Resposta – Dissertativa 01

A arquitetura-alvo deve adotar IaaS para manter o legado em VMs (Windows Server) enquanto a aplicação é gradualmente refatorada para containers em PaaS (orquestração gerenciada), reduzindo esforço operacional. O banco relacional deve migrar para PaaS (DB gerenciado) com replicação e backups, usando SQL com transações/índices e controle de privilégios (GRANT/REVOKE) para reduzir superfícies de ataque. Na rede, separar camadas por VLANs (usuários, servidores, gestão) com roteamento inter-VLAN controlado por ACL/firewall e integrar filiais via VPN site-to-site. Planejar sub-redes IPv4 por função e habilitar IPv6 dual-stack para serviços internos, com roteamento e políticas equivalentes. Garantir DNS resiliente e acesso via HTTP/HTTPS (TLS), com administração básica de serviços, logs e atualizações em Windows/Linux.

Resposta – Dissertativa 02

A exfiltração caracteriza um incidente decorrente de vulnerabilidade explorada por uma ameaça, elevando o risco ao comprometer dados pessoais e a disponibilidade dos serviços. A contenção exige segmentação (VLAN/ACL), reforço de firewall com regras mínimas, ativação/ajuste de IDS/IPS, uso correto de VPN e proteção de Wi-Fi (WPA2/3, 802.1X) para bloquear movimentação lateral. Corrigir causas típicas do OWASP Top 10 (ex.: controle de acesso, injeção, falhas de configuração), aplicando hash forte para senhas, criptografia simétrica para dados em repouso, assimétrica para troca de chaves e assinatura/certificados para autenticação e integridade. Em governança, registrar ativo afetado, lições aprendidas e continuidade (ITIL), alinhar controles a objetivos (COBIT) e testar DR/backup. Legalmente, acionar procedimentos de LGPD (registro, avaliação e comunicação quando aplicável), observar transparência pela LAI sem expor sigilos e reforçar a responsabilidade do agente público na proteção da informação.