

Teletrabajo Seguro: Protegiendo tu Oficina en Casa

Configuración de Router, Redes de
Invitados y VPN



LA OFICINA

La Brecha de Seguridad: Los atacantes buscan el eslabón débil

LA CASA



Un equipo te protege 24/7.



Eres tú y tu router.

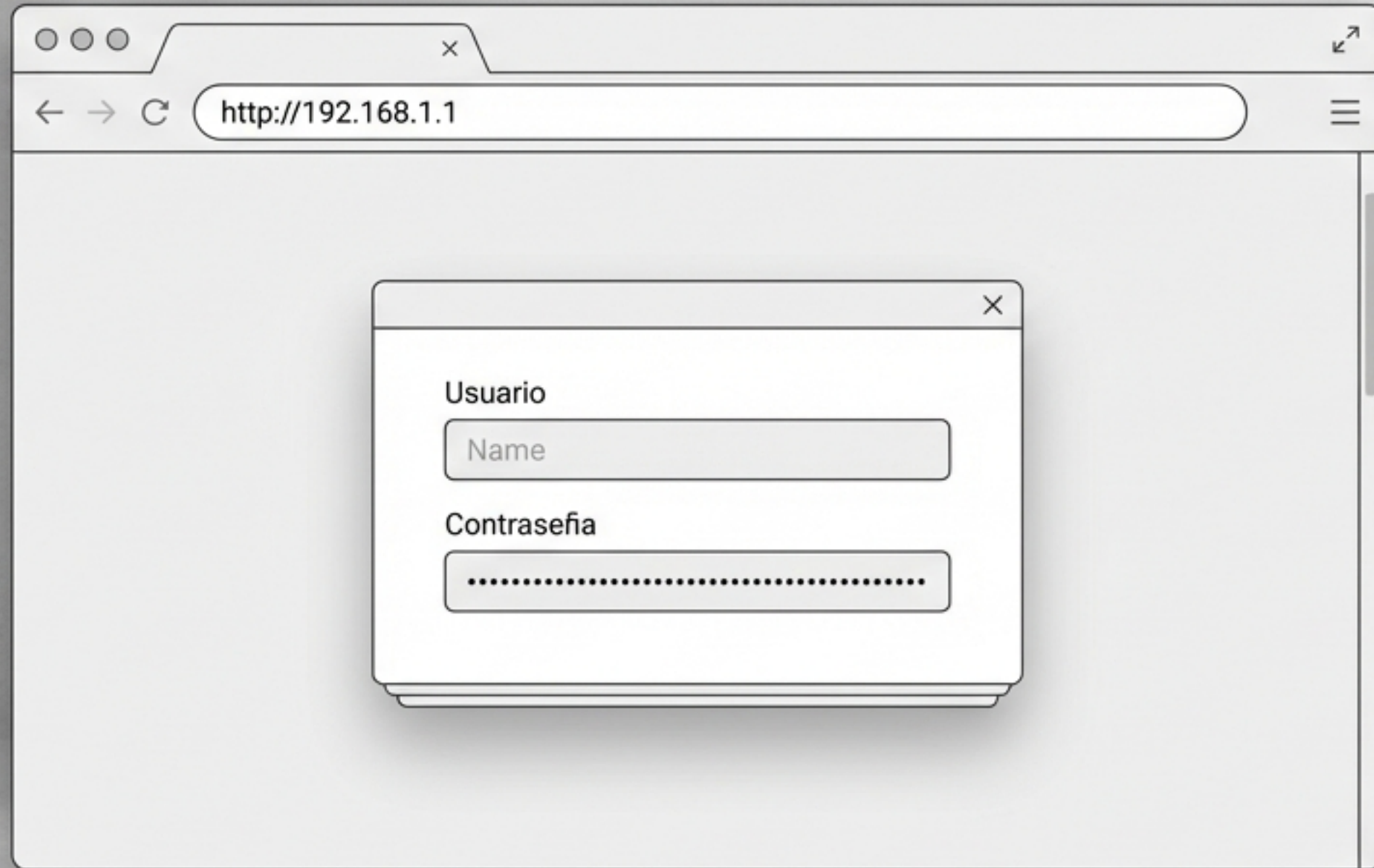
El Router: Tu Primera Línea de Defensa

La configuración de fábrica es una invitación abierta. Si entran a tu Wi-Fi, tienen acceso directo a tu computador de trabajo.

El primer paso no es técnico, es administrativo.



Manos a la Obra: Toma el Control



1 Accede a la IP de tu router.

2 Cambia la clave predeterminada.

3 Tip Pro: Usa una frase larga, no una palabra compleja.



Ocultando el Rastro (SSID)

- No regales información personal en el nombre de tu red.
- Evita apellidos o direcciones exactas.
- Regla de Oro: Sé genérico para no ser un blanco fácil.

El Candado Digital: Protocolos de Cifrado



WEP (Obsoleto)



WPA (Vulnerable)

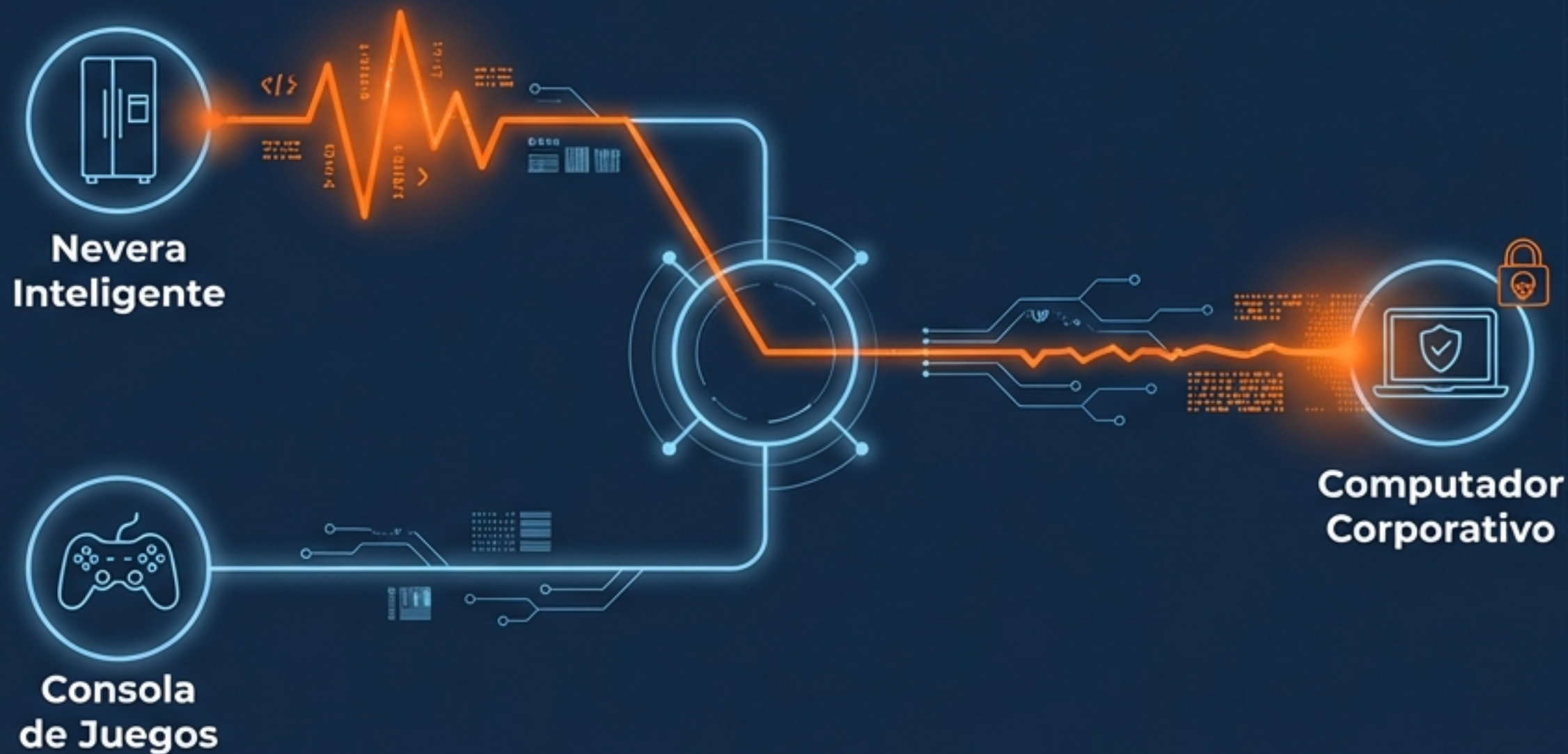


WPA2 / WPA3 (Seguro)

La fuerza de tu muro depende del protocolo. Selecciona WPA2 o WPA3 en tu configuración.

El Peligro de los Dispositivos Inteligentes

“Si tu nevera se resfría,
tu computador se contagia.”



Divide y Vencerás: Red de Invitados

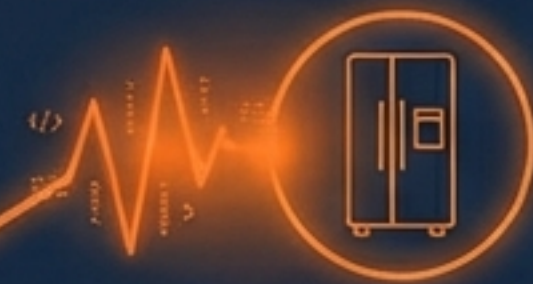
Aísala los dispositivos inseguros.
Activa "Guest Network" en tu router.

RED PRINCIPAL



Computador
Corporativo

RED DE INVITADOS



Nevera Inteligente



Consola



TV

Gestión de Visitas

La hospitalidad no debe comprometer la seguridad.

Nunca des la clave de tu red principal.

Los dispositivos desconocidos siempre van a la Red de Invitados.



El Túnel Seguro: VPN

Un túnel cifrado donde nadie puede ver lo que envías.

Internet Público (Inseguro)

¿Cuándo activar la VPN?



Redes Públicas

VPN **OBLIGATORIA**



En Casa

VPN **RECOMENDADA**

En cafeterías, es como gritar tus contraseñas si no la usas.
En casa, úsala para acceder a servidores de la empresa.



Firewall: **ACTIVO**



Sistema: **ACTUALIZADO HOY**

El Guardián Interno

Tu router protege la entrada; tu sistema operativo protege el interior. Instala los parches de seguridad el mismo día que salen.

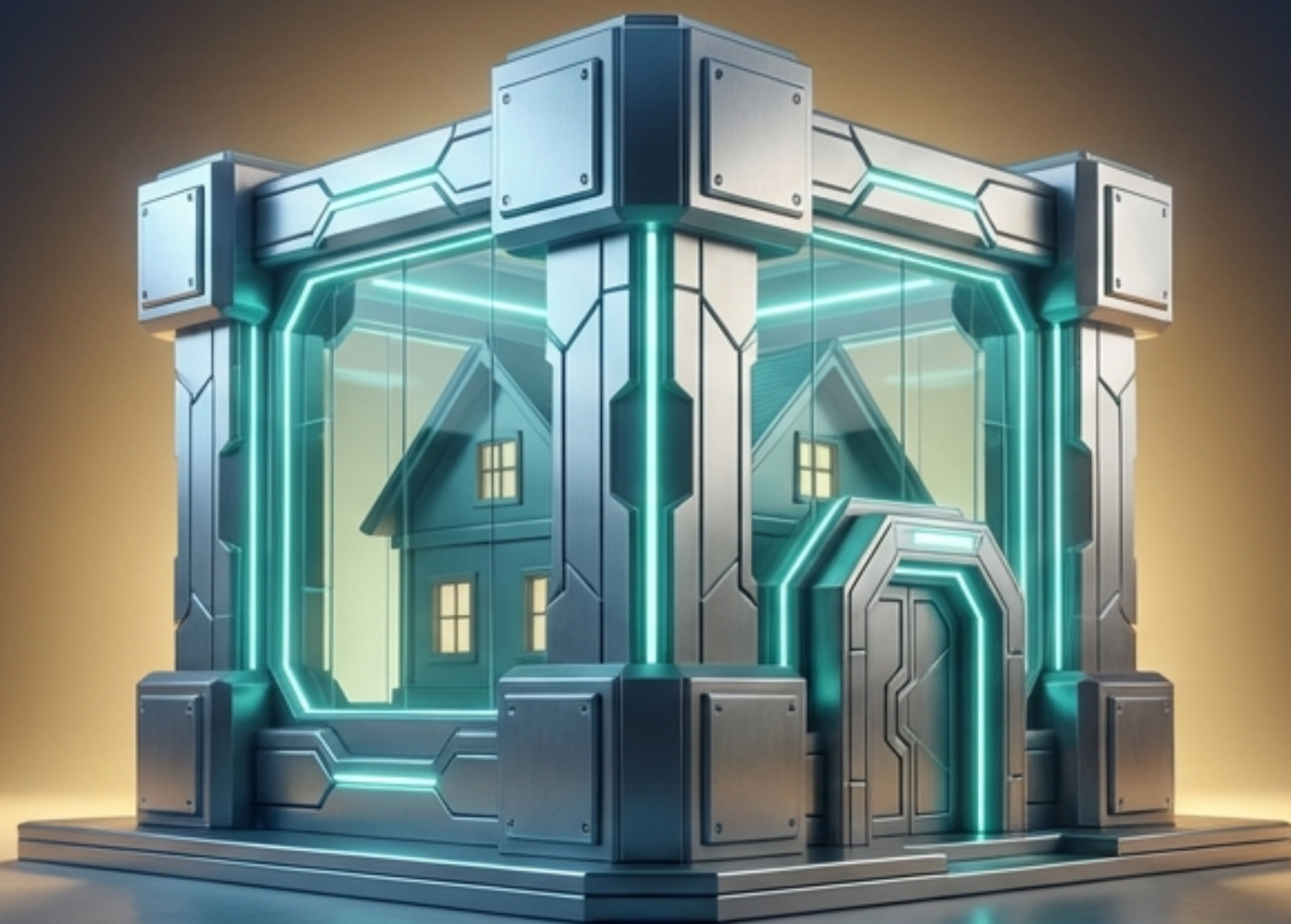
Protocolo de Emergencia

1. **Desconecta:** Quita el cable o apaga el Wi-Fi inmediatamente.
2. **No Apagues:** Deja el equipo encendido para análisis forense.
3. **Reporta:** Llama a Soporte TI. El tiempo es oro.



Resumen: Tu Fortaleza Digital

- Contraseña de administrador cambiada
- Nombre de red (SSID) genérico
- Cifrado WPA2/WPA3 activo
- Dispositivos personales en Red de Invitados
- VPN instalada y lista



Tu hogar es ahora tu fortaleza.
Manténla segura.