



Política Segurança da Informação e Cibersegurança (PSIC)

Versão 1.4

Santa Rosa, Brasil, Fevereiro de 2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA - PSIC

DIREÇÃO EXECUTIVA

Alexandre Luis Machado

Eliseu Marafiga

COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Fernando Krein Pinheiro

COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS

Fernando Krein Pinheiro

Rodrigo Krein Pinheiro

Bruno Lopes

Aline Pereira de Oliveira

Silmar Parodes

Ricardo Leidemer

Lucas Berg

Lucas Frisk

Bruno Borges

Tanize Itermann

Andreia Becker Ferreira

Liziane Maria Schmitt

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS - DPO

Fernando Krein Pinheiro

Equipe Técnica de Elaboração

Fernando Krein Pinheiro

Ricardo Leidemer

Douglas Acosta

Marcus Volkweis

Equipe Revisora

Lucas Laiber

Laura Bikoski

Histórico de versões

Data	Versão	Descrição	Autor
12/05/2025	1.0	Criação da Política de SI e Cibersegurança	Fernando Pinheiro
20/01/2026	1.1	Atualização Zero Trust, I.A Generativa	Direção Executiva
19/02/2026	1.2	Atualização Ativos Core de Rede / ISP	Comitê de Privacidade
23/02/2026	1.3	Alterado Comitê de Privacidade e Proteção de Dados	Fernando Pinheiro
25/02/2026	1.4	Revisão e adequação Auditoria Independente	Fernando Pinheiro

1. OBJETIVO	9
1.1 Finalidade da Política	9
1.2 Alinhamento com os Objetivos Estratégicos do Negócio	9
1.3 Proteção da Informação como Ativo Corporativo	9
1.4 Estrutura e Hierarquia dos Documentos desta Política	9
2. ESCOPO E ABRANGÊNCIA	9
2.1 Abrangência Organizacional	9
2.2 Abrangência Tecnológica	10
2.3 Abrangência de Dados e Informações	10
2.4 Aplicabilidade a Colaboradores, Terceiros e Parceiros	10
2.5 Exclusões e Exceções Formais	10
2.6 Declaração de Aplicabilidade (SoA)	10
3. MARCOS REGULATÓRIOS, NORMATIVOS E REFERÊNCIAS	11
3.1 Leis e Decretos	11
3.2 Normas e Frameworks	11
3.3 Regulamentação Setorial	11
4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO	11
4.1 Confidencialidade	11
4.2 Integridade	11
4.3 Disponibilidade	12
4.4 Autenticidade	12
4.5 Não Repúdio	12
4.6 Privacidade e Proteção de Dados Pessoais	12
4.7 Gestão Baseada em Risco	12
4.8 Criptografia Transversal	12
5. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA	12
5.1 Modelo de Governança	12
5.2 Papel da Alta Direção e do Conselho	12
5.3 Estrutura de CISO, DPO e Comitês	13
5.4 Integração com a Governança Corporativa	13
5.5 Matriz de Responsabilidades (RACI)	13
5.6 Artefatos Mandatórios do SGSI	13
6. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO	14
6.1 Metodologia de Avaliação de Riscos	14
6.2 Identificação e Propriedade de Ativos, Ameaças e Vulnerabilidades	14
6.3 Análise e Tratamento de Riscos	14
6.4 Aceitação, Mitigação e Monitoramento	14
6.5 Registro e Revisão Periódica dos Riscos	14
7. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO	15
7.1 Classes de Informação	15
7.2 Regras de Rotulagem	15
7.3 Tratamento Conforme Classificação	15
7.4 Proteção de Dados Pessoais no Contexto da Classificação da Informação	15
7.5 Ciclo de Vida da Informação	15

8. PROTEÇÃO DE ATIVOS E SEGURANÇA FÍSICA	15
8.1 Segurança Física das Instalações	15
8.2 Controle de Acesso Físico	15
8.3 Proteção de Equipamentos e Mídias	15
8.4 Política de Mesa Limpa e Tela Limpa	16
8.5 Descarte Seguro	16
8.6 Identificação Visual, Credenciais e Crachá	16
9. USO ACEITÁVEL DE TECNOLOGIAS	16
9.1 Uso de E-mail Corporativo	16
9.2 Uso da Internet	16
9.3 Uso de Mídias Sociais	16
9.4 Uso de Softwares de Mensageria	16
9.5 Uso de Mídias Removíveis	17
9.6 Uso de Computadores e Laptops	17
9.7 Uso de Dispositivos Móveis	17
9.8 Uso de Impressoras e Scanners	17
9.9 BYOD – Dispositivos Pessoais	17
9.10 Uso Seguro e Ético de Inteligência Artificial (IA Generativa)	17
10. SEGURANÇA LÓGICA, TECNOLÓGICA E OPERACIONAL	17
10.1 Princípios de Arquitetura Zero Trust	17
10.2 Gestão de Identidades e Acessos (IAM)	18
10.3 Privilégio Mínimo e Segregação de Funções	18
10.4 Segurança de Redes e Perímetro	18
10.5 Acessos Remotos e VPN	18
10.6 Segurança em Nuvem	18
10.7 Desenvolvimento Seguro de Sistemas (SSDLC)	18
10.8 Gestão de Vulnerabilidades e Atualizações	18
10.9 Registro de Logs, Monitoramento e Auditoria	19
10.10 Segurança de Roteamento e Infraestrutura de Rede do Operador (ISP)	19
10.11 Segurança de IPv6	19
10.12 Segurança de DNS (Autoritativo/Recursivo)	19
10.13 Criptografia e Gestão de Chaves	19
10.14 Gestão de Mudanças	20
11. PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS	20
11.1 Malware, Ransomware e Phishing	20
11.2 Engenharia Social	20
11.3 Monitoramento e Detecção	20
11.4 Testes de Segurança e Avaliações Técnicas	20
11.5 Ameaças à Cadeia de Suprimentos	21
11.6 Ataques de Negação de Serviço (DoS/DDoS)	21
12. BACKUP, RETENÇÃO E RECUPERAÇÃO DA INFORMAÇÃO	21
12.1 Política de Backup	21
12.2 Retenção e Proteção de Cópias	21
12.3 Testes Periódicos de Restauração	21

12.4 Recuperação de Dados e Sistemas	21
12.5 Retenção Legal e Corporativa de Registros e Logs	21
13. CONTINUIDADE DE NEGÓCIOS E RESILIÊNCIA	22
13.1 Análise de Impacto no Negócio (BIA)	22
13.2 Serviços e Ativos Críticos	22
13.3 Planos de Continuidade	22
13.4 Recuperação de Desastres	22
13.5 Resiliência Cibernética	22
13.6 SLA, Qualidade, RTO e RPO	22
14. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	23
14.1 Definição, Classificação e Severidade de Incidentes	23
14.2 Comunicação e Notificação	23
14.3 Resposta, Contenção e Erradicação	23
14.4 Comunicação com Autoridades	23
14.5 Lições Aprendidas e Melhoria Contínua	23
15. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS (LGPD)	23
15.1 Princípios da LGPD	23
15.2 Bases Legais de Tratamento	23
15.3 Direitos dos Titulares	24
15.4 Relatório de Impacto à Proteção de Dados (RIPD)	24
15.5 Incidentes Envolvendo Dados Pessoais	24
15.6 Papel do Encarregado pelo Tratamento de Dados (DPO)	24
16. GESTÃO DE PESSOAS, CONSCIENTIZAÇÃO E COMPORTAMENTO	24
16.1 Treinamento e Capacitação Contínua	24
16.2 Termos de Confidencialidade	24
16.3 Responsabilidades Individuais	24
16.4 Gestão de Acessos em Admissões, Mudanças e Desligamentos	25
16.5 Campanhas de Simulação e Testes Comportamentais	25
16.6 Triagem e Verificação de Antecedentes (Background Checks)	25
17. GESTÃO DE TERCEIROS E CADEIA DE SUPRIMENTOS	25
17.1 Avaliação de Riscos de Terceiros	25
17.2 Requisitos Contratuais de Segurança	25
17.3 Monitoramento Contínuo	25
17.4 Responsabilidade Solidária e Compartilhada	25
18. CONFORMIDADE, AUDITORIA E MELHORIA CONTÍNUA	26
18.1 Conformidade Legal e Regulatória	26
18.2 Auditorias Internas e Externas	26
18.3 Indicadores e Métricas de Segurança	26
18.4 Penalidades e Medidas Disciplinares	26
18.5 Gestão de Não Conformidades e Planos de Ação	26
19. EXCEÇÕES À POLÍTICA	26
19.1 Processo Formal de Exceções	26
19.2 Aprovação e Registro	27
19.3 Revisão Periódica das Exceções	27

20. REVISÃO, ATUALIZAÇÃO E VIGÊNCIA DA POLÍTICA	27
20.1 Periodicidade de Revisão	27
20.2 Controle de Versões	27
20.3 Vigência	27
APÊNDICE A — Glossário de Termos Técnicos e Definições	28
APÊNDICE B — Documentos Correlatos do SGSI	34

1. OBJETIVO

1.1 Finalidade da Política

Esta Política de Segurança da Informação e Cibersegurança tem como finalidade estabelecer princípios, diretrizes, responsabilidades e requisitos mínimos para a proteção das informações, dos ativos de informação e dos ambientes tecnológicos da organização, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e privacidade das informações, independentemente de sua forma, meio ou ciclo de vida.

1.2 Alinhamento com os Objetivos Estratégicos do Negócio

A presente Política está alinhada aos objetivos estratégicos, à governança corporativa e ao modelo de gestão de riscos da organização, contribuindo para a sustentabilidade do negócio, a continuidade das operações, a preservação da reputação institucional e o atendimento às exigências legais, regulatórias, contratuais e normativas aplicáveis. A organização define e mantém objetivos de segurança da informação SMART (Specific, Measurable, Achievable, Relevant, Time-bound), formalmente documentados e revisados no mínimo anualmente pela Alta Direção, para direcionar a melhoria contínua do SGSI.

1.3 Proteção da Informação como Ativo Corporativo

A informação é reconhecida como um ativo corporativo essencial, devendo ser protegida contra acessos não autorizados, uso indevido, divulgação indevida, alteração, destruição ou indisponibilidade, de forma proporcional ao seu valor, criticidade, sensibilidade e impacto ao negócio.

1.4 Estrutura e Hierarquia dos Documentos desta Política

Esta Política de Segurança da Informação e Cibersegurança é um documento de nível estratégico e de alto nível. Ela estabelece os "o quê" e "porquê" da segurança da informação na organização e é desdobrada obrigatoriamente em Normas Corporativas, que definem regras mandatórias e requisitos mínimos, e em Procedimentos Operacionais (POPs), que descrevem o "como fazer" para garantir a implementação, execução e evidência dos controles de segurança. Esta estrutura visa garantir a agilidade na atualização e a clareza para diferentes públicos. O não cumprimento das Normas e Procedimentos vinculados a esta Política caracteriza não conformidade e está sujeito às medidas disciplinares previstas.

2. ESCOPO E ABRANGÊNCIA

2.1 Abrangência Organizacional

Esta Política aplica-se a todas as unidades organizacionais, áreas de negócio, subsidiárias, filiais, controladas e demais estruturas sob responsabilidade da organização, no território nacional ou internacional.

2.2 Abrangência Tecnológica

Esta Política abrange todos os ambientes tecnológicos utilizados pela organização, incluindo, mas não se limitando a:

- Tecnologia da Informação (TI);
- Tecnologia Operacional (OT);
- Ambientes em nuvem;
- Infraestruturas híbridas;
- Dispositivos móveis;
- Internet das Coisas (IoT);
- Sistemas próprios ou de terceiros.

2.3 Abrangência de Dados e Informações

Esta Política aplica-se a todas as informações sob responsabilidade da organização, independentemente do formato (digital ou físico), meio de armazenamento, processamento, transmissão ou compartilhamento, incluindo dados pessoais e dados pessoais sensíveis.

2.4 Aplicabilidade a Colaboradores, Terceiros e Parceiros

Esta Política é de observância obrigatória por:

- Colaboradores, empregados, estagiários e aprendizes;
- Administradores, conselheiros e dirigentes;
- Prestadores de serviços, fornecedores, parceiros e terceiros;
- Qualquer pessoa física ou jurídica que tenha acesso às informações ou ativos da organização.

2.5 Exclusões e Exceções Formais

Qualquer exceção ao cumprimento desta Política é formalmente solicitada, justificada, avaliada sob a ótica de risco, aprovada pela autoridade competente e registrada, conforme o processo de exceções estabelecido nesta Política.

2.6 Declaração de Aplicabilidade (SoA)

O escopo do Sistema de Gestão de Segurança da Informação (SGSI) da Brphonia está formalmente definido e é mantido em uma Declaração de Aplicabilidade (SoA), que inclui as interfaces, exclusões justificadas e o mapeamento dos controles da ABNT NBR ISO/IEC 27002 aplicáveis, servindo como documento de referência obrigatório para auditorias e certificações.

3. MARCOS REGULATÓRIOS, NORMATIVOS E REFERÊNCIAS

3.1 Leis e Decretos

Esta Política observa a legislação e os decretos relacionados à segurança da informação, cibersegurança, privacidade e proteção de dados, incluindo, mas não se limitando a:

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 12.965/2014 - Marco Civil da Internet;
- Decreto nº 8.771/2016 - Regulamentação do Marco Civil da Internet;
- Decreto nº 11.856/2023 - Política Nacional de Cibersegurança (PNCiber);
- Decreto nº 12.573/2025 - Estratégia Nacional de Cibersegurança (E-Ciber);
- Lei nº 12.737/2012 - Tipificação de delitos informáticos (Lei “Carolina Dieckmann”);

3.2 Normas e Frameworks

Esta Política está alinhada às seguintes normas, padrões e frameworks de boas práticas:

- ABNT NBR ISO/IEC 27001:2022 - Sistemas de Gestão da Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2022 – Controles de Segurança da Informação;
- NIST Cybersecurity Framework (CSF) 2.0;
- CIS Critical Security Controls – versão 8.

3.3 Regulamentação Setorial

Esta Política observa ainda a:

- Resolução Anatel nº 740/2020 – Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações.

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação e a cibersegurança na organização são orientadas pelos seguintes princípios:

4.1 Confidencialidade

Garantia de que a informação seja acessada apenas por pessoas, sistemas ou processos devidamente autorizados.

4.2 Integridade

Garantia de que a informação seja protegida contra alterações não autorizadas ou acidentais, preservando sua exatidão e completude.

4.3 Disponibilidade

Garantia de que a informação e os serviços associados estejam acessíveis e utilizáveis sempre que necessários, conforme requisitos do negócio.

4.4 Autenticidade

Garantia da identificação inequívoca das partes envolvidas nos processos de comunicação e acesso à informação.

4.5 Não Repúdio

Garantia de que ações realizadas em sistemas e informações possam ser atribuídas de forma inequívoca aos seus autores.

4.6 Privacidade e Proteção de Dados Pessoais

Garantia de que o tratamento de dados pessoais observe os princípios, direitos e obrigações previstos na legislação aplicável, em especial a LGPD.

4.7 Gestão Baseada em Risco

Adoção de medidas de segurança proporcionais aos riscos identificados, considerando impactos operacionais, legais, regulatórios, financeiros e reputacionais.

4.8 Criptografia Transversal

A criptografia é um controle fundamental para proteger a confidencialidade e a integridade de dados sensíveis e críticos, tanto em repouso quanto em trânsito, sendo aplicada em todos os sistemas e ambientes da organização onde a avaliação de risco determina sua necessidade, conforme diretrizes estabelecidas em norma específica.

5. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

5.1 Modelo de Governança

A organização estabelece um modelo de governança de segurança da informação e cibersegurança que assegura:

- Direcionamento estratégico;
- Definição clara de responsabilidades;
- Supervisão e monitoramento contínuos;
- Integração com a governança corporativa.

5.2 Papel da Alta Direção e do Conselho

A Alta Direção e, quando aplicável, o Conselho de Administração são responsáveis por:

- Aprovar esta Política e suas revisões;

- Garantir recursos adequados para sua implementação;
- Patrocinar a cultura de segurança da informação;
- Supervisionar a gestão de riscos cibernéticos.

Além disso, a Alta Direção realiza análises críticas do SGSI (Management Review) no mínimo anualmente, conforme cadência definida em procedimento específico, para garantir sua adequação, eficácia e melhoria contínua, considerando o desempenho de segurança, incidentes, resultados de auditorias, feedback de partes interessadas e a eficácia das ações corretivas.

5.3 Estrutura de CISO, DPO e Comitês

A organização designa:

- Um responsável pela segurança da informação e cibersegurança (CISO);
- Um Encarregado pelo Tratamento de Dados Pessoais (DPO), conforme a LGPD;
- Comitês ou fóruns de governança para apoio à tomada de decisão, quando houver justificativa formal e aprovada para sua constituição.

Independentemente da existência de comitês formais, a Brphonia assegura que as responsabilidades de direção, supervisão e revisão do SGSI são atribuídas, executadas e evidenciadas por meio de papéis e rotinas formalizadas. A organização também garante a adequada segregação de funções e/ou implementa controles compensatórios robustos e documentados para mitigar riscos de conflito de interesse em posições que acumulam responsabilidades de CISO e DPO.

5.4 Integração com a Governança Corporativa

A governança de segurança da informação e cibersegurança integra-se aos processos de governança corporativa, gestão de riscos, conformidade, auditoria e continuidade de negócios.

5.5 Matriz de Responsabilidades (RACI)

As responsabilidades relativas à segurança da informação e à cibersegurança estão formalmente definidas e são mantidas atualizadas, com evidências da sua revisão e comunicação, por meio de uma matriz RACI, assegurando clareza quanto aos papéis de responsáveis, executores, consultados e informados.

5.6 Artefatos Mandatórios do SGSI

A gestão da segurança da informação e cibersegurança é suportada pelos seguintes artefatos mandatórios, cujos critérios, responsabilidades, cadência de revisão e evidências aceitáveis estão definidos em normas e procedimentos específicos:

- Registro de Riscos;
- Critérios de avaliação e aceitação de riscos;
- Plano de Tratamento de Riscos;
- Declaração de Aplicabilidade (SoA);
- Programa de Auditoria Interna;

- Atas e registros das Análises Críticas pela Direção (Management Review);
 - Registro e Gestão de Não Conformidades.
-

6. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

6.1 Metodologia de Avaliação de Riscos

A organização adota e mantém uma metodologia formal de gestão de riscos de segurança da informação e cibersegurança, baseada em boas práticas reconhecidas, que permite identificar, analisar, avaliar, tratar e monitorar riscos de forma contínua e documentada. Os critérios de risco (probabilidade e impacto) e de aceitação de risco estão formalmente definidos e aprovados pela Alta Direção.

6.2 Identificação e Propriedade de Ativos, Ameaças e Vulnerabilidades

São identificados, classificados e mantidos inventários atualizados de todos os ativos de informação, incluindo dados, sistemas, infraestruturas (físicas e lógicas, incluindo as de rede core/ISP), ambientes de nuvem, IoT, OT e serviços, bem como as ameaças e vulnerabilidades associadas, considerando fatores tecnológicos, humanos, físicos e organizacionais.

Cada ativo de informação possui um proprietário (owner) formalmente designado, que é responsável por sua proteção ao longo de todo o ciclo de vida. O inventário de ativos contém informações como classificação, criticidade, localização e ciclo de vida, sendo mantido em uma fonte de verdade (ex: CMDB).

A Infraestrutura Crítica de Telecom está formalmente categorizada como uma classe de ativo crítico, sujeita a requisitos mínimos mandatórios de hardening, controle de acesso, gestão de mudanças, logging e segregação lógica e física.

6.3 Análise e Tratamento de Riscos

Os riscos identificados são analisados quanto à probabilidade e impacto, e tratados por meio de medidas de mitigação, aceitação, transferência ou eliminação, conforme critérios definidos e aprovados.

6.4 Aceitação, Mitigação e Monitoramento

A aceitação de riscos é formal, restrita e baseada em justificativa e avaliação documentada, com definição de responsáveis e prazos de revisão. Riscos mitigados possuem plano de ação, evidências e acompanhamento contínuo.

6.5 Registro e Revisão Periódica dos Riscos

Os riscos de segurança da informação e cibersegurança são registrados em repositório oficial (Registro de Riscos) e revisados no mínimo anualmente, ou sempre que ocorrerem mudanças relevantes no ambiente de negócio, tecnologia, ameaças ou regulamentação.

7. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

7.1 Classes de Informação

A organização estabelece e mantém classes de informação e critérios de classificação compatíveis com o impacto ao negócio, requisitos legais, regulatórios e contratuais.

7.2 Regras de Rotulagem

As informações são devidamente rotuladas conforme sua classificação, de modo a orientar o tratamento adequado durante todo o seu ciclo de vida.

7.3 Tratamento Conforme Classificação

O acesso, o uso, o armazenamento, o compartilhamento, a transmissão e o descarte das informações observam as regras definidas para cada classe de informação, incluindo controles técnicos e administrativos apropriados.

7.4 Proteção de Dados Pessoais no Contexto da Classificação da Informação

Os dados pessoais e dados pessoais sensíveis recebem tratamento compatível com sua classificação e com os requisitos legais aplicáveis, garantindo medidas de segurança adequadas à prevenção de acessos não autorizados, incidentes e violações de dados.

7.5 Ciclo de Vida da Informação

A informação é protegida durante todo o seu ciclo de vida, desde a criação ou coleta até o descarte, assegurando controles adequados em cada fase.

8. PROTEÇÃO DE ATIVOS E SEGURANÇA FÍSICA

8.1 Segurança Física das Instalações

A organização implementa controles de segurança física para proteger suas instalações contra acessos não autorizados, danos, interferências e ameaças ambientais.

8.2 Controle de Acesso Físico

O acesso físico a áreas críticas ou restritas é controlado, monitorado e registrado, utilizando mecanismos apropriados de autenticação e autorização.

8.3 Proteção de Equipamentos e Mídias

Equipamentos, documentos e mídias que contêm informações da organização são protegidos contra perda, roubo, dano ou uso indevido, inclusive durante transporte e

armazenamento. Regras para devolução de ativos no desligamento de colaboradores estão formalizadas em procedimento específico.

8.4 Política de Mesa Limpa e Tela Limpa

São adotadas práticas de mesa limpa e tela limpa, com o objetivo de reduzir o risco de acesso não autorizado a informações, especialmente em ambientes compartilhados ou de acesso público.

8.5 Descarte Seguro

O descarte de documentos, mídias e equipamentos que contêm informações é realizado de forma segura, garantindo a irrecuperabilidade dos dados, conforme procedimentos definidos.

8.6 Identificação Visual, Credenciais e Crachá

São utilizados mecanismos adequados de identificação visual e credenciais para controle de acesso às dependências da organização, observadas regras claras de uso e proteção. O uso de crachá é obrigatório para todos os colaboradores e terceiros.

9. USO ACEITÁVEL DE TECNOLOGIAS

9.1 Uso de E-mail Corporativo

O e-mail corporativo é utilizado exclusivamente para fins profissionais, sendo vedado o uso indevido, ilegal ou que possa comprometer a segurança da informação ou a imagem da organização. É expressamente proibido o tratamento de dados de clientes, colaboradores, terceiros e fornecedores da Brphonia por meio de contas de email particulares, ainda que instaladas ou acessadas em dispositivos corporativos.

9.2 Uso da Internet

O acesso à internet observa as políticas internas, sendo proibido o acesso a conteúdos ilícitos, inseguros ou incompatíveis com as atividades profissionais.

9.3 Uso de Mídias Sociais

A utilização de mídias sociais respeita as diretrizes corporativas, preservando a confidencialidade das informações e a reputação institucional.

9.4 Uso de Softwares de Mensageria

Ferramentas de mensageria são utilizadas de forma responsável, sendo vedado o compartilhamento não autorizado de informações corporativas. É expressamente proibido o tratamento de dados de clientes, colaboradores, terceiros e fornecedores da Brphonia por meio de contas ou aplicações de mensageria particular, ainda que instaladas ou acessadas em dispositivos corporativos.

9.5 Uso de Mídias Removíveis

É expressamente proibido o uso de mídias removíveis pessoais. O uso de mídias removíveis corporativas é estritamente controlado e autorizado, mediante a aplicação de medidas de segurança que mitigam riscos de perda, vazamento de dados ou contaminação por softwares maliciosos.

9.6 Uso de Computadores e Laptops

Os equipamentos computacionais são utilizados conforme as diretrizes corporativas, mantendo configurações seguras e protegidos contra uso indevido.

9.7 Uso de Dispositivos Móveis

O uso de dispositivos móveis observa controles de segurança compatíveis com os riscos associados, incluindo autenticação, criptografia e gerenciamento remoto, conforme diretrizes da norma específica.

9.8 Uso de Impressoras e Scanners

A utilização de impressoras e scanners é realizada de forma a evitar exposição indevida de informações, observando práticas seguras de manuseio e descarte.

9.9 BYOD – Dispositivos Pessoais

O uso de dispositivos pessoais para fins corporativos é previamente autorizado e condicionado ao cumprimento de requisitos mínimos de segurança definidos pela organização. Os requisitos de segurança, processo de autorização e formalização estão detalhados em norma e procedimento correlatos.

9.10 Uso Seguro e Ético de Inteligência Artificial (IA Generativa)

O uso de soluções de inteligência artificial, incluindo IA generativa, observa princípios éticos, legais e de segurança. É expressamente proibida a inserção de informações confidenciais, credenciais de acesso ou dados pessoais durante o uso dessas ferramentas. A organização incentiva a conscientização contínua sobre os riscos da IA Generativa e a necessidade de diretrizes de uso ético e seguro, através de guias internos de boas práticas e treinamentos.

10. SEGURANÇA LÓGICA, TECNOLÓGICA E OPERACIONAL

10.1 Princípios de Arquitetura Zero Trust

A organização adota e implementa princípios de arquitetura Zero Trust, baseados na premissa de “nunca confiar, sempre verificar”, aplicando controles de verificação contínua de identidade, contexto e acesso.

10.2 Gestão de Identidades e Acessos (IAM)

Os acessos a sistemas e informações são concedidos com base em identidades individualizadas, devidamente autenticadas e autorizadas, seguindo critérios formais de concessão, revisão e revogação. É mandatório o uso de Autenticação Multifator (MFA) para acesso a: e-mail corporativo, VPN/acesso remoto, consoles de gestão em nuvem, contas privilegiadas e servidores bastion/jump server. A recertificação de acessos é realizada no mínimo trimestralmente para contas privilegiadas e semestralmente para as demais contas, ou conforme risco superior justificado. Requisitos de senhas/chaves, processos de Joiner/Mover/Leaver (JML) com prazos estabelecidos, controle de contas privilegiadas e uso obrigatório de bastion/jump server para administração de infraestrutura crítica estão detalhados em norma específica.

10.3 Privilégio Mínimo e Segregação de Funções

Os acessos são concedidos com base no princípio do privilégio mínimo e na segregação de funções, reduzindo o risco de uso indevido ou fraude.

10.4 Segurança de Redes e Perímetro

As redes corporativas são protegidas por controles adequados de segmentação, monitoramento e proteção contra acessos não autorizados e ataques cibernéticos. Para ambientes de rede do operador (core, borda, distribuição, acesso e ambientes de suporte), controles específicos estão detalhados em norma correlata.

10.5 Acessos Remotos e VPN

Os acessos remotos são realizados por meio de mecanismos seguros, incluindo autenticação forte e uso de redes privadas virtuais (VPN), conforme diretrizes estabelecidas em norma específica.

10.6 Segurança em Nuvem

Os ambientes em nuvem observam controles de segurança compatíveis com os riscos associados, incluindo responsabilidades compartilhadas entre a organização e os provedores de serviço.

10.7 Desenvolvimento Seguro de Sistemas (SSDLC)

O desenvolvimento, aquisição e manutenção de sistemas seguem práticas de desenvolvimento seguro, incorporando requisitos de segurança desde as fases iniciais do ciclo de vida.

10.8 Gestão de Vulnerabilidades e Atualizações

São implementados processos para identificação, avaliação, correção e monitoramento de vulnerabilidades, bem como para a aplicação tempestiva de atualizações e correções de segurança. Os detalhes de gestão de vulnerabilidades e atualizações para infraestrutura de rede do operador, incluindo classificação por criticidade, prazos máximos de aplicação,

acompanhamento de boletins de segurança e tratamento de equipamentos End-of-Life, estão definidos em norma correlata.

10.9 Registro de Logs, Monitoramento e Auditoria

Os sistemas e ambientes tecnológicos mantêm registros de eventos e atividades relevantes, possibilitando monitoramento contínuo, detecção de incidentes e suporte a auditorias e investigações. Os logs críticos de segurança têm sua integridade assegurada por mecanismos de hash/assinatura ou imutabilidade (WORM) e possuem acesso restrito com trilha de auditoria, conforme diretrizes do Decreto nº 8.771/2016.

Os detalhes sobre eventos mínimos a serem logados para cada classe de sistema/serviço, o responsável pela guarda, o repositório oficial, controle de acesso estrito aos logs, preservação de integridade, rastreabilidade e retenção, incluindo uma matriz corporativa de retenção para diferentes tipos de logs (segurança, autenticação, administração, SIEM, backups, evidências de incidente) e métodos de descarte seguro, estão definidos em norma correlata. **Qualquer exceção aos requisitos de logging e retenção deve seguir o processo formal de gestão de exceções.**

10.10 Segurança de Roteamento e Infraestrutura de Rede do Operador (ISP)

A organização implementa e evidencia controles robustos de segurança de roteamento e engenharia de tráfego, conforme as melhores práticas e padrões da indústria para ISPs (e.g., BGP, RPKI, MANRS, IX.br), detalhados em Normas Corporativas específicas. As ações MANRS são implementadas de forma obrigatória, dada a adesão da Brphonia à iniciativa, e qualquer justificativa para não aplicação pontual de alguma ação está formalmente documentada e baseada em avaliação de risco. A proteção da Infraestrutura Crítica de Telecom é um requisito mandatório.

10.11 Segurança de IPv6

É obrigatório considerar IPv6 no modelo de segurança de redes, garantindo política formal de endereçamento e alocação IPv6, controles de camada 2/3 para IPv6, revisão de regras de firewall e inspeção para dual-stack, e logs e telemetria contemplando eventos relevantes em IPv6.

10.12 Segurança de DNS (Autoritativo/Recursivo)

Para serviços DNS sob responsabilidade da Brphonia, é obrigatório segmentar e proteger ambientes de DNS autoritativo e recursivo, proteger contra abuso, e manter governança e integridade de zonas e alterações. A implementação de DNSSEC para domínios/zona(s) sob gestão da organização é realizada com base em avaliação de criticidade e viabilidade técnica formalmente documentada.

10.13 Criptografia e Gestão de Chaves

A organização implementa controles criptográficos para proteger a confidencialidade e integridade da informação sensível e crítica. A criptografia é obrigatória para: backups de sistemas e dados, notebooks e dispositivos móveis corporativos, dados pessoais e sensíveis em repouso (armazenados), e uso de TLS (Transport Layer Security) para todo

tráfego administrativo e aplicações web sensíveis/públicas. Uma política de criptografia abrangente está definida, estabelecendo onde a criptografia é obrigatória, os algoritmos mínimos aprovados, a gestão segura de chaves (incluindo KMS/HSM, rotação e segregação de funções), a obrigatoriedade do uso de TLS e os critérios para exceções. **Qualquer exceção aos requisitos de criptografia ou uso de TLS deve seguir o processo formal de gestão de exceções.**

10.14 Gestão de Mudanças

Todas as mudanças em sistemas, configurações de rede (incluindo roteadores, switches, firewalls), regras de firewall, políticas de IAM, configurações de ambientes em nuvem e pipelines de desenvolvimento são submetidas a um processo formal de gestão de mudanças. Este processo inclui planejamento, avaliação de impacto, aprovação formal, janela de manutenção, plano de rollback, testes e registro de evidências, visando minimizar riscos e garantir a estabilidade e segurança dos serviços. A gestão de mudanças é um requisito mandatório para a Infraestrutura Crítica de Telecom.

11. PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

11.1 Malware, Ransomware e Phishing

A organização adota medidas técnicas e administrativas para prevenir, detectar e mitigar ameaças cibernéticas, incluindo, mas não se limitando a malware, ransomware, phishing e outras formas de código ou atividade maliciosa.

11.2 Engenharia Social

São implementadas ações preventivas e educativas para reduzir riscos associados a técnicas de engenharia social, incluindo campanhas de conscientização, controles de verificação e procedimentos de validação de solicitações sensíveis.

11.3 Monitoramento e Detecção

A organização mantém mecanismos de monitoramento contínuo para detecção tempestiva de eventos e atividades suspeitas, alinhados às boas práticas de detecção previstas em frameworks reconhecidos de cibersegurança.

11.4 Testes de Segurança e Avaliações Técnicas

Testes de segurança, tais como varreduras de vulnerabilidades, testes de intrusão (pentests) e avaliações técnicas, são realizados no mínimo anualmente, ou conforme definido em norma específica, com o objetivo de identificar fragilidades e melhorar continuamente a postura de segurança.

11.5 Ameaças à Cadeia de Suprimentos

Os riscos associados à cadeia de suprimentos são considerados na gestão de ameaças cibernéticas, incluindo dependências tecnológicas, fornecedores críticos e componentes de terceiros.

11.6 Ataques de Negação de Serviço (DoS/DDoS)

Considerando a criticidade de disponibilidade para operações de telecomunicações/ISP, ataques DoS/DDoS são tratados como ameaça prioritária. A organização mantém capacidade de detecção e resposta a DDoS, estabelece estratégia de mitigação, adota mecanismos operacionais de mitigação por roteamento (RTBH/Flowspec) e mantém registros e evidências de ataques. Os detalhes operacionais e as condições para aplicação de cada mecanismo estão formalizados em norma correlata. A proteção contra ataques DoS/DDoS é um requisito mandatório para a Infraestrutura Crítica de Telecom.

12. BACKUP, RETENÇÃO E RECUPERAÇÃO DA INFORMAÇÃO

12.1 Política de Backup

A organização mantém uma política formal de backup que assegura a cópia periódica e confiável das informações e sistemas críticos, de acordo com requisitos do negócio e critérios de risco.

12.2 Retenção e Proteção de Cópias

As cópias de backup são protegidas contra acessos não autorizados, alteração, perda ou destruição, incluindo armazenamento seguro, segregação e, quando aplicável, criptografia.

12.3 Testes Periódicos de Restauração

Testes de restauração são realizados no mínimo trimestralmente, ou conforme definido em procedimento específico, para verificar a integridade, a confiabilidade e a efetividade dos processos de backup e recuperação.

12.4 Recuperação de Dados e Sistemas

Os procedimentos de recuperação asseguram a restauração tempestiva de dados e sistemas, minimizando impactos operacionais e garantindo a continuidade das atividades essenciais.

12.5 Retenção Legal e Corporativa de Registros e Logs

Além das regras corporativas de backup e retenção, é obrigatório cumprir os prazos e requisitos legais aplicáveis para guarda de registros no contexto de provimento de conexão e aplicações (Marco Civil da Internet). Está definida e mantida uma matriz corporativa de retenção, que abrange não apenas os logs do Marco Civil, mas também logs de segurança, autenticação, administração, SIEM, backups e evidências de incidentes, com prazos

específicos para cada classe e métodos de descarte seguro (incluindo WORM/imutabilidade quando aplicável). Os logs críticos de segurança têm sua integridade assegurada por mecanismos de hash/assinatura ou imutabilidade (WORM) e possuem acesso restrito com trilha de auditoria.

13. CONTINUIDADE DE NEGÓCIOS E RESILIÊNCIA

13.1 Análise de Impacto no Negócio (BIA)

A organização realiza análises de impacto no negócio para identificar processos, serviços e ativos críticos, bem como os impactos decorrentes de interrupções.

13.2 Serviços e Ativos Críticos

Os serviços e ativos críticos são identificados, priorizados e protegidos de forma proporcional à sua importância para a continuidade das operações.

13.3 Planos de Continuidade

São elaborados, mantidos e testados planos de continuidade de negócios, assegurando a capacidade de resposta a eventos adversos, inclusive incidentes cibernéticos.

13.4 Recuperação de Desastres

A organização mantém planos de recuperação de desastres que contemplem cenários plausíveis de falhas, indisponibilidades e incidentes graves, com definição clara de responsabilidades e tempos objetivos de recuperação.

13.5 Resiliência Cibernética

A resiliência cibernética é promovida por meio da capacidade de antecipar, resistir, responder e se recuperar de incidentes cibernéticos, assegurando a continuidade dos serviços essenciais.

13.6 SLA, Qualidade, RTO e RPO

Para serviços críticos e serviços regulados, é obrigatório definir e manter documentados SLA (Service Level Agreement) e parâmetros de qualidade, alinhados ao regulamento de qualidade aplicável e compromissos contratuais; definir e manter documentados RTO (Recovery Time Objective) e RPO (Recovery Point Objective) por serviço/processo crítico, aprovados pela Alta Direção, e referenciados nos planos de continuidade e recuperação; e garantir que testes de continuidade/DR validem os RTO/RPO definidos e gerem evidências auditáveis.

14. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

14.1 Definição, Classificação e Severidade de Incidentes

A organização estabelece critérios formais para definição, identificação, classificação por severidade (com impacto, criticidade e abrangência) e tratamento de incidentes de segurança da informação e cibersegurança. O tempo máximo para triagem, critérios para ativação de equipes de plantão (on-call) e as condições que caracterizam um "incidente maior" estão definidos.

14.2 Comunicação e Notificação

Os incidentes de segurança são comunicados e registrados de forma tempestiva, observando fluxos internos de escalonamento e, quando aplicável, obrigações legais e regulatórias de notificação.

14.3 Resposta, Contenção e Erradicação

A organização mantém procedimentos para resposta a incidentes, incluindo ações de contenção, erradicação das causas e mitigação de impactos, de forma coordenada e documentada. Os requisitos mínimos de evidência (linha do tempo, impacto, RCA - Análise de Causa Raiz) para cada tipo de incidente estão definidos.

14.4 Comunicação com Autoridades

A organização comunica incidentes às autoridades competentes (ANPD, Anatel, CERT.br, etc.) nos prazos e condições previstos na legislação e regulamentação aplicáveis. Os detalhes sobre os canais, procedimentos de reporte e cooperação, prazos de notificação, modelos de comunicação e responsáveis por cada tipo de notificação estão formalizados em norma e procedimento operacional correlato.

14.5 Lições Aprendidas e Melhoria Contínua

Após a resolução de incidentes relevantes, são conduzidas análises de lições aprendidas, com a implementação de ações corretivas e preventivas para evitar recorrências.

15. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS (LGPD)

15.1 Princípios da LGPD

O tratamento de dados pessoais observa os princípios previstos na legislação aplicável, incluindo finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização.

15.2 Bases Legais de Tratamento

O tratamento de dados pessoais somente ocorre com fundamento em bases legais válidas, devidamente identificadas e documentadas.

15.3 Direitos dos Titulares

A organização assegura mecanismos para o atendimento aos direitos dos titulares de dados pessoais, conforme previsto na legislação vigente.

15.4 Relatório de Impacto à Proteção de Dados (RIPD)

Quando aplicável, são elaborados relatórios de impacto à proteção de dados pessoais, com identificação de riscos e medidas de mitigação adequadas.

15.5 Incidentes Envolvendo Dados Pessoais

Os incidentes de segurança que envolvem dados pessoais são tratados de forma prioritária, com adoção de medidas para mitigação de danos e cumprimento das obrigações de comunicação previstas em lei.

15.6 Papel do Encarregado pelo Tratamento de Dados (DPO)

O Encarregado pelo Tratamento de Dados Pessoais atua como canal de comunicação entre a organização, os titulares de dados e a autoridade competente, conforme atribuições legais.

16. GESTÃO DE PESSOAS, CONSCIENTIZAÇÃO E COMPORTAMENTO

16.1 Treinamento e Capacitação Contínua

A organização promove treinamentos e ações contínuas de capacitação em segurança da informação, cibersegurança e proteção de dados pessoais, compatíveis com os riscos, funções exercidas e responsabilidades atribuídas a cada público interno.

16.2 Termos de Confidencialidade

Colaboradores, administradores, terceiros e demais pessoas com acesso às informações da organização firmam termos de confidencialidade e responsabilidade, conforme aplicável, comprometendo-se a observar esta Política e demais normativos internos.

16.3 Responsabilidades Individuais

Cada pessoa que tem acesso às informações ou ativos da organização é responsável por:

- Cumprir esta Política e normas correlatas;
- Proteger as informações sob sua responsabilidade;
- Comunicar imediatamente suspeitas ou ocorrências de incidentes de segurança;
- Realizar os treinamentos obrigatórios e participar de reuniões sobre temas relacionados a essa política.

16.4 Gestão de Acessos em Admissões, Mudanças e Desligamentos

Os acessos a sistemas e informações são concedidos, alterados ou revogados de forma tempestiva e controlada nos processos de admissão, movimentação interna e desligamento de pessoas. Os prazos e procedimentos para os processos de Joiner, Mover e Leaver (JML) estão detalhados em norma específica.

16.5 Campanhas de Simulação e Testes Comportamentais

A organização realiza campanhas de simulação, incluindo testes de phishing e engenharia social, com o objetivo de avaliar o nível de conscientização, reforçar boas práticas e aprimorar continuamente o comportamento seguro dos usuários.

16.6 Triagem e Verificação de Antecedentes (Background Checks)

São realizadas triagens e verificações de antecedentes (background checks) para colaboradores que ocupam cargos com acesso privilegiado, posições sensíveis ou que lidam com informações críticas, conforme as diretrizes e a legislação aplicável.

17. GESTÃO DE TERCEIROS E CADEIA DE SUPRIMENTOS

17.1 Avaliação de Riscos de Terceiros

A contratação e o relacionamento com terceiros consideram a avaliação dos riscos de segurança da informação e cibersegurança, especialmente quando houver acesso a informações, sistemas e infraestruturas críticas.

17.2 Requisitos Contratuais de Segurança

Os contratos firmados com terceiros contêm cláusulas específicas de segurança da informação, confidencialidade, proteção de dados pessoais, responsabilidade e obrigações de comunicação de incidentes, conforme aplicável.

17.3 Monitoramento Contínuo

O desempenho e a conformidade dos terceiros em relação aos requisitos de segurança são monitorados periodicamente, considerando o nível de risco associado à relação contratual.

17.4 Responsabilidade Solidária e Compartilhada

Quando aplicável, a organização observa a responsabilidade solidária ou compartilhada decorrente de relações contratuais e legais, especialmente no tratamento de dados pessoais e na prestação de serviços críticos.

18. CONFORMIDADE, AUDITORIA E MELHORIA CONTÍNUA

18.1 Conformidade Legal e Regulatória

A organização assegura a conformidade contínua com a legislação, regulamentações, normas e obrigações contratuais aplicáveis à segurança da informação, cibersegurança e proteção de dados pessoais.

18.2 Auditorias Internas e Externas

As auditorias internas de segurança da informação e cibersegurança são obrigatórias e são realizadas no mínimo anualmente; auditorias externas são conduzidas conforme critérios de risco, maturidade e exigências regulatórias aplicáveis. O programa de auditoria interna está formalmente documentado.

18.3 Indicadores e Métricas de Segurança

Indicadores e métricas (KPIs) estão definidos, são acompanhados e analisados para avaliar o desempenho da segurança da informação em relação aos objetivos de segurança da informação definidos, e apoiar a tomada de decisão pela Alta Direção. As metas, responsáveis e frequência de medição e revisão estão formalmente estabelecidos.

18.4 Penalidades e Medidas Disciplinares

O descumprimento desta Política pode resultar na aplicação de medidas disciplinares, sanções administrativas, contratuais ou legais, conforme a gravidade da infração e a legislação aplicável.

18.5 Gestão de Não Conformidades e Planos de Ação

As não conformidades identificadas são registradas, analisadas e tratadas por meio de planos de ação corretivos e preventivos, acompanhados até sua efetiva conclusão. O processo de gestão de não conformidades está formalmente documentado.

19. EXCEÇÕES À POLÍTICA

19.1 Processo Formal de Exceções

Exceções ao cumprimento desta Política somente são concedidas mediante solicitação formal, devidamente justificada e fundamentada em análise de risco formal e documentada. Toda exceção aprovada possui um prazo de expiração (sunset) definido, está acompanhada de controles compensatórios que são efetivamente implementados e monitorados, e possui um owner responsável formalmente atribuído, ciente de sua responsabilidade na gestão e monitoramento contínuo da exceção.

19.2 Aprovação e Registro

As exceções são avaliadas e aprovadas pela autoridade competente (CISO, Comitê de Segurança ou Alta Direção, conforme a materialidade do risco), registradas formalmente e revisadas periodicamente quanto à sua necessidade, validade e à eficácia dos controles compensatórios.

19.3 Revisão Periódica das Exceções

As exceções concedidas são revisadas em intervalos definidos (no mínimo anualmente) ou sempre que houver mudanças relevantes no contexto de risco, exigindo uma reavaliação completa de risco para sua continuidade. O owner responsável é diligente na revisão da necessidade e eficácia dos controles compensatórios, garantindo sua atualização e adequação.

20. REVISÃO, ATUALIZAÇÃO E VIGÊNCIA DA POLÍTICA

20.1 Periodicidade de Revisão

Esta Política é revisada no mínimo anualmente e sempre que ocorrerem mudanças relevantes no ambiente organizacional, tecnológico, regulatório ou de riscos.

20.2 Controle de Versões

As versões da Política são controladas, registrando-se histórico de alterações, datas de aprovação e responsáveis, garantindo a integridade e rastreabilidade do documento.

20.3 Vigência

Esta Política entra em vigor na data de sua aprovação pela Alta Direção e permanece válida até que seja formalmente revisada ou substituída.

Alexandre Luis Machado
Diretor Executivo Comercial

Eliseu Marafiga
Diretor Executivo de Infraestrutura

Fernando Krein Pinheiro
Encarregado do Tratamento Dados
Pessoais

Rodrigo Krein Pinheiro
Responsável pelo Comitê de Privacidade

APÊNDICE A — Glossário de Termos Técnicos e Definições

Este glossário tem por finalidade facilitar a compreensão dos termos técnicos utilizados nesta Política, servindo como referência para colaboradores, gestores, auditores e demais partes interessadas. Em caso de dúvida sobre a aplicação de um termo no contexto operacional, consulte a área de Segurança da Informação ou o DPO.

Anti-spoofing (BCP38/BCP84) Conjunto de boas práticas e filtros técnicos implementados em roteadores para impedir que pacotes com endereços IP de origem falsificados (forjados) trafeguem pela rede. O BCP38 e o BCP84 são documentos de melhores práticas da IETF amplamente adotados por operadoras responsáveis para mitigar ataques de negação de serviço e abuso de rede.

ASN — Autonomous System Number Número de Sistema Autônomo. Identificador numérico único atribuído a um conjunto de redes IP sob controle de uma única entidade (operadora, empresa ou organização) que define uma política de roteamento comum. A Brphonia opera com ASN próprio registrado junto ao NIC.br/LACNIC.

BGP — Border Gateway Protocol Protocolo de roteamento inter-domínio utilizado na Internet para troca de informações de alcançabilidade entre sistemas autônomos. É o protocolo responsável pelo roteamento global da Internet e, por sua criticidade, requer controles rigorosos de segurança, filtragem e governança.

BIA — Business Impact Analysis (Análise de Impacto no Negócio) Processo de identificação e avaliação dos impactos potenciais decorrentes de interrupções em processos, serviços e ativos críticos, utilizado como base para os planos de continuidade e recuperação de desastres.

CERT.br — Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil Grupo de resposta a incidentes de segurança mantido pelo NIC.br, responsável por tratar incidentes de segurança em redes conectadas à Internet no Brasil e promover a cultura de segurança na rede.

CGI.br — Comitê Gestor da Internet no Brasil Entidade responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordenando e integrando as iniciativas de serviços de Internet no país.

CISO — Chief Information Security Officer Responsável executivo pela segurança da informação e cibersegurança da organização. Pode ser denominado internamente como Coordenador ou Gestor de Segurança da Informação, mantendo as atribuições estratégicas e operacionais da função.

CMDB — Configuration Management Database Banco de dados que armazena informações sobre todos os componentes de um serviço de TI (itens de configuração) e as relações entre eles. Essencial para a gestão de ativos e serviços.

CVE — Common Vulnerabilities and Exposures Sistema de referência público para identificação e catalogação de vulnerabilidades de segurança conhecidas em softwares e

hardwares. Cada vulnerabilidade recebe um identificador único (ex.: CVE-2024-XXXX) utilizado para rastreamento e priorização de correções.

DDoS — Distributed Denial of Service Ataque de negação de serviço distribuído, no qual múltiplos sistemas comprometidos são utilizados simultaneamente para sobrecarregar um alvo (servidor, rede ou serviço), tornando-o indisponível para usuários legítimos.

DNSSEC — Domain Name System Security Extensions Extensão do protocolo DNS que adiciona autenticação criptográfica às respostas DNS, protegendo contra ataques de envenenamento de cache e falsificação de respostas de resolução de nomes.

DPO — Data Protection Officer (Encarregado pelo Tratamento de Dados Pessoais) Profissional designado pela organização, conforme exigência da LGPD, responsável por atuar como canal entre a organização, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

Dual-stack Configuração de rede na qual um dispositivo ou serviço opera simultaneamente com os protocolos IPv4 e IPv6, garantindo compatibilidade e transição entre as duas versões do protocolo de Internet.

End-of-Life / End-of-Support (EoL/EoS) Condição em que um equipamento ou software deixa de receber suporte ativo do fabricante, incluindo atualizações de segurança e correções de vulnerabilidades, representando risco elevado quando mantido em produção sem mitigações adequadas.

Firmware / NOS — Network Operating System Software embarcado em equipamentos de rede (roteadores, switches, firewalls) que controla suas funções operacionais. Atualizações de firmware são essenciais para correção de vulnerabilidades e manutenção da segurança dos equipamentos.

Flowspec Extensão do protocolo BGP (RFC 5575) que permite a distribuição de regras de filtragem de tráfego de forma dinâmica entre roteadores, utilizada principalmente para mitigação automatizada de ataques DDoS e anomalias de tráfego.

IAM — Identity and Access Management (Gestão de Identidades e Acessos) Conjunto de processos, políticas e tecnologias para gerenciar identidades digitais e controlar o acesso de usuários a sistemas, aplicações e dados, garantindo que apenas pessoas autorizadas acessem recursos específicos.

Infraestrutura Crítica de Telecom Ativos físicos e lógicos essenciais para a operação da Brphonia como Provedor de Serviços de Internet (ISP), incluindo roteadores de core e borda, switches, firewalls, sistemas de autenticação (AAA), sistemas de gestão de rede (NMS/telemetria) e pontos de presença. Tais ativos requerem medidas de segurança aprimoradas devido ao seu alto impacto na continuidade do negócio.

IRR — Internet Routing Registry Base de dados distribuída e pública onde operadoras registram suas políticas de roteamento, prefixos anunciados e objetos de roteamento (route objects, aut-num, as-set). A consistência entre IRR e operação BGP é fundamental para prevenção de vazamentos de rotas.

IPv6 — Internet Protocol version 6 Versão atual do protocolo de Internet, desenvolvida para substituir o IPv4, com espaço de endereçamento vastamente superior. A Brphonia possui certificação NIC.br de implementação IPv6 e opera em ambiente dual-stack.

IX.br / PTT.br — Internet Exchange Brasil / Ponto de Troca de Tráfego Infraestrutura neutra operada pelo NIC.br que permite a interconexão direta entre operadoras, provedores de conteúdo e outros participantes para troca de tráfego de Internet no Brasil, reduzindo custos e melhorando a qualidade das conexões.

JML — Joiner, Mover, Leaver Processos de gestão de identidade e acesso que abordam a criação de acessos para novos colaboradores (Joiner), modificação de acessos para colaboradores que mudam de função (Mover) e revogação de acessos para colaboradores que deixam a organização (Leaver).

KMS/HSM — Key Management System / Hardware Security Module Soluções tecnológicas para o gerenciamento seguro (criação, armazenamento, distribuição, rotação e revogação) de chaves criptográficas, essenciais para a proteção de dados.

LGPD — Lei Geral de Proteção de Dados Pessoais Lei nº 13.709/2018, que estabelece as regras para coleta, armazenamento, tratamento e compartilhamento de dados pessoais no Brasil, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade dos titulares.

MANRS — Mutually Agreed Norms for Routing Security Iniciativa global de segurança de roteamento que define um conjunto de ações concretas que operadoras de rede devem implementar para reduzir ameaças comuns de roteamento, como prefix hijacking, route leaks e spoofing. A Brphonia é membro do MANRS.

Marco Civil da Internet Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, incluindo obrigações de guarda de registros de conexão e acesso a aplicações por provedores.

MFA — Multi-Factor Authentication (Autenticação Multifator) Método de autenticação que exige a apresentação de dois ou mais fatores de verificação independentes (ex.: senha + token, senha + biometria) para acesso a sistemas, reduzindo significativamente o risco de acesso não autorizado.

NIC.br — Núcleo de Informação e Coordenação do Ponto BR Entidade civil, sem fins lucrativos, que implementa as decisões e projetos do CGI.br, sendo responsável pelo registro de domínios .br, distribuição de endereços IP no Brasil (junto ao LACNIC) e operação do IX.br e CERT.br.

NMS/Telemetria — Network Management System / Telemetry Sistemas e dados que permitem o monitoramento, gerenciamento e coleta de informações detalhadas sobre o desempenho e a saúde da rede, essenciais para a detecção de anomalias e incidentes.

OOB — Out-of-Band Management Rede ou canal de gerenciamento segregado e independente da rede de produção, utilizado para acesso administrativo a equipamentos críticos mesmo em situações de falha ou indisponibilidade da rede principal.

PeeringDB Base de dados pública e colaborativa utilizada pela comunidade de operadoras e provedores de Internet para registrar informações de peering, incluindo ASN, prefixos, pontos de presença, políticas de peering e contatos técnicos/NOC.

Peering / Transit Peering é o acordo de interconexão entre operadoras para troca de tráfego mútuo, geralmente sem custo financeiro direto. Transit é o serviço pelo qual uma operadora paga outra para obter acesso à Internet completa, incluindo rotas além do âmbito do acordo bilateral.

Prefix Hijacking Ataque ou incidente no qual um sistema autônomo anuncia indevidamente prefixos IP pertencentes a outro operador, desviando o tráfego destinado à vítima para si, podendo resultar em interceptação, blackhole ou degradação de serviços.

RIPD — Relatório de Impacto à Proteção de Dados Documento exigido pela LGPD em situações de tratamento de dados pessoais que possam gerar riscos elevados aos titulares, descrevendo os processos, riscos identificados e medidas de mitigação adotadas.

Route Leak Propagação não intencional ou indevida de informações de roteamento BGP além do escopo pretendido pela política do operador, podendo desviar tráfego e causar instabilidade na Internet.

RPO — Recovery Point Objective Ponto Objetivo de Recuperação. Define a quantidade máxima de dados que pode ser perdida em caso de incidente, expressa em unidade de tempo (ex.: RPO de 4 horas significa que backups devem ser realizados a cada 4 horas no máximo).

RPKI — Resource Public Key Infrastructure Infraestrutura de chave pública para recursos de Internet que permite a validação criptográfica da legitimidade dos anúncios de prefixos BGP por meio de objetos ROA (Route Origin Authorization), prevenindo prefix hijacking e route leaks.

RTBH — Remotely Triggered Black Hole Técnica de mitigação de ataques DDoS baseada em roteamento BGP, na qual prefixos ou endereços IP atacados são anunciados com uma comunidade especial para que roteadores upstream descartem o tráfego destinado ao alvo, protegendo a infraestrutura do operador.

RTO — Recovery Time Objective Tempo Objetivo de Recuperação. Define o tempo máximo tolerável para restauração de um serviço ou sistema após um incidente, sendo um parâmetro fundamental nos planos de continuidade e recuperação de desastres.

Scrubbing Center Centro especializado de limpeza de tráfego utilizado para mitigação de ataques DDoS volumétricos, no qual o tráfego suspeito é desviado, analisado e filtrado antes de ser entregue ao destino legítimo.

SGSI — Sistema de Gestão de Segurança da Informação Conjunto de políticas, processos e procedimentos que gerencia riscos à informação, para proteger a confidencialidade, integridade e disponibilidade das informações, conforme um framework de segurança como a ISO/IEC 27001.

SSDLC — Secure Software Development Life Cycle Ciclo de vida de desenvolvimento de software seguro, que incorpora requisitos, controles e práticas de segurança em todas as fases do desenvolvimento, desde o planejamento até a operação e descarte.

SoA — Declaração de Aplicabilidade Documento que identifica os controles de segurança relevantes de um framework (e.g., ISO 27002) que foram implementados ou serão implementados, juntamente com a justificativa para sua inclusão ou exclusão, dentro do escopo de um SGSI.

TLS — Transport Layer Security Protocolo criptográfico que fornece segurança de comunicação pela rede, comumente usado para proteger conexões web (HTTPS), e-mail e outras aplicações cliente-servidor.

uRPF — Unicast Reverse Path Forwarding Mecanismo de filtragem implementado em roteadores para verificar se o endereço IP de origem de um pacote é alcançável pelo caminho reverso esperado, sendo uma das principais técnicas de anti-spoofing (BCP38) em redes de operadoras.

WORM — Write Once Read Many Tecnologia de armazenamento de dados que permite que a informação seja gravada uma única vez e lida múltiplas vezes, sem possibilidade de alteração ou exclusão, garantindo a imutabilidade e integridade dos dados.

Zero Trust Modelo de arquitetura de segurança baseado no princípio de "nunca confiar, sempre verificar", no qual nenhum usuário, dispositivo ou sistema é considerado confiável por padrão, independentemente de estar dentro ou fora do perímetro da rede corporativa.

Este glossário é parte integrante da Política de Segurança da Informação e Cibersegurança (PSI) da Brphonia e deve ser atualizado sempre que novos termos relevantes forem incorporados ao documento principal.

Versão do Glossário: alinhada à PSI v1.5 — Fevereiro/2026 Responsável pela manutenção: Coordenação de Segurança da Informação e Cibersegurança