

OSINT

LIVE CONNECTIONS VIEWER

Qué te está diciendo el panel, qué significan los veredictos y qué hacer con cada uno — en palabras claras.

CÓMO FUNCIONA

MANUAL DEL USUARIO · OCTUBRE DE 2026

777 SOFTWARE GRATIS — Y GRATIS PARA SIEMPRE

1 — QUÉ ES OSINT

Cada programa de tu computadora que toca internet — tu navegador, tu correo, tus actualizaciones, tus juegos — mantiene conexiones: líneas vivas entre tu máquina y direcciones allá afuera, en internet. La mayoría de la gente nunca las ve. OSINT te las muestra, en vivo — cada conexión que tu computadora está manteniendo ahora mismo, en filas claras, actualizadas cada pocos segundos a medida que las conexiones van y vienen.

Ver las líneas es solo la mitad. Para cada dirección externa del panel, OSINT consulta listas públicas de seguridad y servicios de búsqueda — los mismos registros públicos que usa la gente de seguridad — y te da una respuesta clara: ¿esta conexión es conocida como segura, no tiene ningún informe negativo, es sospechosa, o es conocida como mala? Cada respuesta muestra su trabajo: qué dijo cada comprobación, y hace cuánto lo dijo.

Piénsalo como una ventana con un bibliotecario de referencia al lado. El bibliotecario busca las direcciones en libros públicos y te muestra las páginas. La decisión sigue siendo tuya.

OSINT es un visor y un asesor — nada más. Nunca bloquea una conexión, nunca cierra una, nunca cambia nada en tu computadora ni en tu red. No escanea, no hace ping ni sondea el otro extremo. Lee la lista de conexiones que tu computadora ya guarda, lee los registros públicos sobre las direcciones que contiene, y te cuenta lo que encontró. Si una conexión hay que detenerla, eso se hace cerrando el programa que la está haciendo — el §3 te dice, en palabras claras, cuándo vale la pena hacerlo.

OSINT se ejecuta en la máquina donde lo instalas, y muestra las conexiones de esa máquina — ábrelo en tu portátil y verás las líneas de tu portátil. Hay una sola ventana, un solo panel y un solo trabajo: ayudarte a tomar una buena decisión sobre si una conexión es segura.

2 — CÓMO LEER EL PANEL

El panel es una tabla. Cada fila es una conexión. Esto es lo que significa cada columna, de izquierda a derecha:

Columna	Qué significa, en palabras claras
STATE («Estado»)	Lo que la conexión está haciendo ahora mismo. ESTABLISHED significa que la línea está abierta y hablando. LISTEN significa que un programa está esperando a que alguien se conecte a él. TIME_WAIT y estados parecidos son una conexión que está terminando y cerrándose. Las filas UDP son un tipo de conexión que no tiene estado de «línea abierta» — eso es normal.
LOCAL	Tu extremo de la línea: la dirección de tu computadora y el número (puerto) que tu lado está usando. Este eres tú.
REMOTE («Remoto»)	El otro extremo de la línea: la dirección externa y el puerto con los que tu computadora está hablando. De este tratan las comprobaciones.
TAG («Etiqueta»)	Una etiqueta según reglas locales sencillas. LOCAL_LAN = una dirección de tu propia red doméstica. LOOPBACK = tu computadora hablando consigo misma. SAFE_... = un nombre que tú escribiste en tu propio archivo de etiquetas (viene vacío — una etiqueta SAFE_ solo existe si tú escribes una). EXTERNAL_NODE_... = todos los demás: un desconocido, con un código corto para que el mismo desconocido lleve la misma etiqueta siempre. Una etiqueta es tu etiqueta — nunca oculta una advertencia (§3).
HOST («Anfitrión»)	El nombre de la dirección remota, cuando hay uno publicado. Si no se encuentra ningún nombre, verás un simple —. OSINT nunca adivina un nombre.
VERDICT («Veredicto»)	La respuesta de seguro o no seguro para esa dirección, en palabras claras — el tema del §3. Las filas de tu propia red y las filas en escucha muestran —: las direcciones privadas nunca se envían a ninguna parte y nunca se juzgan, porque no hay ningún registro público con el que juzgarlas.

Los hábitos del panel

- **Respira.** El panel vuelve a leer tus conexiones cada 5 segundos, y el encabezado muestra la cuenta atrás hasta la próxima actualización. Aparecen conexiones nuevas; las cerradas desaparecen. *Refresh now* («Actualizar ahora») vuelve a leer al instante; *Pause* («Pausar») deja el panel quieto para que puedas leer.
- **El pie cuenta.** La línea de abajo te dice cuántas conexiones hay, cuántas son externas, cómo van las comprobaciones y qué edad tienen las listas de seguridad descargadas — para que la información vieja siempre lleve la etiqueta de vieja.
- **Los oyentes se sientan abajo, atenuados.** Son conexiones en espera — programas listos para aceptar una conexión — parte del panorama completo, apartados para no

estorbar.

- **En el orden estándar, el peligro flota.** El orden propio del panel pone primero KNOWN BAD («conocido como malo»), luego SUSPICIOUS («sospechoso»), luego las filas que aún se están comprobando, luego NO BAD REPORTS («sin informes negativos») y KNOWN SAFE («conocido como seguro») — las filas que merecen tus ojos los reciben primero. (El §5 muestra cómo reordenar el panel tú mismo.)

3 — LOS VEREDICTOS

Un veredicto es la lectura honesta más desfavorable de todo lo que dijeron las comprobaciones sobre una dirección — nunca un promedio, nunca una adivinanza. Hay cuatro veredictos y tres estados honestos de «no es un veredicto»:

Veredicto	Qué significa
✓ KNOWN SAFE («conocido como seguro»)	La dirección está identificada positivamente como un servicio conocido y legítimo — por ejemplo, está en un conjunto público de servicios conocidos como benignos — y no se encontró nada malo en ninguna comprobación. «Sin malas noticias» por sí solo nunca puede ganar esto; lo gana la identificación.
· NO BAD REPORTS («sin informes negativos»)	Las comprobaciones se ejecutaron, y ninguna de las listas públicas tiene nada malo que decir sobre esta dirección. Léelo tal como está escrito: significa que nadie la ha denunciado — no es una promesa de que sea segura. Aquí es donde cae la mayoría de las direcciones ordinarias.
■ SUSPICIOUS («sospechoso»)	Nadie ha demostrado que esta dirección sea mala, pero algo en ella no se ve bien: la gente la ha denunciado por mal comportamiento, uno o dos escáneres la marcan, se la ha visto escaneando internet, o expone fallos conocidos y nadie puede decir quién es. Vale la pena mirarla más de cerca — el panel de detalle (§4) muestra exactamente qué levantó la marca.
KNOWN BAD («conocido como malo»)	La dirección está en una lista pública de direcciones conocidas como malas — por ejemplo, una lista de servidores activos de control de botnets — o varias comprobaciones fuertes coinciden en que es maliciosa. Trata la conexión como peligrosa hasta que sepas exactamente por qué está ahí.
... CHECKING («comprobando»)	Las búsquedas de esta dirección aún se están ejecutando. El panel sigue actualizándose; la respuesta se completa debajo. Espera unos segundos.
NOT CHECKED («no comprobado»)	Aún no se ha ejecutado ninguna comprobación sobre esta dirección — acaba de aparecer, o se agotó una cuota gratuita. El panel dice cuál de las dos. Es una afirmación sobre las comprobaciones, no sobre la dirección.

Veredicto	Qué significa
LOOKUP FAILED («la búsqueda falló»)	Las comprobaciones no pudieron completarse — un servicio no respondió, o no hay conexión con la que preguntar. Esta dirección es desconocida, no aprobada. Si no tienes conexión, el panel dice OFFLINE — CACHED ONLY («sin conexión — solo caché») y cada veredicto viene de las listas descargadas y las búsquedas guardadas, con sus edades mostradas.

Qué hacer con cada uno

- **KNOWN BAD — detente y mira.** Si no sabes exactamente por qué tu computadora está hablando con esa dirección, cierra el programa que crees que hizo la conexión, ejecuta tu análisis antivirus normal, y no envíes nada sensible hasta que lo hayas aclarado. OSINT no puede bloquearla por ti — cerrar el programa es el bloqueo.
- **SUSPICIOUS — sin pánico, una mirada más cercana.** Abre el panel de detalle y lee qué levantó la marca. Si no reconoces qué estabas haciendo cuando apareció la conexión, cierra las apps que no estabas usando y observa si vuelve.
- **NO BAD REPORTS — nada que hacer.** Mantén la regla normal: si reconoces el servicio — tu navegador, tus actualizaciones, tu correo — esto es tráfico ordinario de internet.
- **KNOWN SAFE — nada que hacer.** Este es el tipo de conexión que tu computadora hace todo el día: DNS, actualizaciones, grandes servicios públicos.
- **CHECKING / NOT CHECKED / LOOKUP FAILED — aún no hay consejo, porque las comprobaciones no han terminado o no respondieron.** Una conexión desconocida no es una conexión mala. Mientras tanto, usa la sección WHO IS THIS? («¿QUIÉN ES ESTE?») del panel, y comprueba de nuevo cuando las búsquedas se completen.

Las reglas honestas, para que puedas exigirnos cuentas: ningún informe es una promesa — una comprobación limpia significa «nadie la ha denunciado», nunca «segura demostrada». Una búsqueda que falla dice FAILED («falló»), en voz alta; OSINT nunca suaviza un fallo hasta convertirlo en una respuesta limpia. Si dos comprobaciones no coinciden, el veredicto sigue la lectura peor y el panel muestra ambas afirmaciones. Y cada dato lleva su edad, para que siempre sepas qué tan fresca es una respuesta.

Una separación más que mantiene el panel: una etiqueta (§2) es tu propia etiqueta — «este lo conozco». Un veredicto es lo que dicen los registros públicos. Si una lista marca una dirección que tú etiquetaste SAFE_, la fila muestra ambas cosas, el veredicto primero. Una etiqueta nunca oculta una advertencia.

4 — CÓMO ELEGIR UNA CONEXIÓN

Haz clic en una fila del panel y se convierte en tu elección — resaltada en un verde oscuro que sigue siendo legible incluso cuando la ventana no tiene el foco. La elección es siempre exactamente una conexión, y sigue a la conexión, no a su lugar en la lista: las actualizaciones, los reordenamientos, el desplazamiento y las pausas nunca pueden deslizar el resaltado a una conexión distinta. Si tu conexión elegida se cierra, el panel lo dice en palabras claras — «This connection has closed — pick another row above» («Esta conexión se ha cerrado — elige otra fila arriba») — en lugar de mostrarte otra en silencio.

El panel de detalle Debajo del panel, el panel de detalle cuenta la historia de tu conexión elegida en tres secciones fijas:

- **WHO IS THIS? («¿QUIÉN ES ESTE?»)** — el nombre publicado (o un honesto «no hay nombre publicado»), la red propietaria de la dirección, aproximadamente dónde está, su país de registro (el país del papeleo — el panel dice claramente que esto no es prueba de ubicación), y cualquier etiqueta tuya que coincida.
- **WHAT THE CHECKS SAID («LO QUE DIJERON LAS COMPROBACIONES»)** — cada fuente, una línea por cada una: las listas de conocidos como malos, lo que la dirección expone, cada comprobación con clave que hayas activado — qué dijo, y cuándo se comprobó. Una fuente que falló lo dice en su propia línea.
- **WHAT SHOULD I DO? («¿QUÉ DEBO HACER?»)** — la orientación para este veredicto, en palabras claras (el §3 tiene los mismos textos).

El panel describe la dirección, no el programa que la usa — las comprobaciones saben de direcciones, y el panel nunca finge que saben más.

Los botones de comprobación Debajo del panel están los botones. Cada uno actúa solo sobre tu elección:

Botón	Qué hace
<i>Check with GreyNoise</i> («Comprobar con GreyNoise»)	Pregunta a GreyNoise por tu dirección elegida: ¿es ruido de fondo de internet — el escaneo que baña a todo el mundo — o algo más raro que eso? Funciona sin clave, dentro de una pequeña cuota diaria gratuita; cuando la cuota del día se agota, el panel lo dice en palabras claras y todas las demás comprobaciones siguen funcionando.
<i>Check with VirusTotal</i> («Comprobar con VirusTotal»)	Pide a docenas de escáneres de seguridad que voten sobre tu dirección elegida, y muestra el recuento a la vista. Necesita tu propia clave gratuita de VirusTotal (§6) — sin clave guardada, el panel te dice que está OFF («apagado») en lugar de fallar en silencio.
<i>Check with URLhaus</i> («Comprobar con URLhaus»)	Pregunta a URLhaus de abuse.ch: ¿ha servido este anfitrión enlaces de malware? Silencioso cuando no hay nada que decir; una línea de advertencia ■ cuando lo hay. Necesita tu propia Auth-Key gratuita de abuse.ch (§6).

Botón	Qué hace
<i>Copy IP</i> («Copiar IP»)	Copia la dirección de tu conexión elegida a tu portapapeles, para que puedas usarla en tus propias herramientas.

La regla sobre la que está construida toda la app: las comprobaciones se ejecutan solo sobre la conexión que has seleccionado de verdad — la misma que el panel de detalle está mostrando — y solo cuando haces clic en el botón propio de esa comprobación. Si no hay nada seleccionado, o tu elección se ha cerrado, no sale ninguna búsqueda; la app te dice que elijas primero una conexión. Las comprobaciones funcionan en conexiones externas — elige una fila de tu propia red doméstica y el panel responde: «Pick an outside connection first» («Elige primero una conexión externa»).

Dos excepciones honestas, ambas a la vista: AbuseIPDB no tiene botón — una vez que guardas su clave, se une a las comprobaciones por sí solo para las direcciones externas de tu panel, y su línea aparece en WHAT THE CHECKS SAID con las demás. Y *Settings* («Ajustes») lleva un interruptor opcional — *Auto-check SUSPICIOUS rows with GreyNoise* («Comprobar automáticamente las filas SUSPICIOUS con GreyNoise») — que está apagado a menos que tú lo enciendas; existe porque la cuota gratuita de GreyNoise es pequeña, y gastarla debe ser tu decisión. Esas son las únicas cosas que pueden pasar sin un clic, y ambas están bajo tu control.

5 — ORDENAR + FILTRAR: TU ORDEN, TU CORTE

Ordenar — haz clic en el nombre de una columna

- Haz clic en STATE, LOCAL, REMOTE, TAG, HOST o VERDICT en la parte superior del panel y todo el panel se reordena por esa columna. Una flecha en el nombre de la columna muestra qué columna manda y en qué dirección va. Haz clic en el mismo nombre otra vez para invertir la dirección.
- VERDICT ordena por peligro, no por alfabeto: el primer clic pone KNOWN BAD arriba, luego SUSPICIOUS, luego las clases que aún están trabajando (CHECKING... / LOOKUP FAILED / NOT CHECKED), luego NO BAD REPORTS, luego KNOWN SAFE. Las filas sin ningún veredicto — los sockets en escucha y tu propia red — se quedan siempre abajo: ningún veredicto no es un nivel de peligro.
- Las direcciones se ordenan por sus números reales, luego por puerto — así 9.9.9.9 va antes que 10.77.0.10, como cuentan las direcciones de verdad, no como se escriben.
- Tu orden sobrevive a las actualizaciones. Las conexiones nuevas se colocan en el orden que elegiste en lugar de derribarlo.

Filtrar — la fila FILTER («Filtro»)

- Elige un veredicto — por ejemplo SUSPICIOUS — y el panel muestra solo las filas que llevan ese veredicto.

- Escribe en el cuadro *Text* («Texto») y el panel muestra solo las filas cuyo HOST, dirección LOCAL, dirección REMOTE o TAG contenga tu texto. Las mayúsculas no importan.
- El contador dice la verdad: «showing X of Y» («mostrando X de Y»).
- *Clear* («Borrar») limpia el filtro. Tu orden se queda.

Un filtro cambia solo lo que VES. Cada conexión sigue comprobándose exactamente como antes; filtrar nunca envía nada a ninguna parte. Y si filtras fuera de la vista la conexión que habías elegido, el panel de detalle lo dice en palabras claras — «this connection is hidden by your filter right now — it is still the connection the check buttons will use» («esta conexión está oculta por tu filtro ahora mismo — sigue siendo la conexión que usarán los botones de comprobación»). Los botones nunca se desvían a una fila que no elegiste.

Ordenar y filtrar son solo para esta sesión: reinicia la app y el panel vuelve completo, en su orden estándar. Nada de eso se guarda, se envía ni se comparte.

6 — AJUSTES + CLAVES

El botón *Settings* («Ajustes») (barra inferior) abre la ventana de Ajustes. Contiene cuatro campos de clave opcionales, dos interruptores y un botón de caché — nada más. Una clave es una línea corta y secreta de texto que un servicio te da, gratis, para que la app pueda hacerle preguntas en tu nombre. Cada clave está apagada hasta que añades la tuya.

Clave (campo de Settings)	Qué activa
AbuseIPDB key («clave de AbuseIPDB»)	La mejor puntuación de «¿ha sido denunciada esta dirección por mal comportamiento?» — una puntuación de confianza de abuso sobre 100, con el número de informes. Una vez guardada, esta comprobación se ejecuta por sí sola (§4) — no hay botón.
VirusTotal key («clave de VirusTotal»)	El botón <i>Check with VirusTotal</i> : docenas de escáneres votan sobre una dirección. Un detalle honesto, en la propia advertencia de VirusTotal: cualquier dirección consultada a través de su API se añade al conjunto de datos de VirusTotal y queda accesible para su comunidad. La misma advertencia está en Settings, junto al campo.
abuse.ch Auth-Key («clave de autenticación de abuse.ch»)	El botón <i>Check with URLhaus</i> : ¿ha servido este anfitrión enlaces de malware?

Clave (campo de Settings)	Qué activa
GreyNoise key («clave de GreyNoise»)	GreyNoise funciona sin clave. Una clave solo eleva un poco la diminuta cuota gratuita (las claves gratuitas llegan a unas 50 consultas por semana). GreyNoise da claves a cuentas de correo laboral; una cuenta de correo personal no recibe ninguna — esa es su regla, y el botón sin clave es la respuesta del producto.

Cómo viven las claves, y los interruptores

- *Save Settings* («Guardar ajustes») guarda TODO — las cuatro claves y ambos interruptores, exactamente como los dejaste, de forma permanente, hasta que los cambies. Siguen ahí cuando abres la app de nuevo.
- Tus claves viven en un solo archivo en tu computadora solamente: `osint_settings.json`, junto al programa, bloqueado para que solo tu propia cuenta de usuario pueda leerlo (permisos 0600). El archivo nunca se sube, nunca se imprime en ningún registro, y nunca forma parte de ninguna descarga. Una clave se envía solo a su propio servicio, cuando ejecutas su comprobación.
- *Live lookups ON* («Búsquedas en vivo activadas») — apágalo y la app funciona en modo sin conexión: el panel sigue mostrando tus conexiones en vivo, y los veredictos vienen solo de las listas descargadas y las búsquedas guardadas, con sus edades mostradas.
- *Auto-check SUSPICIOUS rows with GreyNoise* («Comprobar automáticamente las filas SUSPICIOUS con GreyNoise») — apagado por defecto (§4). Enciéndelo solo si quieres que la app gaste por sí sola la pequeña cuota gratuita de GreyNoise, solo en filas sospechosas.
- *Clear Intel Cache* («Borrar la caché de inteligencia») (en la app) vacía de verdad las listas descargadas y las búsquedas guardadas; las próximas búsquedas simplemente traen copias frescas.
- Quitar una clave: borra su campo y pulsa *Save Settings*. Esa comprobación vuelve a apagarse. (GreyNoise simplemente vuelve a su cuota sin clave.)

Conseguir las claves, paso a paso: la guía complementaria OSINT — Getting Your Keys (OSINT-Getting-Your-Keys.pdf) viene con este programa y recorre cada registro gratuito — dónde ir, en qué enlace del correo hacer clic, dónde se muestra la clave, y cómo pegarla en los campos de arriba. Cada clave en ella es gratis; si una página alguna vez te pide una tarjeta, estás en el plan equivocado.

7 — PRIVACIDAD: TODA LA VERDAD

OSINT no tiene cuentas, ni telemetría, ni analíticas, ni comprobaciones de actualización, ni informes de fallos — y ningún servidor nuestro al que nada pueda llamar. No hay nada a lo

que registrarse con 777 Software, y nada sobre ti se recopila, porque no hay ningún sitio al que pueda ir.

Para dar un veredicto, la app sí pregunta a servicios externos sobre direcciones — las direcciones externas que ya están en tu panel. Pregunta por una dirección, nunca por ti. Aquí está la lista completa de lo que sale de tu computadora:

A dónde va	Qué se envía
Anfitriones de listas públicas de seguridad (Feodo Tracker + SSLBL de abuse.ch, el catálogo de fallos explotados de CISA)	Nada sobre tus conexiones. La app descarga las listas públicas enteras, como quien descarga un periódico. Esas comprobaciones ocurren después en tu propia máquina.
Shodan InternetDB · Team Cymru · ipapi.co	La dirección externa que se está comprobando — una vez, y luego la respuesta se guarda en tu máquina (un día para los dos primeros, una semana para la ubicación aproximada) en lugar de preguntar de nuevo.
GreyNoise · AbuseIPDB · VirusTotal · URLhaus	La dirección externa que se está comprobando — más tu propia clave para ese servicio, solo a ese servicio. GreyNoise, AbuseIPDB y VirusTotal/URLhaus se ejecutan solo como describen el §4 y el §6.
Tu resolver DNS normal	La dirección externa, para convertirla en un nombre (la columna HOST) y para buscar qué red es su propietaria.

- **Nunca se envía, a ninguna parte:** las direcciones de tu propia red, las direcciones propias de tu computadora, tu lista de conexiones como conjunto, qué programas tienes abiertos, tu archivo de etiquetas y tus propios nombres SAFE_, y tus claves (excepto a su propio servicio, por una conexión cifrada).
- **Todo lo que la app guarda, lo guarda en casa:** las listas descargadas, las respuestas de búsqueda guardadas, tus ajustes y claves — todo en archivos junto al programa, en tu máquina, tuyos. La caché de búsquedas tiene un límite de unos 10 MB.
- **Nada se pone en cola para enviarse después.** Desconéctate y la app sigue funcionando con lo que tiene guardado, honestamente etiquetado. Vuelve a conectarte y las búsquedas simplemente se reanudan para las direcciones que aún están en el panel.

8 — LOS LÍMITES, DICHOS CLARO

Una herramienta en la que puedes confiar te dice lo que no puede hacer. Aquí está la lista de OSINT, completa:

- **OSINT asesora; no protege.** No puede bloquear, cerrar ni ralentizar una conexión, y no es un cortafuegos, ni un antivirus, ni un sustituto de ninguno de los dos. Tu protección sigue siendo tu cortafuegos, tu antivirus y tu propio juicio — OSINT alimenta el juicio.
- **Un veredicto limpio no es una garantía.** NO BAD REPORTS significa que nadie ha denunciado la dirección — una dirección mala recién estrenada tampoco tiene informes todavía. KNOWN SAFE exige identificación positiva, e incluso eso es identificación, no una promesa sobre mañana.
- **Muestra conexiones, no culpables.** El panel muestra las líneas que tu computadora mantiene; no promete nombrar qué programa mantiene cada una, y una conexión que se abre y se cierra entre actualizaciones puede pasar sin ser vista — todo visor de conexiones comparte ese límite, y la actualización de 5 segundos mantiene la brecha pequeña.
- **Las comprobaciones conocen direcciones, no intenciones.** Los registros públicos describen qué se ha visto hacer a una dirección y quién es su propietario. No pueden decirte por qué tu programa se conectó a ella — esa parte te toca reconocerla a ti.
- **Los servicios gratuitos tienen límites gratuitos.** Las cuotas se agotan, los servicios se callan, las listas envejecen. Cuando pasa cualquiera de esas cosas, OSINT lo dice en palabras claras en lugar de disfrazar un hueco como una respuesta — pero el hueco es real mientras dura.

Ante la duda, desconecta primero y lee después. Si una conexión te preocupa y no puedes decir por qué está ahí: cierra el programa que crees que la hizo (o desconecta la máquina), y luego lee el panel con calma. Siempre puedes volver a conectarte. Leer es gratis; desdecir algo enviado, no.

Eso es todo. Un panel, veredictos honestos, comprobaciones que se disparan solo cuando tú lo dices, claves que viven en tu propia máquina, y límites dichos a la vista. Abre OSINT, mira con quién está hablando tu máquina, y decide con los ojos abiertos. Para eso está.

OSINT — Live Connections Viewer · 777 Software. Este manual viene con el programa, junto a OSINT — Getting Your Keys. Los servicios nombrados aquí los gestiona su propia gente; sus páginas pueden reorganizarse con el tiempo, pero la forma de esta app — un panel, respuestas honestas, nada llamando a casa — no cambia.