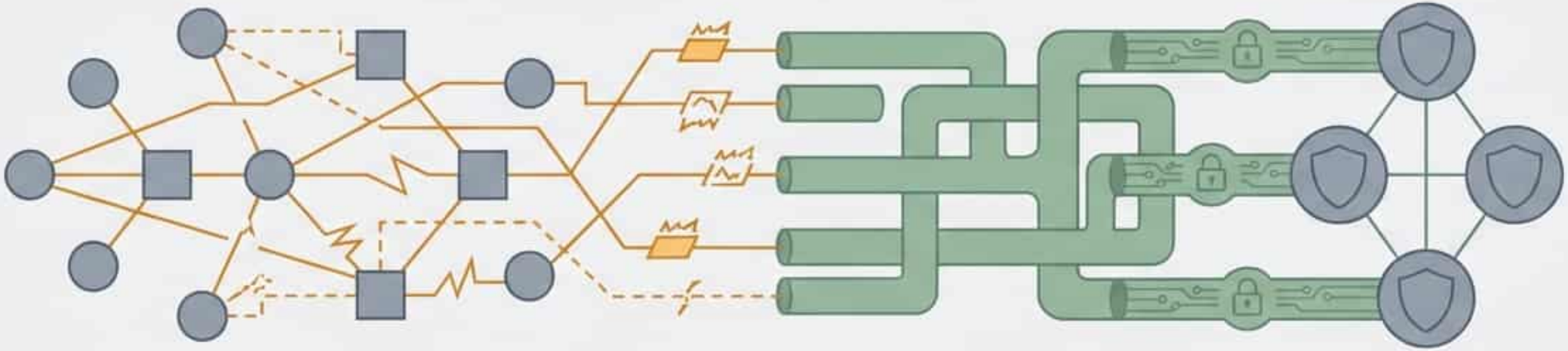
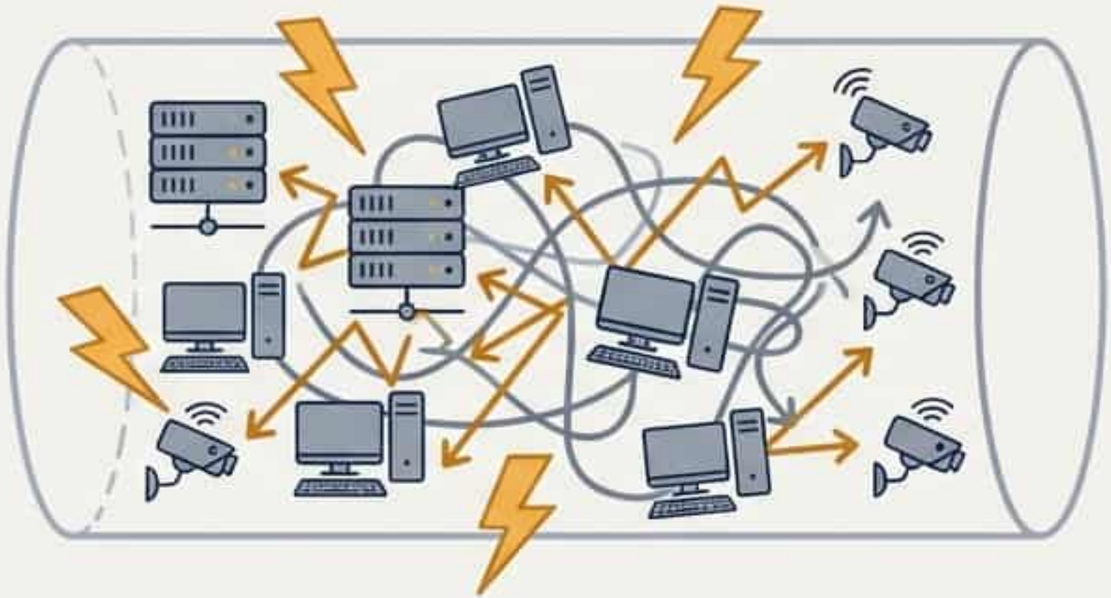
Arquitectura y Seguridad de Redes: De la Segmentación VLAN al Cifrado IPsec



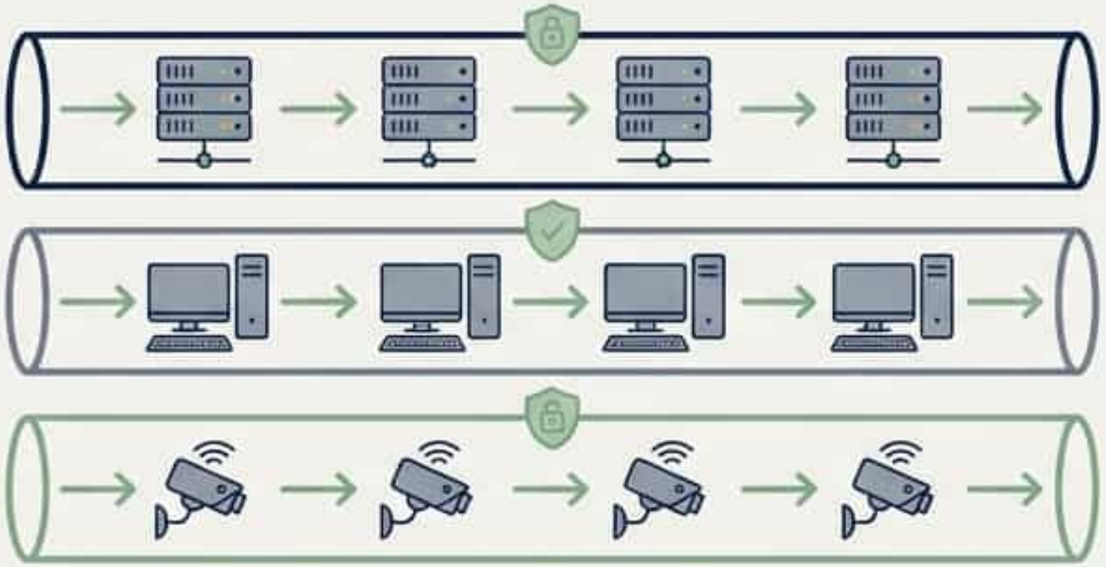
Un recorrido visual sobre el control, la automatización y la protección absoluta del flujo de datos empresariales.

El caos de las redes planas frente al control segmentado



El Riesgo Original: En una red sin segmentar, el tráfico fluye libremente. Un ciberdelincuente que compromete un simple PC puede acceder lateralmente a servidores, bases de datos o sistemas de producción.

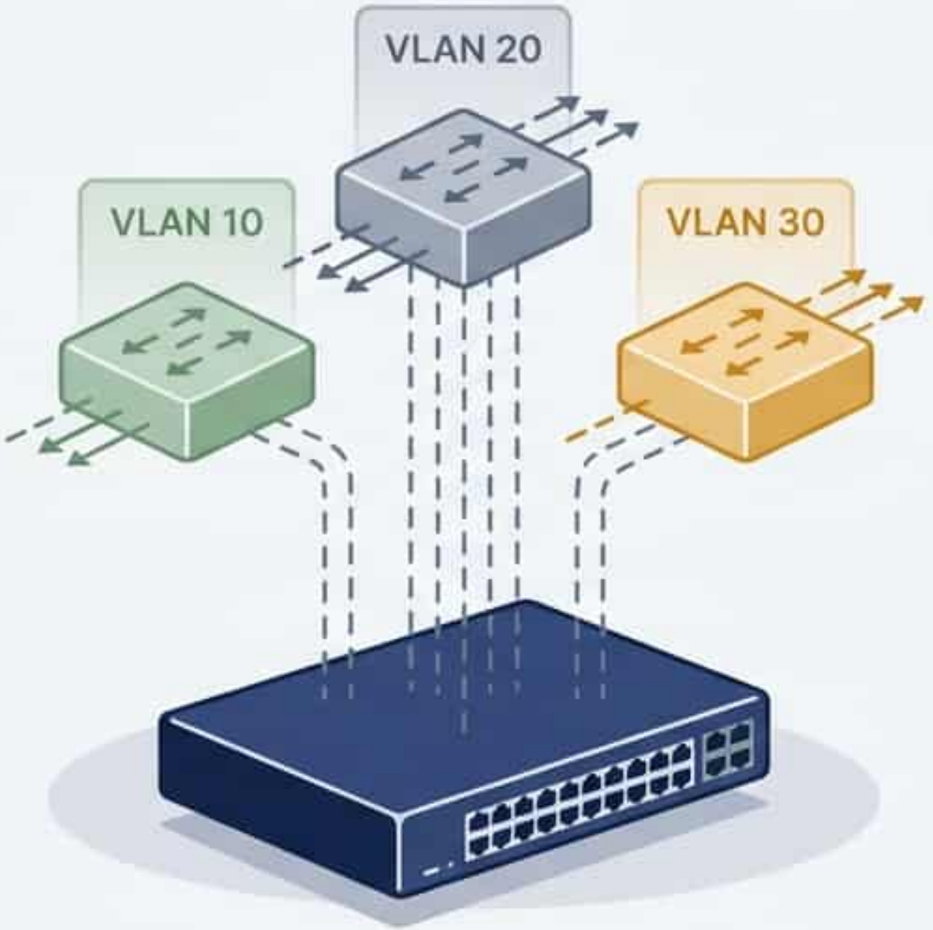
El Rendimiento: Las redes planas sufren congestión constante por el tráfico de broadcast, ralentizando las operaciones críticas.



La Solución: La segmentación mediante VLANs actúa como un sistema de compartimentos estancos, aislando los recursos y conteniendo las amenazas de forma nativa.

Separación lógica sobre infraestructura física

Una VLAN (Virtual Local Area Network) divide un dominio de broadcast físico en múltiples redes lógicas aisladas en la Capa 2 (Capa de Enlace de Datos).



- **El Origen:** En los años 80, W. David Sincoskie (Bellcore) buscaba superar los límites de velocidad física de Ethernet. Su solución fue inventar un puente de múltiples árboles (multitree bridge) asignando 'colores' a las tramas.
- **La Ventaja Moderna:** Permite a los administradores agrupar hosts sin importar su ubicación física, compartiendo el cableado sin interactuar directamente.

Casos de uso reales que transforman la red empresarial

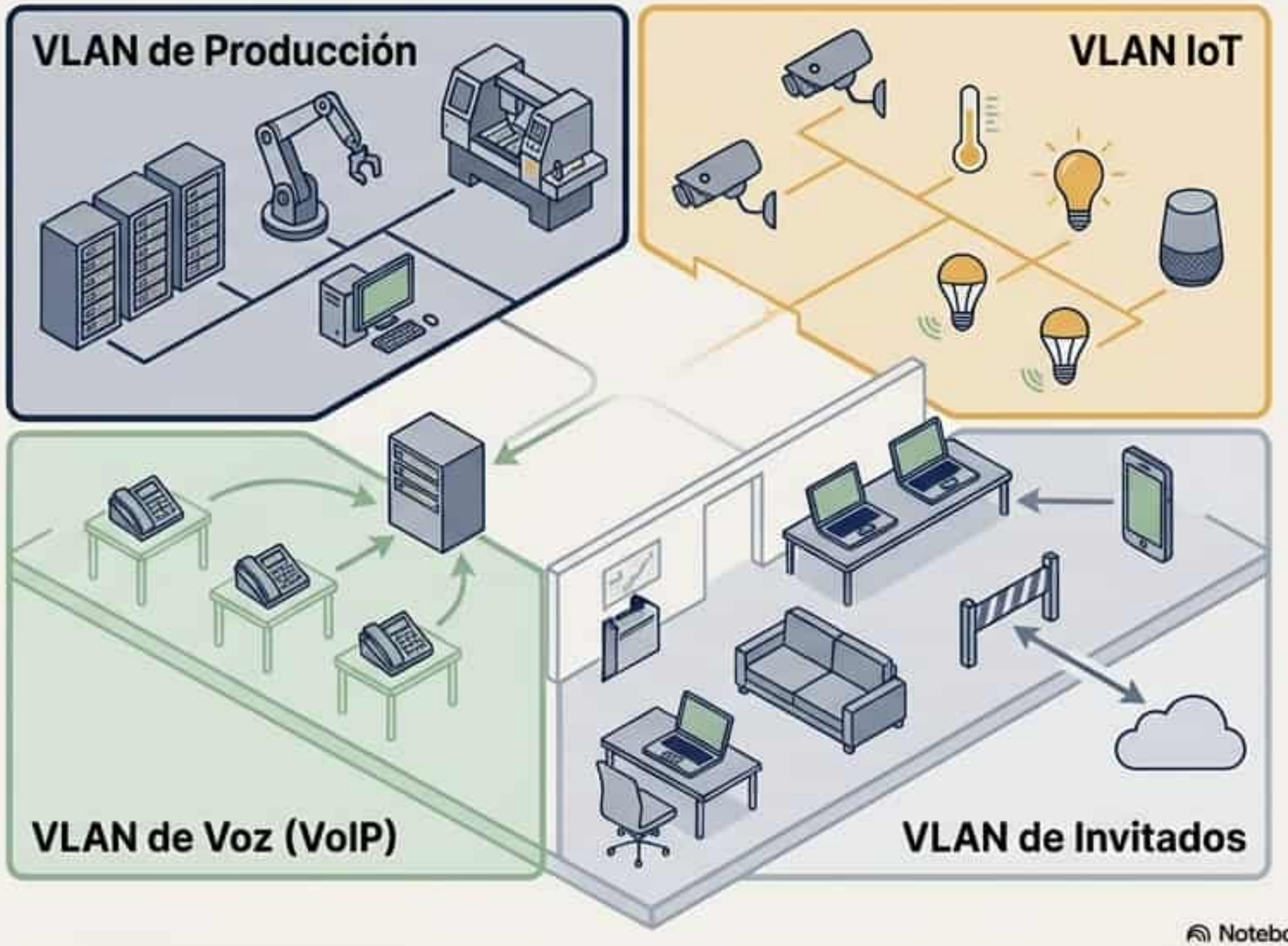
Implementar VLANs prepara la infraestructura para el **ecosistema IoT**, la **nube** y las arquitecturas **Zero Trust**:

VLAN de Producción: Maquinaria y sistemas críticos (OT/IT) aislados de los usuarios generales.

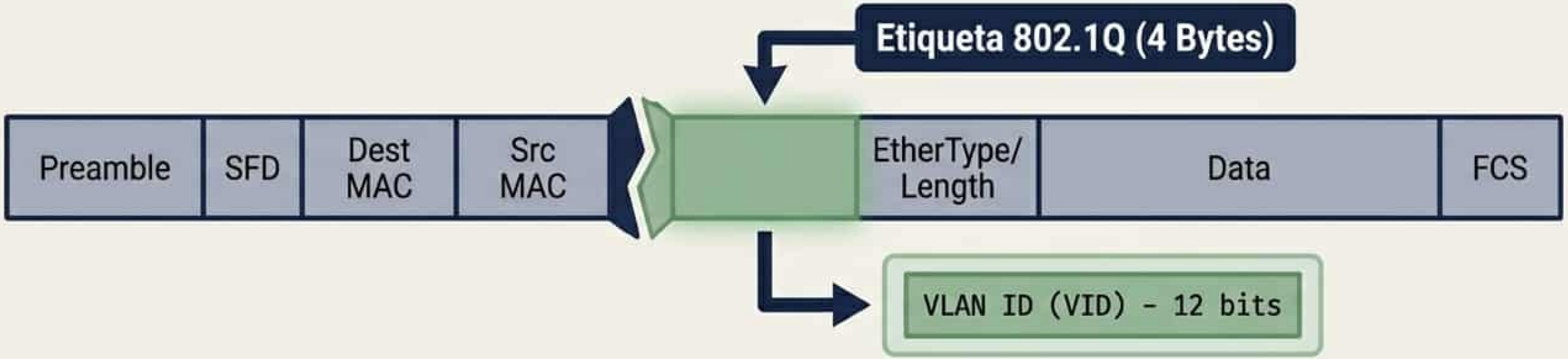
VLAN de Voz (VoIP): Tráfico priorizado con Calidad de Servicio (QoS) para evitar cortes en las llamadas.

VLAN IoT: Cámaras IP, sensores y domótica separados para evitar que dispositivos vulnerables comprometan la red corporativa.

VLAN de Invitados: Acceso exclusivo a Internet, totalmente ciego a los servidores internos.



Bajo el capó: El estándar IEEE 802.1Q y el etiquetado de tramas

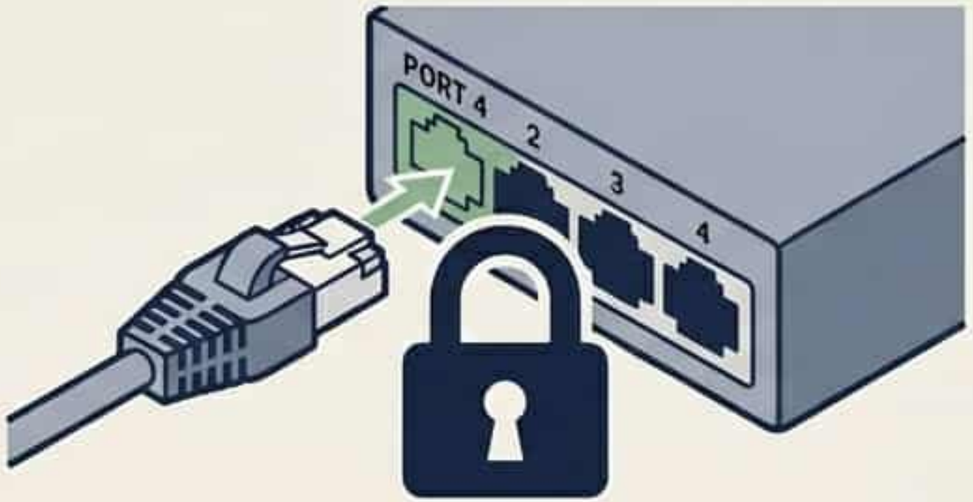


- Para que el hardware estándar diferencie el tráfico, el protocolo 802.1Q modifica la trama Ethernet mediante un etiquetado explícito interno.
- Capacidad: El campo VID de 12 bits permite hasta 4.094 VLANs simultáneas en una red.

Puertos de Acceso vs. Troncales:

- Los puertos de acceso conectan a los usuarios finales (eliminando la etiqueta al salir).
- Los enlaces troncales (Trunks) conectan switches entre sí, preservando las etiquetas para transportar múltiples VLANs por un solo cable.

Dinámicas de asignación: De la configuración manual a las políticas automatizadas



Pertenencia Estática (Basada en el Puerto)

El administrador asigna rígidamente un puerto físico a una VLAN específica. Cualquier dispositivo conectado allí asume esa red.

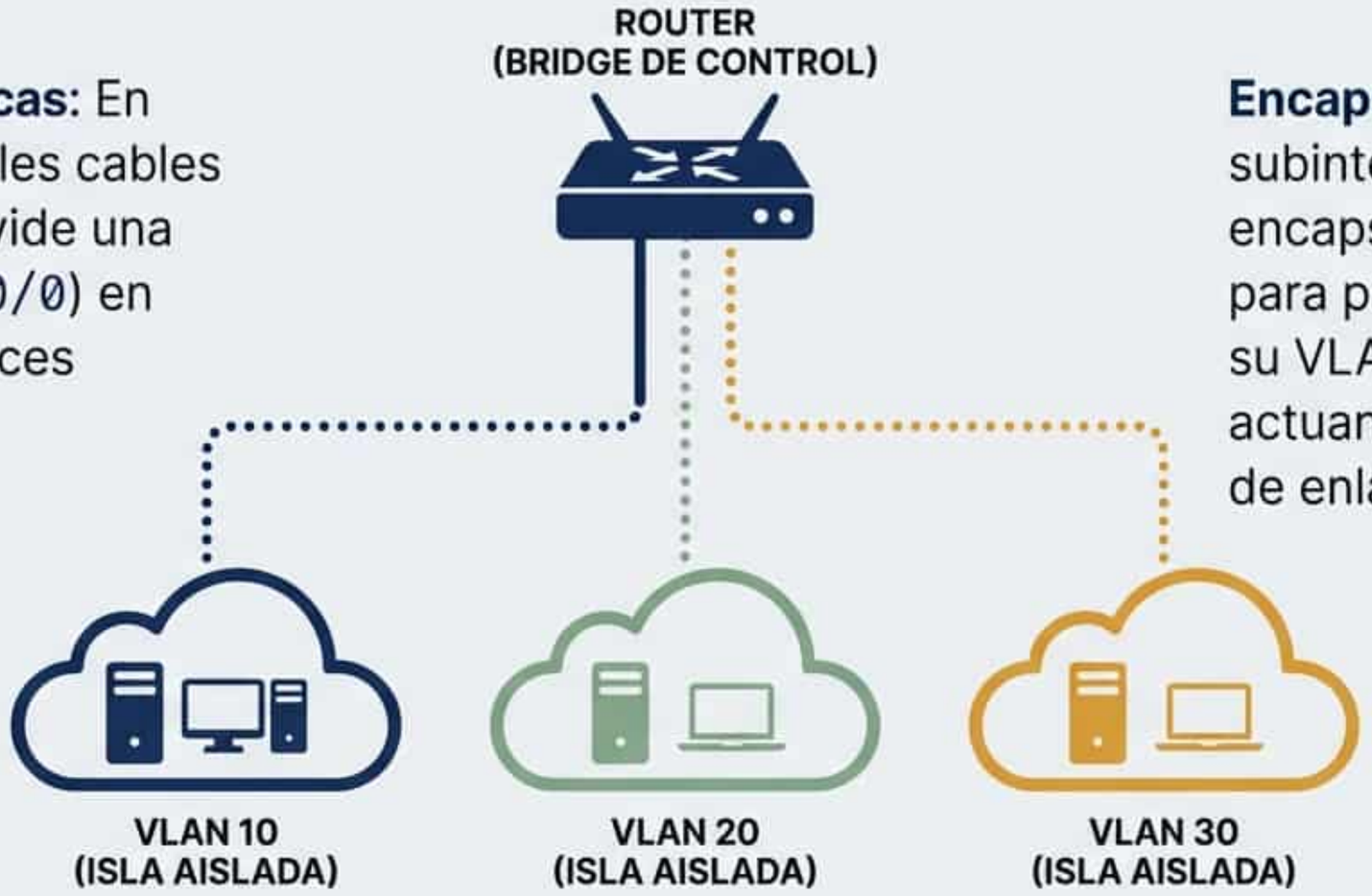
Pertenencia Dinámica (Basada en Políticas)

Utilizando un servidor VMPS, el switch consulta una base de datos. La VLAN se asigna al vuelo basándose en la dirección MAC del dispositivo o en las credenciales del usuario, sin importar dónde se conecte físicamente.

Conectando las islas mediante enrutamiento Inter-VLAN

Las VLANs operan en la Capa 2 y aíslan el tráfico por diseño. Para permitir una comunicación estrictamente controlada entre distintos segmentos, dependemos de la Capa 3.

Subinterfaces Lógicas: En lugar de usar múltiples cables físicos, un router divide una interfaz física (ej. `f0/0`) en múltiples subinterfaces virtuales (`f0/0.10`, `f0/0.20`).



Encapsulamiento: Cada subinterfaz utiliza encapsulamiento dot1Q para procesar el tráfico de su VLAN correspondiente, actuando como la puerta de enlace predeterminada.

Automatización a escala con DHCP

El Protocolo de Configuración Dinámica de Host (DHCP) elimina el trabajo manual propenso a errores.

- **Control Centralizado**: Operando en la capa de aplicación del modelo TCP/IP, automatiza la asignación de direcciones IP, máscaras de subred y puertas de enlace.
- **Escalabilidad**: Indispensable tanto para redes locales pequeñas como para inmensas arquitecturas empresariales fragmentadas en decenas de VLANs, permitiendo que los dispositivos se comuniquen de forma inmediata al conectarse.

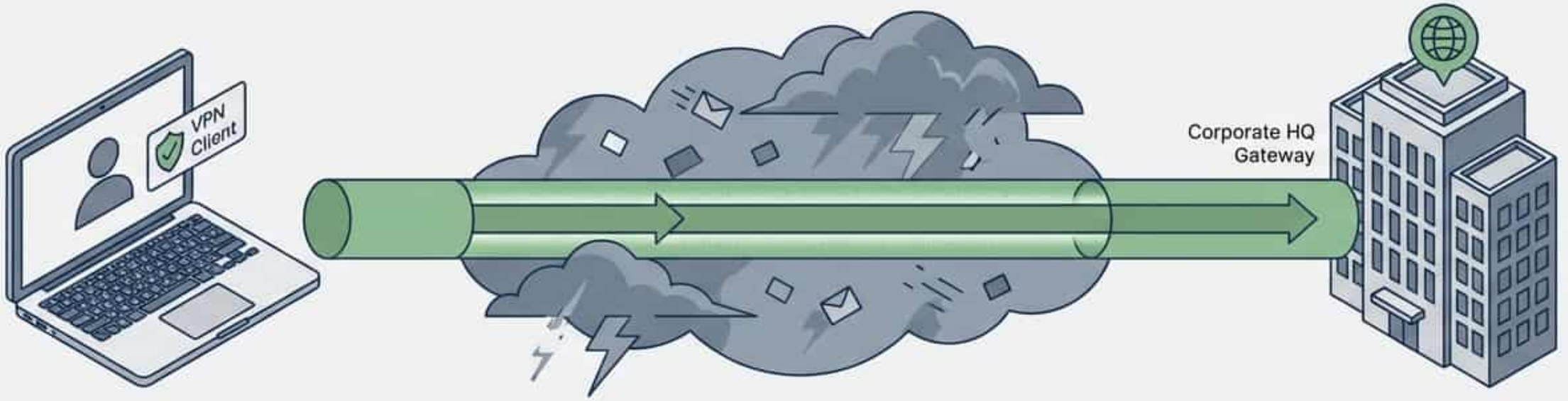
Un vistazo al código: Configuración en Cisco IOS

La creación de una arquitectura segmentada requiere comandos precisos en la consola del switch.

Verificación Eficiente: Comandos como 'show ip interface brief' combinados con filtros pipe ('| include up') permiten auditar el estado de la red filtrando solo la información vital.

Expandiendo la frontera segura mediante VPNs

La segmentación protege el entorno físico, pero el trabajo moderno exige movilidad. Las Redes Privadas Virtuales (VPN) extienden la seguridad corporativa hacia el exterior.



Arquitectura Cliente/Servidor

El cliente VPN (ej. Cisco AnyConnect) se instala en el dispositivo móvil y se comunica con un gateway en el borde de la red empresarial.

Protección Activa

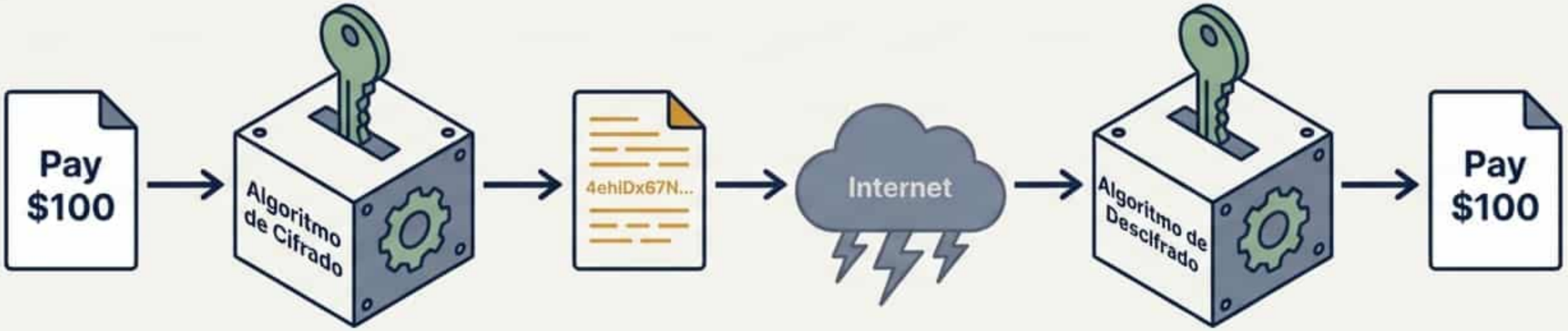
El software encapsula y cifra todo el tráfico antes de enviarlo por la infraestructura pública de Internet, creando un túnel privado e inaccesible para observadores externos.

El núcleo de la seguridad en tránsito: La Tríada CIA

Para que un túnel VPN sea verdaderamente seguro, debe garantizar tres principios fundamentales sobre los datos en tránsito:

- **Confidencialidad (Cifrado):**
  Transformar los datos para que sean ilegibles durante la transmisión.
- **Integridad:**
  Verificar matemáticamente que la información no ha sido alterada o manipulada en el camino.
- **Autenticación:**
  Demostrar de forma inequívoca la identidad del emisor y receptor.
- (Bonus) Protección Anti-Replay:
  Capacidad de detectar y rechazar paquetes interceptados y retransmitidos por atacantes.

Confidencialidad: El poder del cifrado algorítmico



El cifrado se basa en algoritmos y llaves criptográficas. Sin la llave correcta, la decodificación es prácticamente imposible.

Cifrado Simétrico

Utiliza la misma llave tanto para cifrar como para descifrar. Es extremadamente rápido y eficiente para grandes volúmenes de datos.

Cifrado Asimétrico (Ej. RSA)

Emplea un par de llaves: una pública y una privada. Conocer una llave no permite deducir la otra. Esencial para la gestión de certificados digitales.

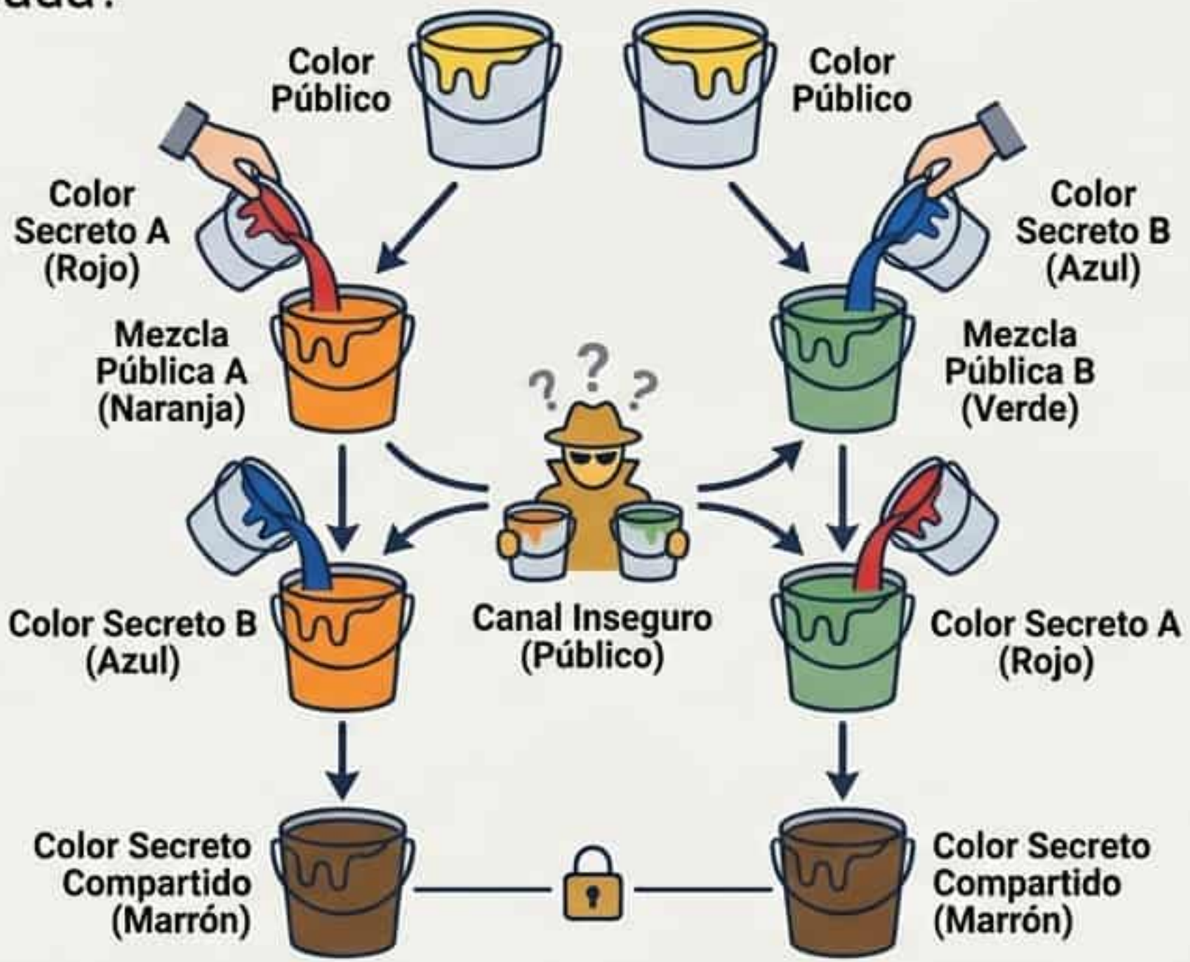
Nota: A mayor longitud de la llave, mayor es la seguridad, pero exige más recursos de procesamiento.

El acuerdo seguro: Intercambio de llaves Diffie-Hellman (DH)

Antes de cifrar los datos, ambos extremos deben compartir una llave secreta. ¿Cómo enviarla por un canal inseguro sin que sea robada?

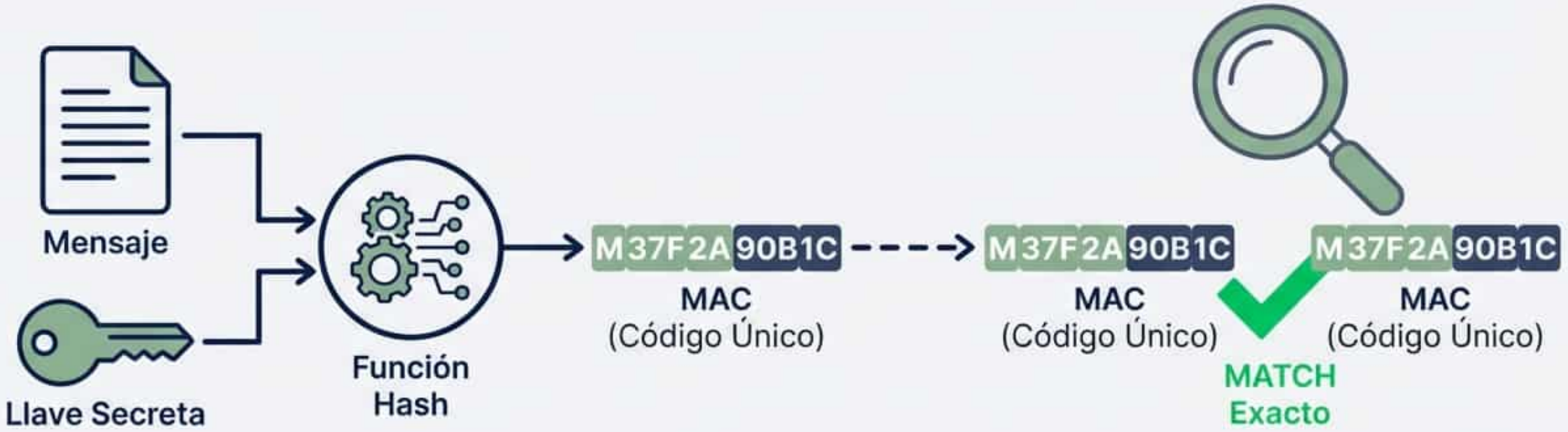
La Magia del DH: Diffie-Hellman no cifra datos, establece llaves. Permite que dos dispositivos acuerden un secreto compartido utilizando un intercambio de variables matemáticas públicas.

El Cimiento: Algoritmos de cifrado como AES y 3DES, o de hashing como MD5 y SHA-1, requieren esta llave simétrica inicial generada de forma segura por DH.



Garantizando la Integridad: Firmas matemáticas (HMAC)

Para asegurar que un paquete no fue alterado, se utiliza un **Código de Autenticación de Mensajes (MAC)**. El emisor combina el mensaje con la llave secreta y lo pasa por una función Hash. El receptor hace lo mismo; si los resultados coinciden, **la integridad es absoluta.**



MD5

Utiliza una llave secreta compartida de 128 bits para generar un hash de 128 bits.

SHA-1

Emplea una llave secreta de 160 bits, generando un hash de 160 bits para una mayor resistencia criptográfica.

El Framework IPsec: El bloque de construcción final

IPsec no es un solo protocolo, es un marco integral que combina todas las tecnologías anteriores para crear **túneles impenetrables** en la **Capa de Red (IP)**. Requiere seleccionar cuatro bloques fundamentales:

1. **Protocolo Base:** Combinar ESP (Encapsulating Security Payload) y AH (Authentication Header). Nota: ESP es esencial porque AH por sí solo no cifra.
2. **Confidencialidad:** Elegir el algoritmo. AES es la recomendación absoluta por su nivel de seguridad superior.
3. **Integridad:** Algoritmos hash como MD5 o SHA para detectar manipulaciones.
4. **Autenticación:** Métodos para verificar la identidad de los extremos (Llaves Pre-Compartidas PSK o certificados asimétricos RSA).