## Segurança da Informação - Análise de Riscos

1. **Identificação e Avaliação dos Riscos de Segurança para a Empresa:** Para garantir a segurança da informação na HealthTech Balderi Solutions, é crucial identificar e avaliar as ameaças e vulnerabilidades que podem comprometer os sistemas e dados da empresa. Abaixo está uma lista de 20 possíveis ameaças e/ou vulnerabilidades

   1- Vazamento de Dados Confidenciais : Comprometimento de informações pessoais e médicas dos pacientes.
   2- Ataques de Malware: Infecção por vírus, ransomware ou spyware nos sistemas da empresa.
   3- Acesso Não Autorizado: Acesso indevido aos sistemas e dados por funcionários ou terceiros não autorizados.
   4- Falhas de Segurança na Rede: Vulnerabilidades na rede que podem ser exploradas por hackers.
   5- Ataques de Engenharia Social: Tentativas de manipulação de funcionários para obter acesso não autorizado às informações.
   6- Phishing: Emails fraudulentos tentando obter informações sensíveis dos funcionários.
   7- Falhas de Software: Bugs e vulnerabilidades em softwares utilizados pela empresa.
   8- Falta de Atualizações de Segurança: Não aplicar patches de segurança e atualizações de software.
   9- Roubo ou Perda de Dispositivos: Dispositivos contendo dados sensíveis que são perdidos ou roubados.
   10- Senhas Fracas ou Comprometidas: Uso de senhas fracas ou reutilização de senhas em múltiplos sistemas.
   11- Ameaças Internas: Funcionários descontentes ou mal-intencionados que podem comprometer a segurança.
   12- DDoS (Ataques de Negação de Serviço Distribuídos): Ataques que visam sobrecarregar os sistemas e torná-los indisponíveis.
   13- Interceptação de Comunicação: Captura de dados sensíveis durante a transmissão pela rede.
   14- Falta de Criptografia: Dados armazenados ou transmitidos sem criptografia adequada.
   15- Configurações de Segurança Padrão: Uso de configurações padrão que não foram personalizadas para segurança.
   16- Desastres Naturais: Eventos como incêndios, inundações ou terremotos que podem danificar infraestruturas.
   17- Erro Humano: Ações não intencionais dos funcionários que podem comprometer a segurança.
   18- Backdoors em Software: Acesso não autorizado através de backdoors em aplicações de software.

19- Exploração de Zero-Day:  Exploração de vulnerabilidades desconhecidas pelos desenvolvedores.
20- Falta de Monitoramento Contínuo:  Não monitorar continuamente sistemas e redes para identificar atividades suspeitas.

Exemplo de Avaliação de Riscos: Para cada ameaça ou vulnerabilidade, é importante avaliar o impacto potencial e a probabilidade de ocorrência. Isso pode ser feito utilizando uma matriz de risco.

**Matriz de Risco**

| Ameaça/Vulnerabilidade | Impacto | Probabilidade | Nível de Risco |
|---|---|---|---|
| Vazamento de Dados Confidenciais | Alto | Médio | Alto |
| Ataques de Malware | Alto | Alto | Alto |
| Acesso Não Autorizado | Alto | Médio | Alto |
| Falhas de Segurança na Rede | Alto | Médio | Alto |
| Ataques de Engenharia Social | Médio | Alto | Alto |
| Phishing | Médio | Alto | Alto |
| Falhas de Software | Médio | Médio | Médio |
| Falta de Atualizações de Segurança | Alto | Médio | Alto |
| Roubo ou Perda de Dispositivos | Médio | Médio | Médio |
| Senhas Fracas ou Comprometidas | Alto | Médio | Alto |
| Ameaças Internas | Alto | Médio | Alto |
| DDoS | Alto | Médio | Alto |
| Interceptação de Comunicação | Alto | Médio | Alto |
| Falta de Criptografia | Alto | Médio | Alto |
| Configurações de Segurança Padrão | Médio | Médio | Médio |
| Desastres Naturais | Alto | Baixo | Médio |
| Erro Humano | Médio | Alto | Alto |
| Backdoors em Software | Alto | Médio | Alto |
| Exploração de Zero-Day | Alto | Médio | Alto |
| Falta de Monitoramento Contínuo | Alto | Médio | Alto |

2. **Análise de Vulnerabilidades e Ameaças Potenciais**
   Avaliação do Impacto e da Probabilidade de Ocorrência de Cada Risco.

A avaliação de riscos deve considerar dois principais fatores: o impacto potencial (a gravidade das consequências caso o risco se concretize) e a probabilidade de ocorrência (a chance de o risco acontecer). Abaixo está a avaliação detalhada dos riscos identificados para a HealthTech Balderi Solutions.

**Critérios de Avaliação:**

- Impacto:

- Alto: Consequências severas que podem afetar significativamente a operação da empresa.

- Médio: Consequências moderadas que podem causar interrupções, mas são gerenciáveis.

- Baixo: Consequências menores com impacto mínimo na operação.

- Probabilidade:

- Alta: Muito provável que ocorra no curto prazo.

- Média: Possível de ocorrer, mas não frequentemente.

- Baixa: Improvável de ocorrer, mas ainda possível. Avaliação de Riscos:

1.Vazamento de Dados Confidenciais

1.1 Impacto: Alto

1.2 Probabilidade: Médio

1.3 Avaliação: O vazamento de dados de pacientes pode levar a sérios problemas de privacidade e regulamentação, além de danificar a reputação da empresa. Probabilidade média devido a controles de segurança existentes.

2. Ataques de Malware

2.1 Impacto: Alto

2.2 Probabilidade: Alto

2.3 Avaliação: Malware pode causar paralisação dos sistemas e perda de dados. Alta probabilidade devido à prevalência de malware.

3. Acesso Não Autorizado

3.1 Impacto: Alto

3.2 Probabilidade: Médio

3.3 Avaliação: Pode resultar em comprometimento de dados sensíveis. Probabilidade média se medidas de segurança apropriadas forem implementadas.

4. Falhas de Segurança na Rede

4.1 Impacto: Alto

4.2 Probabilidade: Médio

4.3 Avaliação: Vulnerabilidades de rede podem ser exploradas para acesso não autorizado. Probabilidade média com boa gestão de segurança de rede.

5. Ataques de Engenharia Social

5.1 Impacto: Médio

5.2 Probabilidade: Alto

5.3 Avaliação: Engenharia social pode enganar funcionários e comprometer dados. Alta probabilidade devido à dependência do fator humano.

6. Phishing

6.1 Impacto: Médio

6.2 Probabilidade: Alto

6.3 Avaliação: Ataques de phishing são comuns e podem resultar em acesso a dados confidenciais. Alta probabilidade devido à prevalência.

7. Falhas de Software

7.1 Impacto: Médio

7.2 Probabilidade: Médio

7.3 Avaliação: Bugs de software podem causar interrupções e problemas de segurança. Probabilidade média dependendo da qualidade do software.

8. Falta de Atualizações de Segurança

8.1 Impacto: Alto

8.2 Probabilidade: Médio

8.3 Avaliação: Não aplicar atualizações pode deixar o sistema vulnerável. Probabilidade média se as atualizações forem gerenciadas adequadamente.

9. Roubo ou Perda de Dispositivos

9.1 Impacto: Médio

9.2 Probabilidade: Médio

9.3 Avaliação: Dispositivos perdidos ou roubados podem conter dados sensíveis. Probabilidade média com políticas adequadas de gestão de dispositivos.

10. Senhas Fracas ou Comprometidas

10.1 Impacto: Alto

10.2 Probabilidade: Médio

10.3Avaliação: Senhas fracas podem ser facilmente exploradas. Probabilidade média com políticas de senha fortes.

11. Ameaças Internas

11.1 Impacto: Alto

11.2 Probabilidade: Médio

11.3 Avaliação: Funcionários descontentes podem comprometer a segurança. Probabilidade média com gestão eficaz de pessoal.

12. DDoS (Ataques de Negação de Serviço Distribuídos)

12.1 Impacto: Alto

12.2 Probabilidade: Médio

12.3 Avaliação: Ataques DDoS podem tornar os sistemas indisponíveis. Probabilidade média com mitigação de DDoS em vigor.

13. Interceptação de Comunicação

13.1 Impacto: Alto

13.2 Probabilidade: Médio

13.3 Avaliação: Dados sensíveis podem ser capturados durante a transmissão. Probabilidade média com uso de criptografia.

14. Falta de Criptografia

14.1 Impacto: Alto

14.2 Probabilidade: Médio

14.3 Avaliação: Dados não criptografados são vulneráveis. Probabilidade média com criptografia adequada implementada.

15. Configurações de Segurança Padrão

15.1 Impacto: Médio

15.2 Probabilidade: Médio

15.3 Avaliação: Configurações padrão podem ser exploradas. Probabilidade média se não modificadas adequadamente.

16. Desastres Naturais

16.1 Impacto: Alto

16.2 Probabilidade: Baixo

16.3 Avaliação: Desastres naturais podem causar danos físicos aos sistemas. Baixa probabilidade, mas planejamento de contingência é essencial.

17. Erro Humano

17.1 Impacto: Médio

17.2 Probabilidade: Alto

17.3 Avaliação: Erros humanos são comuns e podem comprometer a segurança. Alta probabilidade devido à natureza humana.

18. Backdoors em Software

18.1 Impacto: Alto

18.2 Probabilidade: Médio

18.3 Avaliação: Backdoors podem ser usados para acesso não autorizado. Probabilidade média com controle de qualidade de software.

19. Exploração de Zero-Day

19.1 Impacto: Alto

19.2 Probabilidade: Médio

19.3 Avaliação: Vulnerabilidades desconhecidas podem ser exploradas. Probabilidade média com resposta rápida a ameaças emergentes.

20. Falta de Monitoramento Contínuo

20.1 Impacto: Alto

20.2 Probabilidade: Médio

20.3 Avaliação: Sem monitoramento, atividades suspeitas podem passar despercebidas. Probabilidade média com monitoramento implementado.