

## **Caso 1: Controle e autenticação de acesso físico e digital**

Objetivo: Garantir que apenas pessoas autorizadas tenham acesso às áreas físicas e aos sistemas internos da empresa, mantendo segurança e praticidade.

Contrato: “Autenticar o usuário para liberar acesso seguro.”

Implementação A: Biometria (impressão digital ou reconhecimento facial) — usada tanto nas portas de entrada quanto no login dos sistemas.

Implementação B: Cartão RFID para entrada e senha com segundo fator (token ou SMS) para o sistema.

Política: “Para áreas e sistemas críticos → usar biometria (A); para áreas comuns e sistemas administrativos → usar cartão + senha (B).”

Risco/Observação: Biometria oferece maior segurança, mas pode falhar por problemas no leitor; RFID e senha são mais práticas, porém mais vulneráveis a clonagem ou roubo de credenciais.

## **Caso 2: Monitoramento de acessos e auditoria de segurança**

Objetivo: Registrar e monitorar os acessos físicos e digitais para garantir rastreabilidade e detectar tentativas de invasão.

Contrato: “Registrar eventos de acesso de usuários.”

Implementação A: Sistema integrado de logs biométricos com data, hora e local do acesso.

Implementação B: Relatório de registros baseados em uso de credenciais (cartão e login).

Política: “Para auditorias críticas → usar logs biométricos (A) pela precisão e vínculo pessoal; para relatórios operacionais de rotina → usar logs de credenciais (B) pela facilidade de coleta.”

Risco/Observação: Logs biométricos exigem armazenamento seguro de dados sensíveis; logs de credenciais podem gerar falsos positivos se o cartão ou senha forem compartilhados.