INFRA S.A.

www.infrasa.gov.br

POSIN

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

infrasaoficial

infra.oficial

infra-oficial

infrasa.oficial

infra.oficial

CIP. Brasil Catalogação-na-Publicação
Superintendência de Tecnologia da Informação - SUPTI

I43p INFRA S.A.

Política de Segurança da Informação: POSIN / INFRA S.A. – Brasília : INFRA S.A, 2024.

15 p.

1. Política de Segurança da Informação - POSIN.
2. Tecnologia da Informação e Comunicação - TIC.
3. Governança.
4. INFRA S.A. I. Título.

CDU: 004.056(083.74)

INFRA S.A
SAUS, Quadra 01, Bloco G
Lotes 3 e 5, Asa Sul
Brasília - DF - 70.070-010

Presidência da República

Luiz Inácio Lula da Silva
Presidente

Ministério dos Transportes

José Renan Vasconcelos Calheiros Filho
Ministro de Estado dos Transportes

INFRA S.A.

Jorge Luiz Macedo Bastos
Diretor-Presidente

Elisabeth Alves da Silva Braga
Diretora de Administração e Finanças

André Luis Ludolfo da Silva
Diretor de Empreendimentos

Cristiano Della Giustina
Diretor de Planejamento

Marcelo Vinaud Prado
Diretora de Mercado e Inovação

Superintendência de Tecnologia da Informação e Comunicação

Renato Ricardo Alves

Gerência de Segurança da Informação e Governança

Luciana Muniz Costa

Elaboração

Luciana Muniz Costa
Fernando Mitev Sánchez
Juliana Guimarães Garcia da Costa

Colaboração

Arlon Salvador Santuche
Célio Eduardo Peixoto Normando
Rafael de Faria Costa
Robério Ximenes de Sabóia

Instância de Aprovação

Diretoria Executiva - DIREX
Conselho de Administração - CONSAD

SUMÁRIO

O **CONSELHO DE ADMINISTRAÇÃO** da **INFRA S. A.**, no uso das atribuições que lhe foram conferidas pelo **art. 44, inciso XII** do Estatuto Social vigente, bem assim o deliberado na sua **4ª Reunião Ordinária** realizada em **25 de abril de 2024**.

Art. 1º Aprovar a Política de Segurança da Informação (POSIN), no âmbito da Infra S.A.

CAPÍTULO I
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 2º A POSIN está posicionada em nível estratégico e tem por finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, além de endossar a segurança e o tratamento adequado dos ativos de informação produzidos ou custodiados pela Infra S.A., assim como a conservação, guarda e a proteção das informações e maior proteção aos dados pessoais, tendo como base as diretrizes e valores adotados pela Empresa, sempre, visando ao interesse da sociedade.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º Para os efeitos desta Política, aplicam-se os termos e definições conceituados na Portaria nº 93/GSI/PR, Glossário de Segurança, de 18 de outubro de 2021 e outras definições adotadas no âmbito do Governo Federal.

CAPÍTULO III
DOS OBJETIVOS

Art. 4º A POSIN tem como objetivos:

I - assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações de propriedade ou custodiadas pela Empresa, bem como a privacidade das informações;

II - garantir o atendimento à legislação vigente e requisitos contratuais;

III - estabelecer sistema de gestão de segurança da informação e de proteção de dados pessoais;

IV - promover a capacitação de seus colaboradores;

V - praticar a melhoria contínua do sistema de gestão da segurança da informação e de proteção de dados pessoais; e

VI - assegurar que dados e informações estejam protegidos, independentemente dos locais de exercício das atividades vinculadas à Infra S.A..

CAPÍTULO IV
DA ABRANGÊNCIA

Art. 5º Estão submetidos a esta POSIN todos os agentes públicos, profissionais, estagiários, parceiros, terceiros e todos que, de alguma forma, exerçam atividades no âmbito da Infra S.A. e ainda qualquer pessoa, física ou jurídica, que venha a ter acesso a qualquer informação desta Empresa ou por ela custodiada.

Parágrafo único. Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela Infra S.A. devem incluir dispositivos de forma a viabilizar ou facilitar a implementação do disposto nesta Política.

CAPÍTULO V
DOS PRINCÍPIOS

Art. 6º Esta Política e sua execução devem guiar-se pelos seguintes princípios:

I - **disponibilidade:** característica de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

II - **integridade:** característica de que a informação não sofreu alterações ou exclusões de maneira não autorizada ou acidental;

III - **confidencialidade:** característica de que a informação não esteja disponível ou divulgada a pessoa física, sistema, órgão ou entidade não autorizada; e

IV - **autenticidade:** manutenção das condições iniciais dos dados de maneira autêntica.

Art. 7º A informação protegida pelo sigilo, tal como o disposto nos incisos X e XII do art. 5º da Carta Magna, no art. 325 do Código Penal, e demais instrumentos normativos aplicáveis, deve receber especial atenção para que apenas as partes devidamente autorizadas tenham os devidos privilégios de acesso, manuseio e descarte.

Art. 8º As atividades de tratamento de dados pessoais devem observar a boa-fé e os seguintes princípios: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização; e prestação de contas.
Parágrafo único. O tratamento de dados pessoais deve obrigatoriamente atender ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e suas alterações, e em políticas e normas correlatas. I - II - III - IV -

CAPÍTULO VI
DAS DIRETRIZES

Art. 9º A POSIN adota a abordagem finalística, baseada em riscos e oportunidades, visando à efetividade da segurança da informação centrada em pessoas, para promover maior autonomia, agilidade e flexibilidade nas ações e decisões de segurança da informação, ao mesmo tempo em que reforça a responsabilização e o monitoramento.

Art. 10. O detalhamento desta Política poderá ser regulamentado em normas complementares ou instruções normativas, quando necessário, e poderá ter:

I - padrões, que definam os procedimentos a serem seguidos;

II - boas práticas, que apresentem modelos aderentes à POSIN; e

III - manuais operacionais que formalizem o seu modus operandi em termos de segurança da informação.

Art. 11. A informação poderá ser classificada de acordo com os níveis definidos conforme a legislação e as normas vigentes.

§ 1º Categorias adicionais poderão ser estabelecidas pela POSIN ou pelas suas normas complementares.

§ 2º As diretrizes para o tratamento de dados pessoais no âmbito público abarcam o tratamento transparente, a garantia expressa aos direitos de personalidade e o consentimento do titular para a disponibilização de suas informações àqueles que não possuam a necessidade de conhecê-la no exercício de sua função pública.

Art. 12. A segurança da informação deve estar presente na gestão de projetos, independentemente de sua natureza.

Art. 13. A informação documentada deve ser:

I - elaborada, mantida, controlada e protegida nos moldes estabelecidos nesta Política e normas complementares;

II - detalhada em função do tamanho e complexidade da informação, assim como da capacidade das pessoas envolvidas; e

III - controlada em termos de distribuição, acesso, obtenção, uso, armazenamento, preservação, controle de mudanças, retenção e descarte.

Art. 14. A gestão de segurança da informação de proteção de dados pessoais será constituída pelos seguintes processos:

I - mapeamento de ativos de informação;

II - gestão de riscos de segurança da informação;

III - gestão de continuidade de negócios em segurança da informação;

IV - gestão de mudanças nos aspectos de segurança da informação;

V - avaliação de conformidade de segurança da informação; e

VI - adoção dos controles CIS (Controles Críticos de Segurança).

Art. 15. As orientações e diretrizes estabelecidas nesta Política devem ser respeitadas em atividades internas, externas ou em teletrabalho, uma vez que:

I - as boas práticas "Mesa e Tela Limpa" devem ser adotadas por todos os usuários;

II - as informações e ativos podem estar em um de seus lugares mais vulneráveis (sujeitos a divulgação ou uso não autorizado); e

III - a adoção desta POSIN e das boas práticas de "Mesa Limpa e Tela Limpa" é uma das principais estratégias a se utilizar na tentativa de reduzir os riscos de brechas de segurança de informação e de proteção de dados pessoais.

CAPÍTULO VII
DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 16. As atividades relacionadas ao gerenciamento de riscos e controle devem ser gerenciadas com cuidado, para garantir que os processos de riscos e controle sejam conduzidos como intencionado.

Parágrafo único. Os riscos de segurança da informação e de proteção de dados pessoais devem ser considerados na contratação de serviços terceirizados, sendo os gestores das unidades organizacionais e dos ativos relacionados, gestores e fiscais de contrato, além dos fornecedores e custo diantes, os responsáveis por manter os níveis apropriados de segurança da informação na entrega dos serviços.

Art. 17. As normas e procedimentos da Infra S.A. devem considerar controles de riscos para a troca de informações, tanto internamente quanto externamente, de forma a manter o nível adequado de segurança da informação e de proteção de dados pessoais.

Parágrafo único. A gestão dos riscos de segurança da informação e de proteção de dados pessoais deve ser implementada e mantida de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos da Infra S.A..

CAPÍTULO VIII
DA GESTÃO DE ATIVOS

Art. 18. Ações e controles específicos de segurança devem garantir a proteção adequada dos ativos de informação, em níveis compatíveis com seu grau de importância para a consecução das atividades e objetivos estratégicos da Empresa.

Parágrafo único. Os ativos de informação devem ser associados a controles de segurança implementados independentemente do meio em que se encontram, devendo ser protegidos contra divulgação, modificação, remoção ou destruição não autorizada.

Art. 19. As pessoas que possuem acesso aos ativos de informação da Infra S.A. devem ser periodicamente conscientizadas, capacitadas e sensibilizadas acerca do tema privacidade e segurança da informação.

Parágrafo único. Os processos e atividades que sustentam os serviços críticos disponibilizados pela

empresa devem ser protegidos de forma a garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações e comunicações, bem como a privacidade das informações com restrição de acesso e dos dados pessoais, observadas as normas em vigor sobre a matéria.

CAPÍTULO IX
DOS BACKUPS EM RELAÇÃO À GESTÃO DA CONTINUIDADE DO NEGÓCIO

Art. 20. A Infra S.A. declara seu compromisso claro com relação às obrigações legais e regulamentares e à melhoria contínua do processo de gestão de continuidade de negócios, e para isso deve:

I - manter controles internos efetivos sobre os procedimentos de backup com vistas a assegurar a disponibilidade e a continuidade do negócio e a consequente prestação de serviços públicos por parte da Empresa; e

II - estabelecer processo de gestão de continuidade de negócios, em conjunto com as áreas intervenientes responsáveis pelos ativos de informação, a fim de minimizar os impactos decorrentes de eventos que causem a indisponibilidade dos serviços.

CAPÍTULO X
DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 21. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, pela Equipe de Tratamento e Resposta a Incidentes de Rede (ETIR), de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos da Infra S.A., sem prejuízo de sua comunicação à Estrutura de Segurança da Informação e, no caso de envolver dados pessoais, ao Encarregado pelo tratamento de dados pessoais.

CAPÍTULO XI
DA COMPUTAÇÃO EM NUVEM

Art. 22. Sempre que desejar utilizar computação em nuvem, a Infra S.A., deverá formalizar um ato normativo sobre seu uso seguro.

§ 1º O ato normativo de que trata o caput deverá, no mínimo:

I - atender à Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que 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, e suas alterações;

II - ser elaborado com base nesta Política;

III - ser homologado pela alta administração e divulgado a todas as partes interessadas;

IV - relacionar as metas a serem alcançadas e os objetivos que regem o serviço de computação em nuvem;

V - definir as funções e as responsabilidades dos agentes designados para o gerenciamento dos serviços de computação em nuvem; e

VI - estabelecer a periodicidade para sua revisão, a qual não deve exceder dois anos.

§ 2º A revisão do ato normativo previsto poderá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação, que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

CAPÍTULO XII
DOS TEMAS INTERCONECTADOS DA SEGURANÇA

Art. 23. A segurança da informação está intrinsecamente ligada à infraestrutura tecnológica e à segurança de tecnologia da informação, abrangendo diversos temas interconectados, os quais, embora não subordinados, devem operar de forma conjunta para garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, a saber:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física e a proteção de dados organizacionais; e

IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO XIII
DOS PAPÉIS E DAS RESPONSABILIDADES

Art. 24. Papéis e responsabilidades em segurança da informação devem ser definidos e atribuídos:

I - de maneira apropriada e efetiva, devendo-se aplicar a sua segregação sempre que possível para reduzir vulnerabilidades; e

II - de forma que se estabeleçam responsabilidades, para que cada área entenda os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de segurança da informação e riscos.

SEÇÃO I
DA ALTA ADMINISTRAÇÃO

Art. 25. A Alta Administração da Infra S.A. deve:

I - designar gestor de segurança da informação interno;

II - instituir Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à POSIN;

III - viabilizar a promoção de ações de capacitação para os agentes responsáveis, visando ao aperfeiçoamento de seus conhecimentos sobre a segurança da informação;

IV - prover recursos para as iniciativas que visem suportar a efetividade do Sistema de Gestão de Segurança da Informação (SGSI);

V - designar formalmente o encarregado pelo tratamento de dados pessoais; e

VI - prover a estrutura necessária para garantir a proteção de dados pessoais na InfraS.A..

SEÇÃO II
DE TODOS OS PROFISSIONAIS

Art. 26. É responsabilidade de todos que têm acesso, parcial ou total, à informação de propriedade ou que transite pela Infra S.A.:

I - assumir postura proativa no que diz respeito à proteção das informações e atenção em relação a ameaças externas, fraudes, roubo de informações, e acesso indevido a sistemas;

II - observar que assuntos confidenciais não devem ser expostos publicamente;

III - observar que senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

IV - observar que somente softwares homologados podem ser utilizados no ambiente computacional da Infra S.A.;

V - observar que documentos impressos e arquivos contendo informações confidenciais devem ser armazenados, protegidos e descartados na forma da legislação pertinente;

VI - observar que todos os dados imprescindíveis aos objetivos da Infra S.A. devem ser protegidos e salvaguardados;

VII - observar que todas as criações, códigos ou procedimentos desenvolvidos para a Infra S.A. por qualquer profissional, estagiário ou terceiro são de propriedade da Infra S.A.;

VIII - engajar-se na busca pelo conhecimento e promover ações no sentido de consolidar a cultura de segurança da informação e da proteção de dados pessoais;

IX - contribuir de forma ativa e constante no processo de melhoria da segurança da informação e da proteção de dados pessoais na Empresa;

X - buscar o melhor aproveitamento dos recursos e serviços disponíveis;

XI - dedicar-se nos processos de formação em nível de capacitação, educação e conscientização, buscando atuar como disseminador das melhores práticas;

XII - buscar a segurança dos ativos de informação;

XIII - participar e contribuir na busca e compartilhamento do conhecimento, na troca de experiências, bem como de grupos de trabalho e eventos que tratem do tema;

XIV - buscar o conhecimento, entendendo que a segurança da informação e a proteção de dados pessoais abrangem os contextos estratégico, tático e operacional da Infra S.A.;

XV - agir em conformidade com a legislação vigente, as normas internas e melhores práticas em segurança da informação e proteção de dados pessoais;

XVI - zelar pela segurança da informação e pela proteção de dados pessoais, segundo preceitos desta Política e das normas complementares ou instruções normativas;

XVII - adotar ações preventivas e reativas com relação a não conformidades em termos de segurança da informação;

XVIII - adotar e promover a cultura da segurança da informação e de dados pessoais, participando de atividades de sensibilização, conscientização e capacitação;

XIX - facilitar a disseminação da segurança da informação no âmbito da sua atuação, seguindo os procedimentos definidos como boas práticas;

XX - cumprir com os deveres dispostos na POSIN e nas demais normas de segurança da informação e de proteção de dados pessoais;

XXI - buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

XXII - buscar orientação do encarregado pelo tratamento de dados pessoais em caso de dúvidas relacionadas à proteção de dados pessoais;

XXIII - assinar os termos ou instrumentos equivalentes, que venham a ser instituídos por normas de segurança da informação;

XXIV - formalizar a ciência e o aceite da política, das normas e procedimentos e assumir responsabilidade por seu cumprimento;

XXV - utilizar os recursos de segurança que lhe forem disponibilizados, para proteger as informações a que tenha acesso; e

XXVI - sugerir melhorias em termos de segurança da informação e da proteção de dados pessoais no âmbito das suas atividades, competências ou conhecimentos.

SEÇÃO III
DOS GESTORES

Art. 27. O Gestor no âmbito da POSIN será o:

I - responsável pela área ou unidade, que poderá delegar expressamente, inclusive por meio eletrônico, essa atribuição; e

II - responsável pela gestão da segurança da informação no âmbito da unidade.

Art. 28. Cada Gestor tem como atribuições:

I - implementar as ações dentro da sua competência, conforme legislação vigente e boas práticas, para a proteção de todos os ativos sob sua responsabilidade;

II - promover a cultura da segurança da informação e proteção de dados pessoais em suas equipes, incentivando a participação em atividades de conscientização e capacitação;

III - atuar como facilitador para a disseminação e a implantação da segurança da informação e da proteção de dados pessoais no âmbito das suas áreas de atuação;

IV - orientar seus subordinados quanto à existência e aplicabilidade, à sua unidade, desta Política, assim como de normas complementares, boas práticas e manuaisoperacionais;

V - propor e implementar melhorias e procedimentos de segurança da informação e proteção de dados pessoais, relacionados às suas áreas de competência;

VI - gerir, dentro dos limites da sua atuação e da sua área, os controles a serem realizados em termos de segurança da informação e proteção de dados pessoais;

VII - comunicar imediatamente casos relevantes de violação de segurança da informação e da LGPD ao gestor de segurança da informação e ao Encarregado pelos dados pessoais;

VIII - participar e apoiar integralmente a apuração de incidentes de segurança da informação;

IX - prover informações acerca da segurança da informação para o comitê de segurança da informação e adicionalmente para o Encarregado pelos dados pessoais, sobrea atuação da sua área;

X - manter as informações documentadas na extensão necessária e suficiente para a efetividade da segurança da informação e da proteção de dados pessoais; e

XII - participar da execução das atividades de gestão dos riscos de segurança da informação e de proteção de dados associados aos ativos de informação sob sua responsabilidade.

SEÇÃO IV
DOS SISTEMAS DE INFORMAÇÃO

Art. 29. Deve haver um Gestor de Negócio, que será responsável pela gestão do sistema de informação, em termos de regras de negócio.

§ 1º O Gestor terá o apoio técnico da área de tecnologia da informação.

§ 2º Caso o sistema seja gerido apenas por uma unidade organizacional ou implemente regras de negócio de apenas uma unidade organizacional, o Gestor de Negócio vinculado ao sistema será dessa unidade.

§ 3º Caso o sistema seja gerido ou implemente regras de negócio de mais de uma unidade, o primeiro superior hierárquico comum a todas designará o Gestor de Negócio associado ao referido sistema, dentre as unidades envolvidas.

§ 4º Em caso de indefinição sobre qual unidade realiza a gestão do sistema, o Gestor de Negócio associado será o da área cujas competências funcionais estejam mais alinhadas com as regras de negócio implementadas pelo sistema.

§ 5º A partir da publicação desta Política, novos sistemas só poderão entrar em produção se houver um Gestor previamente associado consoante os critérios elencados nos parágrafos anteriores.

§ 6º Os sistemas já em produção no momento da publicação desta Política terão seus respectivos Gestores definidos.

§ 7º Áreas que possam prescindir de um Gestor de Negócio serão eventualmente especificadas por normas complementares.

SEÇÃO V
DO E-MAIL INSTITUCIONAL

Art. 30. O serviço de e-mail institucional da Infra S.A. é destinado ao desempenho das funções laborais concernentes à empresa, sendo vedado o uso para fins particulares.

§ 1º O e-mail institucional é considerado um meio formal e oficial de comunicação eletrônica; portanto, os documentos e mensagens enviados para o e-mail institucional são considerados entregues, sendo responsabilidade de cada usuário a leitura periódica de seus e-mails.

§ 2º A concessão de uma conta de e-mail institucional não atribui ao usuário poder de representação institucional.

§ 3º As informações produzidas ou recebidas no serviço de e-mail institucional poderão ser acessadas pela Instituição nos casos de determinação judicial.

§ 4º O acesso ao conteúdo de informações produzidas ou recebidas no serviço de e-mail institucional poderá ocorrer mediante justificativa formalizada ao CSIC, ou órgão colegiado aplicável, e submetida à prévia autorização da autoridade máxima da Infra S.A. preservando o sigilo do processo.

Art. 31. A criação de endereços de e-mail da Infra S.A. deve adotar preferencialmente o padrão composto pelo primeiro nome do agente público, seguido por pontuação e seu último sobrenome ([nome.últimosobrenome]@infrasa.gov.br).

§ 1º Caso já tenha sido utilizado por outro agente público, será adotado o penúltimo sobrenome ([nome.penúltimosobrenome]@infrasa.gov.br).

§ 2º Caso haja alguma excepcionalidade, deverá ser informada e justificada.

CAPÍTULO XIV
DAS SANÇÕES

Art. 32. Desvios de conduta em termos de segurança da informação, de proteção de dados pessoais e as ações que violem esta Política deverão ser apurados nos termos da legislação em vigor, sendo passíveis de sanções civis, penais e administrativas.

Art. 33. A resolução de casos de violação da legislação correlata será tratada pelo CSIC ou Comitê aplicável.

Art. 34. Os casos omissos devem ser resolvidos pela Diretoria Executiva e pelo Conselho de Administração da Infra S.A.

CAPÍTULO XV
DAS REFERÊNCIAS

Art. 35. A presente Política está fundamentada em instrumentos legais e baseada em boas práticas:

I - Constituição da República Federativa do Brasil de 1988 (Carta Magna).

II - Lei nº 13.853, de 8 de julho de 2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados.

III - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais (Lei Geral de Proteção de Dados Pessoais - LGPD).

IV - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

V - Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos.

VI - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações (Lei de Acesso à Informação - LAI).

VII - Lei nº 9.610, de 19 de fevereiro de 1998, que dispõe sobre o Direito Autoral.

VIII - Lei nº 9.279, de 14 de maio de 1996, que dispõe sobre Marcas e Patentes.

IX - Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados.

X - Lei nº 3.129, de 14 de outubro de 1982, que regula a Concessão de Patentes aos autores de invenção ou descoberta industrial.

XII - Decreto nº 11.200, de 15 de setembro de 2022, que aprova o Plano Nacional de Segurança de Infraestruturas Críticas.

XIII - Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos.

XIV - Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022.

XV - Decreto nº 10.996, de 14 de março de 2022, que atualizada a Estratégia de Governo Digital.

XVI - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética (E-CIBER).

XVII - Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados (CGD).

XVIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI).

XIX - Decreto nº 9.573, de 22 de novembro de 2018, que aprova a Política Nacional de Segurança de Infraestruturas Críticas (PNSI).

XX - Decreto nº 10.139, de 28 de novembro de 2019, que dispõe sobre a revisão e a consolidação dos atos normativos inferiores a decreto.

XXI - Portaria nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação.

XXII - Instruções normativas publicadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI)/PR.

XXIII - Instruções normativas, frameworks e guias publicados pela Secretaria de Governo Digital.

XXIV - Acordão: 1.889/2020 - TCU - Plenário (Tecnologia da Informação - Levantamento de Sistemas Críticos).

XXV - Normas ABNT NBR ISO/IEC 27001: 2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.

XXVI - Normas ABNT NBR ISO/IEC 27002: 2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.

XXVII - Normas ABNT NBR ISO/IEC 27002: 2022 - Segurança da Informação, Segurança Cibernética e Proteção à Privacidade — Controles de Segurança da Informação.

CAPÍTULO XVI
DAS DISPOSIÇÕES FINAIS

Art. 36. A partir de sua identificação na Infra S.A., os usuários são responsáveis por quaisquer ações que venham a ferir a disponibilidade, a integridade, a confidencialidade, a autenticidade e a privacidade da informação, observadas as normas em vigor sobre a matéria.

Art. 37. Esta POSIN deve ser revisada e atualizada a cada três anos, ou quando houver fatos relevantes que exijam revisão extemporânea.

Art. 38. Fica revogada a Resolução CONSAD-VALEC nº 8, de 07 de abril de 2021, que define a Política de Segurança da Informação no âmbito da Valec.

Art. 39. Os casos omissos serão analisados e resolvidos pela Diretoria Executiva.

Art. 40. Esta Resolução entra em vigor em 02 de maio de 2024.

Endereço: SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5, Asa Sul, Brasília - DF.

CEP: 70.070-010

Telefone: +55 (61) 2029 6061

www.infrasa.gov.br

institucional@infrasa.gov.br

infrasaoficial

infra.oficial

infra-oficial

infrasa.oficial

infra.oficial