***obs:** montar um slide de forma dinâmica, a seu pedido.

Controle de Acesso Físico:

- Esperaríamos encontrar uma restrição de acesso entre os departamentos de administração e da tecnologia da informação e segurança, onde, por exemplo, os funcionários de outras áreas não teriam acesso ao departamento de TI, o mesmo que contém diversos dados e informações importantes que devem ser restritos, para isso, seria necessário a implementação da biometria facial para o acesso em cada departamento. O que geraria em média um custo de 30 mil reais anualmente, mas que, ainda sim, valeria muito a pena, comparado aos gastos de uma perda de dados importantes da empresa e na recuperação deles.

- Percebemos a presença de vulnerabilidade e desatualização na entrada do prédio através da garagem, o controle manual pode estar sujeito a enganos, erros ou pessoas mal intencionadas, assim facilitando o acesso de pessoas não permitidas. Para isso, seria fundamental a implementação do acesso automático através da biometria facial de cada um dos membros da empresa. Obtendo um gasto médio de 20 mil reais, valor muito satisfatório em relação ao prejuízo de um possível tipo de roubo, furto ou danificação na empresa.

- Também é perceptível, que o acesso para entrar no prédio, é feito através de autenticação de crachá com nome e foto do funcionário para liberação. Mesmo tendo um certo nível de segurança, tem uma grande possibilidade de termos falhas, como por exemplo: furto de cartão de funcionários, assim concedendo acesso ao prédio para qualquer pessoa com o cartão deste funcionário. Pensando neste projeto como um todo, achamos que a melhor solução é expandirmos as restrições de biometria facial, adicionando-as também na entrada do nosso prédio, o que nos custaria em média de 20 a 35 mil reais. Onde todos os funcionários teriam sua biometria facial cadastrada. Essa implementação, além de proporcionar um controle de acesso mais eficiente e seguro, contribuirá para a melhoria contínua dos processos de segurança, alinhando-se com as melhores práticas adotadas no mercado para proteção de espaços corporativos.

- Visto que em uma empresa que possui 5 edificações interligadas e contém, uma única câmera na instalação apresenta falhas no controle de acesso, esperávamos ao menos três câmeras por departamento, em lugares estratégicos como: portas de entrada, áreas sensíveis e áreas externas. A implementação de câmeras vai custar em média 45 mil reais, contando com a instalação e cabeamento, sistema de armazenamento e custo das câmeras.

Controle de Acesso Lógico:

- Esperaríamos encontrar um método mais seguro para os funcionários realizarem o acesso nos servidores. Como o acesso é feito apenas com o usuário e senha, tem uma grande probabilidade de funcionários deixarem estes dados vulneráveis e expostos em muitos casos, tendo em vista que eles podem acessar de qualquer lugar, por conta do home office. A solução para isto, seria a empresa solicitar um reforço na senha, com o mínimo de 8 caracteres, incluindo caracteres especiais. O acesso, só pode ser feito através de dispositivos previamente autorizados pelo sistema de segurança da empresa, através de uma validação instalada no dispositivo de acesso. Permissões para alterações em servidores com dados sensíveis, serão permitidas apenas com a aprovação de no mínimo 2 administradores responsáveis pelo servidor. O custo estimado para a implementação inicial fica entre 15 a 45 mil reais com custos recorrentes de manutenção e suporte que podem variar de R$500,00 a R$2.000,00 por mês.

- Além da evolução e segurança no controle de acesso, também é necessário saber quem está tentando acessar os servidores, portanto, é inadmissível o desligamento dessa funcionalidade, deve-se ativar essa função, plenamente configurada para identificar todas as informações de possíveis intrusos em caso de falhas ao tentar acessar o sistema.

Riscos Físicos:

- 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.

- 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.

- vulnerabilidades em sistemas desatualizados.

- **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.
    - **Danos à reputação:** Vazamentos de dados de clientes podem gerar perda de confiança entre empresa e usuários.

- **Exemplo:** Uma falha em atualizar o firewall permitiu a entrada de um ransomware, criptografando todos os dados e paralisando as operações até o pagamento de resgate.

- **Soluções e mitigação:**

    - **Treinamento de funcionários:** Promover a conscientizaç
    -
    - **Riscos Lógicos:**

    -
    - **Possíveis ameaças:** Malware, ataques de phishing; ão sobre ataques de phishing e boas práticas de segurança.
    - **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.

Plano de Contingência:

1. Recursos Críticos:

- Energia: Gerador com capacidade limitada (4 horas).
- Segurança: Catracas, câmeras e controle manual na garagem.

2. Análise de Impacto nos Negócios:

- Falta de energia prolongada: Impacta sistemas essenciais, inclusive servidores e segurança física.
- Falhas no controle de acesso físico: Vulnerabilidades permitem acessos não autorizados, expondo a empresa a furtos e sabotagem.

3. Estratégias de Recuperação:

Energia Alternativa:

- Fechar contrato com fornecedores locais de diesel para reabastecimento imediato em emergências.

Segurança Física:

- Ampliar o uso de biometria facial em todos os pontos de entrada.
- Instalar câmeras de segurança adicionais em áreas estratégicas (garagem, depósitos e entradas).
- Automatizar o controle de acesso na garagem, eliminando a dependência de operadores manuais.

4. Plano de ação:

Contrato com Fornecedores: Fechar parceria para reabastecimento rápido de combustível diesel.

- Responsável: Equipe de Administração
- prazo e valores médios: 1 mês. ((R$ 20.000/anual)

Ampliar Biometria**:** Instalar biometria facial em todas as entradas de prédios.

- Responsável: Segurança Patrimonial.
- prazo e valores médios: 1 mês. (R$ 20.000–35.000)

Câmeras de Segurança**:** Adicionar câmeras em áreas externas e internas em pontos estratégicos.

- Responsável: Equipe de Segurança
- prazo e valores médios: 1 mês. Médio (R$ 45.000)

5. Teste do Plano

Simulação de Falha de Energia:

- Testar o acionamento do gerador primário e secundário.

Testes de Segurança Física:

- Simular tentativas de entrada sem autorização em diferentes áreas.
- Testar a eficácia da biometria e câmeras no monitoramento e registro.

Ameaças Físicas:

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:

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.

Como mitigar as ameaças:

- **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.

- Realizar campanhas regulares de treinamento sobre phishing para os colaboradores.

Solução 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.

Artur Rosa Correia - **824135943**

Gustavo Silveira Benicio - **824134160**

Luan Bernardo Alves - **824134204**