

# ESTUDO DE CASO



by:

**Artur Rosa Correia - 824135943**  
**Gustavo Silveira Benicio - 824134160**  
**Luan Bernardo Alves - 824134204**



# CONTROLE DE ACESSO FÍSICO

- **Restrição de acesso aos departamentos:** Sugere-se a utilização de biometria facial para controlar o acesso aos departamento de TI e de administração , visando proteger dados importantes. O custo estimado é de R\$30.000,00.
- **Controle de acesso na entrada do prédio:** A proposta é substituir o controle de acesso manual por um sistema automatizado com biometria facial, reduzindo o risco de erros e acessos não autorizados. O custo estimado é de R\$45.000,00.
- **Expansão da biometria facial para a entrada do prédio:** Além da biometria facial nos departamentos, sugere-se a implementação desse sistema na entrada principal do prédio, aumentando a segurança e eliminando o risco de uso indevido de crachás. O custo estimado é de R\$40.000,00.
- **Instalação de câmeras de segurança:** Para melhorar o monitoramento e controle de acesso em todas as edificações da empresa, é proposta a instalação de ao menos 3 câmeras em cada departamento, em locais estratégicos, como portas de entrada e áreas sensíveis. O custo estimado é de R\$60.000,00.



# CONTROLE DE ACESSO LÓGICO:

Atualmente o acesso aos servidores da empresa é feito apenas por meio de nome de usuário e senha, o que expõe os dados a riscos, especialmente em um ambiente de home office.

## Soluções:

- **Fortalecimento das senhas:** Exigir senhas mais complexas, com pelo menos 8 caracteres e caracteres especiais, para dificultar a quebra.
- **Restrição de dispositivos:** Permitir o acesso apenas a dispositivos pré-aprovados pela empresa, aumentando a segurança.
- **Aprovação dupla:** Exigir a aprovação de dois administradores para alterações em servidores com dados sensíveis, reduzindo o risco de ações não autorizadas.
- **Monitoramento de tentativas de acesso:** Ativação de um sistema para identificar e registrar todas as tentativas de acesso, facilitando a detecção de intrusos.



## Custos:

- **Implementação:** Estima-se um custo inicial entre R\$20.000,00 e R\$45.000,00.
- **Manutenção:** Custos mensais entre R\$500,00 e R\$2.000,00.

# RISCOS



## FÍSICOS

- **Energia:** De acordo com a infraestrutura da empresa, em possíveis mudanças climáticas, gerando falta de energia, problemas poderiam ser sinalizados. O ideal seria adquirir combustíveis adicionais para garantir suporte acima de 4 horas, tendo em vista que pode não ter hora prevista para a volta da energia, o que pode gerar prejuízo nas operações da empresa como um todo. Uma opção muito inteligente e econômica é fechar parcerias com fornecedores de combustíveis, combinando a prontidão assim que necessário.
- **Incêndio:** Analisando a infraestrutura do prédio, percebemos a existência de uma proximidade muito perigosa entre o gerador, os botijões de gás e o diesel, podendo gerar grandes riscos a todos, como severos incêndios. Para evitar isto e garantir a segurança de todos na empresa, seria fundamental instalar sensores de fumaça em todos os prédios e criar uma certa separação e barreira entre os botijões e o tanque de diesel.



## LÓGICOS

### Ameaças:

- Malware, ataques de phishing; vulnerabilidades em sistemas desatualizados.

### Soluções:

- **Atualização de sistemas:** Garantir que todos os softwares estejam atualizados com os patches de segurança mais recentes.
- **Backups regulares:** Realizar backups diários e armazená-los em local seguro para rápida recuperação.

### Intensidade de riscos:

- **Impacto financeiro:** Um ataque de ransomware, por exemplo, pode causar prejuízos financeiros consideráveis devido à indisponibilidade de sistemas e custos de recuperação.

# PLANO DE CONTINGÊNCIA

## 1 - Recursos Críticos

- **Energia:**
  - Gerador com capacidade limitada a 4 horas.
  - Necessidade de garantir operação contínua em falhas prolongadas.
- **Segurança Física:**
  - Dependência de catracas, câmeras limitadas e controle manual na garagem, expondo vulnerabilidades.



## 2 - Análise de Impacto nos Negócios

- **Falta de Energia Prolongada:**
  - Prejuízo para sistemas essenciais, incluindo servidores e segurança física.
  - Potencial de perda de dados e interrupção de operações.
- **Falhas no Controle de Acesso Físico:**
  - Acessos não autorizados aumentam o risco de furtos, vandalismos e sabotagem.



## 3 - Estratégias de Recuperação

- **Energia Alternativa:**
  - Fechar contrato com fornecedores locais de diesel para reabastecimento imediato em emergências.
- **Segurança Física:**
  - Implementar biometria facial em todos os pontos de entrada.
  - Adicionar câmeras de segurança em áreas estratégicas, como garagens e depósitos.
  - Automatize o controle de acesso na garagem, eliminando a dependência de operadores manuais.



# PLANO DE CONTINGÊNCIA

## 4 - Plano de Ação

- **Contrato com Fornecedores de Combustível:**
  - **Responsável:** Equipe de Administração.
  - **Prazo:** 1 mês.
  - **Custo:** R\$ 40.000/ano.
- **Ampliação da Biometria Facial:**
  - **Responsável:** Segurança Patrimonial.
  - **Prazo:** 1 mês.
  - **Custo:** R\$ 75.000 - 90.000
- **Instalação de Câmeras:**
  - **Responsável:** Equipe de Segurança.
  - **Prazo:** 1 mês.
  - **Custo:** R\$50.000

## 5 - Teste do Plano

- **Simulação de Falha de Energia:**
  - Testar acionamento dos geradores (primário e secundário).
- **Testes de Segurança Física:**
  - Simular tentativa de entrada não autorizada.
  - Avaliar eficiência de biometria e monitoramento por câmeras.



# AMEAÇAS



FÍSICAS



LÓGICAS

- **Ameaças físicas ao ambiente e aos negócios:** Acesso não autorizado, desastres naturais, furtos e vandalismo;
- **Vulnerabilidades:** Ausência de controles físico e infraestrutura frágil;
- **Soluções (Mitigação):** Controle de acesso, Proteção contra desastres: Usar gabinetes resistentes e sensores ambientais, Monitoramento contínuo: Vigiar áreas críticas e usar alarmes contra invasões.

- **Ameaças lógicas ao ambiente e aos negócios:** Ataques cibernéticos (Phishing, ransomware), vazamento de dados sensíveis, exploração de vulnerabilidades (Erros em atualizações de patches, configurações erradas feitas por funcionários, etc.);
- **Vulnerabilidades:** Falta de treinamento, sistemas desatualizados, falta de monitoramento contínuo e senhas fracas ou compartilhadas.
- **Soluções:** Proteção contra ataques cibernéticos (Malware):
  - Implemente firewalls e softwares antivírus em todos os dispositivos conectados à rede.
  - Utilização de soluções de sandboxing para análise de anexos e links antes de sua abertura.



# SOLUÇÕES DE TI

## Redundância e Armazenamento de Backups:

- Adotar a regra 3-2-1 para backups:
  - Três cópias dos dados;
  - Armazenadas em dois tipos de mídia por segurança (disco local e nuvem);
  - Uma cópia mantida em local remoto (servidores fora do site principal).
- Realize backups automáticos e diários para minimizar perdas em caso de ataques ou falhas.
- Teste regularmente a integridade dos backups e dos processos de restauração para garantir sua eficácia.



## Aprimoramento de Acesso Remoto:

- Restringir acessos remotos apenas a dispositivos registrados e certificados pela empresa.
- Implementar autenticação multifator (MFA) para todos os acessos aos servidores.

## Reativação e Monitoramento de Tentativas de Acesso:

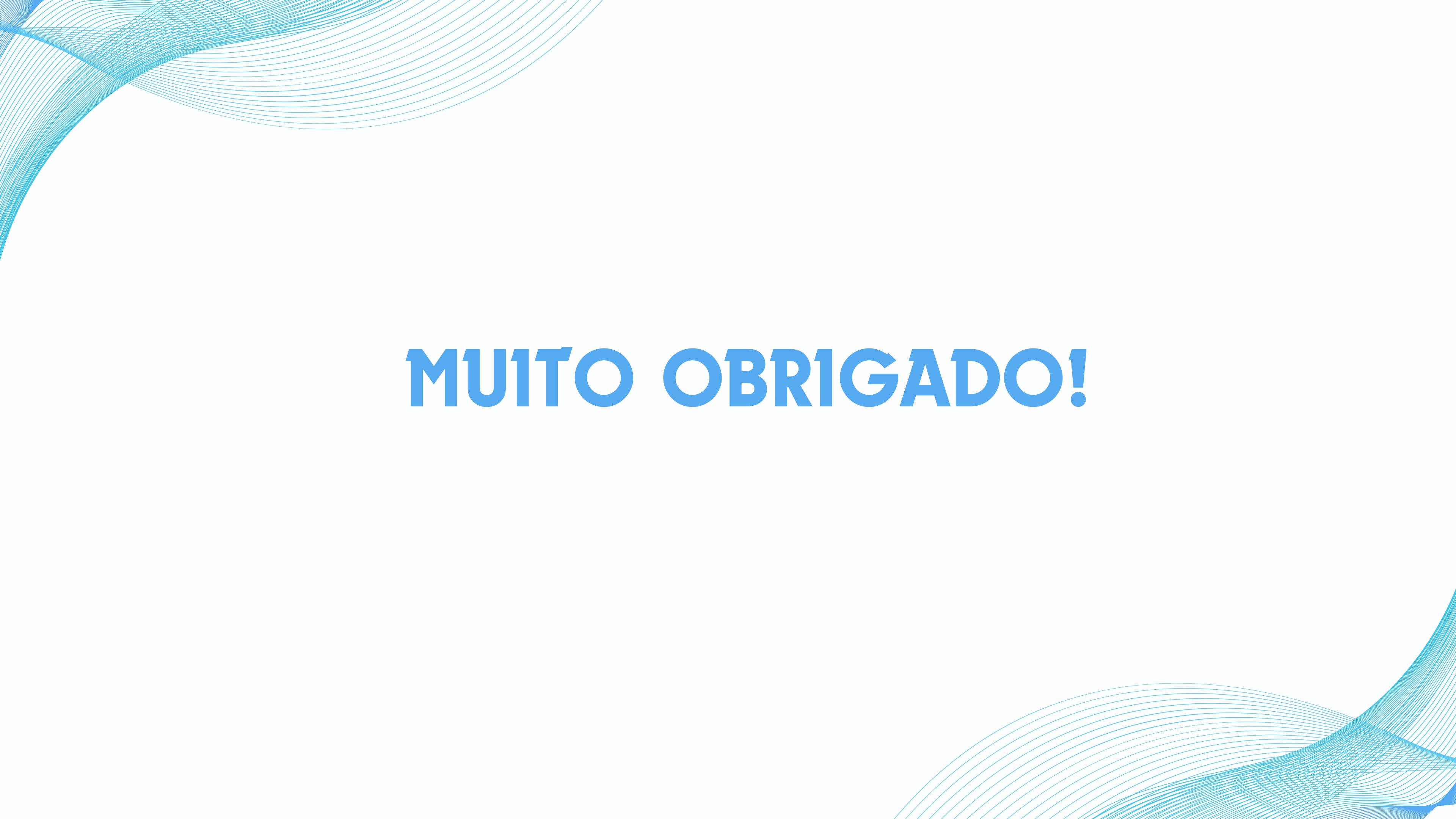
- Reativar o registro de tentativas de acesso falhas e integrá-lo com sistemas de alerta em tempo real.
- Configurar relatórios automatizados para destacar tentativas suspeitas.

## Segmentação de Rede:

- Criar redes segmentadas para isolar sistemas críticos (departamento de TI, segurança e administrativos).
- Limitar o acesso entre as redes para reduzir o impacto de ataques cibernéticos.

# TABELA DE VALORES

ITEM	Descrição	Custo Estimado	%
<b>Biometria Facial (Departamentos)</b>	Restrição de acesso a TI e Administração.	R\$ 30.000,00	13,64%
<b>Biometria Facial (Entrada do Prédio)</b>	Substituir crachás por biometria facial.	R\$ 40.000,00	18,18%
<b>Automatização da Garagem</b>	Controle de acesso automático na garagem com biometria facial.	R\$ 45.000,00	20,45%
<b>Câmeras de Segurança</b>	Instalação de câmeras em áreas estratégicas (3 por departamento).	R\$ 60.000,00	27,27%
<b>Controle de Acesso Lógico</b>	Senhas complexas, dispositivos aprovados e monitoramento de tentativas.	R\$ 45.000,00	20,45%
<b>VALOR TOTAL</b>	O valor total de todo o investimento	R\$ 175.000,00	100%



**MUITO OBRIGADO!**