POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DADOS PESSOAIS	
Identificação:	P-003
Versão	2.0
Início da Vigência:	14/06/2022
Data de Revisão	14/06/2024
Aprovação	Aprovado na 478ª ROCA, em 28/01/2022
Campo de Aplicação	Todas as unidades organizacionais da Telebras
Processo de Negócio:	Gestão da Segurança da Informação
Nível de Acesso	Interno
Código de Classificação	000.067.210
Unidade Elaboradora	Comitê Gestor de Segurança da Informação
Unidade de Impacto	Comitê de Governança e Proteção de Dados Pessoais
Alteração em relação à versão anterior:	Adequação à Lei Geral de Proteção de Dados Pessoais – LGPD

NORMATIVOS INTERNOS VINCULADOS	
Cód.	**Descrição**
N/A	Estatuto Social da Telebras;
N/A	Regimento Interno da Telebras;
D-236	Regime Disciplinar

NORMATIVOS INTERNOS REVOGADOS	
Cód.	**Descrição**
N/A	N/A

NORMATIVOS EXTERNOS APLICÁVEIS – LEGISLAÇÃO

Decreto nº 3.505, de 13 de junho de 2000; Decreto nº 9.637, de 26 de dezembro de 2018; Decreto nº 9.832, de 12 de junho de 2019, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012; Lei nº 13.709, de 14 de agosto de 2018 e altera a Lei nº 12.965, de 23 de abril de 2014; Lei nº 12.965, de 23 de abril de 2014; Lei Nº 12.527, de 18 de novembro de 2011; Lei nº 8.159, de 8 de janeiro de 1991; Decreto nº 7.724, de 16 de maio de 2012; Lei no 12.527, de 18 de novembro de 2011; Constituição Federal; Instrução Normativa nº 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República; Instrução Normativa nº 02, de 5 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República; Norma Complementar nº 03 da IN 01, de 30 de junho de 2009, do Gabinete de Segurança Institucional da Presidência da República; Norma Complementar nº 04 da IN 01, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República; Norma Complementar nº 05 da IN 01, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República; Norma Complementar nº 06 da IN 01, de 11 de novembro de 2009, do Gabinete de Segurança Institucional da Presidência da República; Norma Complementar nº 07 da IN 01, de 06 de maio de 2010, do Gabinete de Segurança Institucional da Presidência da República; Norma Complementar nº 08 da IN01/DSIC/GSIPR; Norma Complementar nº 10

da IN01/DSIC/GSIPR; Norma Complementar nº 12 da IN01/DSIC/GSIPR; NBR ISO/IEC 27001:2006: Sistemas de gestão de Segurança da Informação; NBR ISO/IEC 27002:2007: Código de prática para a gestão da Segurança da Informação

Sumário

1. OBJETIVO 4
2. DAS DISPOSIÇÕES PRELIMINARES 4
3. CONCEITOS E DEFINIÇÕES 4
4. COMPETÊNCIAS 8
5. PRINCÍPIOS 11
6. DIRETRIZES GERAIS 11
7. DIRETRIZES ESPECÍFICAS 12
8. PENALIDADES 19
9. ATUALIZAÇÃO 19
10. APROVAÇÃO 19

1. OBJETIVO

1.1. A Política de Segurança da Informação e Dados Pessoais (POSI) da Telebras tem como objetivo estabelecer a governança da Segurança da Informação visando à preservação da disponibilidade, integridade, confidencialidade, autenticidade e o não repúdio das informações pertencentes a Telebras. Assim como as informações de seus empregrados, clientes e parceiros, de acordo com os seus objetivos estratégicos e de negócios, provendo o direcionamento para toda a organização;

1.2. Esta Política visa atender ao que dispõe a legislação em vigor, em especial o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, bem como ao Decreto nº 9.832, de 12 de junho de 2019, que altera o Decreto nº 9.637 e ao Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação.

1.3. Igualmente esta Política atende o que dispões a legislação em vigor no que tange a Lei Geral de Proteção de Dados Pessoais – LGPD, lei nº 13.709, de 14 de agosto de 2018 e sua alteração pela Lei nº 13.853, de 8 de Julho de 2019.

2. DAS DISPOSIÇÕES PRELIMINARES

2.1. A POSI alinha-se às estratégias da Telebras e busca garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas ou custodiadas pela Telebras, independentemente do meio onde estejam registradas, assim como a conformidade e normatização das atividades de gestão de Segurança da Informação;

2.2. Também fazem parte desta POSI todos os documentos que a complementam, os quais destinam à proteção da informação e à disciplina de sua utilização;

2.3. Os colaboradores da Telebras, incluindo controladores, controlados, gestores, empregados, estagiários, terceiros, prepostos e prestadores de serviços que exerçam atividades no âmbito da Telebras, bem como qualquer pessoa ou ente que venham a ter acesso aos ativos de informação, estão submetidos a esta Política e devem estar comprometidos com a Segurança da Informação na Telebras;

2.3.1. Deverá ser assinado um termo específico de ciência da POSI-TB, contendo cláusula de responsabilidade e sigilo, quando a natureza do trabalho ou as informações a que tem acesso assim o exigirem.

2.4. Os acordos, contratos, convênios e instrumentos congêneres devem atender, no que couber, a esta Política e às demais normas relacionadas, prevendo a obrigação de conhecimento por todos os envolvidos nas atividades do contrato, por meio da assinatura de termo de ciência;

2.4.1. Estes instrumentos devem conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas o exigirem.

3. CONCEITOS E DEFINIÇÕES

3.1. Para os efeitos desta Política de Segurança da Informação e Dados Pessoais da Telebras foram estabelecidos os significados dos seguintes termos e expressões:

3.1.1. **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. (Ref.: NC07/IN01/DSIC/GSIPR/2010);

3.1.2. **Ameaça:** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (Ref.: 04/IN01/DSIC/GSI/PR/2013);

3.1.3. **Armazenamento:** ação ou resultado de manter ou conservar em repositório um dado;

3.1.4. **Arquivamento (no âmbito de Tecnologia):** ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a sua vigência;

3.1.5. **Ativo de informação:** qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

3.1.6. **Ativo:** qualquer bem, tangível ou intangível, que tenha valor para a organização;

3.1.7. **Autenticidade:** qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema (Ref.: Lei nº 12.527/2011);

3.1.8. **Avaliação (no âmbito de Tecnologia):** analisar o dado com o objetivo de produzir informação;

3.1.9. **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;

3.1.10. **Coleta:** recolhimento de dados com finalidade específica;

3.1.11. **Comitê Gestor de Segurança da Informação – CGSI:** comitê instituído no âmbito da Telebras com caráter consultivo, normativo e deliberativo para assuntos relativos à Segurança da Informação;

3.1.12. **Comunicação:** transmitir informações pertinentes a políticas de ação sobre os dados;

3.1.13. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados;

3.1.14. **Continuidade de negócios:** capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. (Ref.NC06/IN01/DSIC/GSIPR/2009);

3.1.15. **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

3.1.16. **Controle:** ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

3.1.17. **Consentimento**: manifestação favorável do titular de dados ao tratamento destes. Deve referir-se a finalidades determinadas. As autorizações genéricas para o tratamento de dados pessoais são nulas, assim como no fornecimento ao titular de informações com conteúdo enganoso ou abusivo, ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

3.1.18. **Criticidade:** grau de importância da informação;

3.1.19. **Desastres:** evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação (Ref.: NC06/IN01/DSIC/GSIPR/ 2009);

3.1.20. **Difusão:** ato ou efeito de divulgação, propagação, multiplicação dos dados;

3.1.21. **Disponibilidade:** qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados (Ref.: Lei nº 12.527/2011);

3.1.22. **Distribuição:** ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

3.1.23. **Documento:** unidade de registro de informações, qualquer que seja o suporte ou formato (Ref.: Lei nº 12.527/2011);

3.1.24. **Eliminação (no âmbito de Tecnologia):** ato ou efeito de excluir ou destruir dado do repositório;

3.1.25. **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

3.1.26. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR):** grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores (Ref.:NC03/IN01/DSIC/GSIPR/ 2009);

3.1.27. **Extração:** ato de copiar ou retirar dados do repositório em que se encontrava;

3.1.28. **Gestão da 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, à tecnologia da informação (Ref.: IN GSI/PR 01/2008);

3.1.29. **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;

3.1.30. **Gestão de Riscos:** a Gestão de Riscos de Segurança da Informação é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

3.1.31. **Gestor de Segurança da Informação:** empregado responsável pela coordenação das ações de Segurança da Informação no âmbito da Telebras;

3.1.32. **Incidente de Segurança da Informação:** evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, de computação ou das redes de computadores;

3.1.33. **Informação:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (Ref.: Lei nº 12.527/2011);

3.1.34. **Integridade:** qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino (Ref.: Lei nº 12.527/ 2011);

3.1.35. **Modificação:** ato ou efeito de alteração do dado;

3.1.36. **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

3.1.37. **Princípios:** são ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional;

3.1.38. **Processamento:** ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

3.1.39. **Produção:** criação de bens e de serviços a partir do tratamento de dados;

3.1.40. **Proprietário do ativo de informação:** autoridade legal responsável pelo ativo e que tem a concessão de acesso ao ativo de informação;

3.1.41. **Recepção:** ato de receber os dados ao final da transmissão;

3.1.42. **Recursos de tecnologia da informação:** servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer hardware e software que compõem soluções e aplicações de Tecnologia da Informação;

3.1.43. **Reprodução:** cópia de dado preexistente obtido por meio de qualquer processo;

3.1.44. **Risco:** é o 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;

3.1.45. **Segurança da Informação (SI):** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Ref.: IN GSI/PR 01/2008);

3.1.46. **Terceiros:** quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à Telebras;

3.1.47. **Transferência:** mudança de dados de uma área de armazenamento para outra, ou para terceiro;

3.1.48. **Transmissão:** movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;

3.1.49. **Tratamento da informação:** conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (Ref.: Lei nº 12.527/ 2011);

3.1.50. **Tratamento de incidentes de segurança:** são as atividades que consistem em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

3.1.51. **Usuário:** qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas, recursos computacionais e à rede corporativa disponibilizados pela Telebras;

3.1.52. **Utilização:** ato ou efeito do aproveitamento dos dados;

3.1.53. **Vulnerabilidade:** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de Segurança da Informação (Ref.: NC04/IN01/DSIC/GSIPR/2013).

4. COMPETÊNCIAS

4.1. Da Diretoria Executiva da Telebras:

4.1.1. Aprovar a Política de Segurança da Informação e Dados Pessoais e demais normas de Segurança da Informação;

4.1.2. Definir diretrizes para a sua institucionalização;

4.1.3. Assegurar que as responsabilidades e autoridades dos papéis relevantes para a Segurança da Informação sejam atribuídos e comunicados;

4.1.4. Assegurar que o sistema de gestão da Segurança da Informação esteja em conformidade com os requisitos desta Política;

4.1.5. Divulgar sobre o desempenho do sistema de gestão da Segurança da Informação para a Telebras;

4.1.6. Assegurar que a Política de Segurança da Informação e Dados Pessoais e os objetivos de Segurança da Informação estejam estabelecidos e sejam compatíveis com a direção estratégica da organização;

4.1.7. Fomentar a integração dos requisitos do sistema de gestão da Segurança da Informação dentro dos processos da organização;

4.1.8. Assegurar que os recursos humanos, financeiros e tecnológicos necessários para o sistema de gestão da Segurança da Informação estejam disponíveis;

4.1.9. Comunicar a importância de uma gestão eficaz da Segurança da Informação e da conformidade com os requisitos do sistema de gestão da Segurança da Informação;

4.1.10. Assegurar que o sistema de gestão da Segurança da Informação alcance seus resultados pretendidos;

4.1.11. Orientar e apoiar os colaboradores para eficácia do sistema de gestão da Segurança da Informação;

4.1.12. Assegurar que todos os colaboradores sejam competentes em Segurança da Informação, nos diversos níveis, com base na conscientização, treinamento ou cursos apropriados;

4.1.13. Quando aplicável, tomar ações para promover a competência necessária e avaliar a eficácia das ações tomadas;

4.1.14. Promover a melhoria contínua.

4.2. Do Comitê Gestor de Segurança da Informação (CGSI), não obstante aos definidos no Regimento Interno do Comitê:

4.2.1. Assessorar a implementação das ações de Segurança da Informação no âmbito da Telebras;

4.2.2. Constituir grupos de trabalho específicos para tratar de temas e propor soluções específicas sobre Segurança da Informação;

4.2.3. Propor normas e procedimentos relativos à Segurança da Informação no âmbito da Telebras;

4.2.4. Revisar e analisar periodicamente as diretrizes e normas estabelecidas nesta política, visando à sua aderência e concordância aos objetivos estratégicos da empresa e às legislações vigentes;

4.2.5. Propor alterações da Política de Segurança da Informação e Dados Pessoais;

4.2.6. Propor normas relativas à Segurança da Informação.

4.3. Da Comissões Permanentes de Avaliação de Documentos Ostensivos e Sigilosos

4.3.1. Promover a conscientização do corpo de funcionários em relação à relevância dos documentos e das informações da Telebras, reforçando seu caráter público e a necessidade de serem geridas e estarem acessíveis, resguardados os devidos graus de sigilo;

4.3.2. Gerir o conjunto documental arquivístico sigiloso;

4.4. Do Gestor de Segurança da Informação, não obstante aos definidos no Regimento Interno do Comitê:

4.4.1. Estabelecer os objetivos e os planos da Equipe de Tratamento de Incidentes em Redes – ETIR;

4.4.2. Orientar as atividades da Equipe de Tratamento de Incidente em Redes – ETIR;

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

4.4.4. Acompanhar as investigações e as avaliações dos danos decorrentes de quebra de segurança;

4.4.5. Reportar-se ao CGSI-TB nas reuniões do comitê;

4.4.6. Propor melhorias nos processos relacionados à Segurança da Informação;

4.4.7. Propor, perante ao Comitê Gestor de Segurança da Informação, normas relativas à Segurança da Informação;

4.4.8. Acompanhar e avaliar a aplicação e eficácia dos controles de Segurança da Informação que estão sendo aplicados.

4.5. Do Comitê Gestor de Proteção de Dados Pessoais:

4.5.1. Avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade da TELEBRAS com as disposições da Lei n. 13.709, de 14 de agosto de 2018;

4.5.2. Formular princípios e diretrizes para a gestão de dados pessoais e propor sua normatização;

4.5.3. Supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei n. 13.709, de 14 de agosto de 2018;

4.5.4. Prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na Lei n. 13.709, de 14 de agosto de 2018 e nas normas internas; e

4.5.5. Promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos.

4.6. Do Controlador:

4.6.1. Instituir o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais e definir as respectivas atribuições, em conformidade com a LGPD;

4.6.2. Designar o(s) Encarregado(s) pelas informações relativas aos dados pessoais;

4.6.3. Fornecer as orientações relativas à governança dos dados pessoais e respectivos normativos, a fim de que os processos sejam auditáveis e contemplem metodologias de Gestão de Riscos e de Segurança da Informação, no tratamento dos dados pessoais;

4.6.4. Assegurar a capacitação dos operadores para que atuem com responsabilidade, critério e ética;

4.6.5. Supervisionar a observância das instruções e das normas sobre tratamento de dados pessoais na instituição;

4.6.6. Comunicar a Autoridade Nacional e aos titulares de dados, eventualmente afetados, a ocorrência de incidentes de segurança que envolvam dados pessoais;

4.6.7. Promover a disseminação da cultura da privacidade de dados pessoais na Telebras;

4.6.8. Determinar o desenvolvimento dos respectivos programas.

4.7. Do encarregado:

4.7.1. Acolher reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

4.7.2. Receber comunicações da autoridade nacional e adotar providências;

4.7.3. Compor o Comitê de Segurança da Informação e Comunicação de Incidentes com Dados Pessoais;

4.7.4. Orientar os empregados e os contratados da entidade a respeito das práticas a serem observadas em relação à proteção de dados pessoais; e

4.7.5. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

4.8. Dos operadores:

4.8.1. Atuar com responsabilidade, critério e ética;

4.8.2. Manter fiel observância dos princípios gerais e da garantia dos direitos dos titulares de dados pessoais;

4.8.3. Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito; e

4.8.4. Informar ao Encarregado qualquer incidente, intencional ou não, que ofereça risco à proteção de dados pessoais tratados na empresa.

5. PRINCÍPIOS

5.1. A Segurança da Informação no âmbito da Telebras e suas ações, em consonância com a Política Nacional de Segurança da Informação, devem abranger:

5.1.1. A segurança cibernética;

5.1.2. A defesa cibernética;

5.1.3. A boa governança no uso e compartilhamento de dados pessoais de colaboradores e clientes;

5.1.4. A segurança física e a proteção dos dados organizacionais; e

5.1.5. As ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

6. DIRETRIZES GERAIS

6.1. A Segurança da Informação tem como premissa principal a proteção da informação, assegurar a continuidade do negócio minimizando seus riscos e maximizando o retorno sobre os investimentos e as oportunidades pertinentes. (Ref. ISO/IEC 27.002:2006);

6.2. As diretrizes de Segurança da Informação devem considerar, prioritariamente, processos, objetivos estratégicos, requisitos legais e a estrutura da Telebras;

6.3. Estas diretrizes devem ser observadas por todos os usuários que executam atividades vinculadas a Telebras ao longo de todas as etapas do tratamento da informação a saber: recepção, classificação, acesso, transmissão, distribuição, produção, arquivamento, armazenamento, reprodução, eliminação, transporte, utilização, avaliação, destinação ou controle da informação;

6.4. É vedado a qualquer Colaborador o uso dos Recursos de Tecnologia da Informação e Comunicações para fins pessoais, próprios ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem terceiros ou a imagem da Telebras, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações;

6.5. A partir desta Política deverão ser estabelecidas diretrizes, gerais e específicas, de Segurança da Informação, assim como procedimentos complementares com a finalidade de proteção da informação e à disciplina de sua utilização, no âmbito da Telebras;

6.6. O cumprimento desta Política, bem como dos normativos que a complementam, deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas pela Coordenação de Segurança da Informação, buscando a certificação do cumprimento dos requisitos de Segurança da Informação e garantia de cláusula de responsabilidade e sigilo;

6.7. A Telebras deve se orientar pelas melhores práticas e procedimentos de Segurança da Informação recomendados por órgãos e entidades, públicas e privadas, responsáveis pelo estabelecimento de padrões;

6.8. Toda a infraestrutura, incluindo os recursos tecnológicos, sistemas de informação e as aplicações devem ser protegidos contra a indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

7. DIRETRIZES ESPECÍFICAS

7.1. Para as diretrizes específicas constantes deste item deve ser avaliada a necessidade de elaboração de normativos complementares, como novas políticas, diretrizes, práticas e/ou manuais que disciplinem ou facilitem o seu entendimento.

7.2. Tratamento da Informação

7.2.1. Instrumento normativo sobre o tratamento da informação, de classificação, de manipulação, de transferência e de destruição deve ser estabelecido, documentado e analisado criticamente, baseado nos requisitos de Segurança da Informação e dos negócios;

7.2.2. Todos os colaboradores, os terceiros, os prestadores de serviço, os sem vínculos, os temporários, os efetivos, os ocupantes de cargo em comissão, os cedidos, os requisitados ou ainda os que estiverem em trânsito, independente do dispositivo utilizado, que acessarem as redes de dados da Telebras estarão sujeitos às determinações desta política, dentro dos limites estabelecidos nas leis, decretos e outros normativos supervenientes.

7.2.3. Classificação da Informação / Enquadramento Legal

7.2.3.1. A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizado baseado no enquadramento legal ou classificação da informação;

7.2.3.2. Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela Telebras;

7.2.3.3. Procedimentos para o tratamento dos ativos devem ser desenvolvidos e implementados de acordo com um esquema de classificação da informação adotado pela organização em normativo especifico.

7.2.4. Manipulação da Informação

7.2.4.1. A Informação deve ser manipulada apenas por quem de direito e conforme sua classificação, necessidade e autorização.

7.2.4.2. A Informação não deve ser manipulada ou disponibilizada em locais não autorizados, como serviços de armazenamento público ou privados não previamente autorizados pela Telebras.

7.2.5. Transferência da Informação

7.2.5.1. Políticas, procedimentos e controles de transferências formais devem ser estabelecidos para proteger a transferência de informações, referente aos tipos de recursos de comunicação em uso pela Telebras;

7.2.5.2. Devem ser estabelecidos acordos para transferência segura de informações, que possuem restrições ou sigilo, entre a organização e partes externas;

7.2.5.2.1. Na hipótese de troca e tratamento de informação classificada em qualquer grau de sigilo com país ou organização estrangeira, o credenciamento de segurança no território nacional se dará somente se houver tratado, acordo, memorando de entendimento ou ajuste técnico firmado entre o país ou organização estrangeira e a República Federativa do Brasil

7.2.5.3. As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas;

7.2.5.4. Os requisitos de confidencialidade ou acordos de não divulgação, que reflitam as necessidades da organização para a proteção da informação, devem ser identificadas, analisadas criticamente e documentadas.

7.2.6. Destruição da Informação

7.2.6.1. A destruição de informações deve seguir os procedimentos e legislações definidas além dos procedimentos adotados pela Telebras.

7.3. Gestão e Tratamento de Incidentes

7.3.1. Os ativos devem ser gerenciados e controlados para proteger as informações nos sistemas e aplicações;

7.3.2. Deverá ser instituída, no âmbito da Telebras, a Equipe de Tratamento de Incidentes em Redes Computacionais (ETIR), por meio de DEG emitida pelo Gestor de Segurança da Informação devendo respeitar os seguintes aspectos:

7.3.2.1. Fundamentada na Norma Complementar nº 05/IN01/DSIC/GSIPR e seu anexo, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal;

7.3.2.2. Utilizar o modelo 1, conforme a referida Norma Complementar, onde a equipe será de unidades chaves e com dedicação compartilhada com suas funções regulares;

7.3.2.3. A Telebras deverá comunicar à autoridade nacional e aos titulares de dados afetados, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante;

7.3.2.4. Ter Autonomia entre as diversas Gerências envolvidas de forma compartilhada.

7.3.3. Uma Diretriz de Gestão de Incidentes de Rede deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios;

7.3.3.1. Este instrumento deve estar alinhado com a Norma Complementar nº 08/IN01/DSIC/GSIPR que estabelece as diretrizes para Gerenciamento de Incidentes em Redes Computacionais;

7.4. Gestão de Risco

7.4.1. Uma Diretriz de Gestão de Riscos de Segurança da Informação deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios;

7.4.1.1. Deve-se implementar e manter um processo de Gestão de Riscos com vistas a minimizar possíveis impactos associados aos ativos de informação. Esse processo deve possibilitar a seleção e priorização dos ativos a serem protegidos, bem como a definição e implantação de controles para a identificação e tratamento de problemas de segurança. Estas medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança;

7.4.1.2. A Diretriz de Gestão de Riscos de Segurança da Informação deve estar alinhada com a Norma Complementar nº 04/IN01/DSIC/GSIPR (Revisão 01) e seu anexo, que trata das diretrizes para o processo de Gestão de Riscos de Segurança da Informação e comunicações – GRSIC;

7.4.2. Uma Diretriz de Gestão de Ativos de TI deve ser estabelecida, documentada e analisada criticamente a fim de apoiar a Gestão de Riscos;

7.4.2.1. A Diretriz deverá estar em conformidade com a Norma Complementar nº 10/IN01/DSIC/GSIPR, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação.

7.5. Gestão de Continuidade

7.5.1. Uma Diretriz de continuidade do negócio deve ser estabelecida, documentada, pela área responsável, e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios;

7.5.2. Deverão ser implementado, mantido e testado periodicamente um processo de gestão da continuidade de negócios visando reduzir, para um nível aceitável, o tempo de interrupção causado por desastres ou incidentes de segurança que afetem os ativos de informação;

7.5.3. A continuidade com foco na Segurança da Informação deve ser contemplada nos sistemas de gestão da continuidade do negócio organizacional da Telebras;

7.5.4. Deverá ser estabelecidos os requisitos para a Segurança da Informação e a continuidade do negócio, com foco na gestão da Segurança da Informação, em situações adversas, por exemplo, durante uma crise ou desastre;

7.5.5. Deverão ser estabelecidos, documentados, implementados e mantidos processos, procedimentos e controles para assegurar o nível requerido de continuidade para a Segurança da Informação durante uma situação adversa;

7.5.6. Os controles de continuidade da Segurança da Informação, estabelecidos e implementados, devem ser verificados a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas;

7.5.7. Os recursos de processamento da informação devem ser implementados com a redundância necessária para atender aos requisitos de disponibilidade.

7.5.8. Diretriz de Cópias de Segurança de Informações Digitais (Backup) deve ser estabelecida, documentada e analisada criticamente a fim de apoiar a Gestão de Continuidade

7.5.8.1. Dados, configurações, sistemas e demais informações relevantes, devem ser realizadas periodicamente e testadas regularmente conforme a Prática de Procedimentos, Tipos e Retenções das Copias de Segurança a ser estabelecida em complemento da diretriz.

7.6. Auditoria e Conformidade

7.6.1. As atividades e requisitos de auditoria envolvendo a verificação nos sistemas, dados e demais informações relevantes, devem ser cuidadosamente planejados e acordados para minimizar interrupção nos processos do negócio;

7.6.2. Para a preservação da integridade dos dados, dos serviços aos usuários ou dos recursos computacionais da Telebras poderá ser efetivada a suspensão temporária de qualquer credencial, seja ou não o colaborador suspeito de alguma violação;

7.6.3. As auditorias e verificações de conformidade devem ser realizadas periodicamente, em existindo orçamento, no mínimo a cada 2 (dois) anos, a fim de avaliar a aplicação e eficácia dos controles de segurança e atendimento das normativos estabelecidos.

7.7. Monitoramento

7.7.1. O acesso e a utilização dos recursos de Tecnologia da Informação e Comunicações disponibilizadas pela Telebras são passíveis de monitoramento e auditoria, independentemente de aviso prévio.

7.7.2. A Telebras poderá manter registros e procedimentos, como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna, aos serviços de telecomunicação, à rede de telecomunicações e à Internet.

7.8. Controles de Acesso

7.8.1. Qualquer que seja a forma de identificação, ela deve ser pessoal, intransferível, permitindo de maneira clara e indiscutível o reconhecimento de qualquer COLABORADOR, de acordo com os critérios de segurança estabelecidos pela Telebras.

7.8.2. Uma Diretriz de Controle de acesso e circulação de pessoas na Telebras, deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios;

7.8.2.1. Em qualquer ambiente da Telebras é obrigatório o uso de crachá, carimbo ou etiqueta de identificação, independentemente da forma, deve ser pessoal e intransferível, e possibilitar de maneira clara e inequívoca o reconhecimento de seu portador;

7.8.3. Uma Diretriz de Controles de Acessos lógicos, deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios;

7.8.3.1. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada colaborador, conforme a Diretriz de Uso dos Recursos Computacionais que deverá ser estabelecida;

7.8.3.2. Os privilégios de acesso às informações devem ser definidos pelo gestor da área responsável pela informação, conforme prática de perfis de acesso a ser estabelecida;

7.8.4. Os controles de acesso serão definidos a partir da classificação do perímetro de segurança, dos serviços de rede, dos recursos, dos ativos, do ambiente e das informações que forem acessados ou estiverem associados;

7.8.5. Sempre que houver mudança nas atribuições de determinado colaborador, os seus privilégios de acesso às informações e aos recursos computacionais devem ser removidos imediatamente e novas solicitações de acesso requisitadas, devendo ser cancelados em caso de desligamento da Telebras;

7.8.6. Demais regras para o Controle de Acesso serão definidas em diretrizes e práticas específicas em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

7.9. Uso de E-mail e Aplicações de Mensagem Instantânea

7.9.1. Uma Diretriz de uso de e-mail e de mensagem instantânea deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios, ou estas orientações deverão estar contempladas em outra diretriz;

7.9.2. O correio eletrônico é um meio de comunicação corporativa da Telebras. As regras de acesso e utilização serão definidas por diretriz específica, em conformidade com esta Política e demais orientações e diretrizes de governo.

7.10. Acesso à Internet

7.10.1. O acesso à Internet no ambiente de trabalho da Telebras deverá regido por diretriz específica, em conformidade com esta Política e demais orientações governamentais e legislação em vigor.

7.11. Uso de Aplicações

7.11.1. As aplicações para uso corporativo e em dispositivos corporativos devem ser homologadas e aprovadas pela área de Tecnologia da Informação, desta forma uma ferramenta ou aplicação só pode ser utilizada se devidamente homologada.

7.11.2. Uma Diretriz de Uso de aplicativos, deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios de forma a gerenciar os riscos decorrentes do uso destes aplicativos;

7.12. Uso de Dispositivos Móveis e Pessoais

7.12.1. Uma Diretriz de Uso de Dispositivos Móveis e Pessoais, deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios de forma a gerenciar os riscos decorrentes do uso destes dispositivos;

7.12.2. Esta diretriz deve contemplar o uso de dispositivos pessoais como notebooks, tablets, pen drives, e outros, de colaboradores, prestadores de serviço, terceirizados, etc., com objetivo de adotar medidas que apoiam a Segurança da Informação para proteger as informações acessadas, processadas ou armazenadas no ambiente da Telebras e em locais de trabalho remoto;

7.12.3. A diretriz e as medidas que apoiam a segurança de uso de dispositivos móveis devem estar alinhados com a Norma Complementar nº 12/IN01/DSIC/GSIPR, que estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos à Segurança da Informação.

7.13. Mídias Removíveis

7.13.1. Procedimentos devem ser implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização;

7.13.2. As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais;

7.13.3. Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.

7.14. Computação em Nuvem

7.14.1. Uma diretriz de computação em nuvem deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de Segurança da Informação e dos negócios, ou estas orientações deverão estar contempladas em outra diretriz.

7.15. Informações Classificadas e Tratamento de Dados Pessoais

7.15.1. Uma diretriz e medidas que apoiam a classificação da informação e proteção dos dados pessoais devem ser adotados, baseado nos requisitos de Segurança da Informação e dos negócios;

7.15.2. Deverão ser obedecidas as determinações legais e normas específicas para o tratamento de informações pessoais;

7.15.3. Conforme legislação específica, o tratamento de dados pessoais sensíveis somente poderá ocorrer nas hipóteses listadas abaixo, quando se tratar especificamente de informações pessoais sem relação direta com as competências funcionais e institucionais da Telebras:

7.15.4. Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

7.15.5. observados os princípios que norteiam essa política e aqueles trazidos pelas leis vigentes, sem prejuízo da segurança de dados, estes podem ser compartilhados sem consentimento expresso do titular para as seguintes finalidades:

I. Cumprimento de obrigação legal ou regulatória;

II. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

III. Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

IV. A execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

V. O exercício regular de direitos em processo judicial, administrativo ou arbitral;

VI. A proteção da vida ou da incolumidade física do titular ou de terceiro;

VII. Atender aos interesses legítimos da Telebras ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular, respeitando também as legítimas expectativas de segurança dele.

7.15.6. Toda quebra de segurança de informação classificada, em qualquer grau de sigilo, deverá ser informada, tempestivamente, pela Alta Administração ao GSI/PR, relatando as circunstâncias com o maior detalhamento possível", em razão do Art.24 da IN n°02 do GSI/PR;

7.15.7. Também é dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Política", pela previsão do Art.7°, §4° da Lei n° 13.709/2018.

8. PENALIDADES

8.1. A não observância desta Política e/ou de seus documentos complementares, bem como a quebra de controles de Segurança da Informação, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa;

8.2. Para os empregrados da Telebras, as penalidades pelo descumprimento desta política estão previstas no Estatuto e Regimento Interno da Telebras, Diretriz D-236 – Regime Disciplinar e no seu Código de Ética;

8.3. Para os colaboradores subordinados à Telebras, as penalidades pelo descumprimento desta política estão previstas no contrato e outros atos legais celebrados junto à Telebras, sendo aplicável a legislação civil e criminal correspondente.

9. ATUALIZAÇÃO

9.1. Esta Política, bem como o conjunto de instrumentos normativos gerados a partir dela, deverão ser revisados periodicamente ou sempre que se fizer necessário, preferencialmente, não excedendo o período máximo de 2 (dois) anos;

9.2. Sempre que o detalhamento desta Política de Segurança da Informação e Dados Pessoais se fizer necessário, documentos complementares deverão ser elaborados, a fim de suprir qualquer falta de orientação ou direcionamento.

10. APROVAÇÃO

10.1. O **CONSELHO DE ADMINISTRAÇÃO**, no uso das atribuições que lhe confere o inciso XII do art. 56 do Estatuto Social da Telebras, aprovado pela 107ª Assembleia Geral Extraordinária, de 09/12/2020, **RESOLVE**:

10.2. Aprovar a atualização da Política de Segurança da Informação e Dados Pessoais.

Brasília/DF, 14 de junho de 2022.

gov.br Documento assinado digitalmente
WAGNER PRIMO FIGUEIREDO NETO
Data: 14/06/2022 12:27:21-0300
Verifique em https://verificador.iti.br

WAGNER PRIMO FIGUEIREDO NETO
Presidente do Conselho de Administração Substituto
Representante do MCom