Política de Controle de Acesso

C Controle - CLOSMAQ INFORMATICA LTDA
Site: https://www.ccontrole.com.br
Versão: 1.0
Última atualização: 17 de julho de 2026

1. Objetivo

Esta Política de Controle de Acesso estabelece as diretrizes utilizadas pelo C Controle para restringir, controlar e monitorar o acesso aos sistemas, servidores, dados pessoais, ambientes administrativos e infraestrutura da empresa.

O objetivo é garantir que o acesso às informações seja concedido apenas a pessoas autorizadas, de acordo com a necessidade operacional e seguindo o princípio do menor privilégio.

2. Escopo

Esta política se aplica a:

- Sistemas internos do C Controle.
- Servidores de produção e réplica.
- Bancos de dados.
- Ambientes administrativos.
- Dados pessoais tratados pela plataforma.
- Salas de equipamentos e infraestrutura física.
- Colaboradores, prestadores e usuários autorizados.

3. Princípio do Menor Privilégio

O C Controle adota o princípio do menor privilégio, concedendo aos usuários somente os acessos necessários para executar suas atividades autorizadas.

Acessos administrativos, técnicos ou sensíveis são restritos a colaboradores autorizados e não são concedidos de forma ampla ou permanente sem necessidade operacional.

4. Acesso a Dados Pessoais

O acesso a dados pessoais nos sistemas do C Controle é restrito a usuários autorizados, conforme função, necessidade de suporte, manutenção, operação ou obrigação legal.

Dados pessoais não devem ser acessados, copiados, exportados, compartilhados ou utilizados sem finalidade legítima relacionada à prestação dos serviços, suporte ao cliente, segurança, cumprimento contratual ou obrigação legal.

5. Acesso Físico

O acesso às salas de equipamentos, servidores, infraestrutura de rede e ambientes de backup é restrito a apenas colaboradores autorizados.

Pessoas não autorizadas não devem acessar áreas técnicas, equipamentos de rede, servidores, mídias de backup ou qualquer ambiente físico que possa comprometer a segurança dos sistemas e dados.

6. Acesso Virtual e Administrativo

O acesso virtual aos servidores, bancos de dados, sistemas administrativos, painéis de configuração e ambientes de infraestrutura é restrito a colaboradores autorizados.

Contas administrativas devem ser utilizadas apenas quando necessário e protegidas por credenciais individuais, senhas fortes e controles disponíveis no ambiente Windows e nos sistemas utilizados pela empresa.

7. Senhas e Proteção de Credenciais

Usuários autorizados devem proteger suas credenciais de acesso e não compartilhar senhas, códigos, tokens ou credenciais administrativas.

O C Controle utiliza políticas de senha do Windows e controles de bloqueio de tela para reduzir riscos de acesso não autorizado a estações, servidores e ambientes administrativos.

8. Revisão de Acessos

Os acessos devem ser revisados periodicamente ou sempre que houver alteração de função, desligamento de colaborador, mudança operacional ou identificação de risco.

Acessos que não sejam mais necessários devem ser removidos ou ajustados.

9. Registro e Monitoramento

Quando aplicável, o C Controle mantém registros, logs ou evidências de acesso aos ambientes administrativos, servidores e sistemas, com o objetivo de apoiar auditorias, investigações, suporte técnico, segurança e resposta a incidentes.

10. Responsabilidades

Os colaboradores autorizados são responsáveis por:

- Utilizar acessos apenas para finalidades legítimas.
- Proteger credenciais e dispositivos.
- Não compartilhar senhas ou acessos.
- Reportar suspeitas de uso indevido, vazamento, perda de credenciais ou acesso não autorizado.
- Respeitar o princípio do menor privilégio.

11. Resposta a Incidentes de Acesso

Em caso de suspeita de acesso indevido, credencial comprometida ou exposição de dados pessoais, o C Controle deve avaliar o incidente, restringir acessos, alterar credenciais, preservar evidências e adotar medidas de correção e recuperação.

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, infraestrutura, processos internos, requisitos legais ou controles de segurança.