

Política de Classificação de Dados e Proteção de Dados Confidenciais

C Controle - CLOSMAC INFORMATICA LTDA

Site: <https://www.ccontrole.com.br>

Versão: 1.0

Última atualização: 17 de julho de 2026

1. Objetivo

Esta política estabelece as diretrizes do C Controle para classificação, tratamento e proteção de dados confidenciais, dados pessoais e informações armazenadas ou transmitidas pelos sistemas da empresa.

O objetivo é proteger dados confidenciais em trânsito e em repouso, reduzindo riscos de acesso não autorizado, divulgação indevida, perda, alteração ou uso inadequado das informações.

2. Escopo

Esta política se aplica aos sistemas do C Controle, bancos de dados, servidores, backups, integrações, APIs, ambientes administrativos, colaboradores autorizados e dados tratados em nome dos clientes.

3. Classificação dos Dados

O C Controle classifica as informações conforme sua natureza e sensibilidade:

Dados públicos: informações que podem ser divulgadas publicamente, como site institucional, informações comerciais e materiais autorizados.

Dados internos: informações de uso interno da empresa, como processos operacionais, configurações internas e documentação técnica.

Dados confidenciais: informações que exigem proteção contra acesso não autorizado, incluindo dados de clientes, dados cadastrais, dados comerciais, informações de pedidos, documentos, registros financeiros, dados de integração, logs e credenciais.

Dados pessoais: informações relacionadas a pessoas naturais, incluindo nome, telefone, e-mail, endereço, documentos, dados de usuários, clientes finais, colaboradores ou outros titulares.

4. Proteção de Dados em Trânsito

O C Controle utiliza SSL/TLS no site www.ccontrole.com.br e em serviços aplicáveis para proteger a transmissão de informações entre usuários, sistemas e servidores.

A proteção de dados em trânsito tem como objetivo reduzir riscos de interceptação, alteração ou exposição indevida durante comunicações eletrônicas.

Integrações com plataformas externas, APIs, marketplaces e serviços de terceiros devem utilizar canais seguros sempre que disponíveis, respeitando os requisitos técnicos de cada plataforma.

5. Proteção de Dados em Repouso

Dados armazenados nos servidores e bancos de dados do C Controle são protegidos por controles de acesso, restrição administrativa, permissões operacionais e medidas de segurança do ambiente Windows Server.

O acesso aos bancos de dados, arquivos, backups e ambientes administrativos é restrito a colaboradores autorizados e concedido conforme necessidade operacional, seguindo o princípio do menor privilégio.

Quando aplicável, a empresa utiliza recursos como BitLocker, controles do Windows Server, permissões de acesso, firewall, antivírus, backups e restrição física ao ambiente dos servidores para proteger dados em repouso.

6. Banco de Dados

Os bancos de dados utilizados pelo C Controle armazenam informações necessárias para a operação dos sistemas contratados pelos clientes.

O acesso direto aos bancos de dados é restrito a pessoal autorizado, sendo utilizado apenas para manutenção, suporte, auditoria, segurança, correção de falhas, execução contratual ou necessidade operacional legítima.

Consultas, exportações, cópias ou alterações em dados devem ocorrer apenas quando necessárias e autorizadas.

7. Backups

O C Controle realiza backups diários agendados utilizando recursos originais e licenciados do Windows Server.

Os backups são protegidos por controles de acesso e mantidos para apoiar recuperação operacional, continuidade de negócios e resposta a incidentes.

A empresa também mantém infraestrutura de backup em segundo imóvel, como medida adicional de continuidade em caso de incidente físico ou indisponibilidade do ambiente principal.

8. Controle de Acesso

O acesso a dados confidenciais e pessoais é limitado a colaboradores autorizados, conforme função e necessidade operacional.

Credenciais administrativas devem ser protegidas e não podem ser compartilhadas. Acessos desnecessários devem ser removidos ou ajustados quando houver mudança de função, encerramento de vínculo ou alteração operacional.

9. Compartilhamento de Dados

Dados confidenciais e pessoais não devem ser compartilhados com terceiros sem necessidade operacional, base contratual, obrigação legal, autorização do cliente ou finalidade legítima relacionada à prestação dos serviços.

Quando houver integração com plataformas externas, marketplaces, meios de pagamento, serviços fiscais, transportadoras ou outros provedores, o compartilhamento deve ocorrer apenas na medida necessária para execução da funcionalidade contratada ou configurada pelo cliente.

10. Registros e Logs

Quando aplicável, o C Controle mantém registros técnicos, logs de sistema, eventos de acesso e informações operacionais para apoiar segurança, suporte, auditoria, investigação de incidentes e continuidade dos serviços.

Logs que contenham dados sensíveis devem ser protegidos contra acesso não autorizado.

11. Resposta a Incidentes

Em caso de suspeita de acesso indevido, vazamento, perda, alteração não autorizada ou exposição de dados confidenciais, o C Controle deve avaliar o incidente, restringir acessos, preservar evidências, validar backups e adotar medidas corretivas.

Responsável por incidentes de segurança:

David Prado

Telefone: (32) 9 8852-516

12. Revisão

Esta política é revisada periodicamente e pode ser atualizada sempre que houver mudanças nos sistemas, bancos de dados, infraestrutura, processos internos, requisitos legais ou controles de segurança.