OFFICESOLUTIONS

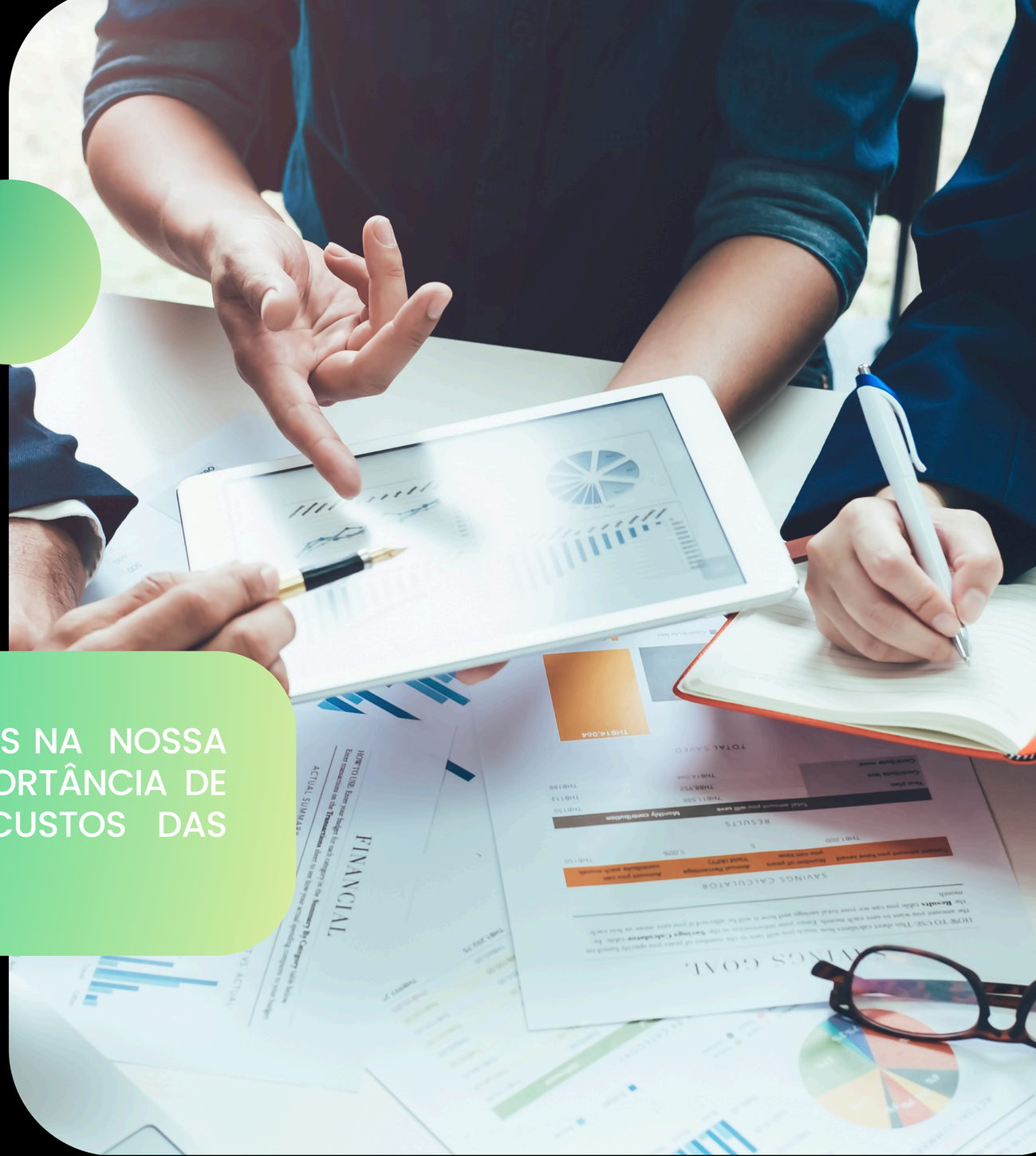
ESTUDO DE CASO

OFFICESOLUTIONS@OUTLOOK.COM.BR

OFFICESOLUTIONS

A DISCUITIR: CASOS

FORAM ANALISADOS FRAGILIDADES E RISCOS NA NOSSA EMPRESA, E FOI DECIDIDO A EXTREMA IMPORTÂNCIA DE MITIGAR OS POSSÍVEIS RISCOS E OS CUSTOS DAS RESPECTIVAS MUDANÇAS.



OFFICESOLUTIONS

ACESSO À EMPRESA

O Acesso por cartão, não entrega segurança, uma vez que qualquer pessoa pode acessar a edificação caso tiver o cartão de outro funcionário.

O controle deveria ser realizado por biometria, tal como o registro de ponto, deixando o cartão do funcionário só para forma de identificação do mesmo e com intuito de restringir o acesso em alguns ambientes por nível de hierarquia.

OFFICESOLUTIONS.

Câmeras deveriam estar espalhadas pela empresa inteira, não somente na porta de entrada, garantindo mais segurança e também filmagens de eventuais acidentes ou furtos para análise e tomada de decisão.

OFFICESOLUTIONS

ACESSO LÓGICO

Não deveria ter somente um administrador, deveria ser no mínimo três administradores, assim caso ocorra algum erro por parte de um administrador, os outros dois podem verificar e mitigar esse erro, ou, nesse caso, que ele o próprio administrador desligou a função de acessos falhos os outros poderiam religar a mesma.

O controle de acesso remoto deve ser somente disponível a TI e chefe da administração, e mesmo assim com autenticação de dois fatores e alguns acessos restritos para maior segurança.

OFFICESOLUTIONS

AMEAÇAS FÍSICAS IDENTIFICADAS

Acesso não autorizado:

- Controle manual nos portões; falhas humanas.
- Entrada por catraca simples sem validação robusta.
- Ausência de câmeras em áreas críticas (exceto TI).

Incêndio ou explosão:

- Botijões de gás próximos ao prédio administrativo e ao tanque de diesel do gerador.

Furtos e sabotagens:

- Servidores de TI centralizados no mesmo prédio sem medidas adicionais de proteção.
- Armazenamento de backups no mesmo local, aumentando o risco em caso de incidentes.

Interrupção de operações:

- Gerador suporta apenas 4 horas, insuficiente para manter operações durante apagões prolongados.

OFFICESOLUTIONS

AMEAÇAS LÓGICAS/DIGITAIS IDENTIFICADAS

Acessos não autorizados:

- Todos os servidores são acessíveis remotamente com credenciais básicas (usuário e senha), sem autenticação multifator.
- Relatórios de tentativas de acesso falhas estão desativados.

Ataques cibernéticos:

- Falta de menção a firewalls, VPNs ou outras barreiras de proteção contra ataques externos.
- Dados confidenciais armazenados apenas localmente, sem backups externos.
- Perda ou comprometimento de dados:
- Backup armazenado no mesmo local que o servidor principal, expondo ambos a desastres físicos.

Phishing e engenharia social:

- Possibilidade de ataques à equipe por e-mail ou outras formas, dado o modelo de trabalho remoto.

OFFICESOLUTIONS

AVALIAÇÃO DA INTENSIDADE

Ameaças Físicas:

- Acesso não autorizado: Alta intensidade.
- Incêndio/explosão: Média a alta intensidade.
- Furtos/sabotagens: Alta intensidade.
- Interrupção de operações: Média intensidade.

Ameaças Lógicas:

- Acessos não autorizados: Alta intensidade.
- Ataques cibernéticos: Alta intensidade.
- Perda de dados: Alta intensidade.
- Phishing: Média intensidade.

OFFICESOLUTIONS

PLANOS DE CONTINGÊNCIA

1. Diversificação do Armazenamento de Dados: implementar backups na nuvem e em local físico externo em caso de perda de dados ter uma forma de recuperá-los.

2. Aprimoramento da Infraestrutura de Energia: adicionar um segundo gerador ou baterias de backup em caso de falhas graves na energia ou desastres naturais.

3. Monitoramento e Relatório de acessos remotos: adotar um sistema de logs mais detalhado para identificar com mais clareza um infrator, funcionário mal intencionado e possíveis ataques cibernéticos.

OFFICESOLUTIONS

AMEAÇAS E VULNERABILIDADES FÍSICAS

1. Incêndios e Desastres Naturais (instalar sprinklers, alarmes de fumaça e treinar os funcionários).

2. Falhas de Energia (implementar redundância de geradores e sistemas de UPS).

3. Roubo e vandalismo (melhorar controle de acesso com biometria e instalar mais câmeras de vigilância).

4. Falhas de Sistema e Cybersecurity (implementar autenticação multifator, firewalls e auditorias regulares de segurança).

OFFICESOLUTIONS

AMEAÇAS E VULNERABILIDADES LÓGICAS

1 . Acessos não autorizados: senhas fracas e falta de autenticação forte (Implementar 2FA e senhas complexas).

2. Phishing: Engano de funcionários para roubo de credenciais (treinamento e simulações de phishing).

3. Malwares/Ransomware: Risco de perda de dados (antivírus atualizado e backups automáticos).

OFFICESOLUTIONS

VULNERABILIDADES E MITIGAÇÕES

- **Falta de automação no monitoramento.**
- Mitigação: Alertas de segurança em tempo real.

- **Dependência de um único servidor de câmera.**
- Mitigação: Backup na nuvem.

- **Gerador limitado a 4 horas.**
- Mitigação: Ampliar reserva ou adicionar outro gerador.

OFFICESOLUTIONS

A ANÁLISE DA INFRAESTRUTURA DE TI DA EMPRES DETECTOU VULNERABILIDADES CRÍTICAS QUE PRECISAM DE ATENÇÃO PARA PROTEGER OPERAÇÕES E INFORMAÇÕES SENSÍVEIS. AS PRINCIPAIS QUESTÕES SÃO:

- **Acesso Remoto** (problemas em usar login com senhas únicas, por expor o sistema a ataques de força bruta).
- **Políticas de Senhas** (reutilização de senhas fracas por funcionários).
- **Monitoramento de ameaças** (ausência de ferramentas robustas para identificação de atividades suspeitas).
- **Controle de Acesso Físico** (dependência de catracas e crachás)
- **Treinamento de funcionários** (falta de conscientização sobre pishing, engenharia social e planos de contingência.

OFFICESOLUTIONS

RECOMENDAÇÕES

- **Acesso Remoto:** Implementar autenticação multifator (MFA) para aumentar a segurança.
- **Políticas de Senhas:** Adotar políticas de senhas fortes, bloqueios automáticos após tentativas falhas e mudanças periódicas de senhas.
- **Monitoramento de ameaças:** Utilizar sistemas IDR/EDR e SIEM para análise e resposta em tempo real.
- **Controle de Acesso Físico:** Implementar biometria, câmeras de alta resolução e armazenamento seguro de gravações.
- **Treinamento de funcionários:** Programas regulares de treinamento e simulações de ataques para aumentar a preparação.

CUSTOS:

INFRAESTRUTURA:

Registros de ponto por biometria (controle de entrada e saída).	- **R$ 900,00**
Câmeras de Segurança (prevenir possíveis furtos).	- **R$ 1.800,00**
Câmeras adicionais (estimativa de **R$ 2.000,00** por câmera, totalizando 5 câmeras).	- **R$ 10.000,00**
Controle de acesso eletrônico (**R$ 5.000,00** por portão, totalizando 3 portões).	- **R$ 15.000,00**
Separação de botijões e tanque de diesel (evitar e prevenir incêndios).	- **R$ 8.000,00**
Upgrade no gerador (dobrar a autonomia para 8 horas).	- **R$ 20.000,00**
Setup externo (aumentar segurança de dados com backups externos)	- **R$ 10.000,00**
Aprimoramento da infraestrutura de Energia (novo gerador ou sistema de baterias)	- **R$ 50 à 40 mil**

OFFICESOLUTIONS

CUSTOS:

INFRAESTRUTURA:

Instalação de sprinklers, alarmes de fumaça e treinamento de funcionários (plano de contingência em caso de incêndio e desastres naturais).

- **R$ 15.000,00 + R$ 3.000,00**

Falhas de Energia (implementar redundância de geradores e sistemas de UPS).

- **Novo gerador ou sistema de baterias (incluso no plano de contingência).**

Roubo e vandalismo (melhorar controle de acesso com biometria e instalar mais câmeras de vigilância).

- **Sistema de Biometria e Câmeras (incluso no plano de contingência).**

OFFICESOLUTIONS

CUSTOS:

AMEAÇAS LÓGICAS/DIGITAIS:

Contratação De 2 Administradores (maior segurança de acessos).	- **R$ 5.000,00.**
Autenticação multifator (configurações e licenças).	- **R$ 12.00,00.**
Firewalls e VPNs robustas.	- **R$ 15.000,00.**
Backups externos.	- **R$ 10.000,00** anuais.
Treinamento de conscientização.	- **R$ 5.000,00** para a equipe completa.
Monitoramento e Relatório de acessos remotos (adotar um sistema de logs mais detalhado).	- **R$ 5.000,00** custo do software.
Falhas de Sistema e Cybersecurity (implementar autenticação multifator, firewalls e auditorias regulares de segurança)	- **R$ 10.000,00** os sistemas e **R$ 2.000/mês** auditorias regulares.

OFFICESOLUTIONS

CUSTOS:

AMEAÇAS LÓGICAS/DIGITAIS:

Implementar 2FA e senhas complexas.

Treinamento e simulações de phishing.

Antivírus atualizado e backups automáticos.

Alertas de segurança em tempo real.

Backup na nuvem.

Ampliar reserva ou adicionar outro gerador.

O custo total estimado da operação varia entre **R$ 20.000,00** e **R$ 150.000,00**, dependendo das soluções escolhidas, como 2FA, antivírus, backups, ferramentas de monitoramento e ampliação de gerador.

OFFICESOLUTIONS

OBRIGADO A TODOS, PELA ATENÇÃO!

- Wesley Gomes dos Santos - 82422607
- Italo Jonas Lima Gomes - 824218750
- Matheus Bovo Ribeiro - 824138656
- Rafael Martins Cezar - 82425725
- Felipe Gatti - 824125546

OFFICESOLUTIONS