Implementação de Medidas de Segurança

Políticas de Acesso e Segurança

1. **Controle de Acesso**: Apenas funcionários e alunos com credenciais têm acesso autorizado às áreas restritas e aos sistemas de informação do curso.
2. **Autenticação de Identidade**: Todos os sistemas de informação devem exigir login com autenticação de identidade.
3. **Senha Segura**: Todos os usuários devem criar senhas fortes e alterá-las a cada 90 dias.
4. **Proteção de Dispositivos**: Dispositivos conectados ao sistema do curso devem ser bloqueados automaticamente após 5 minutos de inatividade.
5. **Limite de Tentativas de Login**: Após três tentativas de login sem sucesso, a conta será temporariamente bloqueada.

Políticas de Uso e Manutenção de Equipamentos

6. **Equipamentos Pessoais**: O uso de dispositivos pessoais, como celulares e notebooks, deve ser autorizado para atividades relacionadas ao curso.
7. **Uso de Equipamentos do Curso**: O equipamento fornecido pelo curso (aparelhos estéticos, computadores, etc.) deve ser usado exclusivamente para práticas e aulas autorizadas.
8. **Limpeza e Higiene de Equipamentos**: Todos os equipamentos e ferramentas devem ser limpos antes e depois do uso, de acordo com as normas de saúde e segurança.
9. **Manutenção de Equipamentos**: Todo equipamento deve passar por manutenção periódica, e qualquer problema deve ser imediatamente relatado ao responsável técnico.
10. **Proibição de Software Não Autorizado**: É proibido instalar softwares não autorizados nos dispositivos da instituição para evitar riscos de segurança.

Políticas de Privacidade e Confidencialidade

11. **Confidencialidade de Dados dos Clientes**: As informações pessoais e de saúde dos clientes devem ser tratadas com confidencialidade, em conformidade com a LGPD.
12. **Política de Fotografia**: É proibido tirar fotos de clientes e colegas sem consentimento, respeitando o direito à privacidade.
13. **Proibição de Uso de Dados Pessoais**: Dados pessoais de alunos e clientes só podem ser usados para fins diretamente relacionados ao curso.
14. **Compartilhamento de Informações Sensíveis**: Informações sensíveis de clientes e alunos não podem ser compartilhadas sem autorização explícita.
15. **Autorização de Publicidade**: Qualquer uso da imagem de clientes ou alunos para fins publicitários deve ter autorização por escrito.

Políticas de Treinamento e Boas Práticas

16. **Treinamento em Higiene e Segurança**: Todos os alunos e funcionários devem passar por treinamentos em higiene e segurança regularmente.
17. **Procedimentos de Emergência**: Todos devem estar cientes dos procedimentos de emergência e conhecer as saídas de segurança e equipamentos de primeiros socorros.
18. **Uso Responsável de Produtos Químicos**: Produtos químicos e cosméticos devem ser manuseados e armazenados adequadamente, respeitando as normas de segurança.
19. **Registro de Procedimentos**: Cada atendimento e procedimento realizado no cliente deve ser registrado, especificando produtos e técnicas utilizadas.
20. **Política de Feedback**: Clientes e alunos devem ser incentivados a fornecer feedback sobre os serviços e a experiência, permitindo melhorias contínuas.

Configuração de sistemas de detecção de intrusão e prevenção de ataques

1. Configurar um IDS/IPS (Intrusion Detection System / Intrusion Prevention System)

- Utilize sistemas IDS/IPS para monitorar a rede e identificar padrões de controle suspeitos. Ferramentas como Snort, Suricata e Cisco Firepower são comuns.
- O IDS detecta ataques e gera alertas, enquanto o IPS pode bloquear ameaças automaticamente

2. Monitoramento de Logs e Análise de Eventos

- Configure um sistema de análise de logs para monitorar atividades suspeitas e detectar padrões anormais.
- Ferramentas como Splunk ou ELK Stack (Elasticsearch, Logstash, Kibana) ajudam a consolidar e analisar os logs em tempo real.

3. Firewall de Aplicações Web (WAF)

- Um WAF protege contra ataques baseados em aplicações web, como SQL Injection, Cross-Site Scripting (XSS) e Cross-Site Request Forgery (CSRF).
- Ferramentas como ModSecu

4. Segmentação de Rede

- Dividir a rede em segmentos (por exemplo, rede de produção, rede de desenvolvimento e rede administrativa) para dificultar o acesso
- Limite o tráfego entre os segmentos

5. Controle de Acesso e Autenticação Multifator (MFA)

- Adote um sistema de controle de acesso rigoroso e implemente autenticação multifatorial para áreas de acesso
- Esta medida reduz a chance de acesso não autorizado, mesmo em caso de comprometimento de crédito

6 Configuração de Honeypots e Honeynets

- Implementar honeypots e honeynets permite a criação de "iscas" para enganar potenciais caçadores e entender as técnicas usadas.
- Isso ajuda a identificar comportamentos

7 Atualização Regular e Patches de Segurança

- Garanta que todos os sistemas e softwares sejam atualizados, aplicando patches de segurança regularmente para eliminar vulnerabilidades conhecidas
- Automatize processos de atualização para redução

8. Análise de Tráfego com IA e Machine Learning

- Use ferramentas com inteligência artificial e aprendizado de máquina para analisar o comportamento do tráfego e identificação
- Soluções como Darktrace e Vectra AI são conhecidas por sua capacidade de detecção a

9 Implementação de Regras de Detecção Personalizadas

- Configurar regras personalizadas no IDS/IPS para detectar ataques específicos ao ambiente da
- Baseie-se nas regras em ameaças recentes e nas necessidades de segurança específicas do seu conjunto

10. Treinamento de Equipes e Simulações de Ataques

- Realize treinamentos regulares para sua equipe de TI e outros funcionários sobre como importância e responder a experimento de
- Simule ataques (ex.: teste de phishing e pentests) para melhorar a resposta de segurança e fortalecer as políticas de segurança da empresa