1) É mencionado no documento que o controle de acesso é feito por meio das catracas com crachás para os funcionários e mencionam que há apenas uma câmera de segurança nessa região, esperaríamos encontrar mais funcionários da segurança e um sistema mais automatizado como a catraca biométrica para auxiliar no acesso dos funcionários nas dependências da empresa e mais câmeras de segurança internas no prédio para a visualização de quem está entrando e saindo do ambiente de trabalho.

   Dito isso propomos uma mudança a alteração da catraca simples para uma catraca biométrica para a maior segurança e controle de acesso dos funcionários e a instalação de mais câmeras internas nessa região.

2) O documento cita que Todos os servidores são acessíveis externamente por meio de nome de usuário e senha. Embora isso permita que a equipe de TI trabalhe remotamente, também representa um risco, no caso das credenciais de acesso forem comprometidas. também não foi mencionado o uso de criptografia para a proteção de dados.

   Dito isso propomos a mudança de login acrescentando um aplicativo de autenticação de 2 fatores para ter a certeza de quem está entrando no sistema e a divisão de acesso do sistema por cargos baseado na posição hierárquica de cada funcionário. E uma criptografia forte para garantir a segurança e integridade dos dados armazenados.

3) **Risco físico de invasão:** Um não funcionário conseguir acessar a empresa através de um cartão de um funcionário por não haver confirmações - Risco Alto.

   Risco físico de explosão: Os botijões de gás estão muito próximos do gerador e dos tanques de Diesel representando um risco alto de incêndios e explosões, a falta de protocolos de segurança contra incêndios, como extintores, sistemas de alarme ou plano de evacuação podendo causar explosões de escalas ainda maiores – Risco Alto.

   Risco do controle manual: O controle manual pode apresentar riscos caso o segurança não esteja disponível a todo momento ou podendo haver erros da parte do mesmo, podendo comprometer a logística da empresa.

   Risco físico de Intoxicação: Vazamento de gás ou cheiros dos produtos perecíveis podendo levar ao mal-estar dos funcionários – Risco Médio.

Risco de infestação animal: Produtos perecíveis vencidos a muito tempo podendo atrair animais peçonhentos ao ambiente - Risco Médio.

Riscos ambientais: Produtos perecíveis e não perecíveis prejudiciais a natureza – Risco Médio.

4) **Risco de invasão:** função de alertar logins falhos desativados, portanto, não sabendo se outros indivíduos estão tentando acessar o sistema – Risco Alto.

   Perda de backup: por ser armazenada em um só local – Risco Alto.

   Registro de acesso: logins enviados apenas uma vez por mês, o que está errado, pois a Administração tem que estar ciente de quem entra e sai do sistema a todo momento - Risco Alto.

   Falha de autenticação e autorização: funcionários do TI tem total acesso a partes restritas do sistema – Risco Alto.

5) Colocar câmeras adicionais nas áreas como depósitos e garagem, isso garantirá o monitoramento contínuo e ajudará a prevenir e identificar incidentes de segurança:

   Substituir o controle manual da abertura de portões pelos seguranças por um sistema automatizado de controle de acesso (como catracas biométricas).

   Implementar sensores de fumaça e um sistema de alarme contra incêndios, especialmente em áreas de risco como a garagem (onde estão o gerador e os botijões de gás) e instalar extintores de incêndio e fornecer treinamento aos funcionários sobre procedimentos de evacuação e segurança contra incêndios.

   Adotar autenticação multifatorial, criptografar dados e monitorar tentativas de acesso falhas.

   Criar um plano de recuperação de desastres, realizar treinamentos e garantir que sistemas estejam protegidos.

6) O posicionamento dos botijões de gás próximo ao gerador de tanques de diesel representa um risco significativo de incêndio. E com a falta de extintores e sistemas de alarmes compromete uma resposta rápida para caso tenha uma emergência.
   A ausência de um plano de evacuação e treinamentos de segurança deixa a equipe totalmente vulnerável. Animais em áreas específicas também mostra um risco.
   As soluções propostas que irá resolver esses erros seria instalar sensores de fumaça e sistema de alarme para detecção rápida de incêndios, desenvolver e implementar um plano de evacuação com treinamentos regulares para cada equipe, relocar os botijões de gás para uma outra área que seja segura, instalar extintores em pontos estratégicos para caso tenha incêndio.

7) Baseado no cenário que foi descrito, conseguimos analisar algumas venerabilidades no sistema que possam ser exploradas para ataques a fim de causar danos e perdas para a sua empresa. Vamos abordar os principais riscos encontrados e sugerir formas para a mitigação.

   Riscos encontrados:

   1-**Acessos não autorizados ao sistema:**
   Vulnerabilidades:
   1. O acesso ao sistema (login) é realizado apenas pelo usuário e senha do funcionário, apresentando um perigo caso a senha do funcionário não seja uma senha com um alto grau de dificuldade.
   2. Falta de autenticação multifatorial, para que seja necessário um código de confirmação para o funcionário que esteja realizando o acesso ao sistema.
   3. Desativação do relatório de tentativas de login falhas, podendo ocultar as tentativas de acesso indevido que o sistema possa sofrer.

   Mitigações: Para este primeiro risco, propomos a alteração de todas as senhas dos usuários exigindo símbolos, números, letras maiúsculas e minúsculas, a fim de tornar mais difícil o acesso de um não funcionário; reativar o monitoramento de logins falhos, para maior controle de sistema e conseguir identificar ameaças e implementação de autenticação multifatorial aumentando a segurança do sistema.

   2-**Ataques de malwares:**
   Vunerabilidades:

1. O fato de todos os servidores estarem conectados à rede e acessíveis externamente pode ser uma porta de entrada para ransomware e outros tipos de malware, especialmente se os sistemas não forem adequadamente protegidos.
2. Funcionários remotos podem inadvertidamente baixar e instalar software malicioso ao acessar a rede da empresa de dispositivos inseguros ou ao clicar em links de phishing.

Mitigações: Propomos a implementação de ferramentas de detecção e prevenção de intrusões (IDS/IPS) para que possam identificar e bloquear atividades maliciosas em tempo real; realizar treinamento para a equipe para que eles consigam identificar phisings e outras ameaças; manter todos os sistemas e softwares atualizados.

3-**Vazamento de dados:**
Vunerabilidades:

1. O armazenamento de dados sensíveis no próprio servidor da empresa, sem criptografia adequada, pode expor informações confidenciais, como dados de clientes e funcionários.

Mitigações: Propomos a implementação de criptografias para garantir que em caso de vazamento as informações sejam ilegíveis; utilizar soluções de backup criptografado e garantir que os backups sejam armazenados em locais seguros e de forma redundante (por exemplo, backups em nuvem ou em servidores externos).

4-**Perda de dados ou falha na infraestrutura:**
Vunerabilidades:

1. O armazenamento de backups no mesmo prédio pode representar um risco de perda de dados se houver um incidente no local (como incêndio ou roubo).
2. Embora a empresa tenha um gerador de backup para manter o prédio funcionando por até 4 horas, uma falha de energia ou um desastre maior pode afetar a continuidade dos negócios, especialmente se os servidores e os sistemas críticos não forem protegidos adequadamente.

Mitigações: Propomos implementar backup em nuvem, garantindo que os dados estejam seguros e possam ser restaurados rapidamente em caso de falha física no prédio da TI e testar periodicamente os procedimentos de recuperação de desastres para garantir que a empresa possa rapidamente retomar as operações caso um incidente aconteça.

8) Análise crítica de uma solução de TI para um negócio em termos de segurança envolve identificar deficiências e propor melhorias.

Deficiências comuns incluem:

Rede de segurança: Firewall fraco e controlos de acesso, Wi-Fi erradamente configurada e falta de rede divisão.

Segurança de dados: Dados não estão sendo criptografado, backups insuficientes e acesso irrestrito a informações sensíveis.

Controle de identidade e acesso Falta de autenticação: senha fraca e permissões não controladas.

Segurança do aplicativo: Vulnerável aplicativo software, falta de processo de atualização e rastreamento de vulnerabilidades de segurança

Formação do pessoal: baixa conscientização da segurança e escassez de treinamento em práticas seguras.

Resposta a incidente: falta de planos de resposta, detecção tardia de ameaças.

Sugestões para melhorias: Fortalecer firewalls, criptografar dados e seccionar a rede.

Estabelecer backups seguros e controlar o acesso com rigor.

Promover a política de senhas fortes e verificar frequentemente os acessos.

Atualizar regimes de atualização de sistemas num intervalo regular e encontrar as suas vulnerabilidades.

Esclareça regularmente os funcionários acerca de práticas de segurança" incluindo simulação ".

Desenvolver um plano de resposta a incidentes e aplicar o monitoramento contínuo da segurança Linha segura de proteção em longo prazo " constitui fazer segurança de TI como processo continuado envolvendo tecnologia, processos bem-organizados e treinamento apropriado visando a proteção das operações e informações, negócios dados contra qualquer golpe.

Valores de todas as implementações:

Mudanças	Valores
Catraca Facial Controlid Idblock Next Com Duas Leitoras	R$9.000,00
Relógio de Ponto iDClass - Eletrônico Biométrico e Proximidade	R$4.000,00
Câmera Inteligente Full Color com Autotracking iM7 Branca Intelbras	R$5.000,00
Armazem para Botijões de gas	R$20.000,00
Implementações de Software	R$20.000,00
Treinamentos	R$14.000,00
Total	R$72.000,00