Excelente! Vamos abordar o "Eixo 3: Infraestrutura, Redes e Segurança" focado na metodologia e prováveis cobranças da banca FGV para o CNU Bloco 3. Pense nisso como seu mapa estratégico para revisar.

A FGV gosta de teoria, modelos, princípios, conceitos e como eles se aplicam. Eles costumam cobrar definições, comparações (OSI vs TCP/IP, TCP vs UDP, diferentes tipos de criptografia), funcionamento básico de protocolos e equipamentos, e os pilares da segurança da informação.

Aqui estão os pontos-chave, estruturados e concisos:

---

\*\*Eixo 3: Infraestrutura, Redes e Segurança (Foco FGV - CNU Bloco 3)\*\*

\*\*1. Infraestrutura de TI: A Base de Tudo\*\*

\* \*\*Conceitos Fundamentais:\*\*

\* \*\*Servidores:\*\* Compreender o papel (processamento, armazenamento), tipos (físicos, virtuais) e a importância da \*\*Virtualização\*\* (VMs, contêineres como Docker/Kubernetes - FGV pode cobrar conceitos básicos e benefícios).

\* \*\*Armazenamento (Storage):\*\* Tipos e propósitos (SAN, NAS, Object Storage - entender \*quando\* usar cada um). Importância de \*\*Backup e Recuperação (Recovery)\*\*.

\* \*\*Data Centers:\*\* Onde a infraestrutura reside. Conceitos de resiliência, energia, refrigeração.

\* \*\*Cloud Computing (Computação em Nuvem): FGV ADORA!\*\*

\* \*\*Modelos de Serviço:\*\* Entender as diferenças e exemplos de:

\* \*\*IaaS (Infrastructure as a Service):\*\* Máquinas virtuais, armazenamento, redes (Ex: EC2, S3, VPC).

\* \*\*PaaS (Platform as a Service):\*\* Ambiente para desenvolver/executar apps sem gerenciar infra (Ex: App Engine, Heroku).

\* \*\*SaaS (Software as a Service):\*\* Software pronto, acessado via web (Ex: Gmail, Office 365).

\* \*\*Modelos de Implantação:\*\*

\* \*\*Pública:\*\* Provedores grandes (AWS, Azure, GCP).

\* \*\*Privada:\*\* Infra dedicada a uma organização.

\* \*\*Híbrida:\*\* Combinação de pública e privada.

\* \*\*Multicloud:\*\* Uso de múltiplos provedores públicos.

\* \*\*Benefícios e Desafios:\*\* Escalabilidade, elasticidade, custo vs. segurança, dependência.

\* \*\*Alta Disponibilidade e Recuperação de Desastres (HA/DR):\*\*

\* \*\*Conceito:\*\* Garantir que sistemas e dados estejam acessíveis mesmo com falhas.

\* \*\*Estratégias:\*\* Redundância, balanceamento de carga, clustering, sites de DR (hot, warm, cold).

\* \*\*BCP/DRP (Business Continuity Plan / Disaster Recovery Plan):\*\* Planos para continuidade de negócio e recuperação.

\*\*2. Redes de Computadores: A Conectividade Essencial\*\*

\* \*\*Modelos de Referência: ESSENCIAL para FGV!\*\*

\* \*\*Modelo OSI (Open Systems Interconnection):\*\*

\* \*\*7 Camadas:\*\* Saber o nome e a \*função principal\* de cada camada (Física, Enlace, Rede, Transporte, Sessão, Apresentação, Aplicação). Não precisa decorar protocolos específicos de cada camada, mas saber \*onde\* eles se encaixam (Ex: IP na Rede, TCP/UDP no Transporte).

\* \*\*Modelo TCP/IP:\*\*

\* \*\*4/5 Camadas:\*\* Mapeamento aproximado com OSI. Entender as principais (Aplicação, Transporte, Internet, Acesso à Rede). Mais prático e usado na internet real.

\* \*\*Principais Protocolos: Conhecer a função de cada um!\*\*

\* \*\*Camada de Rede/Internet:\*\*

\* \*\*IP (Internet Protocol):\*\* Endereçamento e roteamento. \*\*IPv4 vs IPv6\*\* (evolução, tamanho do endereço).

\* \*\*Camada de Transporte:\*\*

\* \*\*TCP (Transmission Control Protocol):\*\* Confiável, orientado à conexão, controle de fluxo e erro. \*Para que usar?\* (Web, E-mail, Transferência de arquivos).

\* \*\*UDP (User Datagram Protocol):\*\* Não confiável, sem conexão, mais rápido. \*Para que usar?\* (Streaming, Jogos online, DNS, VoIP). \*\*Saber a diferença entre TCP e UDP é CRUCIAL para FGV.\*\*

\* \*\*Camada de Aplicação:\*\*

\* \*\*HTTP/HTTPS:\*\* Web (diferença: S de Segurança/SSL/TLS).

\* \*\*DNS (Domain Name System):\*\* Tradução de nomes para IPs. \*\*Como funciona?\*\* (Servidores recursivos, autoritativos).

\* \*\*DHCP (Dynamic Host Configuration Protocol):\*\* Atribuição automática de IPs.

\* \*\*SMTP, POP3, IMAP:\*\* E-mail.

\* \*\*FTP/SFTP:\*\* Transferência de arquivos.

\* \*\*SSH:\*\* Acesso remoto seguro.

\* \*\*Equipamentos de Rede:\*\*

\* \*\*Hub:\*\* Repetidor simples (obsoleto).

\* \*\*Switch:\*\* Camada 2 (Enlace), segmenta redes por MAC Address.

\* \*\*Router (Roteador):\*\* Camada 3 (Rede), conecta redes diferentes por IP Address.

\* \*\*Firewall:\*\* Segurança! Filtra tráfego (Camada 3 e 4, ou superior).

\* \*\*Load Balancer:\*\* Distribui carga de requisições entre servidores.

\* \*\*Redes Sem Fio (Wireless):\*\*

\* \*\*Padrão 802.11:\*\* Família Wi-Fi.

\* \*\*Segurança:\*\* WEP (obsoleto), WPA, WPA2, WPA3.

\*\*3. Segurança da Informação: Protegendo os Ativos\*\*

\* \*\*Pilares da Segurança da Informação (Tríade CIA): ESSENCIAL!\*\*

\* \*\*Confidencialidade:\*\* Garantir que a informação seja acessada apenas por quem tem permissão. (Ex: Criptografia, Controle de Acesso).

\* \*\*Integridade:\*\* Garantir que a informação não foi alterada de forma não autorizada. (Ex: Hashing, Assinaturas Digitais).

\* \*\*Disponibilidade:\*\* Garantir que a informação e os sistemas estejam acessíveis quando necessário. (Ex: Backups, Redundância, Prevenção de DoS).

\* \*(Às vezes adicionam Autenticidade e Irrefutabilidade/Não Repúdio).\*

\* \*\*Gestão de Riscos:\*\*

\* \*\*Conceitos:\*\* Ativos, Ameaças, Vulnerabilidades, Risco (= Ameaça x Vulnerabilidade).

\* \*\*Tratamento de Risco:\*\* Mitigar, Transferir, Aceitar, Evitar.

\* \*\*Tipos de Ataques e Ameaças:\*\*

\* \*\*Malware:\*\* Vírus, Worms, Trojans, Ransomware (Sequestro de dados - MUITO cobrado!).

\* \*\*Phishing/Spear Phishing:\*\* Engenharia social para roubar informações.

\* \*\*DoS/DDoS (Denial of Service):\*\* Ataques para tornar sistemas indisponíveis.

\* \*\*Injeção (SQL Injection, XSS):\*\* Explorar falhas em aplicações web/bancos de dados.

\* \*\*Força Bruta, Ataques de Dicionário.\*\*

\* \*\*Controles de Segurança: Como se proteger?\*\*

\* \*\*Controles Técnicos:\*\*

\* \*\*Firewalls:\*\* Filtram tráfego (estadual/stateful vs. sem estado/stateless). \*\*FGV cobra funcionamento básico.\*\*

\* \*\*IDS/IPS (Intrusion Detection/Prevention System):\*\* Detectar/prevenir atividades maliciosas na rede/sistema. (Baseado em Assinatura vs. Anomalia).

\* \*\*Antivírus/Antimalware.\*\*

\* \*\*WAF (Web Application Firewall):\*\* Protege aplicações web.

\* \*\*Controles de Acesso (AAA):\*\*

\* \*\*Authentication:\*\* Verificar identidade (Usuário/Senha, Certificado, Biometria). \*\*Multi-Factor Authentication (MFA):\*\* Mais de um fator.

\* \*\*Authorization:\*\* O que o usuário pode fazer após autenticado (Permissões, RBAC - Role-Based Access Control é comum).

\* \*\*Accounting:\*\* Registrar o que o usuário fez (Logs).

\* \*\*Criptografia: ESSENCIAL para FGV!\*\*

\* \*\*Conceitos:\*\* Cifragem/Decifragem. Chave.

\* \*\*Criptografia Simétrica:\*\* Mesma chave para cifrar e decifrar (AES, DES). Rápida. Problema da distribuição da chave.

\* \*\*Criptografia Assimétrica (Chave Pública):\*\* Par de chaves (pública e privada). Uma cifra, a outra decifra. Usada para troca segura de chaves simétricas, \*\*Assinaturas Digitais\*\* e \*\*Certificados Digitais\*\*. (RSA).

\* \*\*Funções de Hashing:\*\* Gera um "resumo" fixo de tamanho a partir de dados. \*\*Não é reversível.\*\* Usada para verificar integridade (MD5, SHA-1, SHA-256). \*\*Saber a diferença entre Simétrica, Assimétrica e Hashing é CRUCIAL.\*\*

\* \*\*Certificados Digitais e Assinaturas Digitais:\*\* Garantem autenticidade, integridade e não-repúdio. Baseados em criptografia assimétrica e Hashing. \*\*Hierarquia de Certificação (ICP-Brasil pode ser mencionada).\*\*

\* \*\*Políticas de Segurança:\*\* Regras e diretrizes.

\* \*\*Conscientização e Treinamento:\*\* O elo humano é o mais fraco.

\* \*\*Resposta a Incidentes:\*\* Plano para lidar com violações de segurança.

---

\*\*Dicas Finais para FGV:\*\*

\* \*\*Entenda os \*conceitos\* por trás de cada termo.\*\* Não apenas decore a definição.

\* \*\*Saiba as \*diferenças\* e \*quando usar\* diferentes tecnologias/protocolos\*\* (Ex: TCP vs UDP, Simétrica vs Assimétrica, IaaS vs SaaS).

\* \*\*Foque nos modelos (OSI, TCP/IP) e nos pilares (CIA Triad) -\*\* são bases teóricas que a FGV gosta de explorar.

\* \*\*Criptografia e Cloud Computing\*\* são tópicos quentes. Dedique atenção especial a eles.

\* Revise termos técnicos em inglês, pois a FGV pode usar a sigla ou o termo original.

Estude com foco, interligando os conceitos. Infraestrutura suporta as Redes, e a Segurança permeia tudo! Boa sorte na sua preparação!