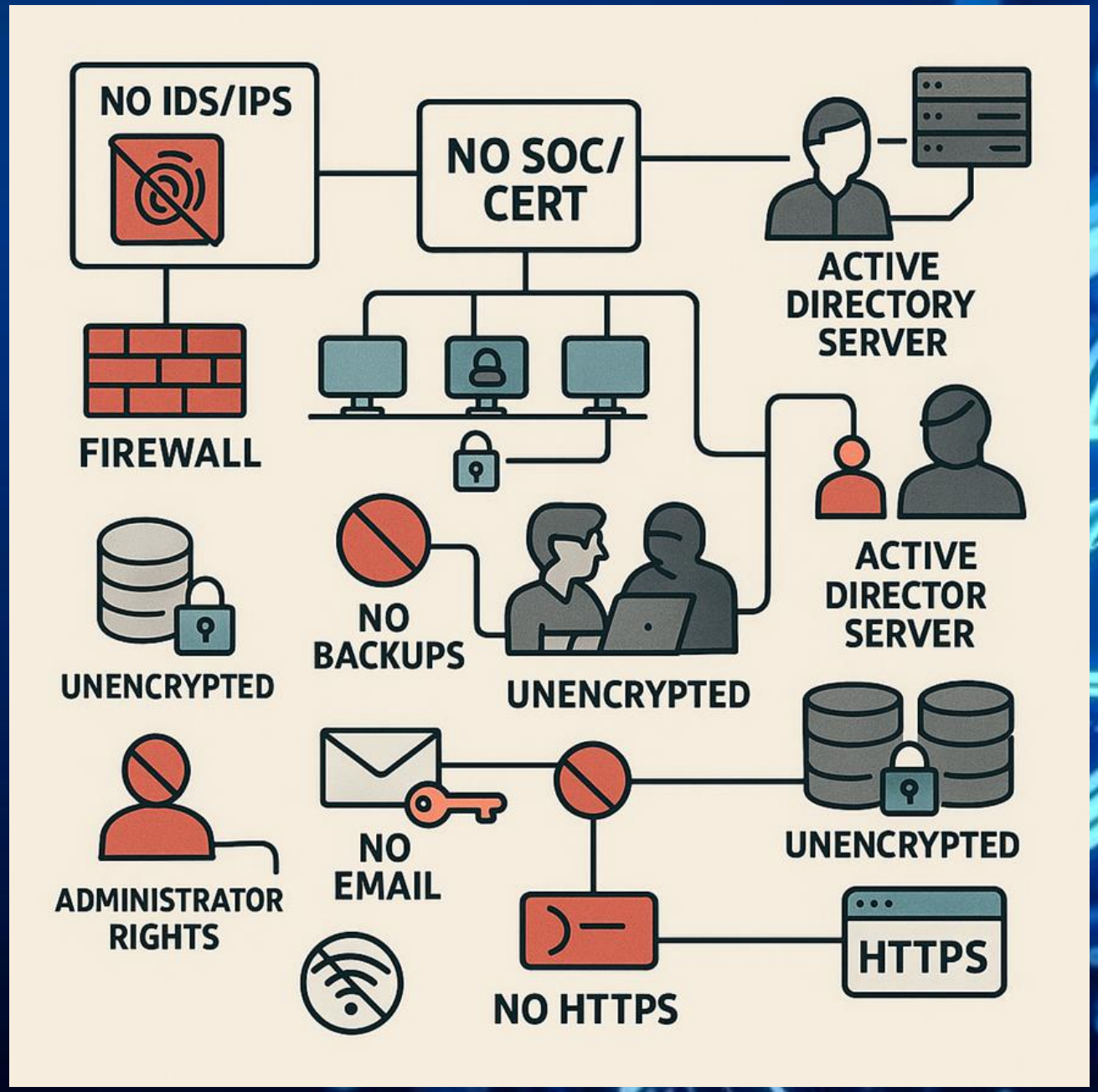
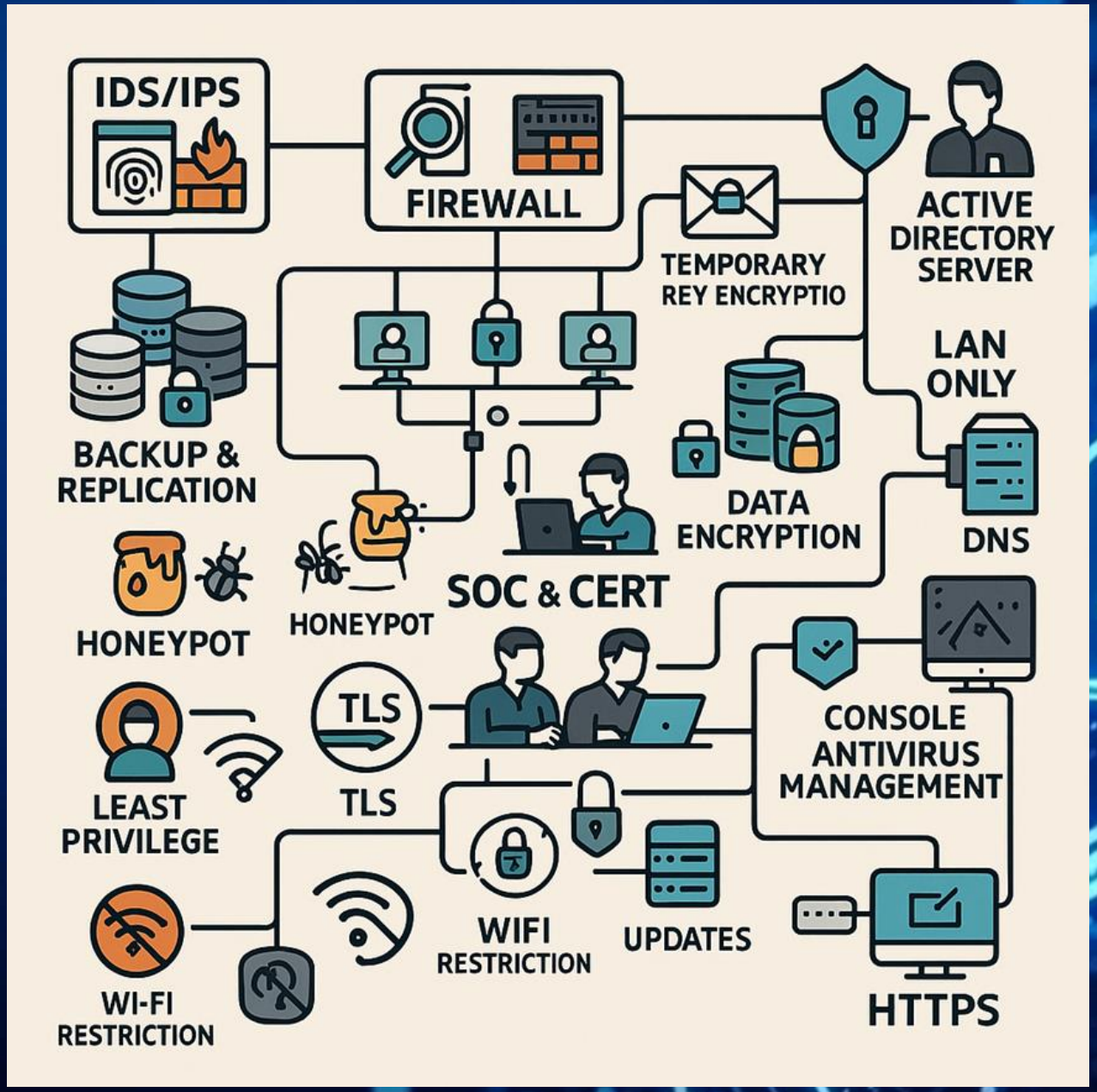
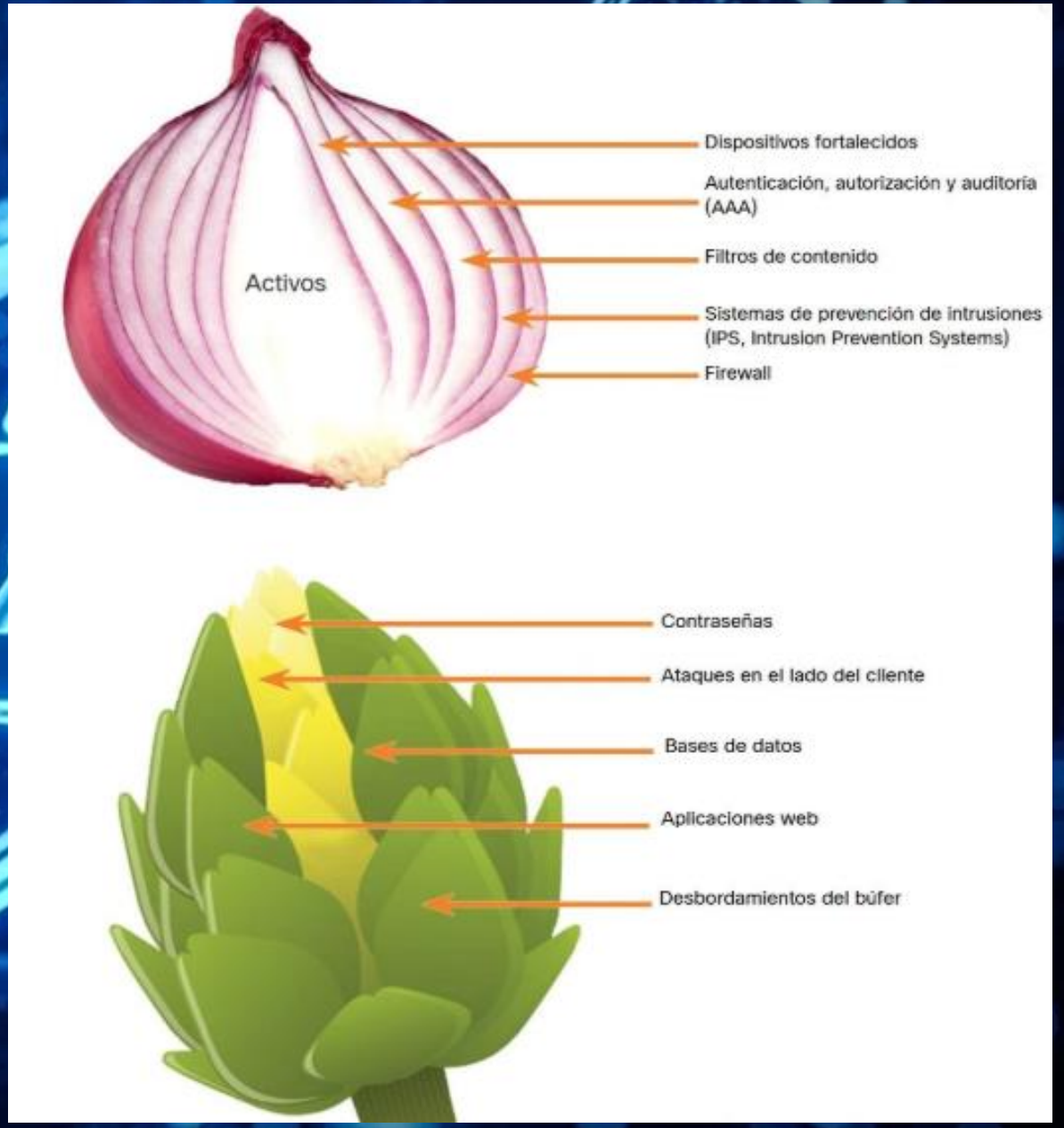
SISTEMA NO HARDENIZADO



SISTEMA HARDENIZADO





1. Capa Perimetral y Segmentación de Red

1.1 Segmentación física y lógica

•División de la red en zonas (producción, administración, SOC, invitados).

•Claves perimetrales únicas para cada segmento.

•VLANs y firewalls internos entre zonas.

1.2 Control de acceso físico

•Instalación de sensores, cerraduras inteligentes y cámaras.

•Restricción de acceso físico a los racks de servidores.

3. Seguridad de la Información y Datos

3.1 Cifrado en reposo

•Cifrado AES-256 en servidores locales y nube.

•Gestión segura de llaves criptográficas.

3.2 Cifrado de correo electrónico

•Llaves temporales por sesión.

•Infraestructura de clave pública/privada (PKI) para cada usuario.

3.3 Copias de seguridad automatizadas

•Backups diferenciales por segmento de red.

•Uso de espejos físicos y virtuales.

•Validación regular de integridad y restauración.

Seguridad de Red y Comunicación

2.1 Firewall perimetral y filtrado de contenido

•Bloqueo de puertos innecesarios.

•Listas blancas y negras de dominios permitidos.

2.2 IDS/IPS

•Monitoreo pasivo (IDS) y activo (IPS) en tiempo real.

•Detección de anomalías y firmas de ataques conocidos.

2.3 TLS y cifrado de tránsito

•Forzar uso de HTTPS, SMTPS, FTPS.

•Certificados válidos y renovaciones automatizadas.

2.4 Trampas de miel (honeypots)

•Implementación de señuelos para engañar y estudiar al atacante.

•Aislamiento de honeypots del entorno real.

4. Gestión de Identidad y Accesos

4.1 Active Directory HardenizadoAutenticación multifactor o tokens físicos para acceso de adminstración.Políticas de bloqueo ante intentos fallidos.

4.2 Políticas de mínimo privilegioRoles definidos según tareas. Acceso segmentado por necesidad operativa.

4.3 Autenticación multifactor en servicios críticos Correos corporativos, VPN, servidores, aplicaciones clave.

4.4 Restricciones de CORS Solo dominios autorizados pueden hacer intercambios Perfiles de acceso por usuario o departamento.

Seguridad de Endpoints

🔸 **5.1 Servidor de Antivirus Centralizado**

•Consola de gestión de antivirus para todos los equipos.

•Políticas de actualización y escaneo obligatorios.

🔸 **5.2 Control de dispositivos y periféricos**

•Bloqueo de puertos USB.

•Autorización previa para dispositivos externos.

Supervisión, Respuesta y Resiliencia

🔸 **6.1 Establecimiento del SOC**

•Monitoreo 24/7 de logs, tráfico, alertas.

•Correlación de eventos y análisis forense.

🔸 **6.2 Activación del CERT**

•Protocolo de acción inmediata ante incidentes.

•Contención y erradicación de amenazas sin escalar.

🔸 **6.3 Gestión de licencias y software legal**

•Políticas de actualización de software.

•Auditorías regulares para evitar software vulnerable.

“En ciberseguridad mucho no es suficiente”