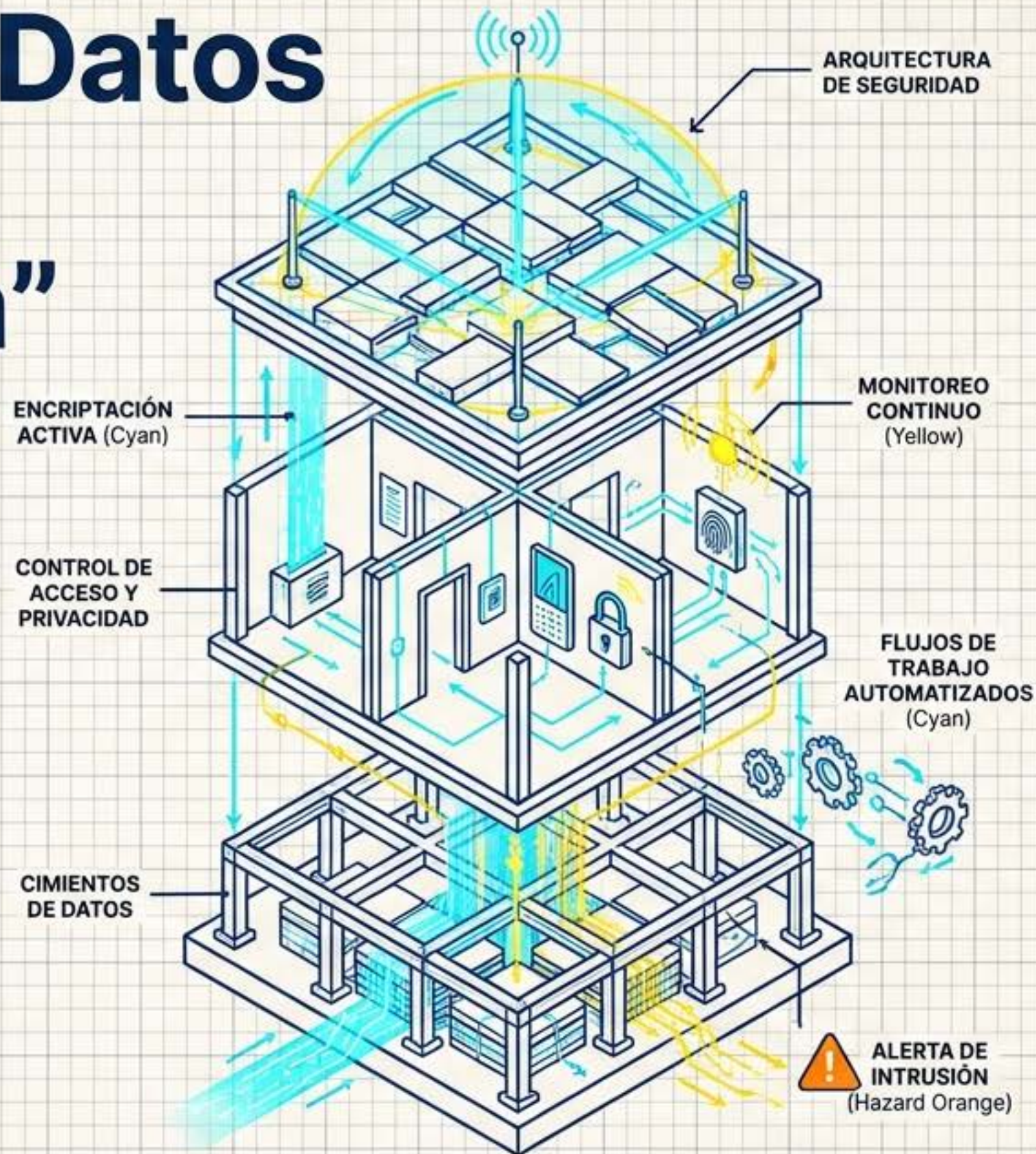


# Gobernanza de Datos y Seguridad de "Andar por Casa"

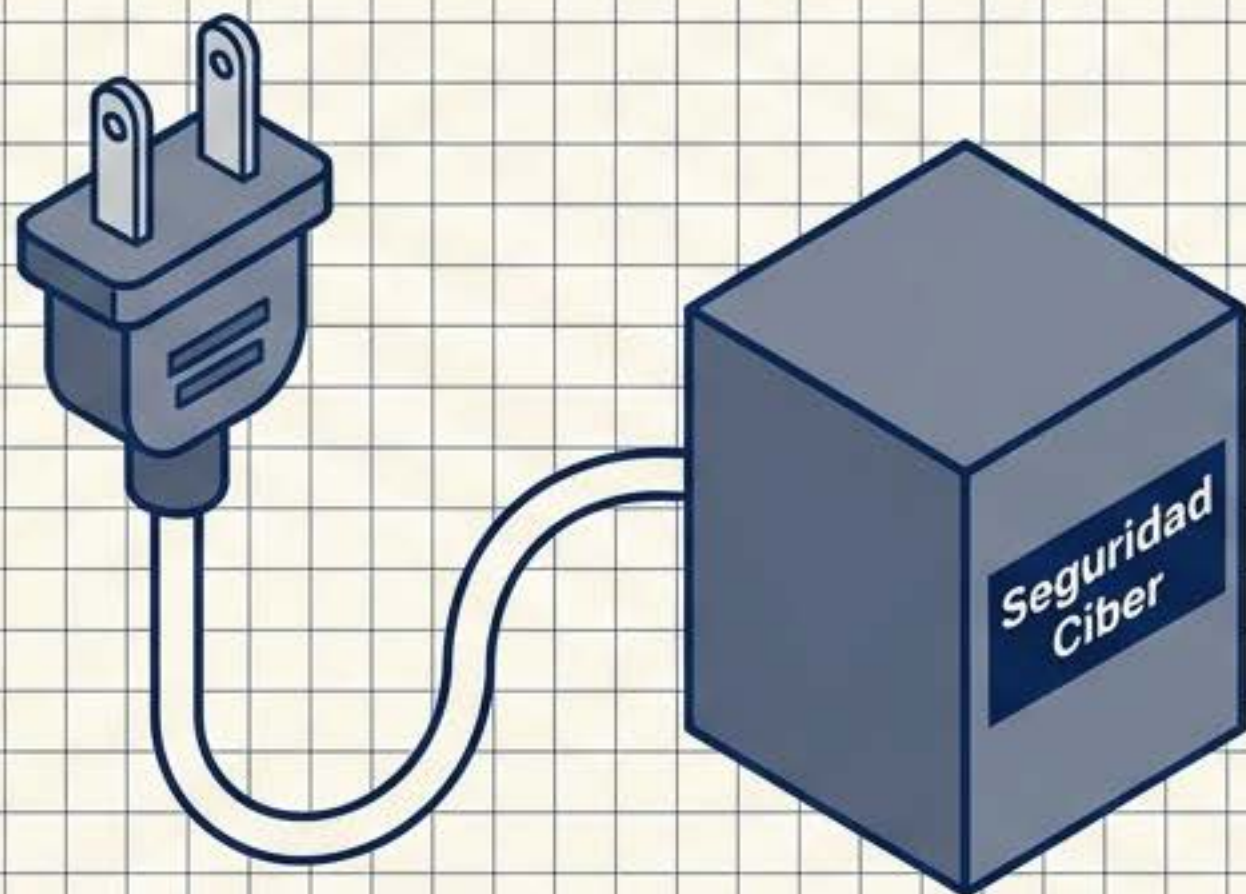
Controles técnicos mínimos para evitar el ridículo digital.



COMPONENTES ESTRUCTURALES	
 POLÍTICAS CLARAS	 POLÍTICAS CLARAS (Navy & Cyan)
 AUDITORÍAS REGULARES (Navy & Yellow)	 AUDITORÍAS REGULARES (Navy & Yellow)
 FORMACIÓN CONTINUA (Navy & Cyan)	 FORMACIÓN CONTINUA (Navy & Cyan)
 RECUPERACIÓN ANTE DESASTRES (Navy & Hazard Orange)	 RECUPERACIÓN ANTE DESASTRES (Navy & Hazard Orange)

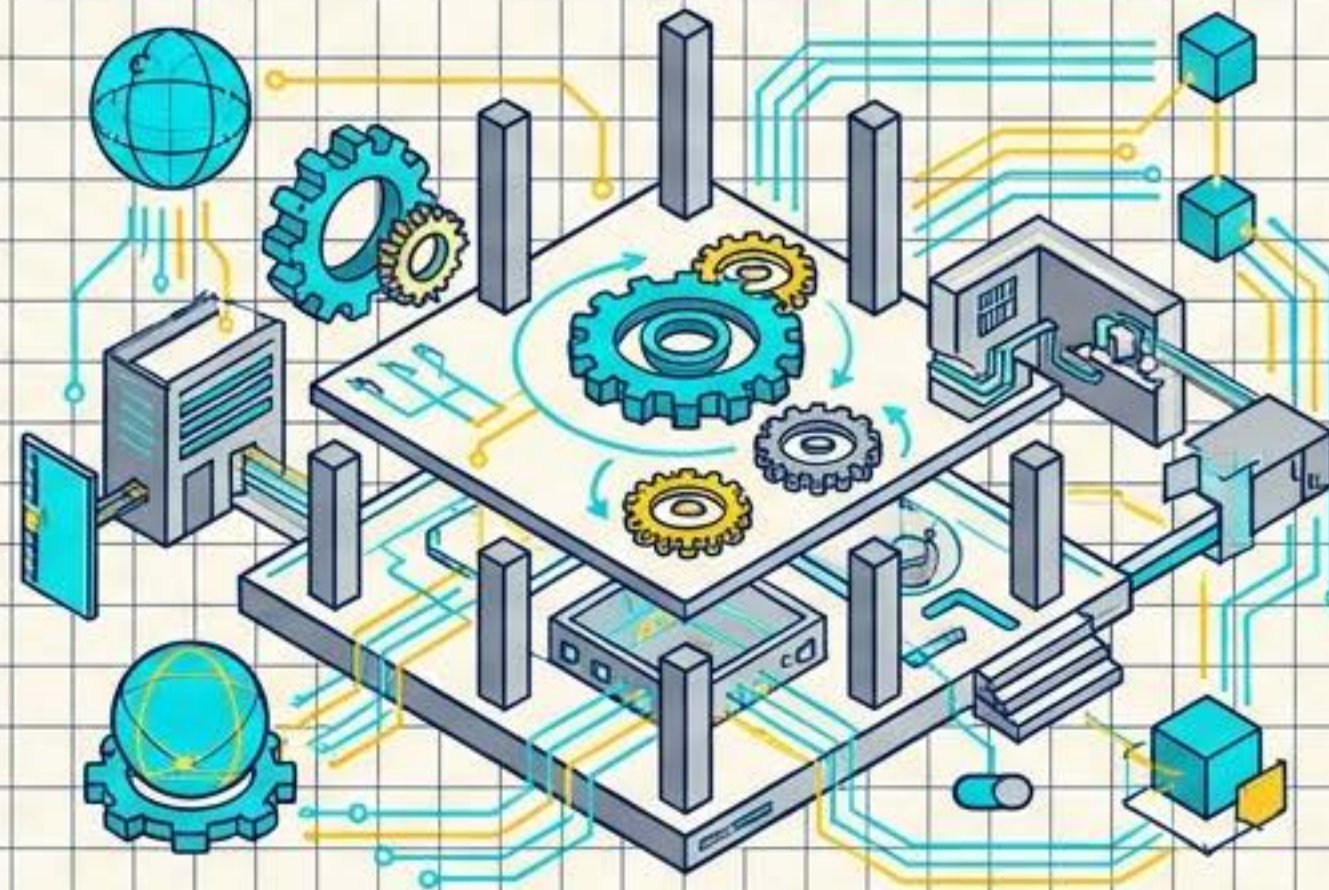
# La seguridad no es un electrodoméstico que se enchufa y se olvida.

## El Mito



Existe una fe casi religiosa: contratar un antivirus o pagar una suscripción en la nube y dar el problema por resuelto.

## La Realidad



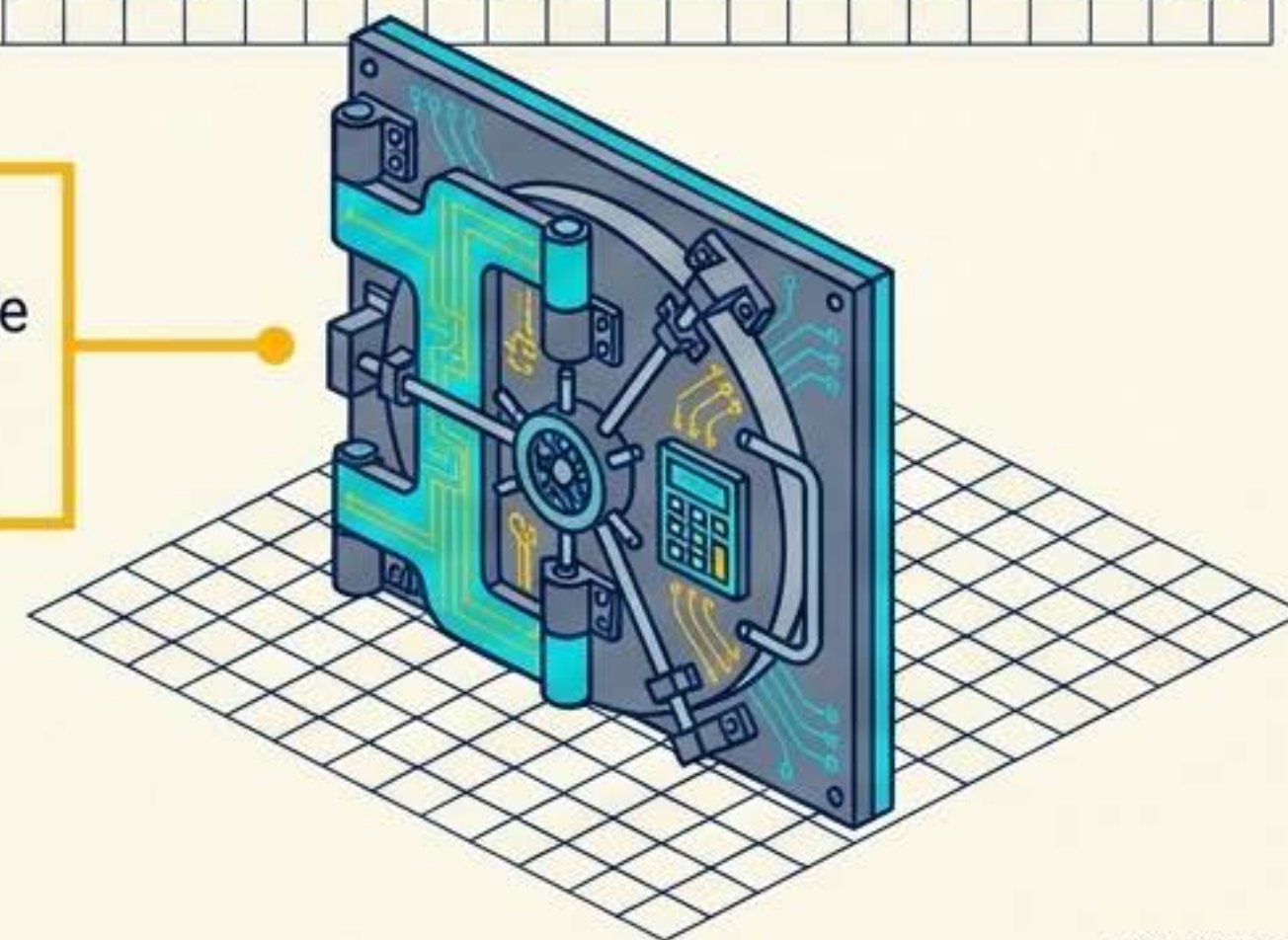
Comprar herramientas sin integrarlas son solo parches caros sobre un diseño que sigue siendo vulnerable.

# La tecnología no arregla lo que la organización no gobierna.



Los controles técnicos son imprescindibles, pero no funcionan en el vacío. Requieren que la organización ya haya "hecho los deberes" con el gobierno del dato.

Sin orden interno, la tecnología es una colección de soluciones mal configuradas o directamente ignoradas.



# El Plano de Seguridad: 4 Capas de Defensa.

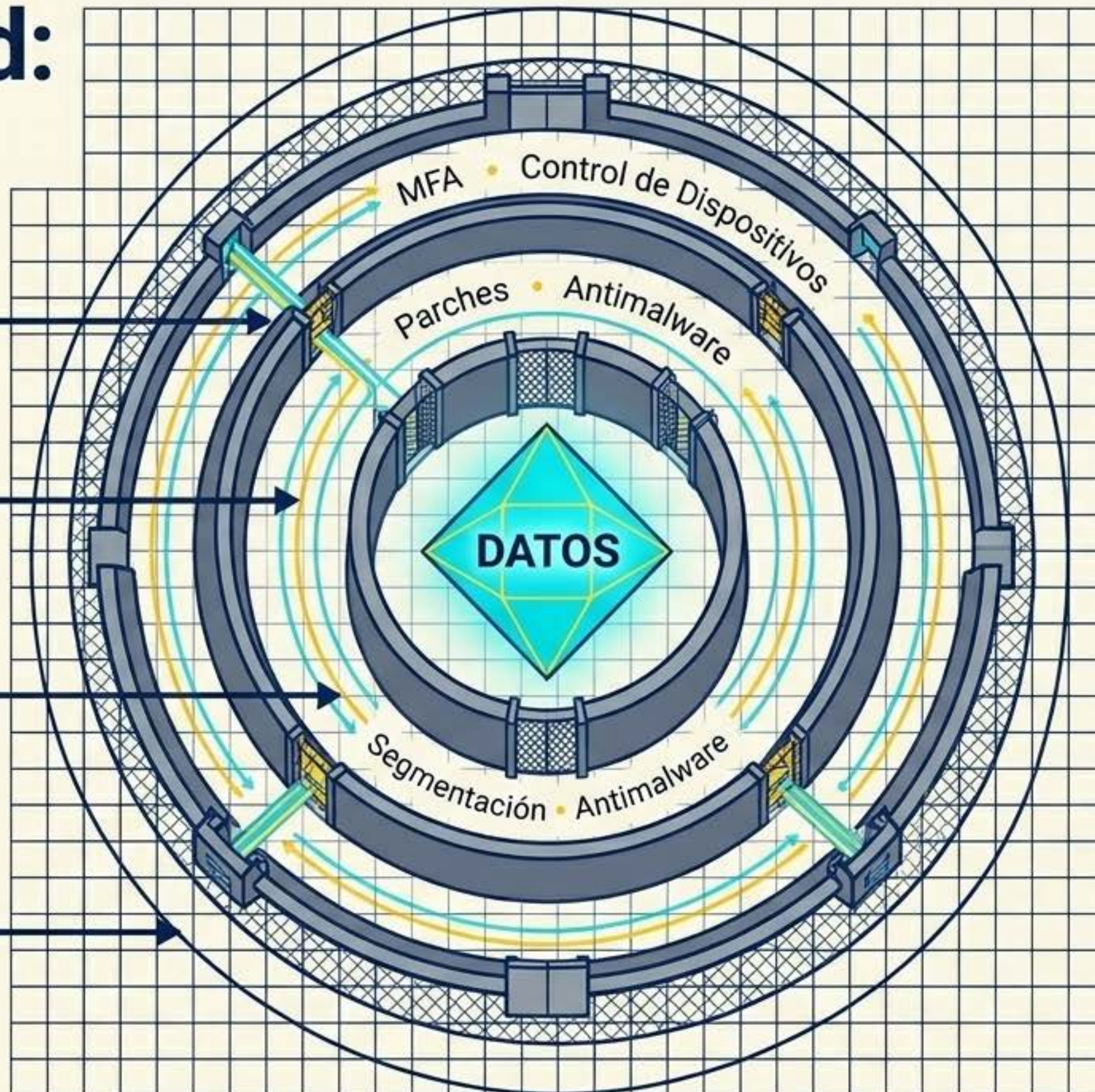
Una pequeña organización no necesita el arsenal de una gran corporación. Necesita aplicar con sentido común una serie de controles básicos organizados por capas.

**Capa 1: Perímetro y Accesos**

**Capa 2: Sistemas Operativos**

**Capa 3: Protección del Dato**  
Segmentación  
Cifrado

**Capa 4: Red de Seguridad**  
Monitorización  
Backups  
Respuesta a Incidentes

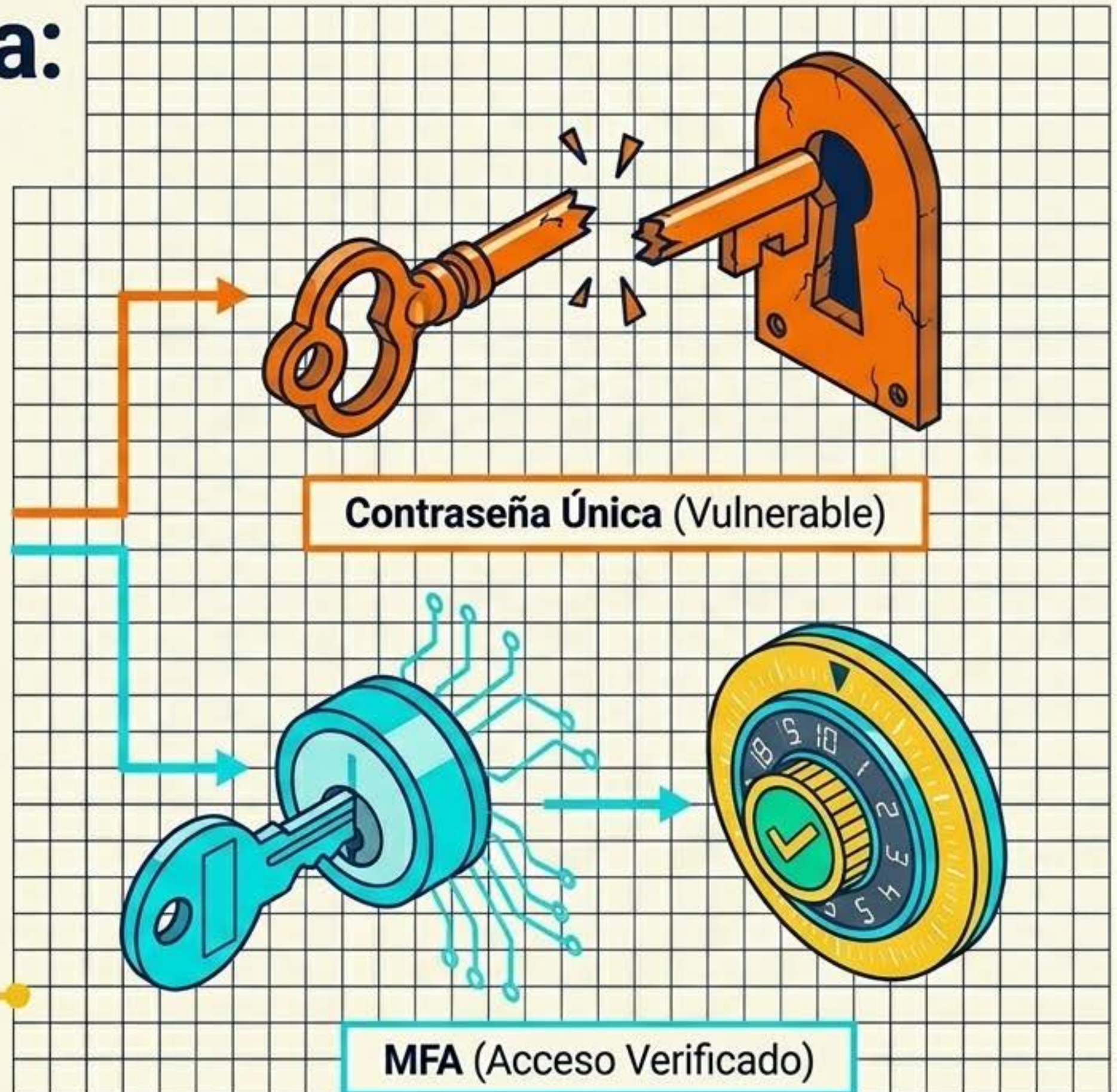


# Autenticación Robusta: La contraseña única ha caducado.

Seguimos usando contraseñas débiles, repetidas y compartidas. Es una contradicción peligrosa.

“  
La pregunta ya no es si  
alguna contraseña se  
filtrará, sino cuándo.”

La **Autenticación Multifactor (MFA)** es el estándar mínimo para reducir drásticamente el riesgo de accesos indebidos.

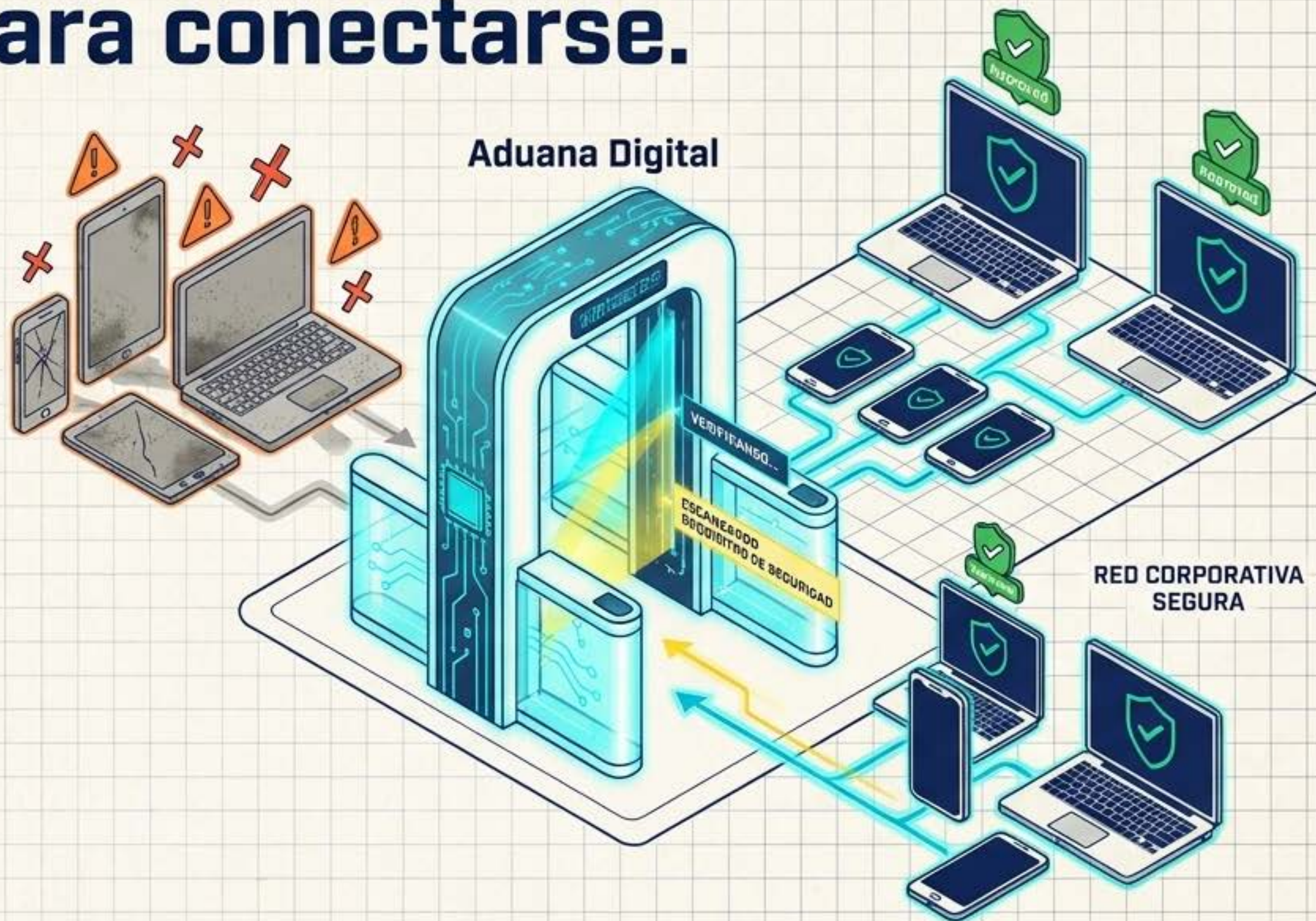


# Control de Dispositivos: No todo vale para conectarse.

El ecosistema de una organización suele ser una mezcla pintoresca de equipos corporativos y personales.

Debes establecer qué dispositivos están autorizados y sus requisitos mínimos.

La seguridad de un sistema es, en muchas ocasiones, tan fuerte como el dispositivo más débil que se conecta a él.



# Actualizaciones y Parches: El reloj corre en tu contra. todas.

Cuando las vulnerabilidades de un sistema o aplicación se hacen públicas, el tiempo de reacción lo es todo.



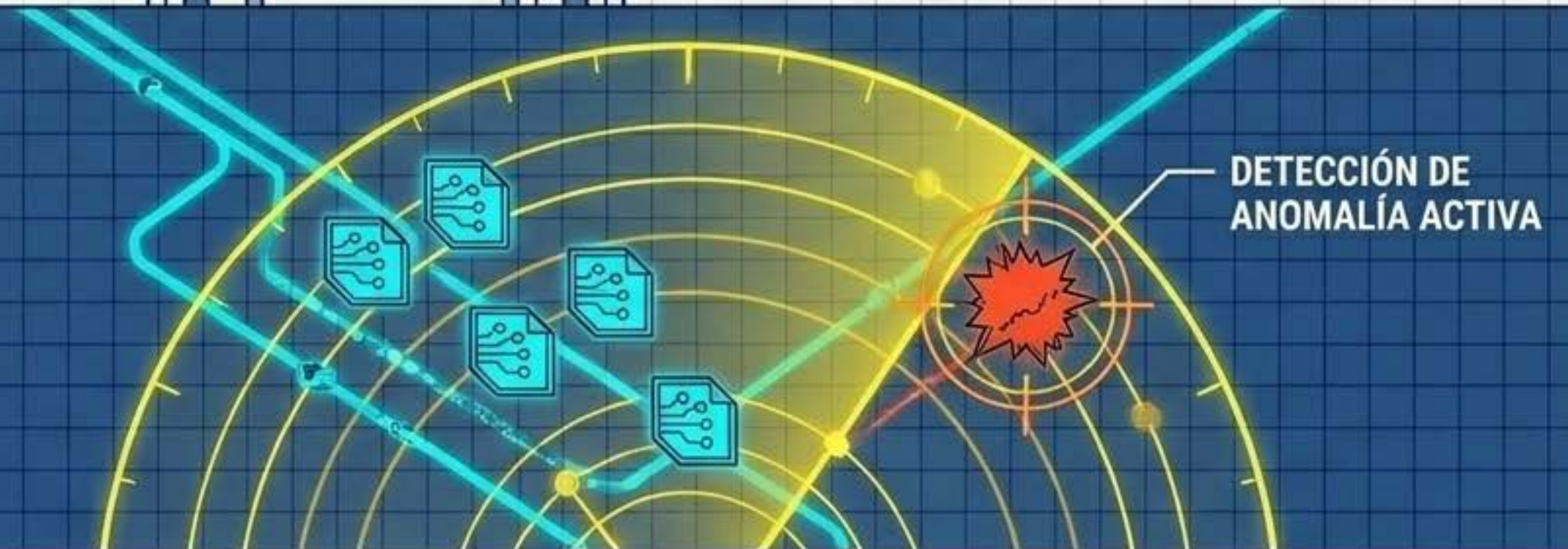
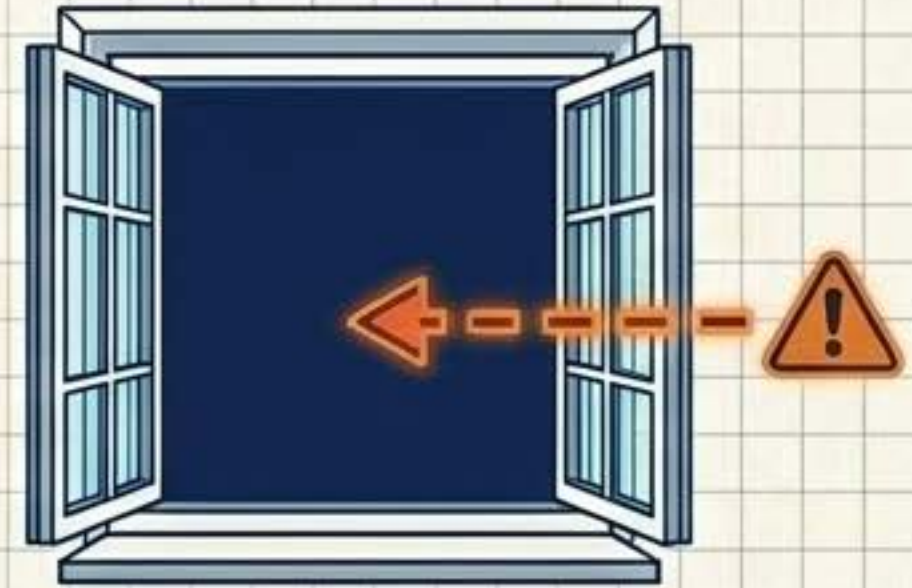
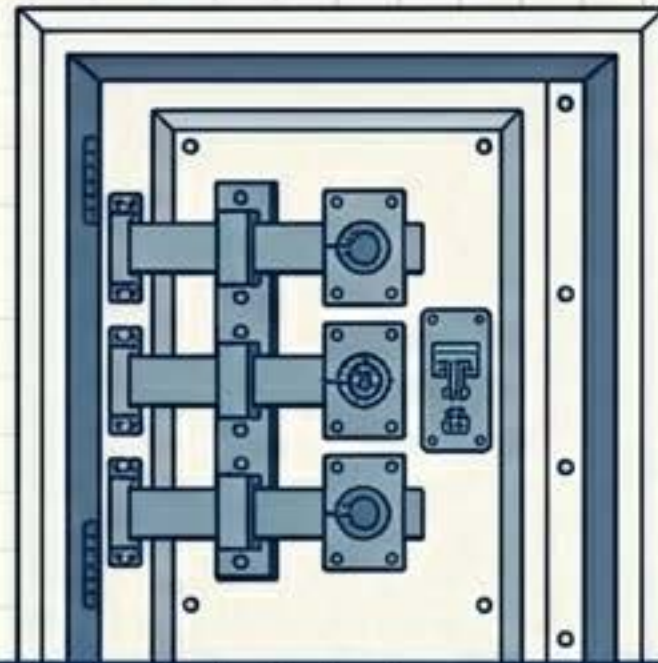
Retrasar actualizaciones por comodidad, miedo a que “algo deje de funcionar” o simple dejadez es una invitación abierta a que alguien aproveche esas debilidades antes de que sean corregidas.



# Protección Activa: Más allá del antivirus de serie.

Confiar exclusivamente en un antivirus tradicional es como proteger una casa con una cerradura mientras dejas la ventana abierta.

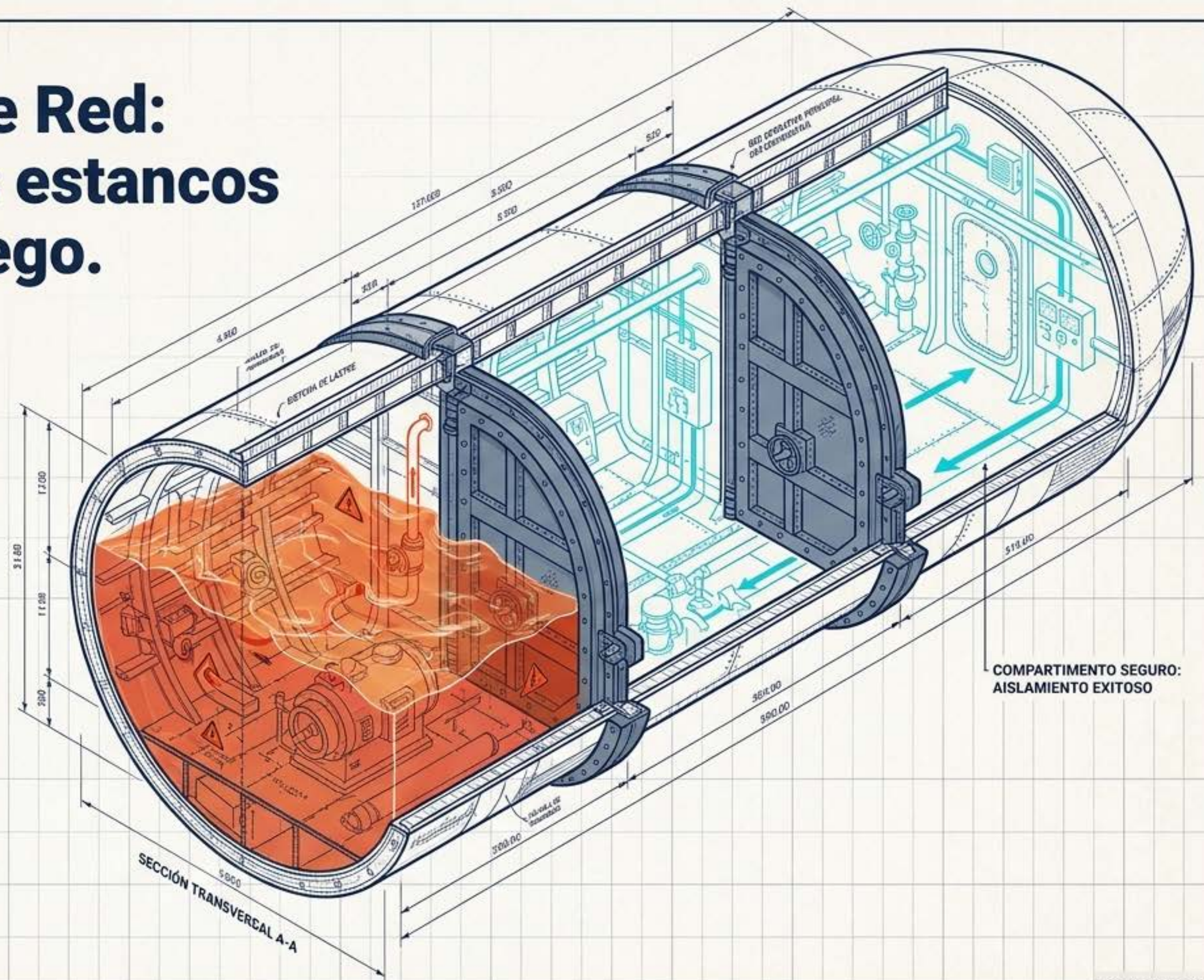
Las soluciones actuales requieren análisis de comportamiento en tiempo real y, sobre todo, configuración y mantenimiento. No sirve instalarlo y no volver a mirarlo nunca más.



# Segmentación de Red: Compartimentos estancos para frenar el fuego.

El error habitual es construir infraestructuras donde todo está conectado con todo, permitiendo que un equipo comprometido se mueva libremente.

**⚠ Limita el movimiento.**  
Separa entornos y restringe accesos para evitar que un problema local se convierta en un incendio generalizado.

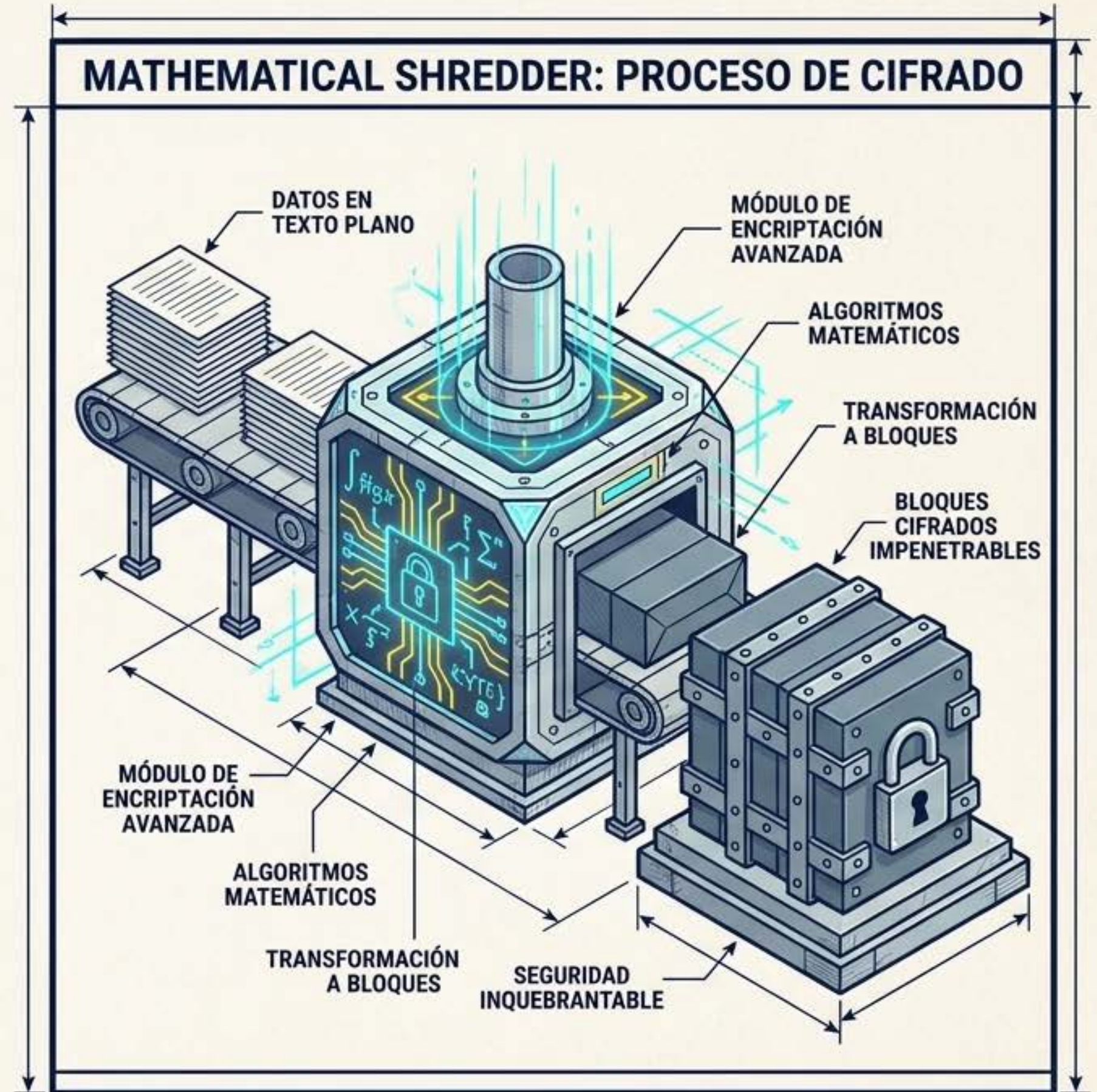


# Cifrado: Inutilizar el trofeo del atacante.

Cifrar discos, dispositivos y comunicaciones es una medida nativa en muchas soluciones.

No usarlo hoy en día es pura dejadez.

**“El cifrado es una forma elegante de decir: aunque consigas el dato, no podrás leerlo.”**



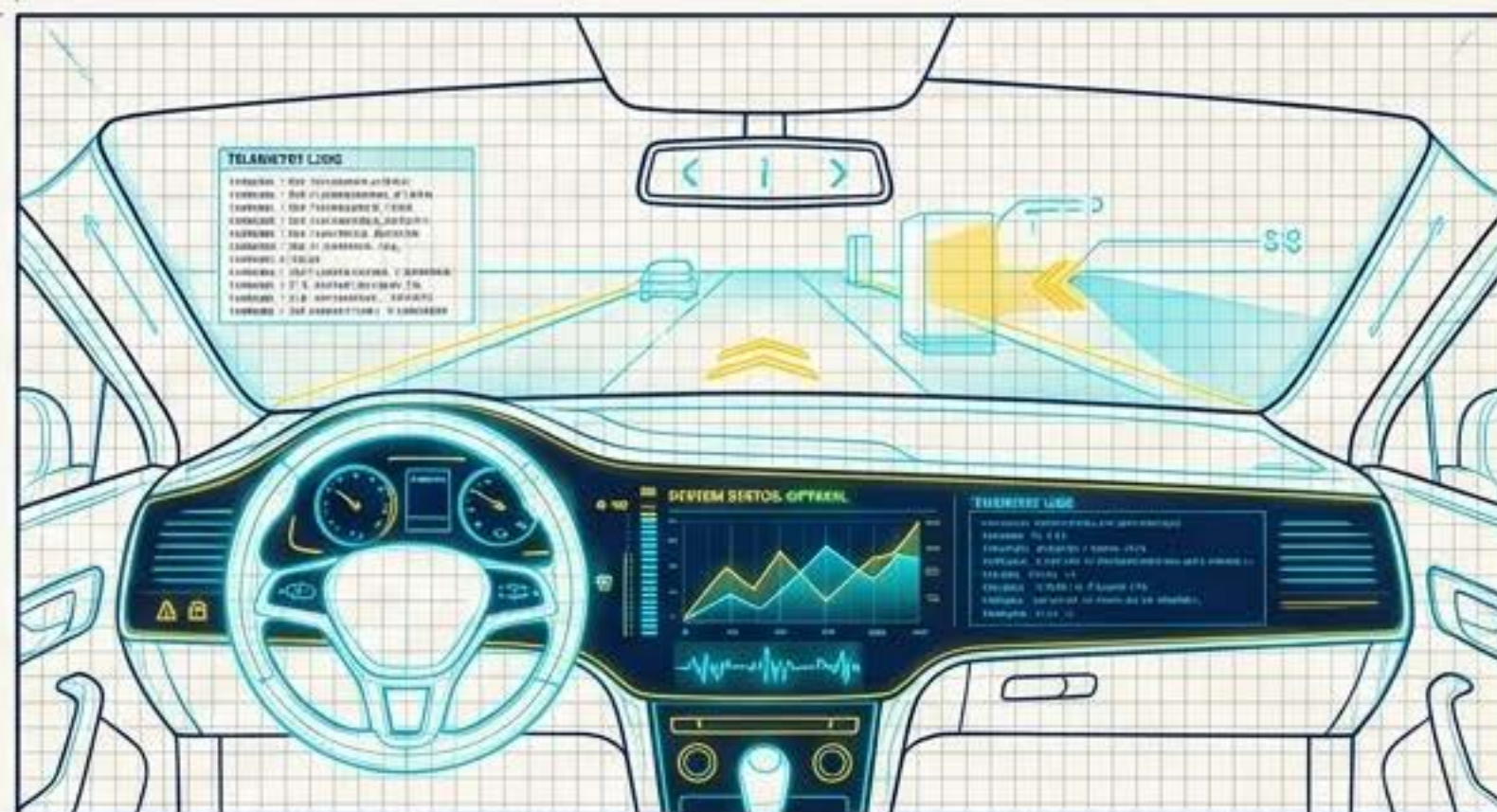
# Monitorización y Registros: Conducir con las luces encendidas.

El mayor problema no es sufrir incidentes, es no enterarse. Todo parece funcionar... hasta que deja de hacerlo.



**SIN VISIBILIDAD:** El peligro es invisible. No hay alerta de problemas.

Registrar actividad y revisar logs permite detectar comportamientos anómalos antes de que escalen. **Lo que no se ve, no se puede gestionar.**

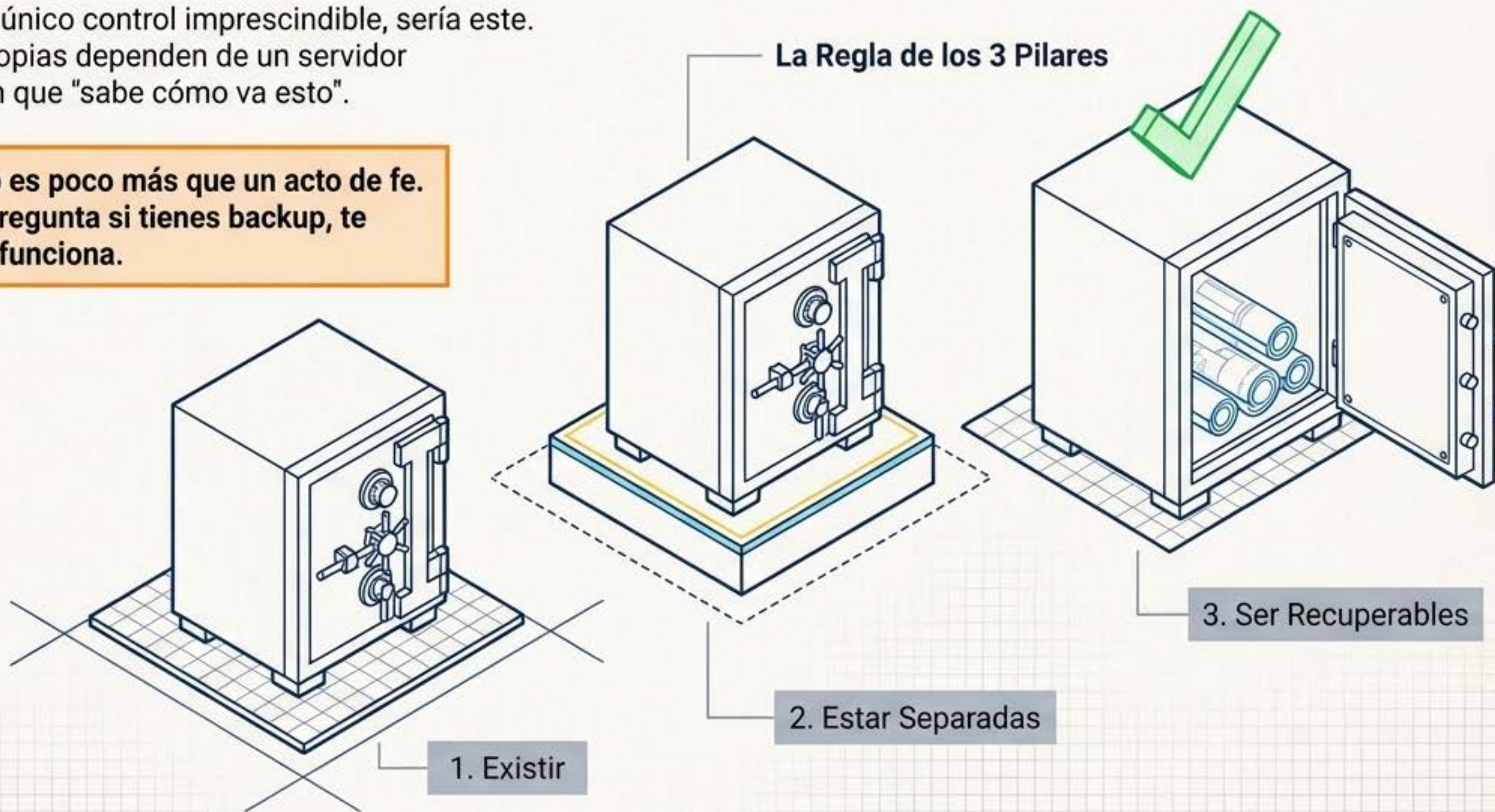


**CLARIDAD TOTAL:** Detección proactiva y gestión informada.

# Copias de Seguridad: El seguro de vida que nadie quiere usar.

Si hubiera que elegir un único control imprescindible, sería este. Sin embargo, muchas copias dependen de un servidor compartido o de alguien que "sabe cómo va esto".

Un backup no probado es poco más que un acto de fe. El ransomware no te pregunta si tienes backup, te obliga a comprobar si funciona.



# Respuesta a Incidentes: La certeza de la crisis.

Hay una certeza incómoda: en algún momento, algo fallará. Puede ser un ataque, un error humano o un fallo técnico. Ocurrirá.

**La diferencia entre el pánico y el control es tener un plan.** Improvisar en mitad de un incidente suele salir muy caro.



# El Factor Multiplicador: Inteligencia Artificial.

Las herramientas de IA prometen detectar amenazas y automatizar respuestas. Bien utilizadas, son valiosas. Mal implantadas, bloquean sistemas legítimos y generan una falsa sensación de seguridad.

“

“La tecnología no sustituye al criterio. Lo amplifica. Para bien o para mal.”



# Tu Matriz de Autodiagnóstico de 'Andar por Casa'.

Matriz de Controles		
Control	Estado de Riesgo (Común)	Objetivo Mínimo (Seguro)
Backups	En el mismo servidor	Separado y Probado
Autenticación	Contraseña única	MFA Activo
Parches	"Ya lo haré"	Inmediatos
Malware	Antivirus por defecto	Análisis en tiempo real
Segmentación	Todo conectado	Compartimentos estancos
Cifrado	Datos en claro	Cifrado por defecto
Monitorización	Ciegos	Logs y Alertas

**Mantén los controles, revísalos y no caigas en la tentación de pensar que "a nosotros no nos va a pasar". Porque siempre le pasa a alguien que pensaba exactamente lo mismo.**