Prepara tu tienda online para los agentes de compras con IA

Ciudad de México, 25 de noviembre de 2026.— Los agentes personales de IA ya pueden navegar por sitios web, agregar productos al carrito y completar compras en nombre de los consumidores. Cuando un agente compara distintas tiendas, busca la misma información en cada una: **precio, disponibilidad, fecha de entrega, costo de envío y política de devoluciones**. Si no puede acceder a una tienda o encontrar estos datos, puede terminar recomendando otra opción.

Cloudflare creó una guía que reúne cinco pasos que se complementan entre sí: identificar qué agentes ya visitan el sitio, decidir cuáles tendrán acceso, publicar la información que necesitan para identificar los productos, revisar la puntuación de *Agent Readiness* y probar una compra de principio a fin. La mayoría de estos pasos requieren únicamente ajustes de configuración o actualizaciones de contenido, por lo que pueden realizarse incluso durante un periodo de *code freeze*.

1. Revisa qué agentes visitan tu tienda

Antes de hacer cualquier cambio en la configuración, es importante identificar qué agentes ya visitan la tienda, qué páginas consultan y en qué parte del proceso encuentran dificultades.

1. En **Security Analytics**, accede a **Bot analysis** y selecciona un agente personal. La vista mostrará únicamente la actividad de ese agente, incluidas las páginas que intenta consultar y los errores que encuentra.
2. Identifica los agentes que llegan a las páginas de productos, pero no logran avanzar hasta el carrito. Se trata de potenciales compradores que estaban cerca de realizar una compra, por lo que conviene revisar primero esas rutas.
3. En **Business Insights**, revisa la relación entre rastreo y referencia (*crawl-to-referral ratio*) de los agentes en páginas dirigidas a personas, como aquellas que dependen de publicidad. Una relación de 12:1 significa que se registran doce visitas de agentes por cada visita humana.

2. Decide qué agentes permitir

Un agente solo puede recomendar una tienda si tiene acceso a ella. Esto puede configurarse desde el panel de Cloudflare en **Security settings > AI Crawler and Agent access policies**.

Para decidir qué hacer con cada agente, conviene considerar tres preguntas:

- **¿El agente es quien dice ser?** Los agentes personales incluidos en la política forman parte del directorio de bots verificados de Cloudflare. Cloudflare recomienda seleccionar **Allow** para estos agentes. El tráfico que simplemente se identifica como un agente continúa sujeto a las protecciones contra bots.
- **¿Los clientes utilizan ese agente?** Los datos del paso 1 permiten identificar qué agentes visitan el sitio y cuántas solicitudes realiza cada uno.
- **¿Qué hace dentro del sitio?** Un agente que consulta páginas de productos y avanza hasta el proceso de pago se comporta como un comprador. Si visita principalmente páginas que dependen de publicidad, puede seleccionarse **Block on pages with ads** en lugar de **Block**.

Para facilitar que los agentes encuentren los productos, se puede permitir el acceso de agentes de búsqueda al sitio para que los índices de búsqueda de IA puedan consultar el catálogo. Si se requiere mayor control, es posible crear una regla personalizada que permita a los agentes personales navegar por el catálogo, pero restrinja su acceso a secciones como la configuración de cuentas.

Si existen dudas sobre un agente, una opción es permitir temporalmente su acceso y observar su comportamiento en **Security Analytics** antes de modificar la política.

Revisa qué protecciones siguen activas aunque un agente tenga acceso

- **Turnstile:** los agentes personales son clientes automatizados, por lo que no pueden superar la validación de Turnstile. En aquellas páginas donde se quiera permitir su acceso, Turnstile no debe mostrarse para estos agentes. Consulta Conditionally enforce Turnstile.
- **Reglas personalizadas:** una regla diseñada para bloquear o desafiar el tráfico automatizado —por ejemplo, una basada en la puntuación de bots— seguirá aplicándose aunque el agente esté permitido. Por ello, conviene revisar las reglas correspondientes en **Security > Security rules > Custom rules** y agregar una excepción para estos agentes cuando sea necesario.

3. Publica la información de los productos en texto

Un agente necesita poder leer la información para utilizarla durante una compra. Por ello, los datos que normalmente consulta un comprador deben aparecer como texto en la página del producto, uno por línea:

- Precio
- Disponibilidad
- Fecha de entrega
- Costo de envío
- Periodo de devolución
- Si aplica un código promocional

Por ejemplo, una fecha límite de envío que aparece únicamente dentro de la imagen de un banner puede pasar desapercibida para el agente. También es importante comprobar que el precio mostrado en la página coincida con el que aparece en el carrito, ya que cualquier diferencia puede impedir que se complete la compra.

La misma información debe incluirse también en Schema.org Product JSON-LD dentro de una etiqueta `<script>`. Esta información no es visible para los compradores, por lo que complementa el texto de la página en lugar de sustituirlo.

```
<script type="application/ld+json">
  {
    "@context": "https://schema.org",
    "@type": "Product",
    "name": "Navy Wool Scarf",
    "sku": "SCARF-NVY-01",
```

```
    "offers": {
      "@type": "Offer",
      "priceCurrency": "USD",
      "price": "48.00",
      "availability": "https://schema.org/InStock"
    }
  }
</script>
```

Cuando cambien el precio o la disponibilidad de un producto, el JSON-LD debe actualizarse al mismo tiempo para evitar que el agente encuentre información contradictoria. Para incluir datos sobre envíos y devoluciones, pueden agregarse las propiedades `shippingDetails` y `hasMerchantReturnPolicy` al mismo bloque `offers`.

4. Revisa la puntuación de Agent Readiness

En el panel de Cloudflare, accede a **Agent Readiness** y realiza un diagnóstico del dominio de la tienda. El análisis revisa el sitio de forma similar a como lo haría un agente y muestra qué tan preparado está para este tipo de interacciones.

Las recomendaciones se agrupan según el nivel de esfuerzo que requieren. Entre los ajustes más sencillos se encuentran contar con un mapa del sitio (*sitemap*), establecer reglas para rastreadores de IA en `robots.txt` y habilitar Markdown for Agents, que puede activarse directamente desde el panel. Cuando **Markdown for Agents** está habilitado, los agentes que solicitan contenido en formato Markdown reciben una versión limpia y en texto de las páginas.

5. Prueba una compra con un agente

Los datos analíticos permiten identificar en qué punto se detienen los agentes; realizar una compra de prueba ayuda a entender por qué. Para hacerlo, se puede pedir a un agente personal que compre un producto en la tienda de la misma manera que lo haría un cliente. Por ejemplo:

> Compra dos bufandas de lana azul marino de example.com para regalar. Utiliza el código HOLIDAY20 y agrega envoltura para regalo. Antes de pagar, comprueba que llegarán antes del 20 de diciembre y que podrán devolverse en enero.

Durante el proceso, conviene revisar:

- ¿El agente selecciona el color y la cantidad correctos?
- ¿Encuentra la opción de envoltura para regalo?
- ¿Aplica correctamente el código promocional?
- ¿Puede confirmar la fecha de entrega y el periodo de devolución antes de pagar?
- ¿Se queda atascado en alguna ventana emergente que no puede cerrar?

Los problemas que puedan resolverse rápidamente pueden corregirse antes de la temporada alta, mientras que aquellos que requieran cambios más amplios pueden registrarse para atenderse posteriormente.

Identifica al comprador detrás del agente

Cuando un agente personal llega a un sitio es porque una persona le pidió realizar una compra. Con **Account Abuse Protection**, es posible identificar qué agentes personales actúan en nombre de un usuario específico y determinar si esa actividad coincide con el comportamiento habitual de la cuenta.

Si la actividad de un usuario parece sospechosa, se pueden tomar medidas sobre esa cuenta sin necesidad de bloquear al mismo agente para el resto de los usuarios.

Para saber más sobre la interacción con agentes de IA, puedes consultar el siguiente contenido relacionado:

- AI Crawl Control
- Bot analytics
- Verified bots
- Markdown for Agents

xxx

Acerca de Cloudflare

Cloudflare, Inc. (NYSE: NET) es la empresa líder en conectividad cloud. Ayuda a las organizaciones a aumentar la velocidad y mejorar la seguridad de sus empleados, aplicaciones y redes en todas partes, al tiempo que reduce la complejidad y los costos. La conectividad cloud de Cloudflare ofrece la plataforma más completa y unificada de productos nativos en la nube y herramientas para desarrolladores, de manera que cualquier organización pueda obtener el control que necesita para trabajar, desarrollar y acelerar su negocio.

Cloudflare, que utiliza una de las redes más grandes e interconectadas del mundo, bloquea por día miles de millones de amenazas en línea para sus clientes. Millones de organizaciones confían en Cloudflare, desde las marcas más importantes, emprendedores y pequeñas empresas hasta organizaciones sin fines de lucro, grupos humanitarios y gobiernos de todo el mundo.Si deseas obtener más información sobre la conectividad cloud de Cloudflare, visita cloudflare.com/connectivity-cloud. Para conocer las nuevas tendencias y perspectivas de Internet, consulta https://radar.cloudflare.com.

Síguenos en: Blog | X | LinkedIn | Facebook | Instagram