**Empresa TechCode**

**Segurança da Informação**

**Análise de Riscos**

**Identificação e avaliação dos riscos de segurança para a empresa:**

* Liste possíveis ameaças e vulnerabilidades
* Liste 20 possíveis ameaças e/ou vulnerabilidades

**Análise de vulnerabilidades e ameaças potenciais:**

* Avalie o impacto e a probabilidade de ocorrência de cada risco.

### **Riscos Identificados para a Empresa Tech Code**

**1. Ameaça: Ataque de Phishing**

* **Vulnerabilidade:** Falta de treinamento em segurança para os funcionários
* **Impacto:** Médio
* **Probabilidade:** Alta

**2. Ameaça: Malware**

* **Vulnerabilidade:** Falta de atualização regular de software de segurança
* **Impacto:** Alto
* **Probabilidade:** Média

**3. Ameaça: Roubo de Dados Pessoais**

* **Vulnerabilidade:** Falta de criptografia adequada dos dados dos clientes
* **Impacto:** Alto
* **Probabilidade:** Alta

**4. Ameaça: Ataques DDoS**

* **Vulnerabilidade:** Infraestrutura de rede insuficiente
* **Impacto:** Alto
* **Probabilidade:** Média

**5. Ameaça: Violação de Privacidade**

* **Vulnerabilidade:** Políticas de privacidade fracas ou inexistentes
* **Impacto:** Alto
* **Probabilidade:** Média

**6. Ameaça: Acesso Não Autorizado**

* **Vulnerabilidade:** Uso de senhas fracas pelos usuários
* **Impacto:** Médio
* **Probabilidade:** Alta

**7. Ameaça: Engenharia Social**

* **Vulnerabilidade:** Falta de conscientização dos funcionários sobre engenharia social
* **Impacto:** Médio
* **Probabilidade:** Alta

**8. Ameaça: Perda de Dados**

* **Vulnerabilidade:** Ausência de backup regular e seguro
* **Impacto:** Alto
* **Probabilidade:** Média

**9. Ameaça: Ransomware**

* **Vulnerabilidade:** Falta de ferramentas de detecção e resposta a incidentes
* **Impacto:** Alto
* **Probabilidade:** Média

**10. Ameaça: Exploração de Vulnerabilidades de Software**

* **Vulnerabilidade:** Uso de software desatualizado
* **Impacto:** Alto
* **Probabilidade:** Média

**11. Ameaça: Interceptação de Comunicações**

* **Vulnerabilidade:** Uso de conexões não seguras (HTTP ao invés de HTTPS)
* **Impacto:** Médio
* **Probabilidade:** Alta

**12. Ameaça: Fraude Financeira**

* **Vulnerabilidade:** Sistemas de pagamento com baixa segurança
* **Impacto:** Alto
* **Probabilidade:** Média

**13. Ameaça: Exfiltração de Dados Internos**

* **Vulnerabilidade:** Falta de controle de acesso adequado aos dados sensíveis
* **Impacto:** Alto
* **Probabilidade:** Média

**14. Ameaça: Configurações de Segurança Improprias**

* **Vulnerabilidade:** Falta de revisões regulares das configurações de segurança
* **Impacto:** Médio
* **Probabilidade:** Média

**15. Ameaça: Insider Threat**

* **Vulnerabilidade:** Falta de monitoramento de atividades internas
* **Impacto:** Alto
* **Probabilidade:** Baixa

**16. Ameaça: Ataque de Força Bruta**

* **Vulnerabilidade:** Implementação inadequada de medidas anti-brute force
* **Impacto:** Médio
* **Probabilidade:** Média

**17. Ameaça: Comprometimento de API**

* **Vulnerabilidade:** APIs mal projetadas ou inseguras
* **Impacto:** Alto
* **Probabilidade:** Média

**18. Ameaça: Vulnerabilidades Zero-Day**

* **Vulnerabilidade:** Falta de resposta rápida a novas vulnerabilidades descobertas
* **Impacto:** Alto
* **Probabilidade:** Baixa

**19. Ameaça: Perda de Confidencialidade**

* **Vulnerabilidade:** Exposição inadequada de informações em ambientes de desenvolvimento
* **Impacto:** Médio
* **Probabilidade:** Média

**20. Ameaça: Falha de Conformidade Regulamentar**

* **Vulnerabilidade:** Desconhecimento ou negligência das normas e regulamentos aplicáveis
* **Impacto:** Alto
* **Probabilidade:** Média

**Implementação de Medidas de Segurança**

1. **Implementação de políticas de controle de acesso aos sistemas e dados:**

* Estabeleça políticas de controle de acesso baseadas nos riscos identificados.
* Forneça no mínimo10 políticas de controle de acessos.

### Políticas de Controle de Acesso para a Empresa Tech Code

#### 1. Acesso aos Dados Financeiros

* **Política:** O acesso aos dados financeiros é restrito exclusivamente aos membros do departamento financeiro.
* **Justificativa:** Minimizar o risco de fraude financeira e garantir a confidencialidade dos dados financeiros.

#### 2. Acesso aos Dados Pessoais dos Clientes

* **Política:** Apenas funcionários autorizados do departamento de atendimento ao cliente e da equipe de TI podem acessar os dados pessoais dos clientes.
* **Justificativa:** Proteger a privacidade dos clientes e evitar violações de dados.

#### 3. Acesso às APIs Críticas

* **Política:** As APIs críticas são acessíveis apenas por desenvolvedores autorizados e pela equipe de operações.
* **Justificativa:** Prevenir o comprometimento de API e a exploração de vulnerabilidades.

#### 4. Acesso a Ambientes de Desenvolvimento e Teste

* **Política:** O acesso aos ambientes de desenvolvimento e teste é restrito aos desenvolvedores e testadores autorizados.
* **Justificativa:** Proteger informações sensíveis e garantir a integridade dos processos de desenvolvimento.

#### 5. Acesso aos Sistemas de Pagamento

* **Política:** O acesso aos sistemas de pagamento é limitado aos membros da equipe financeira e aos administradores de TI.
* **Justificativa:** Garantir a segurança das transações financeiras e reduzir o risco de fraude.

#### 6. Acesso a Configurações de Segurança

* **Política:** Somente os administradores de segurança de TI têm permissão para alterar configurações de segurança.
* **Justificativa:** Prevenir configurações de segurança impróprias e manter a integridade do sistema.

#### 7. Acesso a Ferramentas de Backup

* **Política:** O acesso às ferramentas de backup é restrito aos administradores de sistemas e à equipe de TI responsável pelo backup.
* **Justificativa:** Assegurar a proteção e a disponibilidade dos dados.

#### 8. Acesso a Logs de Auditoria

* **Política:** Apenas auditores internos e administradores de segurança têm acesso aos logs de auditoria.
* **Justificativa:** Monitorar e investigar atividades suspeitas e manter a integridade dos registros de auditoria.

#### 9. Acesso a Dados Sensíveis

* **Política:** O acesso a dados sensíveis, como informações de pagamento e dados pessoais, é concedido apenas com base na necessidade de conhecimento e mediante autorização.
* **Justificativa:** Minimizar o risco de exfiltração de dados internos e proteger informações confidenciais.

#### 10. Acesso ao Sistema de Gestão de Cursos

* **Política:** O acesso ao sistema de gestão de cursos é restrito aos administradores do sistema, desenvolvedores e instrutores autorizados.
* **Justificativa:** Assegurar a integridade e a disponibilidade dos conteúdos dos cursos online.

#### 11. Acesso a Recursos de Rede

* **Política:** O acesso a recursos de rede críticos, como servidores e dispositivos de rede, é restrito aos administradores de rede.
* **Justificativa:** Prevenir ataques DDoS e proteger a infraestrutura de rede.

#### 12. Acesso Remoto Seguro

* **Política:** O acesso remoto aos sistemas da empresa é permitido apenas através de conexões VPN seguras e após autenticação de dois fatores.
* **Justificativa:** Proteger contra interceptação de comunicações e acessos não autorizados.

#### 13. Acesso a Ferramentas de Monitoramento de Segurança

* **Política:** Somente a equipe de segurança tem permissão para acessar e operar ferramentas de monitoramento de segurança.
* **Justificativa:** Detectar e responder rapidamente a incidentes de segurança, como malware e ransomware.

#### 14. Acesso Baseado em Função (RBAC)

* **Política:** Implementar um modelo de controle de acesso baseado em função (RBAC) para assegurar que os funcionários tenham apenas os acessos necessários para desempenhar suas funções.
* **Justificativa:** Reduzir o risco de acesso não autorizado e manter o princípio do menor privilégio.

#### 15. Revisão Regular de Acessos

* **Política:** Realizar revisões regulares dos direitos de acesso dos funcionários para garantir que as permissões estejam atualizadas e adequadas.
* **Justificativa:** Identificar e revogar acessos desnecessários ou inadequados, prevenindo ameaças internas.

1. **Configuração de sistemas de detecção de intrusão e prevenção de ataques:**

* Instale e configure sistemas para detectar e prevenir intrusões.
* Informar pelo menos 10 medidas de detecção e prevenção de ataques na sua empresa

### Medidas de Detecção e Prevenção de Ataques para a Plataforma da Empresa Tech Code

Para proteger a plataforma de cursos online da Tech Code contra ameaças e vulnerabilidades, é fundamental implementar e configurar sistemas de detecção e prevenção de intrusões (IDS/IPS), juntamente com outras medidas de segurança. Segue medidas recomendadas:

#### 1. Implementação de um Sistema IDS/IPS

* **Medida:** Instalar e configurar sistemas de detecção (IDS) e prevenção (IPS) de intrusões na infraestrutura de rede que suporta a plataforma de cursos online.
* **Justificativa:** Detectar e bloquear atividades maliciosas, como tentativas de invasão e exploração de vulnerabilidades, antes que causem danos significativos.

#### 2. Monitoramento Contínuo de Redes

* **Medida:** Utilizar ferramentas de monitoramento contínuo de rede para analisar o tráfego em tempo real, identificando padrões anômalos e comportamentos suspeitos.
* **Justificativa:** Detectar e responder rapidamente a atividades maliciosas ou incomuns na rede que possam comprometer a plataforma de cursos.

#### 3. Uso de Firewalls de Próxima Geração (NGFW)

* **Medida:** Implementar firewalls de próxima geração (NGFW) para inspecionar profundamente o tráfego de rede, aplicando políticas de segurança avançadas e bloqueando ameaças sofisticadas.
* **Justificativa:** Proteger a infraestrutura de rede contra ataques complexos e garantir o controle sobre o tráfego de entrada e saída.

#### 4. Implementação de Sistemas de Detecção de Malware

* **Medida:** Utilizar soluções avançadas de detecção de malware que incluam análise comportamental e sandboxing para identificar e mitigar ameaças de malware.
* **Justificativa:** Prevenir infecções por malware que possam comprometer a plataforma de cursos e os dados dos usuários.

#### 5. Autenticação de Dois Fatores (2FA)

* **Medida:** Implementar autenticação de dois fatores (2FA) para todos os acessos aos sistemas críticos da plataforma de cursos online.
* **Justificativa:** Reduzir o risco de acesso não autorizado por meio de credenciais comprometidas, fortalecendo a segurança das contas dos usuários.

#### 6. Segmentação de Rede

* **Medida:** Segmentar a rede em diferentes zonas de segurança, isolando sistemas críticos, dados sensíveis e serviços da plataforma de cursos online.
* **Justificativa:** Limitar a propagação de ameaças e facilitar o controle e monitoramento do tráfego de rede em segmentos distintos.

#### 7. Análise de Logs e SIEM

* **Medida:** Configurar um sistema de gerenciamento e análise de informações e eventos de segurança (SIEM) para consolidar logs de segurança e detectar padrões de ataque.
* **Justificativa:** Fornecer uma visão centralizada das atividades de segurança, permitindo respostas rápidas e eficazes a incidentes de segurança.

#### 8. Implementação de Honeypots

* **Medida:** Utilizar honeypots para atrair e monitorar atividades maliciosas, coletando informações sobre métodos de ataque e comportamentos dos invasores.
* **Justificativa:** Obter informações valiosas sobre ameaças emergentes e melhorar as estratégias de defesa contra invasores.

#### 9. Controles de Acesso Baseados em Função (RBAC)

* **Medida:** Implementar controles de acesso baseados em função (RBAC) para garantir que os funcionários e usuários tenham apenas os acessos necessários para suas funções.
* **Justificativa:** Minimizar o risco de acessos não autorizados e garantir o princípio do menor privilégio, protegendo dados sensíveis e sistemas críticos.

#### 10. Auditorias e Testes de Penetração Regulares

* **Medida:** Realizar auditorias de segurança e testes de penetração periodicamente para identificar e corrigir vulnerabilidades na plataforma de cursos online.
* **Justificativa:** Manter a segurança do sistema atualizada e robusta contra ameaças novas e emergentes, prevenindo explorações de vulnerabilidades.

#### 11. Atualizações e Patches Regulares

* **Medida:** Implementar um processo rigoroso de gerenciamento de patches para garantir que todos os sistemas e softwares da plataforma de cursos estejam atualizados.
* **Justificativa:** Corrigir vulnerabilidades conhecidas e proteger contra exploits zero-day, mantendo a segurança da plataforma em dia.

#### 12. Treinamento de Conscientização em Segurança

* **Medida:** Realizar treinamentos regulares de conscientização em segurança para todos os funcionários e instrutores, focando em boas práticas de segurança e como identificar ameaças.
* **Justificativa:** Aumentar a resiliência da organização contra-ataques de engenharia social e outros vetores baseados em humanos, fortalecendo a cultura de segurança.