ANÁLISE DE VULNERABILIDADES **DIGITAIS E FÍSICAS**

Estudo de Caso

OfficeSollutions

INTEGRANTES

ANA CAROLINA DOS REIS RAMOS 82413448

MILENA D. PAVANI 824213909

PROFESSORA EDMILA

SOLUÇÕES COMPUTACIONAIS E SEGURANÇA

TÓPICOS

01 CONTROLE DE ACESSO FÍSICO AO EDIFÍCIO

02 CONTROLE DE ACESSO LÓGICO AOS SISTEMAS

03 RISCOS AO NEGÓCIO POR AMEAÇAS FÍSICAS

04 RISCOS AO NEGÓCIO POR AMEAÇAS DIGITAIS

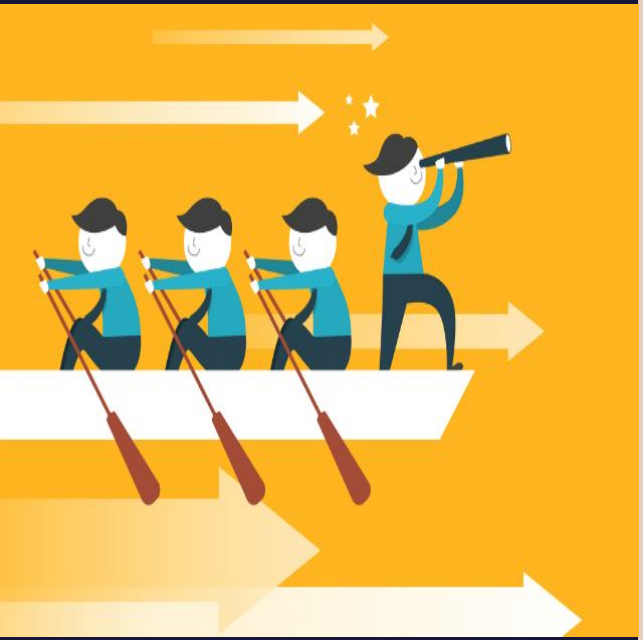
TÓPICOS

05 PLANO DE CONTINGÊNCIA

06 AMEAÇAS FÍSICAS AO AMBIENTE E NEGÓCIO

07 AMEAÇAS LÓGICAS E DIGITAIS AO NEGÓCIO

08 SOLUÇÕES DE SEGURANÇA DE TI AO NEGÓCIO

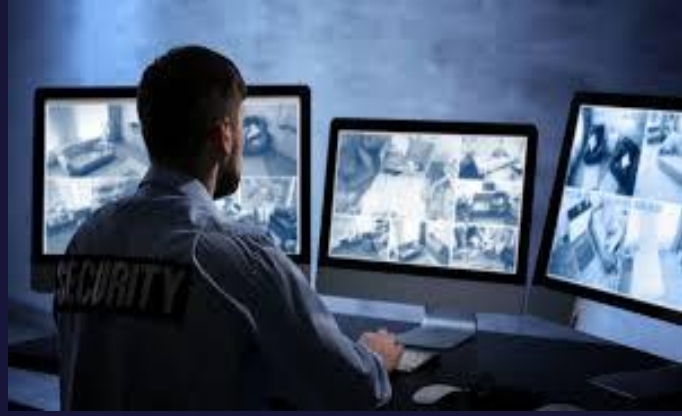


PROPÓSITO

Gerar uma análise detalhada dos aspectos de segurança física e digital das instalações da empresa **OfficeSolutions**.

Cada uma dos seguintes tópicos destaca pontos críticos e sugere mudanças para mitigar riscos e vulnerabilidades ao negócio e aos colaboradores.

01



CONTROLE DE ACESSO FÍSICO AO **EDIFÍCIO**

Situação Atual e Propostas de Melhoria

CONTROLE DE ACESSO FÍSICO

ATUAL

- Catracas sem autenticação dupla
- Câmera apenas na entrada de funcionários e visitantes
- Controle manual de entrada de veículos
- Controle manual de entrada nos setores de depósito
- Todos os funcionário podem acessar todos os setores da empresa.

PROPOSTAS DE MELHORIA

- Catracas com acesso biométrico
- Câmeras em pontos estratégicos do edifício
- Automatização do controle de entrada veículos com acesso biométrico
- Estabelecer níveis de acesso para cada setor e funcionário, catracas nos depósitos
- Apenas funcionários autorizados podem acessar setores específicos

02

CONTROLE DE ACESSO DIGITAL AOS **SISTEMAS**

Situação Atual e Propostas de Melhoria

CONTROLE DE ACESSO DIGITAL AOS SISTEMAS

ATUAL

- Servidores acessados remotamente com o uso de credenciais
- Inexistência de **VPNs** para acessos remotos
- Armazenamento local e centralizado dos dados de **Negócio, TI e Segurança** em apenas um servidor físico no edifício
- Não há **Logs** de acesso ou de tentativas falhas de acesso aos sistemas.

PROPOSTAS DE MELHORIA

- Autenticação multifator para todos os acessos remotos
- Uso de VPN para qualquer acesso remoto e restrição de IPs para tais acessos
- Redundância de servidores, dados e backups em nuvem
- Sistema de Logs de Acesso e tentativas de acessos aos sistemas
- Treinamento dos colaboradores sobre Cybersegurança

03

RISCOS AO NEGÓCIO POR AMEAÇAS **FÍSICAS**

Ameaças e Vulnerabilidades

RISCOS POR AMEAÇAS FÍSICAS

RISCO	INTENSIDADE	IMPACTO AO NEGÓCIO
Invasão ou falha no controle de acesso físico	ALTA	Roubos e danos ao patrimônio e colaboradores
Explosão em tubulações de gás e tanque de diesel	MUITO ALTA	Perda de vidas, patrimônio e interrupção das operações
Incêndios nos setores da empresa	ALTA	Perda de servidores, estoque e operação
Falha ou indisponibilidade do gerador	MÉDIA	Paralisação parcial das operações
Acesso não autorizado de funcionários	ALTA	Desvio de materiais e vazamento de informações
Desastres naturais	ALTA	Impacto generalizado à infraestrutura

04

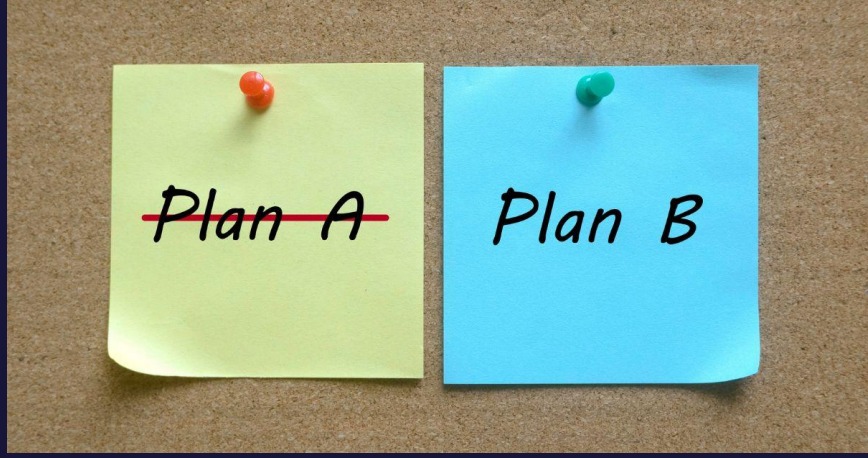
RISCOS AO NEGÓCIO POR AMEAÇAS **DIGITAIS**

Ameaças e Vulnerabilidades

RISCOS POR AMEAÇAS DIGITAIS

AMEAÇA	VULNERABILIDADE	MITIGAÇÃO
Acesso remoto não seguro	Ausência de VPN e criptografia	Configurar VPN corporativa para acesso remoto
Ausência de MFA	Autenticação apenas por nome de usuário e senha	Autenticação multifator para todos os acessos
Tentativas de acesso/logs desativados	Não monitoramento de acessos	Logs para registro de todas tentativas de acesso
Backups centralizados	Ausência de redundância externa	Criar backups externos e criptografados
Falta de monitoramento ativo	Sem firewalls, IDS/IPS ou alertas	Firewalls e ferramentas de monitoramento
Ransomware	Sistemas vulneráveis, backups centralizados	Soluções anti-ransomware e ferramentas de backup com restauração rápida

05



PLANO DE **CONTINGÊNCIA**

Descritivo do Plano

ETAPAS DO PLANO

PREVENÇÃO

O objetivo é reduzir a probabilidade de falhas e mitigar o impacto de incidentes antes que eles ocorram

RESPOSTA

Este passo define como agir durante um incidente para minimizar os danos e retomar o funcionamento o mais rápido possível

RECUPERAÇÃO

Após o incidente, o foco é restabelecer as operações normais e prevenir ocorrências futuras

DESCRIÇÃO DAS ETAPAS

PREVENÇÃO		RESPOSTA		RECUPERAÇÃO	
Implementar MFA, VPN e segmentação de rede	**TI**	Estabelecer equipe de resposta a incidentes	**GERENTE CONT.**	Restaurar sistemas e realizar testes pós-incidente	**TI**
Transferir backups para a nuvem ou outro local externo.	**TI**	Isolar e mitigar incidentes (ransomware, invasão, vazamento)	**TI**	Avaliar e documentar lições aprendidas	**TI – SEG.**
Treinamento de segurança física e digital para funcionários.	**RH – SEC.**	Comunicar clientes e parceiros sobre status das operações	**GERENTE REL.**	Realizar simulações de emergência	**TODOS**

06

AMEAÇAS FÍSICAS AO **AMBIENTE E NEGÓCIO**

Vulnerabilidades e Plano de Mitigação

AMEAÇAS FÍSICAS AO AMBIENTE E NEGÓCIO

AMEAÇA	VULNERABILIDADE	MITIGAÇÃO
Incêndios	– Ausência de sistemas de controle de incêndios, portas contra fogo, extintores e *sprinklers.* – Presença de combustíveis próximos uns aos outros e em setores com grande circulação e acesso – Falta de treinamento dos colaboradores contra incêndios	– Instalar *sprinklers* automáticos em todos os prédios, assim como extintores. – Realocar os botijões para um espaço ventilado e distante de fontes de ignição e do tanque de diesel. – Treinamentos contra emergências para colocabores e a criação de uma **CIPA**
Vazamentos de Gás	– Eventos climáticos extremos podem danificar as instalações – Mal funcionamento das estruturas existentes podem causar vazamentos	– Reforçar a estrutura dos prédios contra tempestades e vedação adequada – Instalar sistemas de detecção de gás

AMEAÇAS FÍSICAS AO AMBIENTE E NEGÓCIO

AMEAÇA	VULNERABILIDADE	MITIGAÇÃO
Falha no Gerador de Emergência	- O tanque de diesel do gerador está em local que pode ser comprometido em caso de incêndio ou vazamento - A falta de manutenção regular pode causar falhas na hora de sua utilização	- Relocar o gerador para um espaço seguro e distante de outras fontes de combustão - Realizar testes e manutenção periódicos no gerador - Estabelecer redundância no fornecimento de energia
Entrada de pessoas não autorizadas	- Controle de acesso físico inadequado nos depósitos e na garagem - Apenas uma câmera de segurança instalada na entrada principal	- Instalar câmeras adicionais em pontos estratégicos: garagens, depósitos e corredores internos. - Adotar travas eletrônicas nos portões de veículos, controladas por senha ou biometria.

07

AMEAÇAS LÓGICAS E DIGITAIS AO **NEGÓCIO**

Vulnerabilidades e Plano de Mitigação

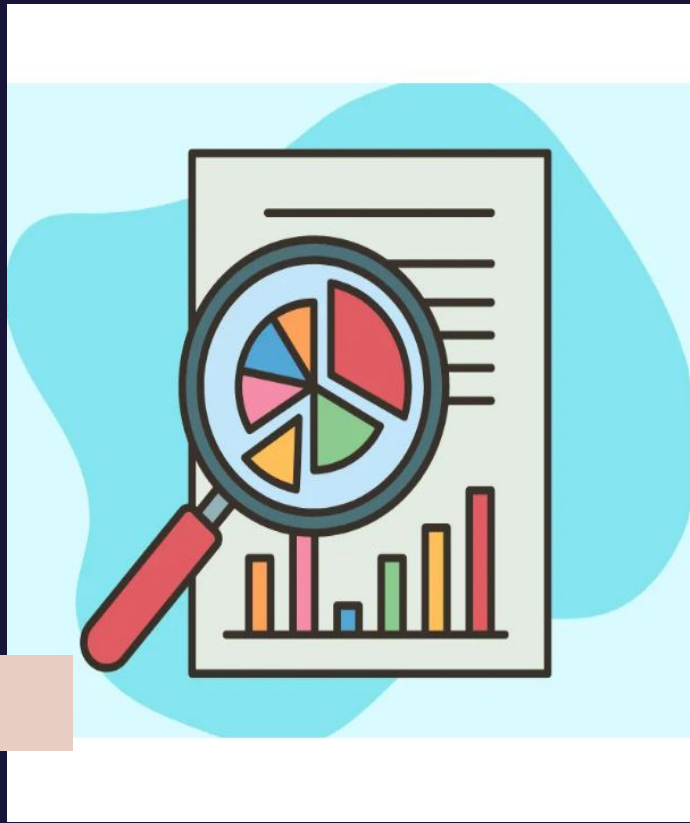
AMEAÇAS LÓGICAS E VULNERABILIDADES

AMEAÇA	VULNERABILIDADE	MITIGAÇÃO
Ataques Ransomware	Backups locais, MFA ausente e notificações desativadas	Backups em serviços externos, implementar MFA e alertas automáticos
Phishing	Falta de treinamento Filtros de e-mail fracos	Treinamento, filtro avançado e políticas de credenciais
Acessos não-autorizados	Ausência de VPN, senhas fracas e rede não segmentada	VPN corporativa, senhas fortes e segmentação da rede
Exploração de vulnerabilidades	Ausência de redundância externa	Plano de atualização, sistema de gerenciamento de falhas
Falta de monitoramento ativo	Softwares desatualizados	Firewalls e ferramentas de monitoramento
Roubo/alteração de dados	Falta de logs e privilégios excessivo de colaboradores	Logs detalhados e controle de privilégios

08

SOLUÇÕES DE SEGURANÇA DO TI AO **NEGÓCIO**

Situação Atual e Propostas de Melhoria

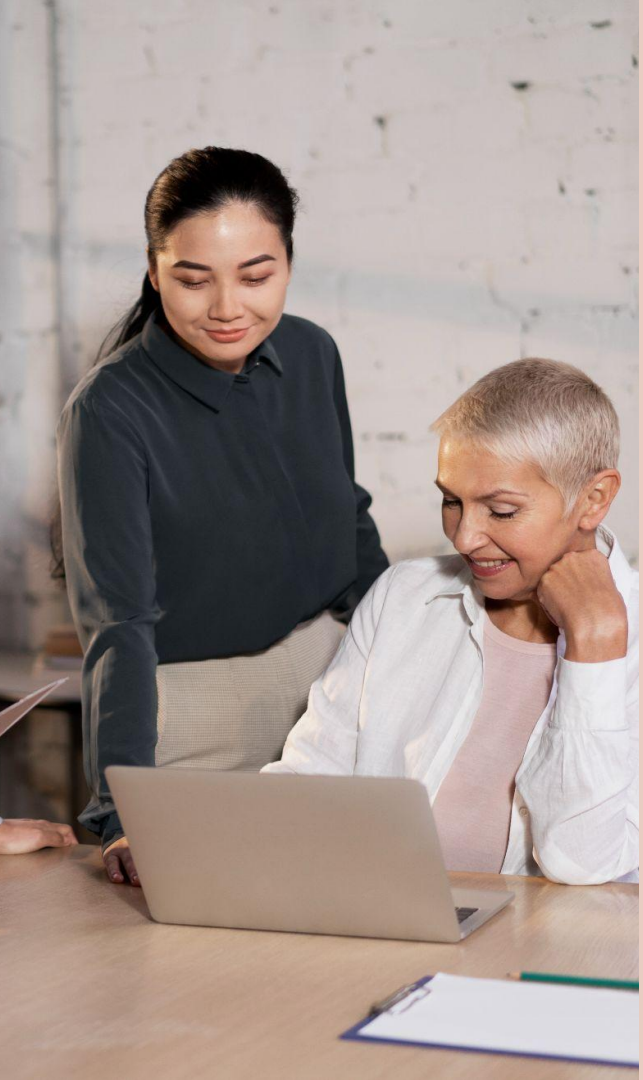


SOLUÇÕES DE SEGURANÇA DO TI AO NEGÓCIO

DEFICIÊNCIA	IMPACTO	SOLUÇÕES PROPOSTAS
Centralização de dados	Perda de dados por incidente único	Backups externos e na nuvem
Acesso remoto inseguro	Invasões por força bruta ou phishing	MFA, VPN e monitoramento ativo
Monitoramento desativado	Falha na detecção de invasões	Alertas automáticos e sistemas de SIEM
Controles de acesso genéricos	Acesso não autorizado a recursos sensíveis	Princípio do menor privilégioRevisões periódicas
Backups vulneráveis	Inutilização de backups por ransomware	Backups offline e armazenamento imutável
Ausência de plano de resposta	Resposta lenta e ineficaz a incidentes	Plano de resposta a incidentes e simulações

ORÇAMENTO PREVISTO

ITEMS	CUSTO INICIAL R$	CUSTO RECORRENTE ANUAL R$
BACKUPS EXTERNOS E REDUNDÂNCIAS	25.000,00	15.000,00
VPN CORPORATIVA E MFA	20.000,00	12.000,00
SISTEMAS DE MONITORAMENTO E ALERTAS	50.000,00	30.000,00
SEGMENTAÇÃO DE REDE E FIREWALL	30.000,00	0,00
BACKUPS OFFLINE	20.000,00	0,00
ATUALIZAÇÕES E GERENCIAMENTO	18.000,00	10.000,00
TREINAMENTOS DE SEGURANÇA	15.000,00	5.000,00
CONSULTORIA E RESPOSTAS À INCIDENTES	12.000,00	0,00
TOTAIS	**≈190.000,00**	**≈72.000,00**



CONCLUSÃO

Uma análise cuidadosa da situação atual da **OfficeSolutions** revelou importantes vulnerabilidades e também oportunidades significativas de melhoria, tanto na segurança física quanto na digital.

Como uma empresa totalmente digital, que opera por meio de sistemas web e aplicativos móveis para oferecer serviços de assinatura de materiais de escritório, a segurança precisa ser encarada como uma prioridade estratégica. Essa atenção é essencial para assegurar a continuidade das operações, proteger dados sensíveis e fortalecer a confiança dos clientes na marca.

OBRIGADA PELA **ATENÇÃO**