Política de Segurança da Informação

Revisado em 11/10/2026

Documento	Política de Segurança da Informação (PSI)
Empresa	Comdados Comércio e Serviços Eletrônicos Ltda. – CNPJ 34.203.752/0001-71
Aprovação	Diretoria (Alta Direção) – Cesar Dias, Diretor
Revisado em	11/10/2026
Próxima revisão	Até 10/2027, ou antes em caso de mudança relevante
Classificação	Pública – divulgação interna e externa

1. Objetivo

Esta Política de Segurança da Informação (PSI) estabelece as diretrizes, responsabilidades e controles adotados pela Comdados Comércio e Serviços Eletrônicos Ltda. para proteger as informações da empresa, de seus clientes, fornecedores, fabricantes parceiros e colaboradores, preservando sua confidencialidade, integridade e disponibilidade.

A PSI é aprovada pela Alta Direção, que se compromete a prover os recursos necessários para sua implementação, a comunicá-la a todas as partes interessadas e a revisá-la periodicamente.

2. Abrangência

Esta Política se aplica a todos os diretores, colaboradores, estagiários, prestadores de serviço, fornecedores e parceiros que tenham acesso a informações, sistemas, equipamentos ou instalações da Comdados, incluindo a Matriz (Cassange) e o Escritório (Hangar Business Park), bem como o trabalho realizado remotamente ou em instalações de clientes.

Abrange informações em qualquer formato (digital, impresso ou verbal) e todos os ativos de tecnologia utilizados pela empresa, próprios ou de terceiros.

3. Referências

- ABNT NBR ISO/IEC 27001 e 27002 – Sistemas de gestão e controles de segurança da informação;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 12.965/2014 – Marco Civil da Internet;
- Política de Privacidade, Código de Ética e Conduta e Programa de Integridade da Comdados.

4. Princípios

- **Confidencialidade:** a informação é acessada somente por pessoas autorizadas;
- **Integridade:** a informação é mantida exata e completa, protegida contra alterações indevidas;
- **Disponibilidade:** a informação e os sistemas estão acessíveis às pessoas autorizadas sempre que necessário;

- **Necessidade de conhecer e menor privilégio:** cada usuário recebe apenas os acessos indispensáveis às suas atividades;
- **Responsabilidade:** cada pessoa responde pelo uso das informações e credenciais sob sua guarda.

5. Diretrizes de Segurança da Informação

5.1 Classificação e tratamento da informação

As informações são classificadas como Pública, Interna, Confidencial ou Restrita, e devem ser armazenadas, compartilhadas e descartadas de acordo com o seu nível. Informações de clientes, contratos, propostas, dados de faturamento e dados pessoais são tratadas, no mínimo, como Confidenciais. O descarte de documentos e mídias deve impedir a recuperação do conteúdo.

5.2 Controle de acesso

- O acesso a sistemas e informações é concedido mediante solicitação do gestor, com credencial individual e intransferível;
- Autenticação multifator (MFA) é adotada sempre que disponível, especialmente para e-mail, acesso remoto e sistemas críticos;
- Os acessos são revisados periodicamente e revogados imediatamente em caso de desligamento ou mudança de função;
- Contas administrativas são restritas a pessoas autorizadas e utilizadas somente para atividades que as exijam.

5.3 Senhas e credenciais

As senhas devem ser fortes, pessoais e sigilosas, não podendo ser compartilhadas, anotadas em local visível ou reutilizadas entre serviços pessoais e corporativos. Credenciais de acesso a ambientes de clientes e portais de fabricantes devem ser guardadas em local seguro e utilizadas exclusivamente para a finalidade autorizada.

5.4 Uso aceitável dos recursos

E-mail, internet, Microsoft Teams, computadores, telefones e demais recursos corporativos devem ser utilizados para fins profissionais, de forma ética e legal. É proibido instalar softwares não homologados ou sem licença, acessar conteúdo ilícito, desativar controles de segurança ou utilizar serviços não autorizados para armazenar informações da empresa. A Comdados pode monitorar o uso de seus recursos, nos limites da lei, para fins de segurança.

5.5 Proteção contra códigos maliciosos e monitoramento

Todos os equipamentos corporativos contam com ferramentas especializadas de proteção contra malware e monitoramento avançado (XDR), que devem permanecer ativas e atualizadas. Sistemas operacionais e aplicações recebem atualizações de segurança de forma periódica. Os colaboradores devem ter cautela com anexos, links e solicitações suspeitas (phishing) e reportá-los imediatamente.

5.6 Cópias de segurança (backup)

As informações relevantes ao negócio são copiadas periodicamente, de acordo com sua criticidade, e as cópias são armazenadas de forma protegida. Testes de restauração são realizados para assegurar a recuperação dos dados.

5.7 Segurança física e do ambiente

O acesso às instalações da Matriz e do Escritório, incluindo áreas de estoque, laboratório e equipamentos de clientes, é restrito a pessoas autorizadas. Visitantes devem ser identificados e acompanhados. Os colaboradores devem manter mesas limpas e bloquear as telas ao se ausentarem.

5.8 Dispositivos móveis e trabalho remoto

Notebooks e dispositivos móveis utilizados para acessar informações da empresa devem estar protegidos por senha ou biometria, com bloqueio automático de tela. No trabalho remoto ou em campo, o colaborador deve utilizar conexões seguras, evitar redes públicas não confiáveis e zelar pela guarda física dos equipamentos. Perda ou furto deve ser comunicado imediatamente.

5.9 Fornecedores, parceiros e clientes

Fornecedores e parceiros com acesso a informações da Comdados devem assumir compromissos de confidencialidade e segurança compatíveis com esta Política. Informações e ambientes de clientes e fabricantes são acessados somente na medida necessária à execução dos serviços contratados, respeitando as regras e políticas de segurança de cada cliente.

5.10 Gestão de incidentes de segurança

Todo evento suspeito ou incidente de segurança da informação (acesso indevido, vazamento, malware, perda de equipamento, entre outros) deve ser comunicado imediatamente ao gestor imediato e à área de TI. Os incidentes são registrados, analisados, tratados e utilizados para melhoria dos controles. Incidentes envolvendo dados pessoais são comunicados ao Encarregado (DPO), que avaliará a necessidade de notificação à ANPD e aos titulares, nos termos da LGPD.

5.11 Continuidade do negócio

A Comdados mantém medidas para garantir a continuidade das operações críticas e a recuperação dos sistemas em caso de falhas, desastres ou incidentes, de forma a preservar o atendimento aos clientes.

5.12 Privacidade e proteção de dados pessoais

O tratamento de dados pessoais segue a LGPD e a Política de Privacidade da Comdados. Dúvidas e solicitações de titulares devem ser encaminhadas ao Encarregado pelo e-mail **privacidade@comdados.com.br**.

6. Papéis e responsabilidades

- **Diretoria (Alta Direção):** aprovar esta Política, prover recursos, apoiar sua aplicação e conduzir sua revisão periódica;
- **Área de TI:** implementar e manter os controles técnicos, gerir acessos, monitorar ameaças e tratar incidentes;

- **Encarregado pelo Tratamento de Dados Pessoais (DPO):** orientar sobre proteção de dados pessoais e atuar como canal com titulares e com a ANPD;
- **Gestores:** garantir que suas equipes conheçam e cumpram esta Política e solicitar ou revogar acessos;
- **Colaboradores e terceiros:** conhecer, cumprir e zelar por esta Política, reportando qualquer violação ou incidente.

7. Comunicação, divulgação e conscientização

Esta Política é comunicada a todas as partes interessadas pelos seguintes meios:

- envio por e-mail corporativo a todos os colaboradores a cada publicação ou revisão;
- disponibilização no site da Comdados (www.comdados.com.br) e nos canais internos;
- apresentação no processo de integração de novos colaboradores;
- ações periódicas de conscientização e treinamento em segurança da informação, com registro de participação;
- comunicação aos fornecedores e parceiros que tenham acesso a informações da empresa.

8. Violações e sanções

O descumprimento desta Política poderá resultar em medidas disciplinares, conforme a legislação trabalhista e os regulamentos internos, e, no caso de terceiros, em sanções contratuais, sem prejuízo das responsabilidades civis e criminais cabíveis. Violações podem ser comunicadas, inclusive de forma anônima, pelo e-mail ouvidoria@comdados.com.br.

9. Revisão e atualização

Esta Política é revisada pela Diretoria no mínimo uma vez ao ano, ou sempre que houver mudanças relevantes no negócio, na legislação, nas tecnologias utilizadas ou após incidentes significativos. A versão vigente estará sempre disponível nos canais indicados no item 7.

10. Aprovação

Esta Política foi aprovada pela Diretoria da Comdados Comércio e Serviços Eletrônicos Ltda. e entra em vigor na data de sua publicação.

Salvador – BA, 11 de outubro de 2026.



_____

Cesar Dias
Diretor / *Director*
E-mail / Teams: cesar@comdados.com.br
www.**comdados**.com.br