Controle de Acesso Físico

Quais seriam as expectativas de um controle de acesso físico sólido:

Detecção e Catracas:

Análise de crachás com imagem e conexão com um sistema de controle de acesso.

Documentação de horários de chegada e partida para auditorias.

Gestão de Automóveis:

Vigilância automatizada, com controle de entrada e saída de automóveis.

Dificuldades físicas, como portões controlados à distância.

Proteção Patrimonial:

Existência de monitoramento físico ou patrimonial ativo.

Gestão de portões de acesso operados manualmente

Análise da segurança da empresa-

Catracas e identificação:

.Sistema atual utiliza crachás para a liberação do acesso e para registrar ponto, o problema que só tem uma câmera no local, limitando a visibilidade de possíveis eventos críticos

Controle de veículos:

.Utilizado portões operados manualmente são vulneráveis, por dependerem da ação da equipe de segurança,

.Não há sistema automatizado para rastrear veículos ou monitorar atividades nos depósitos;

Pontos de melhoria:

Catracas e identificação:

.Crachás com chips RFID: Melhor integração com sistemas de controle de acesso.

-Monitoramento por câmeras:

.Instalar câmeras adicionais em pontos críticos: entradas dos depósitos, garagem, corredores e locais de alta circulação.

Automação no Controle de Veículos:

.Implementar um sistema de leitura automática de placas (LPR – License Plate Recognition) para controle de veículos.

.Instalar cancelas automáticas integradas ao sistema de segurança;

Reforço da Segurança Patrimonial:

.Adicionar rondas de segurança em horários estratégicos.

.Sensores de movimento nas áreas externas e nos depósitos.

.Alarmes conectados ao sistema da equipe de vigilância para detectar atividades não autorizadas.

Controle de Acesso Lógico

Identificação de Pontos Críticos:

Ausência de Autenticação Multifator (MFA): Apenas a senha é utilizada para acesso à distância aos servidores, elevando as chances de invasão.

Registros Incompletos: Falhas de acesso não são documentadas, o que complica a detecção de ataques.

Backups no Mesmo Local: Risco em situações de catástrofes físicas.

Falta de Defesas Avançadas: Não há referência a firewalls, criptografia ou IDS/IPS.

Sugestões de Aprimoramento:

Implementar MFA: Incluir autenticação via aplicativo ou biometria em todas as entradas.

Reativar e Acompanhar Registros: Anotar acessos inválidos e gerar notificações para tentativas duvidosas.

Backups Externos: Transferir cópias de segurança para armazenamento à distância ou na nuvem.

Criptografia de Dados: Garantir a proteção de dados em movimento e em repouso.

Aprimorar a Rede: Implementar firewalls e sistemas IDS/IPS para supervisão constante.

Ameaças Físicas e Vulnerabilidades

Ameaça	Descrição	Vulnerabilidade	Intensidade dos Riscos
Incêndio e explosões	A localização inadequada aumenta o risco de incêndios graves, podendo atingir a área administrativa e interromper as operações.	Proximidade entre gerador e botijões de gás.	Alta.
Acesso físico não autorizado	Ausência de sistemas automatizados de controle dificulta a rastreabilidade e permite invasões ou furtos.	Controle manual de entrada de veículos nos depósitos e garagem.	Alta.
Monitoramento das Áreas Críticas:	A infraestrutura de monitoramento limitada facilita ações mal-intencionadas sem registro.	Falta de câmeras de segurança em áreas críticas (depósitos, garagem e corredores de interligação).	Média.
Interrupções de energia prolongadas	A autonomia do gerador é insuficiente para períodos longos de interrupção elétrica, o que pode afetar os sistemas críticos e o armazenamento de backups.	Gerador limitado a 4 horas de operação.	Alta.
Dados e backup	A centralização das informações no prédio da TI sem redundância física eleva o risco de perda de dados em caso de eventos extremos.	Dados e backups armazenados no mesmo prédio.	Alta.

Análise dos riscos envolvidos ao negócio por ameaças lógicas/digitais

Ameaças Identificadas:

Ataques cibernéticos direcionados (ransomware, phishing, DDoS):

Impacto: Esses ataques podem bloquear ou sequestrar dados essenciais da empresa, causando interrupções nos serviços e perda financeira. Ataques de DDoS podem sobrecarregar os servidores, tornando os sistemas inacessíveis.

Probabilidade: Moderada a alta, dado que os sistemas estão acessíveis remotamente com pouca proteção robusta.

Acessos não autorizados (externos e internos):

Impacto: Possibilidade de roubo, manipulação ou exclusão de dados críticos. Internamente, funcionários mal-intencionados podem explorar brechas de controle.

Probabilidade: Alta, devido à ausência de autenticação multifatorial e controles rigorosos.

Exposição de dados sensíveis:

Impacto: Vazamento de informações sobre contratos, clientes ou operações pode levar a multas legais e danos à reputação.

Probabilidade: Alta, devido à centralização do armazenamento de dados e backups.

Alterações maliciosas no sistema:

Impacto: Sem monitoramento de tentativas de acesso falhas, invasores podem explorar sistemas sem serem detectados, comprometendo a integridade dos dados.

Probabilidade: Alta, considerando a falta de monitoramento em tempo real.

Vulnerabilidades:

Autenticação insuficiente:

Descrição: Ausência de autenticação multifatorial aumenta o risco de acessos não autorizados.

Consequência: Ataques de força bruta ou comprometimento de senhas expõem o sistema.

Centralização do backup:

Descrição: Backups e dados principais estão no mesmo local físico.

Consequência: Em caso de ataque ou desastre, toda a infraestrutura de dados pode ser perdida.

Monitoramento reduzido:

Descrição: O sistema não reporta tentativas de acesso falhas, o que limita a detecção de ataques ativos.

Consequência: Dificuldade em identificar e mitigar ataques antes que causem danos.

Falta de atualizações e auditorias regulares:

Descrição: Ausência de menção sobre práticas de atualização ou auditoria dos sistemas.

Consequência: Vulnerabilidades conhecidas podem permanecer expostas.

Avaliação da Intensidade dos Riscos:

Ataques cibernéticos: Impacto muito alto (disruptivo) e probabilidade moderada.

Acessos não autorizados: Impacto alto e probabilidade alta.

Exposição de dados: Impacto alto e probabilidade alta.

Monitoramento insuficiente: Impacto moderado e probabilidade alta.

Plano de Contingência

Categoria	Risco	Ação	Prioridade	Custo	Responsável
Segurança Física	Tanques de diesel e botijões próximos ao gerador, risco de incêndio/explosão.	Realocar ou isolar tanques e botijões, instalar barreiras e sistemas de detecção de	Alta	Alto	Equipe de Infraestrutura

		vazamentos e incêndios			
	Controle manual de portões e veículos vulnerável a falhas.	Automatizar portões com cancelas e leitura de placas (LPR).	Média	Médio	Setor de Logística
	Monitoramento limitado a uma única câmera.	Instalar câmeras adicionais nos depósitos, garagem e corredores.	Alta	Médio	TI e Segurança
Segurança Lógica	Falta de autenticação multifator (MFA).	Implementar MFA para acessos remotos.	Alta	Baixo	TI
	Registro de tentativas de acesso falhas desativado.	Reativar registros e configurar alertas automáticos.	Alta	Baixo	TI
	Ausência de sistemas de defesa avançados (firewall, IDS/IPS).	Adicionar firewalls avançados e IDS/IPS para proteção de redes.	Média	Médio	TI
Infraestrutura e Dados	Servidores e backups concentrados no prédio da TI, sem redundância.	Criar redundância de backups na nuvem ou em datacenters externos.	Alta	Médio	TI
	Gerador atual com autonomia limitada a 4 horas.	Adquirir um gerador com maior autonomia ou contratar energia alternativa.	Média	Alto	Infraestrutura
Protocolos de Resposta	Ausência de um plano de evacuação estruturado.	Desenvolver e treinar equipe em plano de evacuação para casos de incêndio/explosão.	Alta	Baixo	RH e Segurança
	Falta de coordenação em emergências.	Criar canais de comunicação emergenciais e uma Equipe de Resposta a Incidentes (ERI).	Alta	Baixo	Gerência Geral

Restauração de Sistemas	Demora na recuperação após falhas.	Priorizar o uso de backups externos/nuvem para recuperação rápida.	Alta	Médio	TI
	Falta de monitoramento da origem das falhas.	Implementar ferramentas de monitoramento em tempo real.	Média	Médio	TI
Recuperação e Testes	Falhas desconhecidas no plano de contingência.	Realizar análise pós-incidente e ajustar o plano conforme as necessidades.	Média	Baixo	Gerência Geral
	Necessidade de treinar equipe regularmente.	Realizar simulações e testes bimestrais para verificar a eficácia do plano.	Média	Baixo	RH e TI

Ameaças a Que o Ambiente e os Negócios Estão Sujeitos

Controle de acesso físico:

Na Planta: Os corredores interligam todos os prédios e permitem livre circulação.

Isso pode ser explorado para acessos não autorizados a áreas críticas, como prédios de TI.

Solução: Implementar barreiras físicas ou controles de acessos nos corredores. Pode-se adotar portas com autenticação biométrica nos acessos a prédios mais sensíveis, como o de Tecnologia da Informação e Segurança.

Monitoramento das Áreas Críticas:

Na Planta: Apenas uma câmera cobre as instalações, enquanto áreas sensíveis (TI, depósitos e garagem) são interligadas.

Solução: Adicionar câmeras nos pontos de entrada/saída de cada prédio, além de corredores. Isso garante melhor visibilidade e rastreamento de movimentações.

Segurança Contra Incêndios:

Na planta: A proximidade entre a garagem/manutenção (com gerador e tanque de diesel) e a administração (cozinha com botijões de gás) aumenta o risco de incêndios e acidentes químicos.

Solução: Isolar o gerador e o tanque de diesel em local aberto, deixar o botijão em um abrigo fora da edificação, instalar uma parede de contenção em alvenaria para separar o gerador e o tanque de funcionários, instalar e sinalizar o uso dos extintores em pó (quantidade de extintores irá depender do tamanho em litros do tanque), fazer um dique de contenção para o tanque (ambos do mesmo volume) e uma caixa separadora de água e óleo, além de sistemas automáticos de supressão de incêndio e detector de fumaça.

exemplo de dique de contenção para tanque de diesel

Dados e backup:

Na planta: Os servidores e backup estão localizados apenas no prédio de TI, sem redundância em outras edificações ou locais externos.

Solução: Criar uma redundância de backup no local remoto e/ou na nuvem, também reforçar a proteção no prédio de TI.

Continuidade operacional:

Na planta: O gerador tem uma autonomia limitada apenas a 4 horas, o que pode comprometer a operação em casos de falta de energia prolongada.

Solução: Aumentar a autonomia do gerador ou contratar serviços de backup energético (Fonte de energia alternativa de eletricidade que se ativa automaticamente ou manualmente em caso de falhas na rede elétrica).

Treinamento e procedimentos de segurança:

Na planta: Os corredores e o sistema atual de controle manual podem ser explorados em situações de emergência ou intrusão.

Solução: Realizar treinamentos periódicos com todas as equipes sobre protocolos de emergência e segurança. Além de simulações para situações de evacuação e intrusão.

Aspecto lógico: ameaças, vulnerabilidades e mitigação

Ameaças:

Comprometimento de credenciais:

Exemplo: Um funcionário pode ter sua senha roubada via phishing.

Impacto: Acesso completo a sistemas críticos da empresa.

Invasões externas (ataques remotos):

Exemplo: Hackers explorando portas abertas e vulnerabilidades não corrigidas.

Impacto: Sequestro de dados, interrupções nos serviços e danos financeiros.

Uso indevido de privilégios internos:

Exemplo: Funcionários com acesso além do necessário podem modificar ou excluir dados intencionalmente ou acidentalmente.

Impacto: Perda de dados importantes e possíveis litígios.

Falha no sistema de backups:

Exemplo: Um desastre no prédio da TI pode destruir backups e dados principais simultaneamente.

Impacto: Perda irreparável de informações essenciais.

Vulnerabilidades:

Falta de MFA:

A autenticação por senha única é insuficiente para proteger acessos remotos.

Armazenamento centralizado de dados:

A ausência de redundância geográfica para os backups representa um ponto único de falha.

Relatórios limitados:

Desativar o monitoramento de tentativas falhas reduz a visibilidade de ameaças ativas.

Segurança proativa insuficiente:

Não há menção de firewalls avançados ou sistemas de detecção de intrusão (IDS/IPS).

Medidas de Mitigação:

Implementar autenticação multifatorial (MFA):

Impacto: Aumenta significativamente a proteção contra acessos não autorizados.

Armazenar backups em local externo e na nuvem:

Impacto: Garante redundância em caso de ataques ou desastres físicos.

Reativar monitoramento de tentativas de acesso falhas:

Impacto: Melhora a capacidade de detectar e reagir a ataques antes que causem danos.

Segregar privilégios de acesso:

Impacto: Reduz os riscos de mau uso de permissões.

Realizar auditorias regulares e aplicar patches de segurança:

Impacto: Fecha brechas de segurança conhecidas e mantém o sistema atualizado.

Implementar firewalls avançados e sistemas IDS/IPS:

Impacto: Detecta e bloqueia tentativas de intrusão automaticamente.

Essas medidas envolvem custos adicionais, mas são críticas para proteger os dados e manter a continuidade do negócio. A prioridade deve ser estabelecer MFA e uma solução de backup externa, que oferecem proteção imediata e significativa.

Solução de TI Para o Negócio

1. Acesso físico aos ambientes

Aspectos deficientes:

Controle de acesso no prédio de TI: Embora o acesso ao prédio de TI seja restrito, com a utilização de crachás de identificação para os funcionários, o sistema de segurança no local parece ser limitado a uma catraca simples e uma única câmera. Isso pode representar um risco, pois a câmera única não proporciona cobertura abrangente, e a catraca, por ser simples, pode ser burlada.

Segurança nas áreas de depósito e administração: Não há menção explícita de controles rigorosos para o acesso às áreas de depósito (pericíveis e não pericíveis) ou administração. Embora a área de TI tenha um controle de acesso mais rigoroso, as demais áreas podem estar mais expostas.

Propostas de melhoria:

Upgrade do sistema de controle de acesso: Substituir a catraca simples por um sistema de controle biométrico, que seja mais difícil de ser burlado. Isso garantiria que apenas pessoas autorizadas tivessem acesso às áreas críticas da empresa.

Implementação de barreiras físicas: Instalar barreiras físicas nas áreas críticas (como depósitos e administração) para garantir que o acesso não autorizado seja evitado.

2. Armazenamento de informações e servidores

Aspectos deficientes:

Segurança dos servidores: Os servidores, que armazenam todas as informações críticas, incluindo dados do sistema de TI e backups, estão localizados em um único prédio (prédio de TI). Isso cria um ponto único de falha em caso de ataque físico ou desastre.

Backup de dados: O armazenamento de backups ocorre no mesmo local que os dados originais, o que representa um risco em caso de desastre (ex. incêndio, inundação, etc.), já que ambos os dados poderiam ser perdidos simultaneamente.

Acesso remoto: O acesso remoto aos servidores por parte da equipe de TI à distância, embora conveniente, pode ser um ponto de vulnerabilidade, especialmente considerando que o sistema de registros de acessos falhos foi desativado. Isso dificulta o rastreamento e a análise de tentativas de acesso não autorizadas.

Propostas de melhoria:

Implementação de redundância geográfica para backup: Criar uma solução de backup em locais fisicamente separados (backup em nuvem ou em datacenters terceirizados) para garantir que, em caso de falha no prédio de TI, os dados sejam preservados e recuperáveis.

Fortalecimento da segurança de acessos remotos: Reativar o monitoramento das tentativas de acesso falhas e implementar autenticação multifatorial (MFA) para o acesso remoto aos servidores. Isso dificultará acessos não autorizados, proporcionando maior controle sobre quem está acessando os dados da empresa.

Segurança física do prédio de TI: Melhorar a segurança física do prédio de TI com sistemas de controle de acesso mais robustos, como trancas eletrônicas e biometria, além de reforçar a segurança física com vigilância contínua e alarmes.

3. Gerador e infraestrutura crítica

Aspectos deficientes:

Localização do gerador: O gerador está localizado no prédio da garagem, próximo a tanques de diesel e botijões de gás, o que cria um risco significativo de incêndio ou explosão, com a possibilidade de comprometer toda a infraestrutura de TI e outros prédios críticos da empresa.

Falta de monitoramento constante de itens críticos: Não há informações sobre sistemas de monitoramento contínuo para o gerador e os tanques de combustível, o que pode resultar em falhas inesperadas ou situações de risco.

Propostas de melhoria:

Revisão da localização do gerador: Considerar a realocação do gerador para um local mais seguro e afastado de fontes de risco (como tanques de diesel e botijões de gás). Caso a realocação não seja viável, deve-se reforçar a proteção contra incêndio, com sistemas de extinção automáticos e uma zona de contenção para possíveis vazamentos de combustível.

Monitoramento remoto da infraestrutura crítica: Implementar um sistema de monitoramento remoto para o gerador e tanques de diesel, com alertas automáticos em caso de falhas ou riscos potenciais (como vazamentos, falhas mecânicas ou níveis baixos de combustível).

4. Segurança cibernética e controle de acesso aos sistemas

Aspectos deficientes:

Acesso remoto sem monitoramento completo: O sistema de controle remoto não registra completamente todas as tentativas de acesso (principalmente falhas), o que dificulta a detecção de comportamentos suspeitos e pode abrir brechas para invasões externas ou acessos não autorizados.

Ausência de segregação de redes: A rede de TI parece ser um ambiente único para todas as operações, o que pode representar um risco de propagação de ataques em caso de invasões.

Propostas de melhoria:

Reativação do monitoramento completo de acessos: Reativar a funcionalidade de registro de tentativas de acesso falhas e configurar alertas automáticos para o administrador em caso de múltiplas falhas de acesso em curto espaço de tempo, indicando possíveis tentativas de invasão.

Segmentação da rede interna: Implementar a segmentação da rede interna para isolar dados e sistemas críticos, limitando o alcance de um possível ataque. Isso pode incluir a criação de sub-redes separadas para diferentes departamentos (ex. TI, administração, segurança), com firewalls entre elas.

Atualização e monitoramento constante de sistemas de segurança: Garantir que os sistemas de segurança cibernética (como antivírus, firewalls e sistemas de detecção de intrusão) sejam atualizados regularmente e que haja monitoramento contínuo de tráfego de rede e atividades de acesso para detectar e neutralizar ameaças proativamente.

Tabela de Custos

Câmeras	R$5.000 a R$8.000
Catracas biométricas	R$9.000 a R$15.000
Isolamento do tanque + gerador novo	Cerca de R$120.000
Abrigo para botijão de gás	R$3.000

Ana Beatriz (824213857)

Daniel M (824149395)

Fabrício B (82413485)

Gabriel T (824140830)

Guilherme C (824141375)

Gustavo B. (824154722)