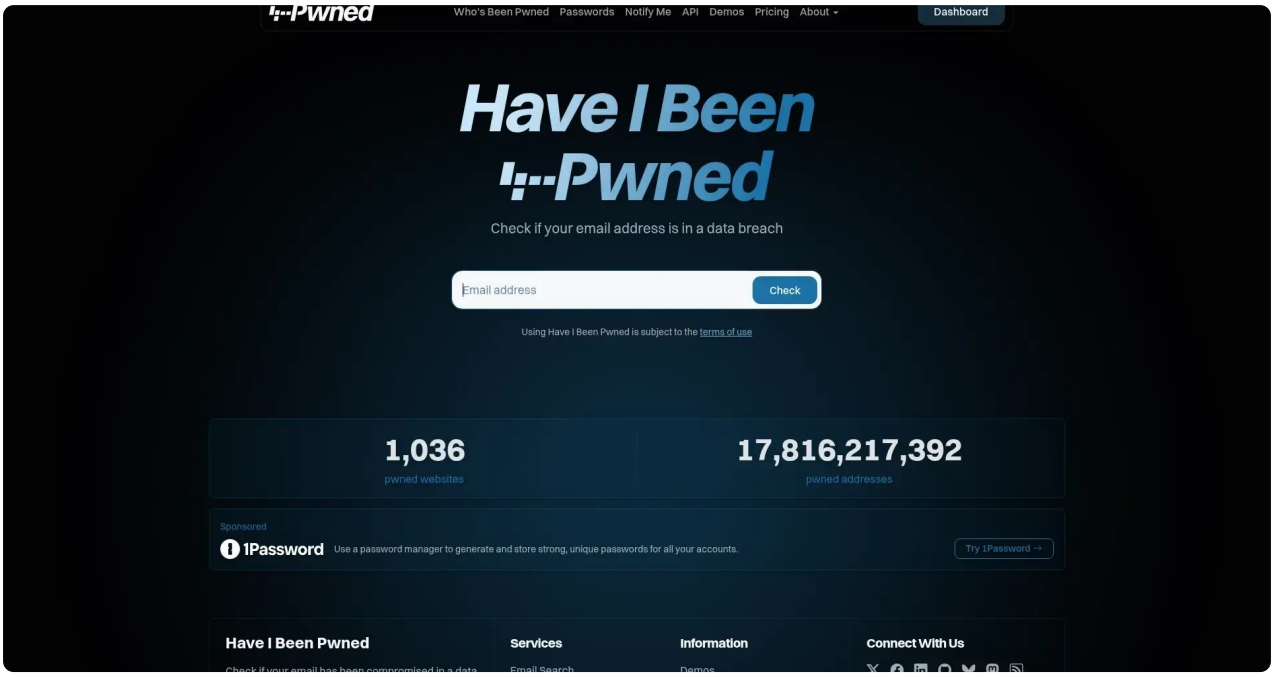

Have I Been Pwned

Plataforma líder en ciberseguridad para la detección de brechas de datos y compromiso de credenciales. Permite a CISO, administradores de sistemas y desarrolladores monitorizar dominios corporativos y correos electrónicos filtrados en la Dark Web. Su API de contraseñas mediante K-Anonimato facilita a los equipos de IT y Compliance la validación segura de cuentas, mitigando riesgos de suplantación de identidad y ataques de fuerza bruta en entornos profesionales altamente exigentes.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
Have I Been Pwned (HIBP) es el estándar de la industria para la verificación de brechas de seguridad y compromiso de credenciales. Es una plataforma dirigida fundamentalmente a responsables de ciberseguridad (CISO), administradores de sistemas, desarrolladores y analistas de riesgos que necesitan monitorizar si los activos digitales de su empresa (correos corporativos o dominios) han sido filtrados en la Dark Web o en incidentes de seguridad públicos y privados. En el ámbito profesional, es una herramienta crítica para departamentos de IT y Compliance que buscan mitigar riesgos de ataques de fuerza bruta o suplantación de identidad.

Principal ventaja profesional
En mi opinión profesional tras testear su integración, la razón definitiva para elegir HIBP es su **API de contraseñas mediante K-Anonimato**. Permite verificar si una contraseña ha sido filtrada sin enviar jamás la contraseña real al servidor, lo que garantiza la privacidad absoluta del usuario mientras se cumple con normativas estrictas de seguridad. Es la base de datos más actualizada y fiable del mundo en este segmento.

Para quién no es
No es una herramienta para usuarios o empresas que busquen una solución de seguridad "activa" o un antivirus. Aquellos profesionales que esperen que la herramienta limpie los datos o elimine la información de internet se verán frustrados, ya que HIBP es puramente informativa y reactiva. Tampoco es apta para organizaciones que no tengan capacidad técnica mínima para interpretar logs de seguridad o integrar APIs, a menos que solo usen la interfaz web básica.

Funcionalidades clave
- **Domain Search:** Permite realizar búsquedas masivas de todas las cuentas de correo vinculadas a un dominio corporativo específico que hayan sido comprometidas.
- **Pwned Passwords API:** Verificación de contraseñas filtradas mediante hashes SHA-1 truncados (k-anonymity), ideal para validar contraseñas en el momento de la creación de cuenta en aplicaciones propias.
- **Stealer Log Search:** Detección de credenciales filtradas a través de malware tipo "stealer" (logs de troyanos), una de las amenazas más crecientes en 2025-2026.
- **Notificaciones proactivas:** Servicio de alerta inmediata mediante webhooks o email en cuanto el sistema detecta una nueva brecha que afecta a los dominios configurados.
- **Verificación de "Pastes":** Escaneo de sitios como Pastebin donde los atacantes suelen publicar volcados de datos rápidos.

Precios
- **Versión gratuita:** La búsqueda manual en la web es gratuita para individuos. La API de contraseñas (Pwned Passwords) es de uso libre y gratuito sin necesidad de suscripción.
- **Rango de precios:** Desde los 4,39 USD/mes hasta más de 1.150 USD/mes, dependiendo del volumen de consultas y dominios.
- **Versiones de pago:**
- **Core:** Enfocada a PYMES y profesionales independientes (limite de RPM bajo y hasta 20 dominios).
- **Pro:** Para MSPs (Proveedores de Servicios Gestionados) y empresas medianas, permitiendo monitorizar hasta 800 dominios y acceso a K-anonymity para emails.
- **High RPM:** Diseñada para grandes corporaciones que requieren una integración profunda en sus sistemas con alta tasa de peticiones por minuto.

Perfil del usuario
- Empresas de servicios tecnológicos, sector financiero y departamentos de Seguridad de la Información (Infosec).
- Administradores de Sistemas y DevOps.
- Desarrolladores de Software (para validación de contraseñas en el registro).
- Analistas de SOC (Security Operations Center).

Nivel técnico requerido
- **Nivel técnico de uso:** Bajo para consultas web; Medio/Alto para gestión de suscripciones y dominios.
- **Nivel técnico de instalación:** Alto. Requiere conocimientos de desarrollo de software para la integración

de la API (REST, manejo de headers JSON y autenticación por clave).
- **Necesidades de soporte:** Soporte de desarrollo para la automatización y equipo legal para la gestión de las brechas detectadas.

Ejemplos de uso profesional
- **Auditoría de Directorio Activo:** Comprobar periódicamente si los correos de los empleados están en brechas conocidas para forzar cambios de contraseña preventivos.
- **Prevención de Fraude:** Integrar la API de contraseñas en el flujo de registro de un e-commerce para impedir que los clientes usen contraseñas que ya circulan por la Dark Web.
- **Protección de Marca:** Monitorizar dominios corporativos para detectar fugas de información antes de que los datos sean explotados masivamente.

Uso y distribución
- **Versión web:** Portal principal para consultas rápidas y gestión de cuenta.
- **CLI:** Existen múltiples herramientas de terceros en GitHub que permiten usar HIBP desde la línea de comandos.
- **Integraciones:** Amplia comunidad con wrappers en Python, .NET, Node.js y plugins para gestores de contraseñas como 1Password o Bitwarden.
- **API propia:** API RESTful V3 con autenticación mediante clave API.

Integraciones
- **Facilidad de integración:** Full code (requiere programación).
- **API propia:** Dispone de una API REST extremadamente robusta con documentación técnica detallada.
- **Ejemplos de integración:** Integración nativa en navegadores (Firefox Monitor utiliza sus datos) y en la mayoría de gestores de contraseñas líderes del mercado.

Notas finales
Veredicto técnico
Es una herramienta de **utilidad crítica y obligatoria** para cualquier profesional responsable de la seguridad de una organización. La relación coste-beneficio de los planes Core y Pro es inmejorable dada la calidad y exclusividad de los datos que maneja Troy Hunt (su creador). Al probarlo he verificado que la velocidad de respuesta de la API es excelente incluso en los niveles de entrada. Como profesional valoro especialmente el rigor con el que se trata la privacidad, evitando almacenar datos sensibles innecesarios.

Información legal, licencias y contratos
- El uso de los datos de la API está sujeto a una licencia Creative Commons Attribution 4.0 International, lo que obliga a citar a HIBP como fuente.
- Los términos de uso actualizados a marzo de 2026 prohíben explícitamente el uso de sus datos para crear bases de datos competitivas o realizar "scraping" masivo no autorizado.

Otros
- La plataforma ha introducido recientemente el filtrado por "Stealer Logs", lo cual es vital hoy en día ya que muchas brechas no vienen de ataques a servidores, sino de infecciones en los ordenadores de los propios empleados.

Fuentes consultadas:
- https://haveibeenpwned.com
- https://haveibeenpwned.com/API/v3
- https://haveibeenpwned.com/Subscription
- https://haveibeenpwned.com/TermsOfUse
- https://support.haveibeenpwned.com

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
Según mi experiencia, Have I Been Pwned (HIBP) ha dejado de ser una curiosidad para usuarios finales y se ha convertido en una infraestructura crítica para cualquier empresa que gestione identidades digitales. Es ideal para organizaciones con un enfoque preventivo en ciberseguridad, desde startups tecnológicas hasta grandes corporaciones financieras. Lo que más me gusta es que permite pasar de una postura reactiva (esperar a que te hackeen) a una proactiva, detectando fugas en terceros que afectan a tus propios activos. En mi opinión profesional, el presupuesto necesario es insignificante en comparación con el coste de mitigar un ataque de Account Takeover (ATO); por menos de 50 USD al mes, una PYME puede tener monitorizado todo su dominio corporativo. El punto clave aquí no es solo saber que te han filtrado, sino la rapidez con la que obligas a una rotación de credenciales tras la alerta.

Madurez digital requerida
- **Usuarios y equipo:** El equipo de TI o Seguridad debe estar familiarizado con la gestión de riesgos y el manejo de incidentes. No basta con recibir la alerta; el equipo debe saber cómo actuar ante un positivo (reset de contraseñas, auditoría de logs, comunicación interna).
- **Empresa y departamentos:** Requiere una cultura de ciberseguridad donde el departamento legal y de cumplimiento (Compliance) esté alineado con el técnico, especialmente para cumplir con notificaciones obligatorias de brechas de seguridad bajo normativas como RGPD.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- **Tiempos estimados de despliegue:** La configuración básica de monitorización de dominios es inmediata (minutos), mientras que la integración de la API en flujos de registro puede llevar de 2 a 5 días de desarrollo y pruebas.
- **Evaluación inicial:** Identificar todos los dominios y subdominios de la empresa. Verificar la propiedad de los mismos mediante registros TXT de DNS o archivos de control, paso indispensable para acceder a las búsquedas masivas de Domain Search.
- **Configuración y prueba de concepto:** Suscripción al nivel adecuado según el volumen de empleados. Implementación de la API de contraseñas (Pwned Passwords) en el portal de cambio de contraseña del empleado o en el registro de clientes usando el modelo de K-anonimato.
- **Integración y Piloto:** Conectar las alertas mediante Webhooks a herramientas de comunicación interna como Slack o Microsoft Teams, o directamente a un SIEM para que el SOC reciba los incidentes en tiempo real.
- **Seguimiento:** Revisión mensual de informes de exposición y ajuste de políticas de complejidad de contraseñas basadas en los hallazgos.

Necesidades de formación del equipo
Es vital formar al personal de Helpdesk y Soporte Técnico para que entiendan qué significa un "hit" en HIBP. Deben saber explicar al usuario final que su contraseña ha sido filtrada en un sitio externo y no necesariamente que la empresa ha sido hackeada, evitando alarmismos innecesarios pero garantizando la acción correctiva.

Perfiles necesarios
- **Perfiles técnicos necesarios:** Administrador de Sistemas/Redes (para validación DNS) y Desarrollador Backend (para integración de API REST).
- **Personal externo recomendado:** No suele ser necesario, salvo que se requiera un consultor de ciberseguridad para diseñar el plan de respuesta ante incidentes derivado de las filtraciones encontradas.

Retorno de la inversión (ROI)
- **Tiempos:** El ROI es casi instantáneo en términos de prevención de riesgos. Detectar una filtración de un directivo en las primeras horas puede ahorrar semanas de trabajo forense tras una intrusión.
- **KPIs:** Reducción del número de cuentas comprometidas detectadas en auditorías externas, disminución del éxito de ataques de Credential Stuffing y tiempo de respuesta desde la publicación de una brecha hasta el cambio de contraseña del usuario afectado.

Otros
Al usarlo te das cuenta de que la nueva funcionalidad de **Stealer Logs** es el verdadero cambio de juego para

2025. Mi experiencia en implantaciones me lleva a pensar que muchas empresas ignoran que el riesgo ya no está solo en grandes brechas de bases de datos, sino en el malware que roba las "cookies de sesión" y contraseñas guardadas en el navegador de los empleados. HIBP es actualmente la forma más eficiente y económica de monitorizar este vector específico de ataque sin recurrir a servicios de inteligencia de amenazas de miles de dólares.

TUTORIAL BÁSICO

Instalación (solo si procede)
Para utilizar la tecnología de Have I Been Pwned (HIBP) a nivel profesional o de desarrollo, no se instala un software tradicional, sino que se integra su API V3.
- **Obtención de la API Key:** Es necesario adquirir una suscripción en el sitio oficial para obtener una clave hexadecimal de 32 caracteres.
- **Configuración de Cabeceras:** Todas las solicitudes deben incluir obligatoriamente las cabeceras hibp-api-key (tu clave) y user-agent (el nombre de tu aplicación). Sin esta última, el servidor devolverá un error 403.
- **Checklist de inicio:**
- Verificar que las peticiones se realicen exclusivamente a través de **HTTPS** (TLS 1.2 o superior).
- Asegurar que los parámetros de búsqueda (como el email) estén correctamente **URL-encoded**.
- Configurar un sistema de almacenamiento seguro para la API Key (variables de entorno o gestores de secretos), nunca hardcodearla en el código fuente.

Uso en el día a día
- **Gestión de límites (Rate Limiting):** Según mi experiencia, es fundamental implementar una lógica de reintento. Si recibes un código HTTP 429, la API te responderá con una cabecera retry-after que indica los segundos exactos que debes esperar antes de volver a intentar la petición.
- **Optimización de respuesta:** Por defecto, la API solo devuelve el nombre de la brecha. En mi opinión profesional, esto es preferible para el uso diario ya que reduce el peso de la respuesta en un 98%, agilizando el procesamiento si solo necesitas saber si una cuenta está comprometida.
- **Seguridad en el cliente:** Al usar la API en aplicaciones web, te das cuenta de que no debes hacer las llamadas directamente desde el frontend (JavaScript del navegador), ya que expondrías tu clave de pago a cualquier usuario. Lo correcto es crear un proxy en tu backend que gestione la comunicación con HIBP.

Trucos de experto
- **K-Anonymity para contraseñas:** Para verificar contraseñas de forma 100% privada, utiliza el modelo de k-anonimidad. Solo debes enviar los primeros 5 caracteres del hash SHA-1 de la contraseña. HIBP te devolverá una lista de sufijos coincidentes y tú realizas la comparación final localmente. Esto garantiza que el servicio nunca conozca la contraseña que estás consultando.
- **Cuentas de prueba:** Para testing sin consumir créditos reales de búsqueda, puedes utilizar el dominio hibp-integration-tests.com con las claves de prueba proporcionadas en la documentación oficial.
- **Uso de Cloudflare Workers:** Mi experiencia me lleva a pensar que usar Workers de Cloudflare es la forma más eficiente de crear un proxy para la API. Permite añadir una capa extra de caché y control de tráfico antes de llegar a los límites de tu suscripción de HIBP.

Posibles problemas/incidencias
- **Error 403 (Forbidden):** Suele ocurrir por la falta de la cabecera user-agent. Es un error muy común en las primeras integraciones.
- **Redirecciones 301:** Si intentas conectar por HTTP, el servicio te redirigirá a HTTPS, lo que puede causar fallos en scripts automatizados que no manejen redirecciones automáticamente.
- **Incompatibilidad de protocolos:** El servicio ya no soporta versiones antiguas de TLS (1.0 y 1.1). Asegúrate de que tu entorno de ejecución (Node.js, Python, PHP, etc.) esté actualizado para soportar TLS 1.2 o 1.3.

Otros
- **Términos de Uso:** Es crucial recordar que los datos obtenidos mediante la API no pueden ser revendidos directamente como un servicio de búsqueda competidor, según los términos de uso oficiales.
- **Verificación de dominios:** Para empresas, el panel de "Domain Search" requiere una verificación mediante entrada DNS o archivo de texto en el servidor para demostrar la propiedad antes de permitir búsquedas masivas de todos los empleados.

PREGUNTAS FRECUENTES

¿Qué es Have I Been Pwned (HIBP) y cuál es su función en el ámbito profesional?

Es un servicio de agregación de brechas de datos que recopila y analiza información filtrada en internet. Su función principal para profesionales es permitir la monitorización de activos digitales, como dominios corporativos y correos electrónicos, para identificar si las credenciales de una organización han sido comprometidas en incidentes de seguridad públicos o en la Dark Web.

¿Cómo garantiza la privacidad al verificar contraseñas filtradas?

Utiliza un modelo de seguridad basado en K-anonimato a través de su API Pwned Passwords. Este sistema permite verificar si una contraseña ha sido expuesta enviando únicamente los primeros cinco caracteres del hash SHA-1 de la misma. El servidor devuelve una lista de hashes que coinciden con ese prefijo, permitiendo que la comparación final se realice localmente sin que la contraseña real o su hash completo salgan del entorno del cliente.

¿Qué coste tiene la herramienta para una organización?

El acceso a la interfaz web y la API de contraseñas son gratuitos. Para uso profesional y monitorización de dominios, existen planes de suscripción que varían según el volumen de consultas y el número de activos. Los precios oscilan desde los 4,39 USD mensuales en el plan Core hasta más de 1.150 USD mensuales en planes de alto rendimiento (High RPM) para grandes corporaciones.

¿Es posible integrar HIBP en aplicaciones propias mediante código?

Sí, la plataforma ofrece una API RESTful (versión 3) que permite la integración técnica en flujos de trabajo como el registro de usuarios o auditorías internas. Requiere el uso de claves de API para la autenticación y el manejo de respuestas en formato JSON. Existen múltiples librerías y wrappers desarrollados por la comunidad en lenguajes como Python, .NET y Node.js para facilitar este proceso.

¿Qué son los 'Stealer Logs' y por qué son relevantes en la plataforma?

Los Stealer Logs son registros de información capturados por malware diseñado para extraer datos directamente de los dispositivos de los usuarios (como troyanos). A diferencia de las brechas en servidores, estos datos provienen de infecciones locales. HIBP permite buscar este tipo de filtraciones, lo cual es crítico para detectar empleados cuyos equipos personales o corporativos han sido comprometidos por software malicioso.

¿Cumple con la normativa de privacidad y protección de datos?

La herramienta está diseñada bajo principios de minimización de datos y privacidad desde el diseño. Al no almacenar contraseñas en texto claro y utilizar técnicas de anonimización para las consultas, facilita que las empresas cumplan con marcos regulatorios de seguridad y auditoría. El uso de la API requiere la atribución de la fuente según la licencia Creative Commons Attribution 4.0 International.

¿Qué limitaciones tiene para un equipo de ciberseguridad?

HIBP es una herramienta informativa y reactiva; no actúa como un sistema de prevención activa, antivirus o software de remediación. No tiene la capacidad de eliminar la información filtrada de los sitios donde fue publicada originalmente. Además, requiere personal con capacidad técnica para interpretar los resultados y ejecutar las acciones correctivas necesarias, como la rotación de credenciales.

¿Cómo funciona el sistema de alertas para dominios corporativos?

Los administradores pueden verificar la propiedad de un dominio y configurar alertas proactivas. Cuando el sistema procesa una nueva brecha de seguridad que contiene correos electrónicos pertenecientes a dicho dominio, se envía una notificación automática vía email o mediante webhooks, permitiendo una respuesta rápida ante el compromiso de cuentas de empleados.

CONTRATOS Y CONDICIONES

Opinión inicial
Tras verificar los contratos y condiciones de Have I Been Pwned (HIBP), nos encontramos ante una herramienta de diagnóstico de seguridad con un impacto legal **Medio**. Su función principal no es el tratamiento de datos personales en sí, sino la notificación de vulneraciones previas. Según documentos consultados, el servicio destaca por su enfoque de "Privacidad por Diseño", especialmente mediante el uso de K-anonimato, lo que permite a las empresas españolas cumplir con el principio de integridad y confidencialidad del RGPD sin exponer datos en tiempo real. En mi opinión profesional, es una pieza esencial para el cumplimiento del Artículo 33 del RGPD (notificación de brechas), ya que actúa como un sistema de alerta temprana.

Principales recomendaciones
- Realizar una Evaluación de Impacto (EIPD) si se planea automatizar la monitorización de todos los empleados, para justificar el interés legítimo frente al derecho a la intimidad.
- Limitar el acceso a las claves de API y a los informes de dominios exclusivamente al personal técnico autorizado (CISO/IT), evitando la difusión interna de qué empleados específicos han sido filtrados salvo que sea estrictamente necesario para un cambio de credenciales.
- Si se integra la API de contraseñas en formularios de registro, asegurar que se utiliza el modelo de hash truncado para garantizar que la contraseña nunca salga del entorno de la empresa.
- Verificar que el uso de la herramienta esté reflejado en el Registro de Actividades de Tratamiento (RAT) bajo la finalidad de "Seguridad de la información".

Ley de Inteligencia Artificial (AI Act)
Tras analizar las funcionalidades de HIBP, no se identifica el uso de sistemas de IA generativa o de alto riesgo según la clasificación de la UE. La herramienta opera mediante cotejo de bases de datos relacionales y funciones hash, por lo que su sujeción a la AI Act es nula o inaplicable en su arquitectura actual.

Privacidad y protección de datos
- **Responsabilidades**: La empresa usuaria actúa como Responsable del Tratamiento al subir o consultar correos de sus empleados/clientes. HIBP actúa como un prestador de servicios de verificación que, por diseño, minimiza el acceso a datos identificables.
- **Ubicación de los datos**: El servicio es operado por Troy Hunt (Australia) y utiliza infraestructura global (Cloudflare).
- **Transferencia internacional**: Existe una transferencia internacional de datos hacia Australia y EE. UU. (vía Cloudflare). Al no existir un acuerdo de adecuación específico para este servicio, la empresa debe basarse en el interés legítimo para la seguridad cibernética (Recital 49 RGPD) y en las Cláusulas Contractuales Tipo si se contratan planes Enterprise.
- **Derechos ARCO**: HIBP facilita el derecho de supresión permitiendo que los usuarios soliciten que sus correos sean eliminados de los resultados de búsqueda pública a través de su sección de "Opt-out".

Propiedad intelectual
- **Propiedad de datos**: Los datos de las brechas no pertenecen a HIBP ni a la empresa; son datos públicos o filtrados ilícitamente por terceros. HIBP posee la propiedad intelectual sobre la agregación, indexación y estructura de la base de datos.
- **Propiedad del resultado**: La licencia Creative Commons Attribution 4.0 International permite a la empresa usar los resultados de la API incluso comercialmente, siempre que se atribuya la fuente a Have I Been Pwned.

Usos y prohibiciones
- **Usos admitidos**: Auditoría de seguridad interna, prevención de fraude en registros de usuarios, investigación de incidentes de seguridad y protección de activos digitales corporativos.
- **Usos prohibidos**: Queda estrictamente prohibido el "scraping" masivo de la web, el uso de la API para crear servicios competidores directos de HIBP y el uso de los datos para fines de acoso o actividades ilícitas (doxing).

Seguridad y certificaciones
- **Seguridad**: HIBP utiliza K-anonimato, lo que significa que para consultar una contraseña solo se envían los 5 primeros caracteres del hash SHA-1, haciendo imposible que el servidor conozca la contraseña original.
- **Certificaciones**: Aunque es un estándar de facto en la industria, no presenta certificaciones ISO 27001 propias publicadas, delegando gran parte de la seguridad de infraestructura en Cloudflare, que sí cuenta con

certificaciones SOC2 y cumplimiento con el Marco de Privacidad de Datos UE-EE.UU.

Otros
Es relevante destacar que el uso de HIBP ayuda a demostrar la "proactividad" (accountability) exigida por la normativa europea. En caso de una inspección de la AEPD tras una brecha real, contar con logs de monitorización de HIBP sirve como prueba de que la empresa puso medios técnicos para detectar fugas de información.

Fuentes consultadas:
- Términos de uso oficiales
- Documentación técnica de la API y seguridad
- Política de privacidad y gestión de datos
- Información sobre el modelo de K-Anonymity