POLÍTICA DE
SEGURANÇA DA INFORMAÇÃO - PSI

AccessBrasil

A **Política de Segurança da Informação (PSI)** da **AccessBrasil** estabelece as diretrizes e normas técnicas que garantem a **confidencialidade, integridade e disponibilidade** de todos os ativos de dados sob nossa gestão. Como especialistas em infraestrutura e desenvolvimento, nossa PSI define protocolos rigorosos para o controle de acessos, criptografia de ponta, gestão de vulnerabilidades e resposta a incidentes, assegurando que tanto nossas operações internas quanto os ambientes de nossos clientes estejam protegidos contra ameaças cibernéticas modernas.

Este documento serve como o pilar de nossa governança tecnológica, orientando colaboradores e parceiros sobre o uso ético e seguro dos recursos de TI. Ao integrar a PSI ao nosso fluxo de suporte e manutenção, a AccessBrasil garante que a inovação digital ocorra em um ambiente controlado e resiliente, mitigando riscos e fortalecendo a continuidade dos negócios de quem confia em nossa expertise.

Abrangência:	Aprovado por:	Data:	Versão:
Corporativa	**Diretoria e RH**	**03/2026**	**V3**

POLÍTICA DE
SEGURANÇA DA INFORMAÇÃO - PSI

AccessBrasil

SUMÁRIO

A ANCHOR Comércio de Peças e Serviços para Informática Ltda., operando sob o nome fantasia ACCESSBRASIL, inscrita no CNPJ/MF sob o nº 58.411.901/0001-56, com sede em São Paulo - SP, tem como core business o fornecimento de soluções de desenvolvimento de sistemas, conectividade e infraestrutura tecnológica.

Por operar dados críticos de clientes e garantir a estabilidade de fluxos de comunicação, a segurança da informação é tratada não apenas como suporte, mas como valor central do produto entregue.

Esta Política estabelece o compromisso da AccessBrasil em proteger seu ecossistema digital e físico contra interrupções, acessos indevidos e vazamentos, assegurando a resiliência operacional necessária para o mercado de tecnologia.

1. TERMINOLOGIA E CONCEITOS

Para fins desta norma, aplicam-se as seguintes definições:

- Ativos de Dados e Infraestrutura: Compreende servidores, roteadores, cabos de fibra óptica, softwares de gestão, bases de dados de clientes, segredos industriais de redes e qualquer informação processada nos sistemas da AccessBrasil.
- Comitê de Segurança e Riscos (CSR): Órgão deliberativo formado pela diretoria técnica (CTO), gestão administrativa e consultoria em conformidade, responsável por validar as defesas da empresa.
- Disponibilidade (Uptime): Garantia de que os serviços de rede e dados da AccessBrasil estarão acessíveis aos clientes e colaboradores sempre que requisitados, conforme os SLAs (acordos de nível de serviço) estabelecidos.
- Parceiro/Terceiro: Qualquer prestador de serviço ou fornecedor de hardware/software que possua conectividade com a rede interna ou manipule dados em nome da AccessBrasil.
- Vulnerabilidade de Rede: Fraqueza técnica em sistemas ou processos que pode ser explorada para comprometer a entrega do serviço.

2. ESCOPO DE APLICAÇÃO

Esta política abrange todos os níveis hierárquicos da AccessBrasil, bem como prestadores de serviços externos que interagem com a nossa malha digital.

A aplicação desta norma estende-se aos escritórios físicos, data centers próprios ou subcontratados e pontos de presença de rede.

A observância desta PSI é obrigatória para a manutenção de contratos de trabalho e parcerias comerciais, sendo o seu descumprimento sujeito a sanções administrativas e legais.

3. DIRETRIZES E OBJETIVOS ESTRATÉGICOS

3.1. A AccessBrasil pauta sua gestão de segurança nos seguintes objetivos:

- Continuidade Operacional: Minimizar o tempo de inatividade através de protocolos de redundância e backups geográficos.
- Confidencialidade por Design: Implementar acessos baseados na necessidade de conhecimento (*need-to-know*), onde colaboradores só acessam dados essenciais às suas funções.
- Integridade de Tráfego: Assegurar que as informações que transitam por nossa infraestrutura não sejam alteradas ou interceptadas por agentes maliciosos.
- Cultura de Vigilância: Capacitar continuamente o corpo técnico para identificar tentativas de *phishing*, engenharia social e intrusões de rede.

3.2. A AccessBrasil compromete-se, por meio desta política, a:

- Instituir normas técnicas e diretrizes de conduta que orientem os usuários na utilização segura dos recursos de rede, mitigando vulnerabilidades operacionais;
- Implementar controles de segurança em múltiplas camadas para a proteção robusta da infraestrutura de TI;

- Agir preventivamente na contenção de falhas que possam acarretar responsabilidade civil ou criminal para a companhia e seus gestores;
- Zelar pela reputação de mercado e saúde financeira da empresa, reduzindo impactos de incidentes de segurança;
- Assegurar a proteção total dos dados corporativos e de clientes, respeitando os critérios de sigilo e integridade.

4. FUNDAMENTOS DA SEGURANÇA

A estratégia de defesa da AccessBrasil baseia-se nos seguintes pilares:

- Confidencialidade: Proteção contra acessos não autorizados, garantindo que o dado chegue apenas ao destino pretendido.
- Integridade: Salvaguarda da precisão e completude das informações, impedindo modificações indevidas em repouso ou trânsito.
- Disponibilidade: Manutenção da continuidade dos serviços e acesso à informação através de redundância e alta disponibilidade de sistemas.
- Autenticidade: Validação irrefutável da identidade de quem acessa ou emite informações nos sistemas da rede.
- Não Repúdio (Irretratabilidade): Garantia de que uma transação ou ação realizada no sistema não possa ser negada por seu autor.
- Conformidade Normativa: Estrita observância aos regulamentos do setor de telecomunicações, leis de proteção de dados e padrões de mercado.

5. PRINCÍPIOS DE GOVERNANÇA

5.1. A AccessBrasil define como princípios fundamentais:

- A segurança da informação como elemento crítico para a perenidade do negócio e confiança dos clientes;
- Gestão proativa de riscos baseada em análise técnica constante de ameaças cibernéticas;

- Promoção de uma mentalidade de "segurança em primeiro lugar" em todos os níveis da organização.

5.2. Regras específicas de utilização:

- Todo ativo intelectual ou dado processado na infraestrutura da AccessBrasil é de propriedade exclusiva da empresa, salvo acordos contratuais específicos em contrário;
- Os recursos tecnológicos são ferramentas de trabalho. O uso pessoal é tolerado de forma incidental, desde que não comprometa a largura de banda, a segurança da rede ou a produtividade;
- A empresa reserva-se o direito de monitorar o tráfego de dados e o uso de sistemas (respeitando a privacidade legal) para auditar a conformidade e prevenir ataques.

6. DIRETRIZES DE EXECUÇÃO

6.1. Fica estabelecido o Comitê de Governança e Segurança (CGS) como autoridade máxima para decisões estratégicas sobre proteção de dados e riscos tecnológicos.
6.2. A diretoria da AccessBrasil assegura o suporte necessário para que esta política seja disseminada e integrada aos processos operacionais.
6.3. O documento será revisado anualmente ou sempre que houver mudanças significativas na infraestrutura tecnológica ou na legislação vigente.
6.4. Os usuários estão cientes de que o uso dos ativos da empresa é passível de auditoria e monitoramento, conforme as diretrizes do Marco Civil da Internet.
6.5. É dever de todo colaborador buscar capacitação e esclarecimentos junto ao CGS sobre práticas seguras de manipulação de dados.
6.6. Todos os contratos com parceiros e fornecedores devem conter cláusulas de confidencialidade e adesão aos padrões mínimos de segurança da AccessBrasil.
6.7. A responsabilidade pela proteção da informação inicia-se no processo de integração do novo colaborador, mediante assinatura de Termo de Confidencialidade.
6.8. Qualquer anomalia ou incidente detectado deve ser reportado imediatamente

ao canal oficial: seguranca@accessbrasil.net.br.
6.9. Serão mantidos registros de acesso (logs) de todas as atividades críticas em sistemas e servidores para fins de auditoria e rastreabilidade.
6.10. A AccessBrasil não se responsabiliza por prejuízos causados pelo uso negligente de acessos cedidos a usuários, podendo acionar legalmente os responsáveis em caso de dolo.
6.11. O descumprimento destas normas configura falta grave, sujeitando o infrator a medidas disciplinares previstas na CLT e legislações pertinentes.

7. MATRIZ DE RESPONSABILIDADES

7.1. Da AccessBrasil (Institucional)

A empresa, como mantenedora da infraestrutura, compromete-se a:

- Consolidar e auditar controles de segurança que protejam o fluxo de dados contra-ataques cibernéticos, intrusões e falhas de hardware;
- Disseminar esta PSI para todos os stakeholders (colaboradores, técnicos de campo, fornecedores e clientes corporativos) que interagem com o ecossistema da empresa;
- Promover workshops e pílulas de conhecimento sobre cibersegurança e proteção de dados;
- Garantir a conformidade com o Marco Civil da Internet, LGPD e normas da ANATEL pertinentes ao setor;
- Gerenciar o ciclo de vida de incidentes, desde a detecção e contenção até o reporte às autoridades e clientes afetados, quando legalmente exigido;
- Investir na atualização tecnológica constante para reduzir a obsolescência de segurança.

7.2. Do Comitê de Governança e Segurança (CGS)

- O CGS é o órgão técnico-estratégico responsável por:
- Validar normas técnicas de segurança e arquitetura de rede;
- Assegurar orçamento e ferramentas para a proteção dos ativos digitais;

- Fiscalizar a aplicação prática desta política em todas as unidades de negócio;
- Liderar a resposta a crises e ataques de larga escala (Ransomware, DDoS, etc.);
- Definir níveis de criticidade e classificação de dados (Público, Interno, Confidencial, Restrito);
- Gerir identidades e acessos, revisando periodicamente quem possui privilégios administrativos nos servidores;
- Exigir a formalização de Termos de Confidencialidade (NDA) antes de qualquer exposição de dados a terceiros em fase de orçamento ou parceria.

7.3. Dos Gestores de Operações e TI

Compete aos líderes de cada área:

- Monitorar o uso de dados sob sua custódia, garantindo que o descarte de informações (físicas ou digitais) siga protocolos de destruição segura;
- Rotular ativos de informação conforme a classificação de sigilo definida pelo CGS;
- Validar mensalmente a lista de usuários ativos em seus sistemas, solicitando o bloqueio imediato de contas em casos de desligamento ou mudança de função.

7.4. Dos Usuários (Colaboradores e Terceiros)

É dever intransferível de cada usuário:

- Zelar pelo sigilo de suas credenciais de acesso (senhas e tokens), nunca as compartilhando;
- Utilizar os ativos tecnológicos (notebooks, VPN, e-mail) estritamente para fins profissionais e lícitos;
- Abster-se de tratar dados confidenciais da AccessBrasil em redes Wi-Fi públicas sem o uso de VPN corporativa;
- Evitar a exposição de estratégias técnicas ou nomes de clientes em redes sociais ou ambientes públicos;

- Notificar imediatamente o suporte técnico sobre qualquer comportamento anômalo em seus dispositivos ou tentativas de golpe (phishing);
- Manter o sigilo profissional mesmo após o encerramento do vínculo com a AccessBrasil, sob pena de processo civil.

8. PROTOCOLO DE INCIDENTES E RESPOSTA

8.1. A AccessBrasil mantém camadas de defesa (Firewalls, Antivírus, Monitoramento de Rede) para prevenir brechas de segurança.
8.2. Qualquer suspeita de vazamento de dados ou invasão de sistema deve ser reportada ao canal seguranca@accessbrasil.net.br.
8.3. O CGS conduzirá a perícia digital para identificar a origem da falha, isolar os sistemas afetados e produzir um Relatório de Impacto à Proteção de Dados (RIPD) se houver comprometimento de dados pessoais.
8.4. Evidências digitais e logs de acesso serão preservados para fins de auditoria interna ou instrução de processos judiciais, caso seja identificada conduta dolosa ou negligente.

9. INFRAÇÕES À POLÍTICA (PSI)

9.1. Define-se como violação desta norma qualquer ação ou omissão, voluntária ou não, que resulte em:

a) Exposição de Risco: Atos que submetam a infraestrutura da AccessBrasil a vulnerabilidades, perdas financeiras ou danos à reputação perante o mercado e clientes;
b) Quebra de Sigilo: Divulgação de topologias de rede, credenciais de acesso, dados de faturamento ou estratégias de expansão sem autorização prévia;
c) Uso Indevido de Ativos: Utilização da rede ou equipamentos para atividades ilícitas, ataques a terceiros, mineração de criptoativos ou qualquer prática que fira a legislação brasileira (Marco Civil e CP).

10. REGIME DISCIPLINAR E SANÇÕES

10.1. O descumprimento das diretrizes aqui estabelecidas, incluindo tentativas não consumadas de burlar controles, sujeitará o infrator às seguintes medidas, graduadas conforme a gravidade:

- Advertência formal (verbal ou escrita);
- Suspensão das atividades sem remuneração;
- Rescisão de contrato de trabalho por Justa Causa, com base no Art. 482 da CLT (indisciplina ou insubordinação).

10.2. A aplicação das penas será deliberada pelo Comitê de Governança e Segurança (CGS), que analisará o histórico do colaborador, a extensão do dano e o dolo envolvido.

10.3. Parceiros e Prestadores: No caso de empresas subcontratadas, a violação poderá acarretar a rescisão imediata do contrato de prestação de serviços, aplicação de multas contratuais e impedimento de futuras contratações.

10.4. Responsabilidade Civil e Criminal: Independentemente das sanções administrativas, a AccessBrasil reserva-se o direito de buscar reparação judicial por danos materiais e morais, além de notificar as autoridades policiais em caso de crimes cibernéticos.

11. DISPOSIÇÕES GERAIS E CASOS OMISSOS

Situações não previstas neste documento serão analisadas e resolvidas pelo CGS em conjunto com a diretoria técnica.
Esta Política não é exaustiva. Dada a natureza dinâmica das ameaças digitais, espera-se que o usuário adote o princípio da precaução, buscando orientações sempre que identificar uma zona cinzenta de segurança.

12. VALIDADE E ATUALIZAÇÕES

Esta PSI entra em vigor imediatamente após sua publicação no portal interno ou comunicação oficial.
A revisão ocorrerá anualmente ou de forma extraordinária sempre que houver mudanças críticas na arquitetura de rede da AccessBrasil.