
FIAP
MBA

MBA - Cyber Security
Governance & Management

Cloud Computing Security, DevOps e DevSecOps
Turma: 67SEG
Prof. Me. Nivaldo T. Marcusso

Prof. Me. Nivaldo Tadeu Marcusso

- 59 anos, formado em Engenharia Eletrônica, MBA em Conhecimento, Tecnologia e Inovação pela FIA/USP e Pós-MBA em Gestão avançada pela FIA / USP, Membro da Wharton Fellows.
- Certificação Executiva em Estratégia e Inovação pela MIT Sloan e Especialização em: Gestão Estratégica de TI (SUIT) pela Universidade de Stanford, Estratégia e Serviços de TI (DIS) pela Universidade de Harvard, Gestão Internacional pela Universidade Euromed de Marseille/FEA-USP e Gestão de Conhecimento pela Universidade de Lyon e FEA/USP.
- Professor de Pós-Graduação Lato Sensu (cursos MBA) em Estratégia, Inovação, Gestão do Conhecimento, Tecnologia da Informação e Educação a distância pela UNISAL, USP, FIA, FIAP, FATEC e e palestrante em conferências nacionais e internacionais de TI, Inovação, Tecnologia Educacional e Educação à distância.
- Eleito em 2010, 2009, 2008, 2007, CIO do ano no segmento de educação no Brasil, pela HITEC, revista Computerworld e 1º lugar entre os CIOs, das 100+ Empresas Inovadoras em TI na categoria de serviços diversos, pela revista Information Week.
- Experiência de negociação e liderança no desenvolvimento de parcerias internacionais com empresas e Universidades, para a transferência de tecnologias aplicadas a educação e banking, tendo visitado mais de 15 países nos últimos 13 anos, como os EUA, China, Inglaterra, França, Alemanha, Irlanda, Tunísia, Espanha, Chile entre outros.
- Membro de Comunidades, Associações e Sociedades focadas em gestão da tecnologia, da estratégia, da inovação e da educação a distância, como o ISPIM (Noruega), IBGC, Praxis (Brasil), ABED (Brasil), e-learning Brasil, Educause (EUA), FIRST (EUA) e BDRA (Inglaterra).
- Coautor e coordenador da coleção “Tecnologia e Educação”, com os livros eletrônicos (eBooks): Tecnologia e Aprendizagem e a Tecnologia transformando a Educação.
- Experiência de mais de 25 anos na gestão da TI, EAD, planejamento estratégico, Inovação, RH, Finanças em empresas como Digilab, Fundação Bradesco, Bradesco, Anhembi Morumbi.
- Atualmente além de Professor da USP, FIA, FDC, FIPE, FIAP, UNISAL e FACAMP, além de Consultor da FIA (TI, Tecnologia Educacional e EAD) , FDC (Processos de Negócios) , 4Strategis (Planejamento Estratégico, Modelagem de Negócios e Inovação) e da MARCX (TI, e-Learning e Mobile Learning).

Agenda

Aula 1 : Arquitetura e Segurança em Cloud

Aula 2: DevOps, DevSecOps e DevRiskOps

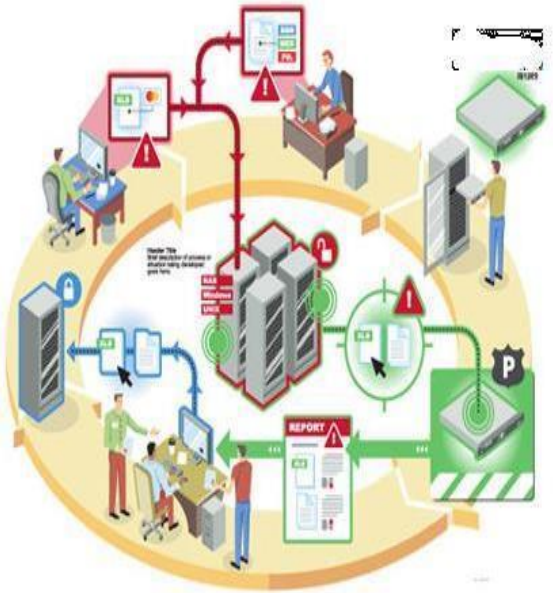
Aula 3: Segurança Adaptativa e SIEM 3.0

Aula 4: Segurança em Serviços em Cloud de IoT, IA, Blockchain e outros

Aula 5: Workshop das Atividades

Agenda

- Aula 1: 25/09/23
- Aula 2: 27/09/23
- Aula 3: 30/10/23 (M)
- Aula 4: 30/10/23 (T)
- Aula 5: 09/10/23



Acesso ao material de apoio:
https://www.dropbox.com/sh/br6gkgfg1301viw/AACL5onRJi5SRF5qRaIwnU6Ya?dl=0

Segurança dos Serviços de Cloud

AWS – Segurança Estratégica

Identificar

Entenda e gerencie riscos com visibilidade e automação profundas.

Prevenir

Definir medidas para permissões e identidades de usuários, proteção de infraestrutura e proteção de dados a fim de estabelecer uma estratégia de adoção na AWS suave e planejada.

Detectar

Adquirir visibilidade para a estratégia de segurança de sua organização a partir de serviços de monitoramento e registro em log. Ingerir estas informações em uma plataforma escalável para garantir o gerenciamento de eventos, testes e auditoria.

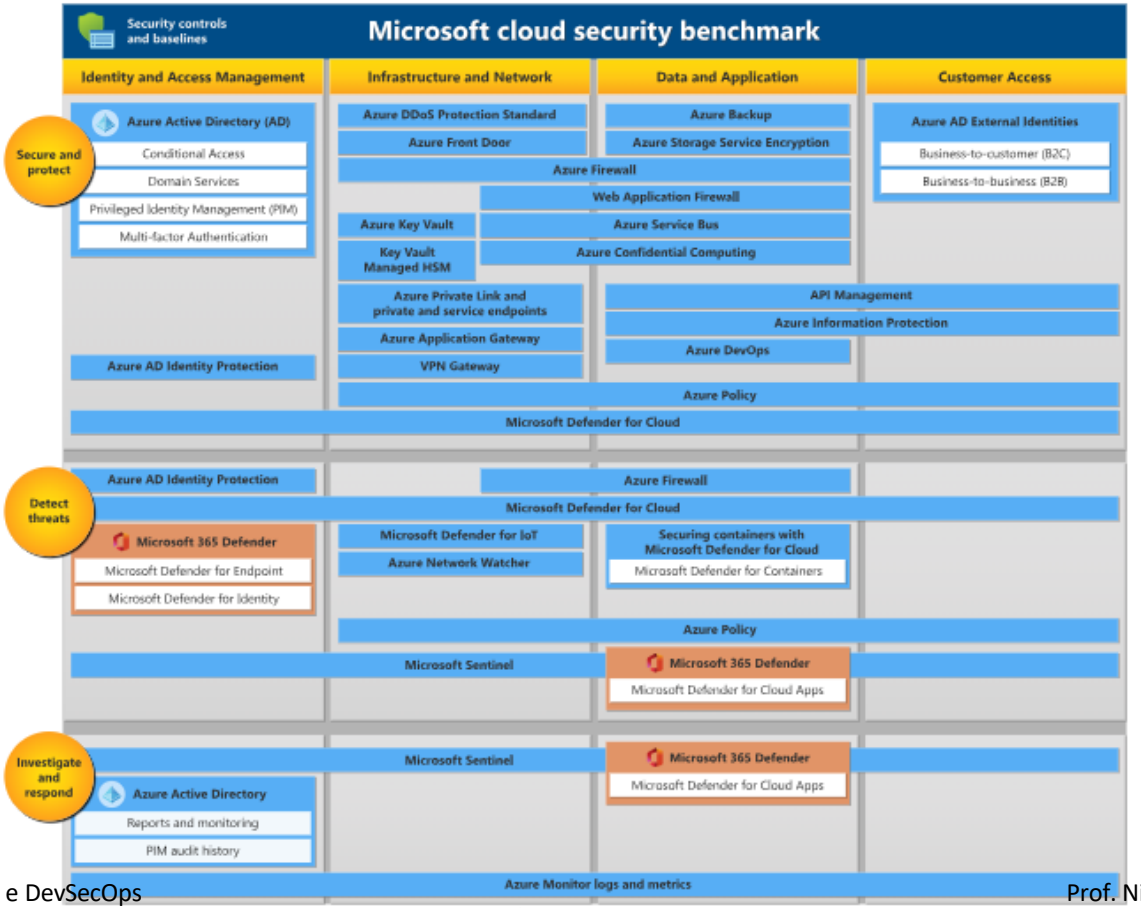
Resposta

Resposta e recuperação automatizadas a incidentes para ajudar a mudar o foco principal das equipes de segurança, de forma que possam se concentrar na análise da causa raiz.

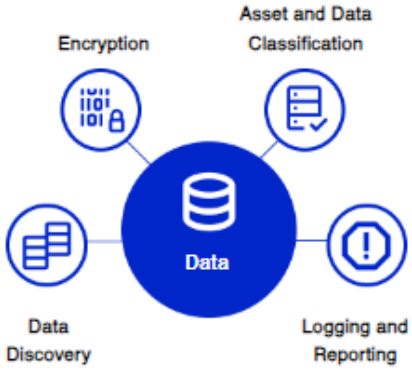
Corrigir

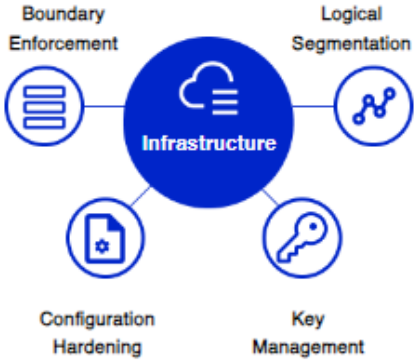
Aproveitar a automação orientada por eventos para corrigir e proteger rapidamente seu ambiente da AWS, praticamente em tempo real.

Microsoft Cloud Security



GCP Security Management





Elementos Chaves de Segurança em Cloud para Aplicações de IA

1. A Natureza dos Dados de IA:

- Dados sensíveis são informações confidenciais ou pessoais coletadas e usadas pelas aplicações de IA.
- Isso pode incluir informações médicas, financeiras, identificadores pessoais e outros dados sensíveis. A proteção desses dados é fundamental para garantir a privacidade e a conformidade regulamentar.

2. Modelos de IA:

- Os modelos de IA são algoritmos e configurações que permitem que as aplicações de IA realizem tarefas específicas.
- Esses modelos podem ser considerados propriedade intelectual e devem ser protegidos contra roubo, cópia não autorizada e adulteração.
- A criptografia e o controle de acesso ajudam a proteger os modelos de IA.

Elementos Chaves de Segurança em Cloud para Aplicações de IA

3. Ameaças em Cloud:

- As ameaças em cloud incluem ataques cibernéticos, como ataques DDoS, injeção de código malicioso, phishing e exploração de vulnerabilidades.
- A compreensão dessas ameaças é essencial para implementar medidas de segurança eficazes.

4. Isolamento de Recursos:

- O isolamento de recursos garante que os recursos de computação, armazenamento e rede usados por diferentes aplicações de IA sejam separados para evitar que uma aplicação comprometida afete outras.
- Isso pode ser alcançado por meio de virtualização e contêineres.

Elementos Chaves de Segurança em Cloud para Aplicações de IA

5. Autenticação e Autorização:

- A autenticação verifica a identidade dos usuários e sistemas que tentam acessar a aplicação de IA. A autorização determina o que cada usuário ou sistema está autorizado a fazer.
- A autenticação multifatorial e o controle de acesso baseado em funções são práticas comuns.

6. Encriptação de Dados:

- A encriptação de dados garante que os dados sejam ilegíveis para qualquer pessoa que não tenha a chave de desencriptação apropriada.
- Isso inclui a encriptação de dados em repouso, em trânsito e durante o processamento.

Elementos Chaves de Segurança em Cloud para Aplicações de IA

7. Monitoramento e Auditoria:

- A implementação de sistemas de monitoramento contínuo permite a detecção de atividades suspeitas em tempo real.
- A auditoria registra todas as ações realizadas na aplicação de IA, o que é útil para investigar incidentes e garantir a conformidade.

8. Recuperação de Desastres:

- Planos de recuperação de desastres (DR) asseguram que a aplicação de IA possa ser restaurada rapidamente após eventos inesperados, como falhas de hardware, desastres naturais ou ataques.
- Isso pode envolver a replicação de dados e sistemas em locais geograficamente distintos.

Elementos Chaves de Segurança em Cloud para Aplicações de IA

9. Compliance e Regulamentações:

- As aplicações de IA devem estar em conformidade com regulamentações relevantes, como a LGPD, o GDPR na Europa, o HIPAA nos Estados Unidos e outros padrões de segurança de dados.
- Isso inclui a coleta adequada de consentimento, o direito ao esquecimento e a notificação de violações.

10. Treinamento e Conscientização:

- Funcionários e usuários devem ser treinados em boas práticas de segurança, incluindo reconhecimento de ameaças, uso de senhas fortes e conscientização sobre a importância da segurança em cloud.

Elementos Chaves de Segurança em Cloud para Aplicações de IA

11. Parceria com Provedores de Cloud:

- A escolha de um provedor de cloud confiável é crucial.
- Importante entender os serviços de segurança oferecidos pelo provedor, bem como as responsabilidades compartilhadas entre o cliente e o provedor em termos de segurança.

12. Desenvolvimento Seguro:

- Implementar práticas de desenvolvimento seguro envolve a verificação de código, a análise de vulnerabilidades e a integração de segurança desde o início do ciclo de desenvolvimento de software.
- Ajuda a mitigar vulnerabilidades antes que elas se tornem uma ameaça.

Serviços de Segurança da AWS para aplicações de IA

1. AWS Identity and Access Management (IAM):

- O AWS IAM permite controlar o acesso aos recursos da AWS. Você pode configurar permissões granulares para os usuários, grupos e papéis que acessam recursos de IA.
- Ajuda a garantir que apenas pessoas e sistemas autorizados possam interagir com os recursos.

2. AWS Key Management Service (KMS):

- O KMS permite criar e gerenciar chaves de criptografia para proteger os dados em repouso e em trânsito.
- Usar o KMS para encriptar os modelos de IA e os dados sensíveis usados em suas aplicações.

Serviços de Segurança da AWS para aplicações de IA

3. AWS Shield:

- O AWS Shield fornece proteção contra ataques DDoS (Distributed Denial of Service).
- Crítico para garantir a disponibilidade contínua de suas aplicações de IA.

4. Amazon GuardDuty:

- O Amazon GuardDuty é um serviço de detecção de ameaças que monitora e analisa o tráfego de rede e o comportamento de API em busca de atividades maliciosas.
- Pode ajudar a identificar possíveis ameaças à segurança de suas aplicações de IA.

Serviços de Segurança da AWS para aplicações de IA

FIAP MBA+

5. AWS Web Application Firewall (WAF):

- O AWS WAF ajuda a proteger suas aplicações de IA contra ataques na camada de aplicação, como injeções de SQL e ataques de cross-site scripting (XSS).

6. Amazon Macie:

- O Amazon Macie é um serviço de segurança que usa machine learning para descobrir e proteger dados sensíveis.
- Particularmente útil para identificar dados confidenciais em suas aplicações de IA e garantir sua segurança.

Serviços de Segurança da AWS para aplicações de IA

7. AWS CloudTrail:

- O AWS CloudTrail registra todas as ações realizadas em sua conta da AWS, permitindo a auditoria e a trilha de atividades.
- Essencial para a conformidade e investigação de incidentes.

8. AWS Secrets Manager:

- O Secrets Manager ajuda a proteger informações confidenciais, como senhas, tokens e chaves de API, que são usadas por suas aplicações de IA.

9. Amazon VPC (Virtual Private Cloud):

1. A Amazon VPC permite criar redes privadas virtuais isoladas para suas aplicações de IA, garantindo que o tráfego permaneça seguro e isolado de outras redes.

10. Amazon Inspector:

1. O Amazon Inspector ajuda a avaliar a segurança de suas aplicações e identificar possíveis vulnerabilidades de segurança que podem ser exploradas por invasores.

11. AWS Firewall Manager:

- O AWS Firewall Manager permite configurar e gerenciar regras de firewall em várias contas da AWS, garantindo uma postura de segurança uniforme em toda a organização.

12. Amazon S3 Object Lock:

- O Amazon S3 Object Lock permite que você proteja objetos no Amazon S3 contra exclusões e alterações acidentais ou maliciosas.

Serviços de Segurança da Azure para aplicações de IA

1. Azure Identity and Access Management (Azure IAM):

- O Azure IAM permite gerenciar o acesso e as permissões dos usuários, grupos e aplicativos que interagem com recursos de IA na plataforma Azure.

2. Azure Active Directory (Azure AD):

- O Azure AD é uma solução de gerenciamento de identidade que permite autenticar e autorizar usuários, fornecendo uma camada adicional de segurança para suas aplicações de IA.

3. Azure Key Vault:

- O Azure Key Vault oferece gerenciamento centralizado de chaves e segredos, ajudando a proteger informações confidenciais, como senhas e chaves de criptografia.

4. Azure DDoS Protection:

- O Azure DDoS Protection ajuda a proteger as aplicações de IA contra ataques de negação de serviço distribuído (DDoS), garantindo disponibilidade contínua.

Serviços de Segurança da Azure para aplicações de IA

5. Azure Security Center:

- O Azure Security Center fornece uma visão geral abrangente da postura de segurança de suas aplicações de IA na plataforma Azure.
- Ajuda a identificar e remediar possíveis ameaças e vulnerabilidades.

6. Azure Web Application Firewall (WAF):

- O Azure WAF ajuda a proteger suas aplicações de IA contra ataques na camada de aplicação, como injeções de SQL e ataques de cross-site scripting (XSS).

Serviços de Segurança da Azure para aplicações de IA

7. Azure Information Protection:

- O Azure Information Protection ajuda a classificar, rotular e proteger documentos e dados confidenciais usados em suas aplicações de IA.

8. Azure Advanced Threat Protection (ATP):

- O Azure ATP oferece detecção avançada de ameaças e monitoramento de atividades suspeitas em sua infraestrutura de IA.

9. Azure Monitor:

- O Azure Monitor fornece monitoramento de integridade e desempenho em tempo real de suas aplicações de IA, permitindo a detecção precoce de problemas de segurança.

10. Azure Sentinel:

- O Azure Sentinel é um serviço de gerenciamento de informações e eventos de segurança (SIEM) que ajuda a analisar e responder a incidentes de segurança em suas aplicações de IA.

Serviços de Segurança da Azure para aplicações de IA

11. Azure Firewall:

- O Azure Firewall oferece uma camada adicional de proteção de rede para suas aplicações de IA, filtrando o tráfego de entrada e saída.

12. Azure Virtual Network (VNet):

- O Azure VNet permite criar redes virtuais isoladas para suas aplicações de IA, garantindo que o tráfego permaneça seguro e isolado de outras redes.

13. Azure Bastion:

- O Azure Bastion fornece acesso seguro a máquinas virtuais e recursos de IA hospedados na plataforma Azure, minimizando riscos de segurança.

Serviços de Segurança da GCP para aplicações de IA

1. Google Identity and Access Management (IAM):

- O Google IAM permite gerenciar permissões de acesso a recursos na GCP, garantindo que somente usuários e serviços autorizados possam interagir com suas aplicações de IA.

2. Google Cloud Identity-Aware Proxy (IAP):

- O Google IAP fornece controle de acesso com base na identidade para aplicativos da Web e APIs, adicionando uma camada adicional de autenticação e autorização.

Serviços de Segurança da GCP para aplicações de IA

3. Google Cloud KMS (Key Management Service):

- O Google KMS permite gerenciar chaves de criptografia para proteger dados e modelos de IA.
- Fundamental para garantir a segurança dos dados confidenciais.

4. Google Cloud Armor:

- O Google Cloud Armor ajuda a proteger suas aplicações de IA contra ataques DDoS e ameaças na camada de aplicação, fornecendo regras de segurança personalizadas.

Serviços de Segurança da GCP para aplicações de IA

5. Google Cloud Security Command Center:

- O Google Cloud Security Command Center oferece visibilidade sobre a postura de segurança de suas aplicações de IA, identificando possíveis ameaças e vulnerabilidades.

6. Google Cloud Web Security Scanner:

- O Google Web Security Scanner ajuda a identificar e remediar vulnerabilidades em suas aplicações da Web de IA, garantindo que elas sejam seguras contra ataques.

Serviços de Segurança da GCP para aplicações de IA

7. Google Cloud Data Loss Prevention (DLP):

- O Google DLP ajuda a descobrir e proteger dados sensíveis em suas aplicações de IA, evitando vazamentos acidentais ou maliciosos.

8. Google Cloud Monitoring:

- O Google Cloud Monitoring fornece monitoramento de integridade e desempenho em tempo real de suas aplicações de IA, permitindo a detecção precoce de problemas de segurança.

9. Google Cloud Logging:

1. O Google Cloud Logging registra atividades e eventos em suas aplicações de IA, ajudando na auditoria e investigação de incidentes de segurança.

10. Google Cloud Identity Services:

1. Os serviços de identidade da GCP, como o Google Cloud Identity e o Google Workspace, garantem que a identidade dos usuários seja gerenciada de forma segura e possa ser integrada a suas aplicações de IA.

Serviços de Segurança da GCP para aplicações de IA

11. Google Cloud Private Service Connect:

- O Private Service Connect permite estabelecer conexões seguras e privadas com serviços gerenciados na GCP, protegendo o tráfego de rede entre serviços de IA.

12. Google Cloud Virtual Private Cloud (VPC):

- O Google VPC permite criar redes virtuais isoladas para suas aplicações de IA, garantindo a segregação do tráfego e a segurança da rede.

Segurança em Cloud para Aplicações de Blockchain

FIAP MBA+

1.Integridade de Dados:

- A integridade dos dados é essencial em sistemas de blockchain. Os dados armazenados na nuvem devem ser protegidos contra alterações não autorizadas. A criptografia e a assinatura digital são usadas para garantir a integridade dos dados da blockchain.

2.Autenticação e Autorização:

- A autenticação e a autorização são cruciais para controlar o acesso aos recursos da blockchain na nuvem. Isso envolve a autenticação de usuários e dispositivos e a atribuição de permissões com base em papéis (RBAC - Role-Based Access Control).

Segurança em Cloud para Aplicações de Blockchain

FIAP MBA+

3. Criptografia:

- A criptografia é usada para proteger dados em repouso e em trânsito. Todos os nós da blockchain na nuvem devem criptografar dados sensíveis, como chaves privadas e transações, para evitar o acesso não autorizado.

4. Gerenciamento de Chaves:

- O gerenciamento seguro de chaves é fundamental. As chaves privadas usadas para assinar transações devem ser armazenadas de forma segura, e serviços de gerenciamento de chaves (KMS) na nuvem podem ser utilizados para isso.

Segurança em Cloud para Aplicações de Blockchain

FIAP MBA+

5. Proteção contra Ataques DDoS:

- Aplicações de blockchain estão sujeitas a ataques de negação de serviço distribuídos (DDoS). Os serviços de proteção DDoS na nuvem podem ajudar a mitigar essas ameaças.

6. Monitoramento e Auditoria:

- A monitorização contínua da atividade da blockchain é fundamental. Os logs de auditoria devem ser mantidos e analisados para detecção de atividades suspeitas.

Segurança em Cloud para Aplicações de Blockchain

FIAP MBA+

7. Segurança de Smart Contracts:

- Os contratos inteligentes são vulneráveis a erros e explorações. Auditorias de segurança e testes são necessários para garantir que os contratos inteligentes sejam seguros.

8. Recuperação de Desastres:

- Planos de recuperação de desastres são necessários para garantir a continuidade das operações em caso de falhas na nuvem, como interrupções de serviço ou violações de segurança.

Segurança em Cloud para Aplicações de Blockchain

FIAP MBA+

9. Conformidade Regulatória:

- As aplicações de blockchain podem estar sujeitas a regulamentações específicas, como a LGPD, GDPR na Europa e outras. Importante garantir que a conformidade regulatória seja mantida na nuvem.

10. Backup de Dados:

- O backup regular dos dados da blockchain é importante para garantir a recuperação de dados em caso de perda ou corrupção.

Segurança em Cloud para Aplicações de Blockchain

FIAP MBA+

11. Atualizações e Patches:

- As atualizações de software e patches de segurança devem ser aplicados regularmente para corrigir vulnerabilidades conhecidas.

12. Treinamento e Conscientização:

- A equipe que opera a aplicação de blockchain na nuvem deve estar ciente das melhores práticas de segurança e ser treinada para reconhecer ameaças.

Serviços de Segurança da AWS para Blockchain

FIAP MBA+

1. AWS Identity and Access Management (IAM):

1. O AWS IAM permite controlar quem tem acesso aos recursos da AWS. Para aplicações de blockchain, é fundamental configurar permissões granulares para controlar o acesso a chaves de criptografia e outros recursos sensíveis.

2. Amazon Virtual Private Cloud (VPC):

1. O Amazon VPC permite criar redes virtuais isoladas para suas aplicações de blockchain, garantindo a segregação do tráfego e a proteção contra acesso não autorizado.

3. AWS Key Management Service (KMS):

1. O AWS KMS oferece serviços de gerenciamento de chaves de criptografia para proteger dados críticos de blockchain, incluindo chaves privadas e registros de transações.

Serviços de Segurança da AWS para Blockchain

FIAP MBA+

4. AWS Shield:

1. O AWS Shield fornece proteção contra ataques DDoS (Distributed Denial of Service), garantindo a disponibilidade de suas aplicações de blockchain.

5. Amazon GuardDuty:

1. O Amazon GuardDuty é um serviço de detecção de ameaças que monitora a atividade da conta e do tráfego de rede em busca de comportamento suspeito ou ameaças à segurança.

6. Amazon Macie:

1. O Amazon Macie é um serviço de segurança que usa machine learning para descobrir e proteger dados sensíveis, ajudando a identificar possíveis riscos de privacidade em registros de blockchain

Serviços de Segurança da AWS para Blockchain

7. AWS CloudTrail:

1. O AWS CloudTrail registra todas as ações realizadas na conta da AWS, permitindo a auditoria e a trilha de atividades para garantir a conformidade e a detecção de ameaças.

8. AWS Web Application Firewall (WAF):

1. O AWS WAF ajuda a proteger aplicações de blockchain contra ameaças na camada de aplicação, como ataques de injeção de SQL e cross-site scripting (XSS).

9. Amazon S3 Object Lock:

1. O Amazon S3 Object Lock permite proteger registros de blockchain contra exclusões ou modificações acidentais ou maliciosas.

Serviços de Segurança da AWS para Blockchain

10. AWS Firewall Manager:

1. O AWS Firewall Manager permite configurar e gerenciar regras de firewall em várias contas da AWS, garantindo uma postura de segurança uniforme em toda a organização.

11. Amazon VPC Flow Logs:

1. Os logs de fluxo da Amazon VPC permitem monitorar o tráfego de rede em tempo real e identificar atividades suspeitas ou anômalas.

12. Amazon Detective:

1. O Amazon Detective é um serviço de análise de segurança que ajuda a investigar e solucionar problemas de segurança em suas aplicações de blockchain.

Serviços de Segurança da Microsoft Azure para Blockchain

1. Azure Key Vault:

- Permite o armazenamento e a administração segura de chaves, segredos e certificados usados na implementação e operação da blockchain.

2. Azure Active Directory:

- Fornece recursos avançados de autenticação e autorização, ajudando a controlar o acesso às aplicações de blockchain.

3. Azure Security Center:

- Oferece monitoramento contínuo de ameaças e vulnerabilidades, além de fornecer recomendações de segurança específicas para as aplicações de blockchain.

Serviços de Segurança da Microsoft Azure para Blockchain

4. Azure Policy:

- Permite a implementação de políticas de conformidade para garantir que a infraestrutura e as configurações estejam alinhadas com os padrões de segurança.

5. Azure Monitor:

- Facilita o monitoramento proativo de desempenho e segurança da aplicação de blockchain, com recursos avançados de análise e diagnóstico.

6. Azure Blockchain Service:

- Fornece uma plataforma gerenciada para criar, implantar e gerenciar redes de blockchain usando diferentes frameworks, como Ethereum e Hyperledger Fabric, com foco na segurança e escalabilidade.

Serviços de Segurança da Microsoft Azure para Blockchain

7. Azure Firewall:

- Ajuda a proteger as redes de blockchain, permitindo a filtragem de tráfego e a implementação de regras de segurança.

8. Azure DDoS Protection:

- Oferece proteção contra ataques de negação de serviço distribuído (DDoS), mantendo a disponibilidade das aplicações de blockchain.

9. Azure Sentinel:

- Um serviço de gerenciamento de informações e eventos de segurança (SIEM) que fornece insights avançados por meio da análise de dados de segurança.

10. Azure Virtual Network:

- Permite a criação de redes privadas virtuais para isolar e proteger as comunicações entre os nós da blockchain e outras partes da infraestrutura.

Serviços de Segurança da GCP para Blockchain

FIAP MBA+

1. Cloud Key Management Service (KMS):

- Oferece gerenciamento de chaves criptográficas para proteger dados e operações críticas na aplicação de blockchain.

2. Identity and Access Management (IAM):

- Permite a configuração de políticas granulares de controle de acesso para garantir que apenas usuários autorizados tenham acesso aos recursos da aplicação de blockchain.

3. Google Cloud Armor:

- Fornece proteção contra ameaças na web, incluindo mitigação de ataques DDoS (negação de serviço distribuído), para garantir a disponibilidade da aplicação de blockchain.

Serviços de Segurança da GCP para Blockchain

4. Cloud Security Command Center:

1. Oferece visibilidade centralizada dos dados de segurança, incluindo alertas e insights para ajudar a identificar e responder a ameaças.

5. Cloud Monitoring e Cloud Logging:

1. Permitem o monitoramento e a análise de registros para identificar anomalias, garantindo a integridade e segurança da aplicação de blockchain.

6. VPC Service Controls:

1. Ajuda a proteger dados sensíveis da aplicação de blockchain ao restringir o acesso a serviços específicos dentro da Virtual Private Cloud (VPC).

Serviços de Segurança da GCP para Blockchain

7. Cloud Security Scanner:

- Identifica e reporta vulnerabilidades na aplicação de blockchain, ajudando a fortalecer a segurança contra ameaças conhecidas.

8. Cloud Audit Logs:

- Oferece trilhas de auditoria detalhadas para monitorar atividades na aplicação de blockchain e garantir conformidade.

9. Binary Authorization

- Controla quais contêineres podem ser implantados na aplicação de blockchain, garantindo a integridade do código em execução.

10. Google Cloud Confidential Computing:

- Oferece uma camada adicional de segurança, permitindo que dados em uso sejam protegidos contra acessos não autorizados, ideal para cenários sensíveis em blockchain

Plano de Segurança para Migração em Cloud

Fase 1: Avaliação e Preparação

- Avaliação de Ativos e Dados:

- Identifique todos os ativos, sistemas e dados que farão parte da migração. Determine a sensibilidade dos dados e qualquer regulamentação aplicável, como dados pessoais ou informações financeiras.

- Equipe de Segurança:

- Forme uma equipe de segurança dedicada responsável por definir e implementar políticas de segurança, realizar análises de risco e garantir a conformidade com os padrões de segurança.

- Revisão de Requisitos de Conformidade:

- Avalie os requisitos de conformidade específicos do setor ou da empresa e identifique como a migração afetará o cumprimento desses requisitos.

- Avaliação de Riscos:

- Realize uma análise abrangente de riscos para identificar ameaças à segurança, vulnerabilidades e pontos fracos na infraestrutura existente e na futura infraestrutura de nuvem.

Plano de Segurança para Migração em Cloud

Fase 2: Projeto e Configuração Segura

- Escolha da Nuvem e Modelo de Implantação:

- Selecione o provedor de serviços em nuvem e o modelo de implantação que melhor atenda às necessidades de segurança e conformidade. Considere fatores como a localização dos data centers, serviços de segurança oferecidos e certificações de conformidade.

- Políticas de Segurança:

- Desenvolva políticas de segurança que abranjam aspectos como autenticação, autorização, criptografia, retenção de dados e conformidade. Essas políticas devem estar alinhadas com os padrões e regulamentações de segurança.

- Acesso Controlado:

- Implemente controles de acesso rigorosos, como autenticação multifatorial (MFA), gerenciamento de identidade e controle de acesso baseado em função (RBAC), para garantir que apenas usuários autorizados tenham acesso aos recursos da nuvem.

- Encriptação de Dados:

- Utilize criptografia para proteger dados em repouso e em trânsito. Implemente serviços de gerenciamento de chaves (KMS) para garantir a segurança das chaves de criptografia.

Plano de Segurança para Migração em Cloud

Fase 3: Migração e Testes

- Testes de Segurança:

- Realize testes de segurança extensivos para garantir que as aplicações migradas estejam protegidas contra ameaças comuns, como vulnerabilidades de segurança, injeções de código e ataques de negação de serviço.

- Monitoramento e Resposta a Incidentes:

- Configure sistemas de monitoramento para detectar atividades anômalas e estabeleça um plano de resposta a incidentes para lidar com eventos de segurança, como intrusões ou violações.

- Backup e Recuperação de Desastres:

- Implemente procedimentos de backup regulares para garantir a recuperação de dados e sistemas em caso de falhas ou incidentes graves.

Plano de Segurança para Migração em Cloud

Fase 4: Implementação e Otimização Contínua

- Atualizações de Segurança:

- Mantenha sistemas, aplicativos e bibliotecas atualizados com as correções de segurança mais recentes. Automatize, sempre que possível, o processo de atualização.

- Auditorias de Segurança:

- Realize auditorias de segurança regulares para avaliar o cumprimento das políticas e requisitos de segurança. Certifique-se de que a infraestrutura da nuvem está em conformidade.

- Conscientização e Treinamento:

- Eduque a equipe e os usuários sobre boas práticas de segurança, incluindo a identificação de ameaças e a importância de proteger credenciais.

- Aprimoramentos Contínuos:

- Realize análises pós-migração para identificar áreas de melhoria e otimização da segurança, e aplique as lições aprendidas em futuras migrações.

- Controle de Acesso e Monitoramento Contínuo:

- Mantenha a configuração de controle de acesso e o monitoramento contínuo para se adaptar a novos requisitos e ameaças em constante evolução. Reavalie regularmente as políticas de segurança à medida que as circunstâncias mudam.

Atividade – Planos de Segurança para Migração de Serviços em Cloud

- Selecionar um cenário de Plano de Segurança para Migração de serviços em Cloud e propor melhorias considerando as melhores práticas e um dos seguintes provedores: AWS, Azure e CGP.
- Incluir no Plano de Segurança, de acordo com o provedor de Cloud selecionado, os serviços de segurança oferecidos pelos provedores.
- Responder as questões do cenário escolhido
- Elaborar uma apresentação
- Acesso em https://www.dropbox.com/scl/fi/oa0h4kk2uo8gez0wp7bhm/Planos-de-Seguran-a-para-Migra-o-em-Cloud.pdf?rlkey=xlu680t5l1hal3i91wz0borxt&dl=0

OBRIGADO!


FIAP