

IX. gerenciamento de vulnerabilidades;

X. defesa contra malware;

XI. uso de equipamentos de TI e softwares;

XII. uso do correio eletrônico corporativo;

XIII. acesso e uso da internet;

XIV. desenvolvimento e aquisição de software seguro;

XV. uso dos serviços de impressão;

XVI. tratamento de incidentes em redes computacionais;

XVII. criptografia; e

XVIII. implementação dos processos de segurança da informação.

CAPÍTULO VII
DO PLANO DE INVESTIMENTOS EM SEGURANÇA DA INFORMAÇÃO

Art. 34 O Plano de Investimentos em Segurança da Informação do Inep deve seguir as seguintes diretrizes:

I. os investimentos necessários em medidas de segurança devem ser dimensionados segundo o valor do ativo que será protegido, de acordo com o risco de potenciais prejuízos para o negócio, para a atividade fim e para os objetivos institucionais.

II. os investimentos serão planejados e integrados ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);

III. o plano será elaborado com base na priorização dos riscos, considerando a probabilidade e o impacto;

IV. o comitê de segurança da informação e comunicação (CSIC) aprovará o plano e a proposta orçamentária, com base em recomendação do Gestor de Segurança da Informação (GSI);

V. se houver restrições orçamentárias, o CSIC revisará o plano de investimentos.

CAPÍTULO VIII
DAS PENALIDADES

Art. 35 O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais o Inep responderá com a aplicação de todas as medidas administrativas e judiciais cíveis e penais cabíveis.

Art. 36 Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo superior hierárquico.

Art. 37 Os dispositivos de identificação e senhas protegem a identidade do colaborador/usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o Inep e/ou terceiros. Portanto, o usuário vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), sendo que o uso dos dispositivos e/ou senhas de identificação de

outra pessoa viola as regras de segurança e poderá resultar na aplicação de medidas administrativas, cíveis e penais cabíveis.

Art. 38 O Código Penal Brasileiro (Decreto-Lei n° 2848/1940) tipifica como crime o ato de invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (art. 154-A), assim como comete crime "quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" (art. 154-B).

Art. 39 Ações que violem a Política de Segurança da Informação do Inep caracterizam infração funcional e poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurado aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO IX
DA ATUALIZAÇÃO E REVISÃO

Art. 40 A Posin do Inep deverá ser revisada em função de alterações na legislação pertinente, das diretrizes superiores do Governo Federal, de alterações nos normativos internos, quando considerada necessária ou no prazo máximo de quatro anos, a contar da data de sua publicação. A revisão deve ser proposta pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e aprovada pelo Comitê de Segurança da Informação e Comunicação (CSIC).

Art. 41 O CSIC poderá expedir normas complementares associadas à Política de Segurança da Informação do Inep, no âmbito de sua competência regimental, com o objetivo de detalhar particularidades e procedimentos relativos à sua implementação no âmbito do instituto.

Art. 42 Cabe à Área de Tecnologia da Informação do Inep expedir e gerir os procedimentos de nível operacional que instrumentalizem o disposto nas normas complementares e nesta Política.

CAPÍTULO X
DA CLASSIFICAÇÃO E INFORMAÇÕES

Art. 43 As informações e dados deverão ser classificados (agrupados em "classes") para otimizar os controles que garantem seu acesso apenas por pessoas autorizadas, conforme processo a ser definido em normativo próprio. As classes devem se alinhar ao disposto na Lei n° 12.527/2011 (Lei de Acesso à Informação) e em outras leis que definem regras de sigilo tais como sigilo fiscal, bancário, comercial e aquele relativo a denúncias.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 44 As dúvidas ou casos omissos relativos a esta Posin serão reportados ao Comitê de Segurança da Informação e Comunicação (CSIC), que deverá esclarecê-los de forma célere.

Art. 45 Cabe ao Gestor de Segurança da Informação promover, com apoio da alta administração, a ampla divulgação da Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, aos usuários e aos prestadores de serviço, a fim de que esses tomem conhecimento de tais instrumentos, inclusive com publicação permanente na página da Inep NET.

ANEXO I

SEÇÃO I
DA GESTÃO DE RISCO

Art. 46 Esta seção tem como objetivo definir as diretrizes e os processos necessários para a gestão de riscos de segurança da informação no âmbito do Inep, garantindo que os riscos relacionados à segurança dos ativos de informação sejam adequadamente identificados, avaliados, tratados e monitorados de forma contínua.

Art. 47 A gestão de riscos de segurança da informação será realizada com base nas seguintes diretrizes:

I. identificação sistemática de riscos que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade das informações.

II. aplicação de metodologias de análise qualitativa e quantitativa de riscos para mensurar o impacto potencial e a probabilidade de ocorrência de cada risco identificado.

III. desenvolvimento de um plano de ação para tratar os riscos identificados, priorizando medidas corretivas e preventivas com base na criticidade e no impacto para os ativos de informação.

IV. assegurar o monitoramento contínuo dos riscos de segurança da informação e revisar periodicamente as avaliações para refletir mudanças no ambiente, nas ameaças e nas vulnerabilidades.

V. alinhamento da gestão de riscos com as diretrizes estabelecidas pela ISO/IEC 27001 e demais normativas legais e regulatórias aplicáveis, como a Lei Geral de Proteção de Dados Pessoais (LGPD) de n° 13.709/2018.

Art. 48 A gestão de riscos de segurança da informação será conduzida com base nas seguintes etapas:

I. **identificação dos riscos:** a identificação de riscos envolve a avaliação de todas as atividades, processos, sistemas e ativos de informação do Inep, com foco na identificação de ameaças, vulnerabilidades e seus potenciais impactos sobre a organização. Esta etapa deverá contar com a participação das principais áreas de negócio e ser documentada de forma estruturada.

II. **avaliação de riscos:** os riscos identificados serão avaliados através de dois métodos:

   a) **análise qualitativa:** avaliação subjetiva do impacto e probabilidade do risco com base em escalas predefinidas, como “alto”, “médio” e “baixo”. Esta análise será usada para priorizar riscos que exigem ações imediatas.

   b) **análise quantitativa:** utilização de métricas financeiras e operacionais para calcular o impacto financeiro dos riscos e a probabilidade de ocorrência em termos numéricos. Este método será utilizado quando for necessário justificar investimentos em medidas de mitigação.

III. **tratamento de riscos:** para cada risco identificado, será definido um plano de tratamento que pode envolver as seguintes estratégias:

a) **mitigação:** implementação de controles ou medidas que reduzam a probabilidade ou o impacto do risco.

b) **aceitação:** aceitação do risco sem ações adicionais, quando o impacto é considerado baixo ou os custos de mitigação superam os benefícios.

c) **transferência:** transferência do risco para terceiros, como seguradoras ou prestadores de serviços externos.

d) **eliminação:** remoção da causa do risco, quando possível, eliminando assim a ameaça.

Parágrafo único. Cada ação de tratamento de risco deverá ser documentada, indicando o responsável, prazo para implementação e os recursos necessários.

IV. **monitoramento e revisão:** os riscos serão monitorados continuamente para garantir que as medidas de controle implementadas sejam eficazes. Será realizada uma revisão periódica dos riscos e dos controles associados, com uma frequência mínima anual ou sempre que houver mudanças significativas no ambiente de negócio, tecnológico ou legal.

Art. 49 Um plano de ação será elaborado para cada risco identificado, detalhando as etapas necessárias para mitigar ou tratar o risco, incluindo:

I. definição de prazos e responsáveis pela implementação das ações de mitigação;

II. monitoramento contínuo das ações até sua conclusão;

III. revisão e atualização do plano de ação conforme necessário;

IV. a alta administração será responsável pela supervisão geral do processo de gestão de riscos, assegurando que os recursos necessários estejam disponíveis e que as ações sejam executadas conforme o planejado.

Art. 50 A gestão de riscos de segurança da informação seguirá um ciclo contínuo composto pelas seguintes fases:

I. **identificação**: coleta regular de informações sobre novos riscos ou mudanças nos riscos existentes.

II. **avaliação**: revisão periódica da probabilidade e impacto dos riscos.

III. **tratamento**: implementação de medidas corretivas e preventivas para os riscos identificados.

IV. **monitoramento**: acompanhamento contínuo da eficácia das medidas adotadas e dos níveis de exposição ao risco.

V. **revisão**: avaliação formal do processo de gestão de riscos, com relatórios anuais para a alta administração.

Art. 51 Relatórios sobre a gestão de riscos serão gerados anualmente e comunicados à alta administração e às partes interessadas, incluindo:

I. sumário dos riscos identificados, avaliados e tratados;

II. medidas de mitigação implementadas e seus resultados;

III. recomendações para melhorias contínuas nos processos de segurança da informação;

IV. esses relatórios servirão como base para decisões estratégicas relacionadas à segurança da informação e para auditorias internas e externas.

Art. 52 A gestão de riscos de segurança da informação será continuamente aprimorada, incorporando as melhores práticas do mercado, mudanças na legislação e regulamentações aplicáveis. As lições aprendidas de incidentes de segurança e auditorias também serão utilizadas para ajustar e melhorar o processo de gestão de riscos.

SEÇÃO II
DA GESTÃO DE MUDANÇA

Art. 53 Esta seção tem como objetivo estabelecer diretrizes e processos para a gestão de riscos relacionados às mudanças nos sistemas de Tecnologia da Informação (TI), garantindo que qualquer alteração seja cuidadosamente planejada, executada e monitorada para assegurar a proteção dos ativos de informação, conforme as melhores práticas de segurança e conformidade com as normas e regulamentações aplicáveis.

Art. 54 A gestão de mudanças em sistemas de TI seguirá as diretrizes abaixo:

I. planejamento e avaliação de impacto: toda mudança em sistemas, processos ou serviços de TI deve ser formalmente planejada e aprovada antes de sua implementação. A avaliação de riscos e o impacto potencial nas operações e na segurança da informação devem ser considerados como parte essencial do planejamento.

II. documentação e controle de mudanças: cada mudança deve ser documentada de forma detalhada, incluindo o escopo, objetivos, justificativas, riscos identificados, recursos necessários, plano de contingência e resultados esperados.

III. execução segura: a execução das mudanças será feita de acordo com os procedimentos estabelecidos, com foco em minimizar os riscos à segurança da informação e garantir que as atividades sejam realizadas com a menor interrupção possível aos serviços críticos.

IV. monitoramento pós-Implementação: após a implementação, a mudança será monitorada continuamente para identificar eventuais falhas ou vulnerabilidades, assegurando que a segurança dos sistemas de informação não tenha sido comprometida.

V. reversão de mudanças (Rollback): para cada mudança, um plano de rollback (reversão) deve ser criado, detalhando os procedimentos necessários para restaurar o ambiente à condição anterior, caso a alteração cause impactos indesejados ou falhas significativas.

Art. 55 A gestão de mudanças nos sistemas de TI será realizada de forma estruturada e organizada em etapas, conforme descrito a seguir:

I. **solicitação e registro de mudança:** toda mudança deverá ser solicitada por meio de um processo formal, que incluirá a identificação do solicitante, a descrição detalhada da alteração, o motivo da mudança e a justificativa de negócio. A mudança deve ser registrada em um sistema de controle de mudanças que permita o acompanhamento e a rastreabilidade de todas as etapas do processo.

II. **avaliação e classificação da mudança:** cada mudança deverá ser avaliada em termos de seu impacto potencial e riscos associados. A classificação das mudanças poderá ser feita com base em categorias, tais como:

   a) **mudança de baixo impacto**: pequenas alterações com impacto mínimo, como atualizações de software que não afetam a operação crítica.

   b) **mudança de médio impacto**: alterações que podem afetar processos ou sistemas essenciais, mas sem comprometer a segurança ou a continuidade dos negócios.

   c) **mudança de alto impacto**: alterações críticas com potencial para interromper serviços essenciais ou expor vulnerabilidades significativas à segurança da informação.

III. **análise de riscos:** cada mudança proposta deverá passar por uma análise formal de riscos. A análise de riscos incluirá:

   a) identificação de ameaças e vulnerabilidades associadas à mudança.

   b) avaliação qualitativa e quantitativa do impacto e da probabilidade de materialização dos riscos.

   c) identificação de controles e medidas preventivas para mitigar os riscos identificados.

IV. **aprovação da mudança:** a mudança só poderá ser implementada após a devida aprovação pelas partes responsáveis, incluindo gestores de segurança da informação e da área de TI. Mudanças de alto impacto ou risco elevado deverão ser escaladas para aprovação pela alta administração ou comitês de segurança, conforme aplicável.

V. **planejamento da mudança:** após a aprovação, um plano detalhado de implementação será desenvolvido. Esse plano incluirá:

   a) cronograma de atividades;

   b) recursos necessários;

   c) plano de comunicação para informar as partes interessadas;

   d) plano de contingência para possíveis falhas durante a implementação;

   e) plano de rollback (reversão) em caso de falhas graves ou impactos indesejados.

VI. **implementação da mudança:** a implementação da mudança será conduzida conforme o plano aprovado, e a equipe de TI responsável deve seguir os procedimentos estabelecidos, garantindo que todos os controles de segurança sejam observados. Durante a implementação, medidas como o monitoramento em tempo real, auditorias de log e verificações de segurança serão aplicadas para minimizar os riscos.

VII. **monitoramento e validação pós-implementação:** após a mudança, será conduzida uma fase de monitoramento para validar que:

a) a mudança foi implementada com sucesso.

b) não há falhas ou vulnerabilidades decorrentes da mudança.

c) a segurança dos sistemas e a continuidade das operações foram mantidas.

d) auditorias ou revisões independentes poderão ser realizadas para garantir que a mudança atendeu aos requisitos de segurança.

VIII. **encerramento da mudança e relatório final:** ao final da implementação e validação da mudança, um relatório final será gerado, documentando:

a) a execução da mudança;

b) quaisquer desvios ou incidentes ocorridos;

c) resultados do monitoramento pós-implementação;

d) lições aprendidas;

e) este relatório será arquivado para referência futura e para auditorias.

Art. 56 As mudanças implementadas serão submetidas a um ciclo contínuo de monitoramento, revisões e melhorias, incluindo:

I. revisão periódica das mudanças aplicadas, com foco em identificar e corrigir falhas ou vulnerabilidades potenciais.

II. realização de auditorias de conformidade para verificar se as mudanças seguiram os processos estabelecidos e não comprometeram a segurança da informação.

III. atualização dos planos de segurança e mitigação de riscos com base nas lições aprendidas durante a implementação de mudanças.

Art. 57 As responsabilidades pela gestão de mudanças nos sistemas de TI serão distribuídas conforme segue:

I. gestor de TI: responsável por coordenar a implementação técnica da mudança e garantir a aplicação dos controles de segurança.

II. gestor de segurança da informação: responsável por revisar e aprovar as mudanças, assegurando que todas as implicações de segurança tenham sido consideradas.

III. comitê de segurança da informação: responsável pela aprovação de mudanças de alto impacto ou risco elevado e por garantir a conformidade com as políticas institucionais de segurança.

IV. equipe de auditoria interna: responsável por conduzir auditorias periódicas para garantir que o processo de gestão de mudanças esteja sendo seguido adequadamente e em conformidade com as normas.

Art. 58 A gestão de mudanças será continuamente revisada e aprimorada com base nas melhores práticas de mercado, mudanças nas regulamentações aplicáveis e resultados de auditorias internas e externas. Novas ferramentas e métodos de segurança serão incorporados ao processo de gestão de mudanças, garantindo a melhoria contínua da proteção dos sistemas e dados da organização.

SEÇÃO III
DAS AUDITORIAS INTERNAS E CONFORMIDADE

Art. 59 Esta seção tem como objetivo estabelecer diretrizes para a realização de auditorias internas periódicas que garantam a conformidade com as leis e normativas externas, como a ISO/IEC 27001. A auditoria interna serve para avaliar a efetividade contínua do Sistema de Gestão de Segurança da Informação (SGSI), identificar não conformidades e promover a melhoria contínua dos controles de segurança.

Art. 60 A auditoria interna é um componente essencial do SGSI, visando garantir:

I. **conformidade**: avaliar se os controles de segurança da informação estão sendo implementados de acordo com as políticas, normas e procedimentos estabelecidos pela Posin, além de verificar a conformidade com normativas externas, como a ISO/IEC 27001 e a Lei Geral de Proteção de Dados (LGPD) de n° 13.709/2018.

II. **efetividade**: garantir que o SGSI continue efetivo em proteger os ativos de informação e minimizar os riscos de segurança.

III. **identificação de não conformidades**: detectar falhas ou desvios nos processos de segurança da informação para corrigir as vulnerabilidades identificadas.

IV. **melhoria contínua**: proporcionar recomendações para o aprimoramento contínuo dos controles de segurança da informação.

Art. 61 O Inep deverá elaborar um cronograma de auditorias internas que devrá garantir a verificação periódica e sistemática da conformidade com as políticas de segurança da informação, conforme os seguintes critérios:

I. **periodicidade das auditorias**:

a) auditorias internas regulares serão realizadas, no mínimo, anualmente, para cobrir todos os processos críticos de segurança da informação.

b) auditorias adicionais poderão ser realizadas sempre que ocorrerem mudanças significativas no ambiente de TI, incidentes de segurança ou alterações em regulamentações.

II. **abrangência das auditorias**:

a) as auditorias cobrirão todos os aspectos do SGSI, incluindo a conformidade com a Posin, a ISO/IEC 27001 e quaisquer outras normativas relevantes.

b) a revisão incluirá a eficácia dos controles implementados, a gestão de riscos, a resposta a incidentes de segurança e a gestão de mudanças nos sistemas de TI.

III. **execução das auditorias**:

a) as auditorias serão conduzidas por uma equipe de auditoria interna qualificada, ou por auditores externos quando necessário, para garantir objetividade e imparcialidade.

b) serão utilizadas metodologias baseadas nas normas ISO/IEC 27001 e nas melhores práticas de auditoria de segurança da informação.

IV. **relatório de auditoria**: ao final de cada auditoria, será gerado um relatório detalhado que incluirá:

a) resumo dos resultados.

b) conformidade com as políticas e normas ISO.

c) não conformidades detectadas e a criticidade de cada uma.

d) recomendações para correções e melhorias.

e) prazos para a implementação das ações corretivas.

Art. 62 As não conformidades identificadas durante as auditorias internas serão tratadas de acordo com o seguinte processo:

I. **identificação e registro**: todas as não conformidades serão registradas e classificadas com base em sua gravidade e impacto potencial para a segurança da informação.

II. **plano de ação corretiva**: um plano de ação será desenvolvido para cada não conformidade, detalhando as etapas necessárias para sua correção, os responsáveis e os prazos para implementação.

III. **monitoramento de ações corretivas**: a implementação das ações corretivas será monitorada pela equipe de auditoria e pelo gestor de segurança da informação para garantir que as medidas sejam executadas de forma eficaz e dentro do prazo estabelecido.

IV. **auditoria de acompanhamento**: uma auditoria de acompanhamento será realizada para verificar se as ações corretivas foram adequadamente implementadas e se as não conformidades foram resolvidas.

Art. 63 Os resultados das auditorias internas serão comunicados regularmente à alta administração e às partes interessadas. O processo de comunicação incluirá:

I. **relatório de auditoria**: um relatório formal será gerado após cada auditoria, detalhando os achados, as não conformidades e as ações corretivas propostas. Esse relatório será compartilhado com a alta administração e as partes responsáveis.

II. **sumário de conformidade**: um sumário geral sobre a conformidade do SGSI com a Posin e normas ISO/IEC 27001 será elaborado periodicamente, refletindo o status geral da segurança da informação.

III. **reuniões de revisão da alta administração**: resultados críticos das auditorias serão discutidos em reuniões de revisão com a alta administração, com foco em tomar decisões estratégicas para melhorar a segurança da informação.

Art. 64 Além das auditorias regulares, será implementado um sistema de monitoramento contínuo para garantir a eficácia dos controles de segurança da informação e para identificar problemas em tempo real. Esse processo incluirá:

I. **monitoramento contínuo**: ferramentas de monitoramento serão utilizadas para acompanhar a performance dos controles de segurança da informação, analisando métricas como tentativas de invasão, falhas de sistema, incidentes de segurança e conformidade com as políticas internas.

II. **revisões periódicas do SGSI**: revisões formais do SGSI serão conduzidas com base nos resultados das auditorias e das atividades de monitoramento contínuo, garantindo que o SGSI permaneça alinhado às normas ISO/IEC 27001 e às melhores práticas de segurança.

Art. 65 O ciclo de auditoria interna será utilizado como base para a melhoria contínua do SGSI. As oportunidades de melhoria identificadas nas auditorias e revisões serão incorporadas nas políticas e procedimentos de segurança da informação para:

I. **aprimoramento dos controles de segurança**: ajustes nos controles existentes ou a implementação de novos controles para responder a riscos emergentes ou vulnerabilidades identificadas.

II. **atualização da Posin**: a Posin será revisada e atualizada conforme necessário para incorporar as lições aprendidas e novas regulamentações ou normas de segurança da informação.

Art. 66 As responsabilidades para a execução das auditorias internas e para a conformidade com as políticas de segurança da informação são divididas da seguinte forma:

I. **gestor de segurança da informação (GSI)**: responsável por coordenar o processo de auditoria interna e por garantir que as políticas de segurança estejam sendo seguidas.

II. **equipe de auditoria interna**: responsável pela condução das auditorias internas, pela análise dos resultados e pela recomendação de ações corretivas.

III. **alta administração**: responsável por fornecer os recursos e o apoio necessários para a implementação das recomendações das auditorias e por supervisionar a execução das ações corretivas.

IV. **comitê de segurança da informação e comunicação (CSIC)**: responsável por revisar os relatórios de auditoria e por garantir a conformidade com as políticas e normas externas.

Art. 67 A conformidade com as políticas de segurança da informação será continuamente reforçada por meio do processo de auditoria interna. As auditorias internas também proporcionarão insights valiosos para a melhoria contínua do SGSI, garantindo que a organização esteja em conformidade com as melhores práticas de mercado e com as regulamentações, como a ISO/IEC 27001.

SEÇÃO IV
DO TRATAMENTO DE NÃO CONFORMIDADES

Art. 68 O objetivo desta seção é estabelecer diretrizes e procedimentos para a identificação, registro, análise, tratamento e monitoramento de não conformidades relacionadas à segurança da informação, garantindo a aplicação de ações corretivas e preventivas que minimizem riscos e assegurem a conformidade com as normas internas e regulamentações externas, como a ISO/IEC 27001 e a Lei Geral de Proteção de Dados (LGPD) de n° 13.709/2018.

Art. 69 Para fins desta política, uma não conformidade refere-se a qualquer falha ou desvio em relação às políticas, procedimentos e controles de segurança da informação estabelecidos, bem como ao não atendimento de requisitos regulamentares, normativos ou de padrões externos, como a ISO/IEC 27001 e a Lei Geral de Proteção de Dados (LGPD) de n° 13.709/2018.

Art. 70 Identificação e Registro de Não Conformidades

I. **identificação**:

   a) as não conformidades podem ser identificadas por meio de auditorias internas e externas, incidentes de segurança, monitoramento contínuo dos sistemas, ou relatórios de colaboradores e terceiros.

   b) todos os funcionários e prestadores de serviço têm a responsabilidade de relatar qualquer não conformidade detectada ao Gestor de Segurança da Informação (GSI) ou ao responsável pela área de conformidade.

II. **registro**: todas as não conformidades identificadas devem ser formalmente registradas em um sistema de gestão de conformidade. O registro deve incluir:

   a) descrição detalhada da não conformidade;

   b) data e hora de identificação;

   c) área ou sistema afetado;

   d) gravidade do impacto;

   e) pessoa ou equipe responsável por monitorar e resolver a não conformidade.

Art. 71 As não conformidades serão classificadas de acordo com sua criticidade, para determinar a urgência de sua correção e o impacto que causam à segurança da informação e aos negócios da organização:

I. **não conformidade crítica**: quando a falha representa um risco elevado para a confidencialidade, integridade ou disponibilidade das informações, com impacto direto nas operações críticas ou em conformidade com regulamentações legais. Requer ação imediata.

II. **não conformidade moderada**: quando a falha tem um impacto significativo, mas não ameaça diretamente as operações críticas ou não leva a uma violação legal iminente. Requer ação corretiva em prazo determinado.

III. **não conformidade menor**: quando a falha tem impacto limitado ou afeta áreas que não são críticas para as operações. Requer ação corretiva, mas com menor prioridade.

Art. 72 Análise de Causa Raiz

I. **investigação**: para cada não conformidade identificada, será realizada uma investigação detalhada para identificar a causa raiz. Esse processo deve incluir:

   a) análise de incidentes anteriores.

   b) revisão de processos e procedimentos afetados.

   c) entrevistas com os responsáveis pela área afetada.

II. **identificação de riscos associados**: durante a análise da não conformidade, todos os riscos associados serão identificados e registrados. Estes riscos serão avaliados para determinar seu potencial impacto e a necessidade de ações corretivas adicionais.

Art. 73 Ação Corretiva e Preventiva

I. **plano de ação corretiva**: um plano de ação corretiva será elaborado para resolver a não conformidade. Este plano deve incluir:

   a) descrição das medidas corretivas a serem implementadas.

   b) definição de responsáveis pela implementação.

   c) prazos claros para a conclusão das ações corretivas.

   d) indicadores de sucesso para monitorar a eficácia das ações.

II. **ação preventiva**: além da correção da falha, serão identificadas ações preventivas para evitar a recorrência da não conformidade. Isso pode incluir:

   a) revisão de processos e políticas.

   b) capacitação de pessoal.

   c) reforço de controles técnicos e administrativos.

III. **aprovação do plano**: o plano de ação corretiva e preventiva deverá ser aprovado pelo Gestor de Segurança da Informação (GSI) e, em caso de não conformidades críticas, pela alta administração.

Art. 74 Implementação e Monitoramento

I. **execução das ações corretivas**: as ações corretivas e preventivas serão implementadas dentro dos prazos estipulados, conforme o plano aprovado.

II. **monitoramento**: o progresso das ações corretivas será monitorado pela equipe de segurança da informação ou auditoria interna, para garantir que a implementação esteja dentro do cronograma. Qualquer atraso ou dificuldade na execução será comunicado à alta administração.

Art. 75 Verificação da Eficácia

I. **verificação pós-implementação**: após a implementação das ações corretivas, será realizada uma verificação para assegurar que a não conformidade foi totalmente resolvida e que as medidas implementadas foram eficazes.

II. **auditorias de acompanhamento**: auditorias de acompanhamento poderão ser realizadas para garantir que a não conformidade não ocorra novamente. Estas auditorias podem incluir revisões de processos e entrevistas com as equipes responsáveis.

Art. 76 Uma não conformidade só poderá ser considerada encerrada quando:

I. as ações corretivas e preventivas forem completamente implementadas.

II. a eficácia das medidas for verificada por auditorias internas ou pela equipe de conformidade.

III. o risco associado à não conformidade tenha sido adequadamente mitigado.

Art. 77 Relatórios de Não Conformidade

I. **relatórios periódicos**: relatórios periódicos serão elaborados para documentar todas as não conformidades identificadas, as ações corretivas tomadas e os resultados das verificações de eficácia.

II. **comunicação à alta administração**: não conformidades críticas e suas respectivas ações corretivas devem ser comunicadas à alta administração, incluindo prazos de resolução e qualquer necessidade de recursos adicionais.

Art. 78 As responsabilidades no tratamento de não conformidades são divididas da seguinte forma:

I. **gestor de segurança da informação (GSI)**: responsável pela coordenação geral do processo de tratamento de não conformidades, pela análise de causa raiz e pela aprovação das ações corretivas e preventivas.

II. **alta administração**: responsável pela aprovação de planos de ação para não conformidades críticas e por garantir os recursos necessários para a implementação das medidas corretivas.

III. **equipe de auditoria interna ou segurança da informação**: responsável por conduzir as auditorias de acompanhamento e monitorar a eficácia das ações corretivas.

IV. **usuários e colaboradores**: responsáveis por reportar não conformidades e colaborar na implementação das ações corretivas e preventivas.

Art. 79 O processo de tratamento de não conformidades será continuamente aprimorado com base nas lições aprendidas. As ações corretivas e preventivas implementadas serão revisadas periodicamente para garantir que continuam adequadas e eficazes, e para adaptar os controles de segurança às novas ameaças e desafios.

SEÇÃO V
DO PLANEJAMENTO DE CONTINUIDADE DE NEGÓCIO

Art. 80 Esta seção tem como objetivo definir diretrizes e procedimentos para a implementação e manutenção de um Plano de Continuidade de Negócios (PCN), garantindo a continuidade das operações críticas da organização em situações de incidentes de segurança, desastres ou interrupções inesperadas, minimizando impactos e assegurando a recuperação eficiente dos serviços essenciais.

Art. 81 A Continuidade de Negócios é a capacidade da organização de continuar a operar de forma eficaz ou de restabelecer rapidamente suas operações críticas após uma interrupção causada por incidentes de segurança, falhas tecnológicas, desastres naturais ou outros eventos imprevistos.

Art. 82 Desenvolvimento do Plano de Continuidade de Negócios (PCN)

I. **identificação de processos críticos**: o PCN deve começar com a identificação de todos os processos, sistemas e ativos críticos para as operações da organização. Esses processos serão priorizados para garantir que a recuperação ocorra de forma eficaz e dentro dos prazos estabelecidos.

II. **análise de impacto nos negócios (BIA - Business Impact Analysis)**: será realizada uma Análise de Impacto nos Negócios para avaliar os efeitos potenciais de uma interrupção prolongada nos serviços críticos. A BIA deve identificar:

   a) o impacto financeiro e operacional de uma interrupção.

   b) o tempo máximo tolerável de inatividade (RTO - Recovery Time Objective).

   c) o ponto de recuperação de dados (RPO - Recovery Point Objective), definindo a quantidade máxima de dados que pode ser perdida.

III. **definição de estratégias de recuperação**: estratégias de recuperação devem ser desenvolvidas para garantir a restauração dos processos críticos. Isso pode incluir:

   a) uso de backups e redundâncias.

   b) deslocamento de operações para locais alternativos.

   c) adoção de contratos de suporte com fornecedores terceirizados para acelerar a recuperação.

   d) plano de recuperação de desastres (DRP) para sistemas de TI.

IV. **plano de contingência**: um plano de contingência será desenvolvido para garantir que as operações essenciais possam continuar, mesmo que temporariamente, até que os serviços completos sejam restaurados. Esse plano incluirá:

   a) procedimentos operacionais temporários.

   b) pessoal, chave responsável pela execução de operações críticas.

   c) recursos alternativos que possam ser utilizados em emergências.

Art. 83 Estrutura do Plano de Continuidade de Negócios (PCN)
O PCN deve conter as seguintes seções:

I. **introdução e escopo**: descrever a importância da continuidade de negócios para a organização e o escopo do plano.

II. **análise de impacto nos negócios (BIA)**: detalhar os resultados da BIA, identificando processos críticos, tempos de recuperação e tolerância a perda de dados.

III. **responsabilidades**: definir as funções e responsabilidades de cada colaborador envolvido na execução e manutenção do PCN. Isso inclui a equipe de gerenciamento de crises, pessoal de TI e comunicação.

IV. **estratégias de recuperação**: descrever as estratégias para manter ou restaurar os serviços críticos após uma interrupção.

V. **planos de contingência e alternativas operacionais**: procedimentos temporários que devem ser implementados até que as operações normais sejam restabelecidas.

VI. **comunicação em crises**: definir como a comunicação interna e externa será realizada durante uma crise. Incluir listas de contatos de emergência, métodos de comunicação alternativos e procedimentos para informar clientes, fornecedores e partes interessadas.

VII. **planos de recuperação de TI**: detalhar os procedimentos de recuperação de desastres para os sistemas de TI, incluindo restauração de dados e reinicialização de sistemas críticos.

Art. 84 Testes e Exercícios de Continuidade de Negócios

I. **testes regulares**: o PCN será testado regularmente para garantir sua eficácia e a prontidão da equipe envolvida. Esses testes devem incluir:

   a) simulações de incidentes.

   b) testes de recuperação de sistemas de TI (backups e restaurações).

   c) exercícios de mesa (tabletop) para avaliação da resposta da equipe a diferentes cenários de crise.

II. **tipos de testes**:

   a) **simulações completas**: exercícios que envolvem a execução total ou parcial do PCN para simular um cenário real de crise.

   b) **testes de backup e restauração**: verificações periódicas para assegurar que os dados críticos podem ser restaurados dentro dos parâmetros de RPO e RTO estabelecidos.

   c) **exercícios de mesa (Tabletop)**: encontros em que a equipe responsável revisa cenários de crise e decide como responder sem executar fisicamente as etapas.

III. **avaliação dos testes**: após cada teste, um relatório será elaborado descrevendo os resultados, identificando falhas e propondo melhorias. Todos os testes serão documentados para auditorias e revisões periódicas.

Art. 85 Manutenção e Atualização do PCN

I. **revisões regulares:** o PCN será revisado e atualizado pelo menos anualmente, ou sempre que houver mudanças significativas nos processos de negócio, infraestrutura de TI, ou riscos identificados.

II. **mudanças organizacionais e tecnológicas**: sempre que ocorrerem mudanças significativas, como a adoção de novas tecnologias, alterações nos processos de negócios ou mudanças na estrutura organizacional, o PCN deverá ser atualizado para refletir as novas condições e requisitos de continuidade.

III. **lições aprendidas**: a cada teste ou incidente real, as lições aprendidas devem ser integradas ao PCN para fortalecer as estratégias de recuperação e mitigação de riscos.

Art. 86 Relatórios periódicos sobre o status da continuidade de negócios serão apresentados à alta administração e ao Comitê de Segurança da Informação, incluindo:

I. **resultados de testes e exercícios**: detalhar os resultados dos testes de continuidade e qualquer falha identificada no PCN, com recomendações de melhorias.

II. **relatórios de incidentes**: se um incidente real ocorrer, um relatório detalhado será apresentado, incluindo o impacto, as ações tomadas e as lições aprendidas.

III. **aprovação e atualização do PCN**: a alta administração será responsável por aprovar as atualizações do PCN, assegurando que ele se mantenha alinhado com os objetivos estratégicos da organização e com os requisitos legais e normativos.

Art. 87 As responsabilidades pela implementação e manutenção do PCN serão distribuídas da seguinte forma:

I. **gestor de segurança da informação (GSI)**: responsável pela coordenação do desenvolvimento, manutenção e testes do PCN, bem como pela comunicação com a alta administração.

II. **equipe de continuidade de negócios**: responsável pela execução das ações de continuidade em caso de incidentes, incluindo a coordenação das atividades operacionais e tecnológicas necessárias para restabelecer os serviços críticos.

III. **alta administração**: responsável por fornecer os recursos necessários para a implementação e manutenção do PCN, e por tomar decisões estratégicas durante incidentes de continuidade.

Art. 88 Conformidade e Auditorias

I. **auditorias regulares**: o PCN será auditado regularmente para garantir sua conformidade com as normativas aplicáveis, como a ISO/IEC 27001, e para assegurar que os controles de continuidade estão adequadamente implementados e funcionando conforme o planejado.

II. **conformidade com normas e regulamentações**: o PCN será desenvolvido em conformidade com os padrões internacionais de gestão de continuidade de negócios, como a ISO 22301, e estará alinhado com os requisitos legais e regulamentares aplicáveis à organização.

SEÇÃO VI
DA DOCUMENTAÇÃO E CONTROLE DE REGISTRO

Art. 89 Esta seção tem como objetivo definir as diretrizes e procedimentos para a criação, gerenciamento, controle e retenção de documentos e registros relacionados à segurança da informação. Isso visa assegurar que as informações críticas sejam documentadas, atualizadas, protegidas e disponibilizadas apenas para pessoas autorizadas, em conformidade com regulamentações legais, normativas internas e padrões internacionais como a ISO/IEC 27001.

Art. 90 Definições:

I. **documentação:** refere-se a todas as políticas, procedimentos, normas, diretrizes e manuais relacionados à segurança da informação que orientam e formalizam os processos internos da organização.

II. **registro:** um registro é uma evidência documentada de atividades ou operações realizadas, como auditorias, incidentes de segurança, testes de continuidade, análises de risco, e outras atividades relacionadas à segurança da informação.

Art. 91 O gerenciamento eficaz de documentos e registros de segurança da informação será baseado nos seguintes princípios:

I. integridade: os documentos e registros devem ser protegidos contra alterações não autorizadas, garantindo que reflitam as informações corretas e completas.

II. confidencialidade: o acesso aos documentos e registros de segurança da informação deve ser restrito apenas às pessoas autorizadas, em conformidade com o princípio de mínimo privilégio.

III. disponibilidade: os documentos e registros devem estar disponíveis para as partes autorizadas sempre que necessário, garantindo sua pronta recuperação.

IV. autenticidade: todos os registros devem ser identificáveis e rastreáveis até a pessoa ou sistema que os gerou.

V. conformidade legal: a retenção e eliminação de registros devem seguir as regulamentações e legislações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) de n° 13.709/2018.

Art. 92 Os documentos e registros relacionados à segurança da informação podem incluir, mas não estão limitados a:

I. **políticas e procedimentos**:

   a) política de segurança da informação (Posin);

   b) procedimentos de resposta a incidentes de segurança;

   c) políticas de controle de acesso, criptografia, e gestão de riscos.

II. **relatórios e auditorias**:

   a) relatórios de auditoria interna e externa;

b) relatórios de conformidade com normas ISO/IEC 27001;

c) relatórios de análise de risco.

III. **registros operacionais**:

a) logs de acesso e auditoria;

b) registros de incidentes de segurança;

c) testes de backup e recuperação de dados;

d) testes de continuidade de negócios.

IV. **documentação legal e contratual**:

a) contratos e acordos de nível de serviço (SLAs) com terceiros;

b) termos de responsabilidade e confidencialidade de colaboradores e fornecedores;

c) registros de conformidade legal (LGPD, Marco Civil da Internet).

Art. 93 Controle de Documentos

I. **criação e aprovação**: todos os documentos de segurança da informação devem ser elaborados de acordo com as necessidades organizacionais e estar em conformidade com as normas aplicáveis. Cada documento deve ser aprovado por uma autoridade competente antes de ser implementado.

II. **identificação e rastreabilidade**: cada documento deve conter uma identificação única, incluindo informações como título, data de criação, versão e autor. Isso garante a rastreabilidade e o controle de revisões.

III. **revisão e atualização**: documentos de segurança da informação devem ser revisados periodicamente, ou sempre que houver mudanças significativas nos processos de negócios, infraestrutura ou legislação. O cronograma de revisão será determinado pela criticidade do documento e pelos riscos associados.

IV. **controle de acesso**: o acesso aos documentos deve ser controlado, garantindo que apenas pessoas autorizadas possam visualizar, editar ou aprovar documentos críticos de segurança da informação. Devem ser mantidos registros de quem acessou e alterou os documentos.

V. **armazenamento seguro**: todos os documentos devem ser armazenados em locais seguros, que garantam a proteção contra acessos não autorizados, perda ou destruição acidental. O armazenamento pode ser em meio físico ou digital, desde que siga os requisitos de segurança.

Art. 94 Controle de Registros

I. **geração de registros**: todos os registros gerados a partir das atividades de segurança da informação, como auditorias, incidentes de segurança e testes de continuidade, devem ser documentados e mantidos conforme os requisitos estabelecidos.

II. **retenção e descarte de registros**: os registros de segurança da informação devem ser mantidos por períodos que atendam às exigências legais e operacionais. O período de retenção será

definido com base em normas internas e regulamentações externas, como a LGPD. Após o período de retenção, os registros devem ser descartados de maneira segura, garantindo que nenhuma informação sensível seja recuperável.

III. **auditoria de registros**: os registros de segurança da informação devem ser regularmente auditados para garantir sua precisão e conformidade. A auditoria pode incluir verificações de integridade, rastreabilidade e conformidade com as políticas internas.

IV. **proteção dos registros**: registros devem ser protegidos contra perda, destruição não autorizada ou alteração. Para registros digitais, devem ser implementados controles como criptografia, backups regulares e auditorias de integridade.

V. **acesso a registros**: o acesso aos registros será concedido de acordo com a política de controle de acesso da organização. Devem ser aplicados os princípios de mínimo privilégio e necessidade de conhecimento para garantir que somente pessoas autorizadas possam acessar ou modificar os registros.

Art. 95 Responsabilidades

I. **gestor de segurança da informação (GSI)**: responsável por supervisionar o controle de documentos e registros relacionados à segurança da informação, garantindo que estejam atualizados e sejam devidamente gerenciados.

II. **equipe de conformidade ou auditoria interna**: responsável por realizar auditorias periódicas para verificar a conformidade com a política de controle de documentos e registros, assegurando que os mesmos estejam sendo mantidos e descartados de maneira adequada.

III. **usuários e colaboradores**: responsáveis por garantir que os registros gerados por suas atividades estejam em conformidade com as diretrizes estabelecidas, e por reportar quaisquer inconsistências ou problemas no gerenciamento dos documentos.

Art. 96 O processo de controle de documentos e registros será revisado periodicamente para garantir que continue atendendo às necessidades da organização e em conformidade com as melhores práticas de segurança da informação. Qualquer melhoria identificada durante auditorias ou revisões será implementada de maneira a reforçar a integridade e a segurança do processo de documentação.

Art. 97 A Posin estabelece as diretrizes para a segurança da informação no âmbito do Inep, garantindo a conformidade com a legislação brasileira e as melhores práticas internacionais. Essa política abrange, entre outros, os seguintes referenciais:

I. **o Decreto nº 9.637, de 26 de dezembro de 2018**, que institui a Política Nacional de Segurança da Informação (PNSI);

II. **o Decreto nº 7.724 de 16 de maio de 2012**, que regulamenta a Lei nº 12.527/2011 conhecida como Lei de Acesso à Informação (LAI);

III. **a Lei nº 12.527, de 18 de novembro de 2011**, conhecida como Lei de Acesso à Informação (LAI);

IV. **a Lei nº 13.709, de 14 de agosto de 2018**, Lei Geral de Proteção de Dados Pessoais (LGPD);

V. **a Portaria SGD/MGI nº 852, de 28 de março de 2023**, que dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI); e

VI. alinhamento do processo de controle de documentos e registros às normas internacionais, como a **ISO/IEC 27001**, para assegurar a conformidade com as melhores práticas globais em segurança da informação.

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

- Decreto nº 10.748, de 16 de julho de 2021 - Institui a Rede Federal de Gestão de Incidentes Cibernéticos;
- Decreto nº 10.641, de 2 de março de 2021 Altera o 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 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;
- Decreto nº 10.569, de 9 de dezembro de 2020 - Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas;
- Decreto nº 10.222, de 5 de fevereiro de 2020 - Aprova a Estratégia Nacional de Segurança Cibernética;
- Decreto nº 9.832, de 12 de junho de 2019 Altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação;
- 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. Alterado pelo Decreto nº 9.832, de 12 de junho de 2019. Alterado pelo Decreto nº 10.641, de 2 de março de 2021;
- Decreto nº 9.573, de 22 de novembro de 2018 - Aprova a Política Nacional de Segurança de Infraestruturas Críticas;
- 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;
- Decreto nº 1.171, de 22 de junho de 1994 - Dispõe sobre o Código de Ética do Servidor Público Civil do Poder Executivo Federal;
- Instrução Normativa 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;

- Instrução Normativa GSI 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.
- Instrução Normativa GSI 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.
- Portaria GSI nº 93, de 18 de outubro de 2021 Aprova o Glossário de Segurança da Informação;
- Portaria GSI nº 40, de 8 de outubro de 2014 Homologa a Norma Complementar nº 21/IN01/DSIC/GSIPR - Estabelece 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;
- Portaria GSI nº 57, de 23 de agosto de 2010 Homologa a Norma Complementar nº 08/IN01/DSIC/GSIPR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais - Gestão de ETIR, nos órgãos e entidades da Administração Pública Federal. Portaria GSI nº 38, de 14 de agosto de 2009 Homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR - Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;
- Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;
- NBR ISO/IEC 27001:2013 Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos. NBR ISO/IEC 27002:2022 Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação;
- NBR ISO/IEC 27003:2020 Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Orientações;
- NBR ISO/IEC 27701:2019 Técnicas de segurança para gestão da privacidade da informação – Requisitos e diretrizes;
- NBR ISO/IEC 27017:2016 Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação. 9.2. Proteção de Dados Pessoais Lei nº 13.709, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais;
- Lei nº 12.965, de 23 de abril de 2014 Marco Civil da Internet - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Medida Provisória nº 1.124, de 13 de junho de 2022 Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão;
- Decreto nº 8.771, de 11 de maio de 2016 - Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações;

- Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;
- Lei nº 12.965, de 23 de abril de 2014 Marco Civil da Internet - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Medida Provisória nº 1.124, de 13 de junho de 2022 Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão;
- Decreto nº 8.771, de 11 de maio de 2016 - Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações; e
- Código Penal Brasileiro (Decreto-Lei n° 2848/1940).

INEP MINISTÉRIO DA EDUCAÇÃO