Segurança da Informação

Entrega 1 – Análise de riscos:

1. Acesso a Dados Financeiros: O acesso aos dados financeiros é restrito a
membros do departamento financeiro e deve ser concedido apenas com aprovação do gerente financeiro.

2. Política de Acesso Remoto: O acesso remoto aos sistemas da organização
deve ser controlado através de redes seguras e autenticação robusta. VPNs,
firewalls e controles de acesso à rede devem ser implementados para proteger o acesso externo.

3. Controle de Acesso a Ferramentas de Comunicação: Ferramentas de comunicação (como e-mail corporativo e sistemas de mensagens) devem ser
acessadas apenas por funcionários autorizados e monitorados para evitar vazamento de informações.

4. Acesso a Sistemas de Segurança: O acesso aos sistemas de segurança
(como câmeras de vigilância e alarmes) deve ser restrito a uma equipe específica de segurança e gerenciamento, com registro de todas as atividades de acesso.

5. Controle de Acesso a Recursos de TI: Acesso a recursos de TI, como servidores e equipamentos de rede, deve ser restrito a uma equipe de TI designada e registrada em um sistema de controle de acesso.

6. Política de Acesso a Registros de Transações: Registros de transações
financeiras e comerciais devem ser acessíveis somente ao departamento financeiro.

7. Política de Gerenciamento de Direitos de Acesso: O processo de concessão, modificação e remoção de direitos de acesso deve ser

documentado e controlado rigorosamente. Os direitos de acesso devem ser
revisados regularmente para garantir que estejam de acordo com as necessidades operacionais e de segurança.

8. Política de Acesso a Dados de Clientes: Dados pessoais dos clientes e históricos de compras devem ser acessíveis somente aos vendedores diretamente envolvidos no atendimento ao cliente e à equipe de suporte ao
cliente.

9. Política de Autenticação de Dispositivos: Dispositivos que se conectam à
rede corporativa devem ser autenticados por meio de certificados digitais, tokens ou outros métodos de autenticação. Apenas dispositivos autorizados
devem ter acesso aos sistemas e dados sensíveis.

10. Política de Modificação de Formas de Pagamento: Apenas o gerente financeiro pode modificar as formas de pagamento disponíveis no sistema.

11. Política de Senhas Seguras: Senhas devem ser fortes, contendo uma combinação de letras, números e caracteres especiais, e devem ser alteradas periodicamente.

12. Política de Acesso ao Estoque: Apenas o departamento de controle de
estoque pode visualizar e atualizar a quantidade de produtos no estoque. Vendedores não têm permissão para alterar essas informações.

13. Política de Monitoramento de Tentativas de Acesso: O sistema deve ser
configurado para detectar e alertar sobre múltiplas tentativas de acesso sem
sucesso. Medidas devem ser tomadas para bloquear ou investigar acessos
indevidos, minimizando riscos de ataques de força bruta.
14. Política de Desativação de Acessos em Caso de Desligamento: Acesso

de funcionários que saem da organização ou mudam de função deve ser desativado imediatamente. Todos os direitos de acesso devem ser revogados, e as credenciais de login devem ser removidas ou invalidadas para garantir que não haja acessos indevidos após o desligamento.

15. Política de Privilégios Mínimos: Os usuários só devem ter acesso aos recursos mínimos necessários para realizar suas funções. Isso limita a exposição de dados e reduz o risco de incidentes de segurança.

16. Política de Controle de Acesso a Redes Wi-Fi: O acesso às redes Wi-Fi
corporativas deve ser segmentado. A rede de convidados deve ser separada
da rede interna, e a rede interna deve exigir autenticação forte para acesso.

17. Política de Backup de Dados: Implementar backups regulares e criptografados para proteger as informações digitais de incidentes como falhas de sistema ou ataques cibernéticos.

18. Política de Controle de Inventário: Implementar um sistema rigoroso de
controle de inventário com atualizações periódicas para evitar desvios e perdas.

19. Política de Controle de Dispositivos USB e Mídias Externas: Restringir o
uso de Pen drives e mídias externas nos computadores da empresa para evitar a introdução de malwares.

20. Política de Segurança para E-mails: Implementar filtros de spam e treinar
os funcionários para reconhecer e-mails de phishing e outros tipos de ataques.

Entrega 2 - Implementação de Medidas de Segurança::

1. Monitoramento de Logs: Ativar o registro detalhado de eventos em

servidores, roteadores e dispositivos de rede. Analisando regularmente os logs em busca de atividades incomuns.

2. Sistema de Detecção de Intrusão (IDS): Implementar um IDS que monitore
e envie alertas em caso de atividades incomuns ou suspeitas na rede, como
tentativas de acesso não autorizadas ao banco de dados de clientes e vendas.

3. Segmentação de Rede: Separar a rede da empresa em diferentes segmentos, isolando o banco de dados de clientes e transações financeiras
da rede de uso geral, minimizando o impacto de possíveis invasões.

4. Autenticação de Dois Fatores (2FA): Adotar autenticação de dois fatores
para acessar o sistema de gestão da empresa, garantindo uma camada adicional de segurança contra-ataques de login comprometidos.

5. Monitoramento Contínuo: Implementar uma solução de monitoramento
contínuo de segurança para identificar ameaças em tempo real. Estando preparado para responder rapidamente a incidentes de segurança.

6. Testes de Penetração Regulares: Realizar testes de penetração e avaliações de vulnerabilidades no sistema para identificar e corrigir possíveis
falhas antes que sejam exploradas por atacantes.

7. Backup Regular de Dados: Manter backups regulares dos dados armazenados, incluindo informações de clientes, estoque, vendas e fornecedores, para garantir a recuperação em caso de falhas ou ataques de
ransomware.

8. Monitoramento de Transferências de Arquivos: Configurar o IDS para monitorar transferências de arquivos grandes ou incomuns, o que pode indicar movimentação não autorizada de dados sensíveis.

9. Integração com Firewall: Combine o IDS/IPS com o firewall da empresa para bloquear automaticamente tentativas de invasão e ataques de força bruta.

10. Monitoramento de Atividades Fora do Horário Comercial: Configurar o IDS para detectar e alertar sobre atividades de rede incomuns que ocorrem
fora do horário normal de operação da loja.

PROBLEMAS	GRAVIDADE (1-5)	URGÊNCIA (1-5)	TENDÊNCIA (1-5)	TOTAL	PRIORIZAÇÃO
Vazamento de dados confidenciais	5	5	5	125	1º
Queda do sistema	5	5	4	100	3º
Falta de backup de dados	4	4	4	64	6º
Uso de senhas fracas pelos colaboradores	5	4	5	100	4º
Desempenho lento de sistemas	5	4	4	80	5º
Desatualização de processos	4	4	3	48	8º
Baixa eficiência operacional	4	3	3	36	10º
Dificuldades na implementação de novas tecnologias	4	4	4	64	7º
Problemas com a manutenção de equipamentos	4	3	4	48	9º
Ataque de vírus no sistema	5	5	5	125	2º

Entrega 3 - Matriz Gut: