

ILUZONA SL / DOSSIER CORPORATIVO

Inteligencia artificial. Control empresarial. Seguridad por capas.



Hub Bot | Orquestación de agentes IA

Informe de seguridad para dirección, tecnología,
compras y responsables de seguridad de la información.

Hub Bot añade una capa de identidad, permisos y control de ejecución al uso de agentes IA, herramientas y recursos corporativos.

ENTIDAD	DOCUMENTO
Iluzona SL CIF B75648386	Hub Bot · iabot.io Informe de seguridad empresarial
Edición corporativa para clientes Distribución empresarial	HB-SEG-2026-09 · Versión 2.0 Fecha de referencia: 24/09/2026

Controles de plataforma, infraestructura de soporte y evidencias técnicas organizados para facilitar la evaluación de Hub Bot como proveedor tecnológico.

01 / PROPUESTA DE SEGURIDAD

Agentes IA dentro de un marco de control

Hub Bot es un orquestador de agentes IA orientado al trabajo empresarial. Coordina identidades, espacios de empresa, documentos, herramientas e integraciones con controles propios de autorización y ejecución.

La capacidad del agente y la autoridad para actuar son decisiones distintas. Hub Bot incorpora controles de servidor para vincular cada operación con su contexto autorizado.

PROTECCIÓN	APORTACIÓN DE HUB BOT	UTILIDAD EMPRESARIAL
Identidad	Acceso humano con doble factor y validación de sesión.	Refuerza la protección de las cuentas que utilizan la plataforma.
Permisos	Comprobaciones de empresa, pertenencia, rol y recursos.	Organiza el acceso según las responsabilidades de cada usuario.
Agentes IA	Herramientas autorizadas y capacidades firmadas por tarea y ejecución.	Acota la autoridad técnica de los agentes.
Documentos	Permisos de biblioteca, versiones y controles de archivo.	Apoya el uso compartido y controlado de información.
Conexiones	Vinculación de integración, empresa y operación.	Evita que el modelo elija libremente la identidad corporativa con la que actúa.
Evidencias	Eventos de acceso, pruebas seleccionadas y validación de despliegues.	Facilita la revisión técnica de los controles.

Valor para una organización con varios departamentos

La dirección puede organizar empleados IA y recursos de trabajo; los usuarios operan dentro de sus asignaciones y el equipo técnico dispone de una capa común para aplicar autorizaciones. El diseño permite estructurar la implantación por áreas, casos de uso e integraciones, conservando el contexto empresarial de cada tarea.

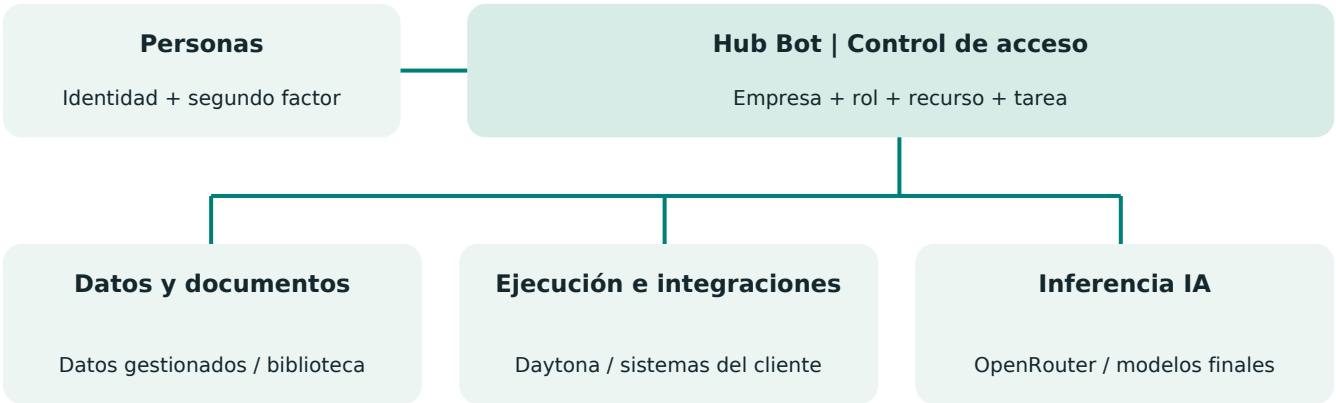
El alcance de los accesos y las acciones sensibles se concreta durante la implantación. La política de aprobación humana se define según la operación, el encargo y los requisitos de la empresa.

Contenido: arquitectura (p. 3), identidad (p. 4), agentes y permisos (p. 5), datos (p. 6), infraestructura (p. 7), validación y certificación (p. 8), evaluación del proveedor (p. 9).

02 / ARQUITECTURA

Orquestación con control propio

Hub Bot integra componentes especializados y añade controles de aplicación para relacionar a la persona, la empresa, el agente, la tarea y los recursos autorizados.



COMPONENTE	FUNCIÓN DENTRO DEL SERVICIO
Hub Bot	Identidad, autorización de peticiones, asignaciones de agentes, permisos de recursos y mediación de herramientas.
Hermes	Motor de ejecución utilizado en parte de los flujos de trabajo. Hub Bot lo integra con capacidades firmadas y controles de herramientas asociados a cada ejecución.
Daytona	Entorno de trabajo para tareas que requieren un ordenador virtual. Hub Bot coordina su utilización y el acceso a recursos dentro del contexto de la tarea.
OpenRouter y modelos	Acceso a modelos para inferencia. El contenido procesado depende de la función y del contexto de trabajo enviado a la ruta seleccionada.
Infraestructura VPS	Alojamiento de servicios de aplicación y procesos de ejecución, con administración técnica de la plataforma.
Servicios gestionados de datos	Persistencia, almacenamiento y funciones de soporte a la identidad, complementadas por la autorización propia de Hub Bot.

Qué añade la orquestación empresarial

En una instalación directa de un motor de agentes, la organización debe integrar su identidad corporativa, permisos, credenciales, recursos y trazabilidad. Hub Bot incorpora una capa común para estas funciones. Su aportación de seguridad se sitúa en cómo gobierna el uso del motor y sus herramientas.

Esquema funcional: no representa aislamiento físico dedicado ni implica que todos los componentes intervengan en todas las tareas.

03 / IDENTIDAD

Acceso protegido desde el inicio

El acceso humano a Hub Bot requiere verificación en dos pasos mediante una aplicación autenticadora. La obligatoriedad y el recorrido de acceso se comprobaron por HTTPS público el 24/09/2026.

Del acceso inicial a la sesión de trabajo

Después del primer factor, el servidor utiliza una sesión provisional limitada para configurar o verificar el autenticador. Solo tras superar el desafío y comprobar el estado de la cuenta se emite la sesión completa de trabajo.

CONTROL	IMPLEMENTACIÓN DOCUMENTADA
Doble factor TOTP	Códigos de seis dígitos y periodos de 30 segundos, compatibles con aplicaciones autenticadoras TOTP.
Secreto del autenticador	Cifrado AES-256-GCM con clave dedicada e IV aleatorio; vinculación criptográfica a usuario y propósito.
Recuperación de acceso	Diez códigos aleatorios de 128 bits, almacenados como hashes y de un solo uso.
Control de intentos	Bloqueo de 15 minutos tras cinco intentos fallidos dentro de la ventana de control de 15 minutos.
Protección frente a repetición	Comprobación del intervalo TOTP aceptado y consumo del desafío. Transición de estado protegida frente a concurrencia.
Sesiones y cookies	Cookies HttpOnly, SameSite=Lax y Secure con HTTPS configurado. Sesión completa de hasta 12 horas y provisional MFA de hasta 10 minutos.
Revocación técnica	Revalidación de cuenta y versiones de sesión/factor. Mecanismos de revocación por versión comprobados en las pruebas.
Contraseña local	Hash scrypt con sal aleatoria para verificar la contraseña sin conservarla en claro.

Protección aplicada en el servidor

La sesión completa no depende únicamente de que el navegador muestre una pantalla de acceso. El backend comprueba el desafío y la vigencia de la cuenta; las cookies antiguas sin prueba MFA se rechazaron en la validación pública.

El segundo factor complementa la protección del dispositivo y del correo de recuperación. El cierre local del navegador y la revocación global de sesiones son operaciones diferentes.

04 / AUTORIZACIÓN

Permisos para personas, agentes y tareas

Los controles de Hub Bot sitúan la autorización en el servidor y la relacionan con el espacio de empresa, los recursos y la operación solicitada.

Empresa, miembros y documentos

Las peticiones privadas pasan por comprobaciones de identidad y pertenencia al espacio. Existen controles para distinguir roles de dirección y miembros, asignar agentes IA a personas y regular el acceso a carpetas, archivos e hilos. El modo obligatorio de autorización de peticiones se observó durante la revisión técnica.

Autoridad limitada para la ejecución IA

Las capacidades firmadas de Hermes vinculan empresa, agente, tarea, revisión, ejecución y herramientas permitidas. En la configuración de código revisada, su duración predeterminada es de 30 minutos, con un máximo de una hora. El router comparte controles entre la ejecución nativa y Hermes.

DIMENSIÓN	CONTROL DOCUMENTADO	APLICACIÓN PRÁCTICA
Recursos	Permisos y asignaciones del espacio de empresa.	Asociar usuarios y agentes con la información que corresponde a su función.
Herramientas	Listas autorizadas y validación del contrato de trabajo.	Acotar las funciones disponibles para ejecutar el encargo.
Delegación	Restricciones y contexto de ejecución.	Conservar la relación de la tarea con su autoridad al coordinar agentes.
Correo	Distinción entre lectura, borrador y envío; comprobaciones de titularidad.	Tratar el envío como una acción diferenciada y ligada a la conexión autorizada.
Conexiones	Empresa y destino autorizados por el servidor.	Evitar que argumentos aportados por el modelo amplíen libremente el ámbito corporativo.

Una instrucción escrita al agente no es una barrera de seguridad suficiente. Hub Bot añade comprobaciones técnicas de autorización a los flujos y herramientas revisados.

La validación de cada implantación debe incluir sus conectores y herramientas habilitados, especialmente navegador y terminal. Las aprobaciones humanas se aplican según el flujo acordado; no se presume una confirmación nueva para toda acción de escritura.

05 / INFORMACIÓN CORPORATIVA

Protección y tratamiento de los datos

La plataforma combina permisos sobre recursos, protección de autenticación y controles de comunicación con servicios especializados de almacenamiento y procesamiento.

INFORMACIÓN	TRATAMIENTO EN LA PLATAFORMA
Identidad y acceso	Datos de usuario, estado y versiones para autenticar y autorizar. El secreto MFA se cifra y los códigos de recuperación se conservan como hashes.
Conversaciones y actividad	Mensajes, referencias, estados y metadatos para continuidad del trabajo y ejecución de tareas. El historial y el contexto enviado al modelo son elementos distintos.
Documentos y resultados	Biblioteca con versiones y permisos. Se identificaron validaciones de extensión, tamaño y formato, y confinamiento de rutas de archivos locales.
Copias de trabajo	Archivos utilizados por el entorno de ejecución para consultar, editar y producir resultados. Forman parte del alcance de tratamiento de la tarea.
Inferencia IA	Contexto y, cuando la función lo requiere, capturas enviadas a los proveedores de la ruta utilizada, incluidos OpenRouter y modelos finales.
Registros de seguridad	Eventos MFA y decisiones de acceso que aportan información para revisión e investigación. No se registran los códigos MFA utilizados.

Comunicaciones y almacenamiento

La revisión verificó HTTPS en el origen público y una conexión a base de datos con TLS y validación estricta del certificado. El servicio gestionado de datos declara cifrado AES-256 en reposo y TLS en tránsito dentro de su plataforma. [2]

Condiciones de tratamiento por implantación

El alcance contractual debe identificar las categorías de datos, funciones habilitadas, proveedores que intervienen, conservación, ubicación, devolución y eliminación. Las condiciones de uso de los datos por modelos se concretan por ruta y modalidad contratada; no se presume una misma condición para todos los proveedores.

El detalle de proveedores y subencargados se trata en la evaluación técnica y contractual. En este dossier, los servicios de infraestructura y datos se presentan por su función; OpenRouter, Daytona y Hermes se identifican como componentes de la arquitectura.

Los controles de archivos descritos no equivalen a un análisis antivirus integral. El cifrado en transporte y almacenamiento no se presenta como cifrado de extremo a extremo de todo el servicio.

06 / INFRAESTRUCTURA

Protección que se suma por capas

Los controles de los proveedores de infraestructura contribuyen a proteger los componentes que Hub Bot utiliza. Sobre esa base, Hub Bot añade autorización y control de ejecución propios.

CAPA DE SOPORTE	REFERENCIAS DE SEGURIDAD DEL PROVEEDOR	APORTACIÓN AL SERVICIO
Infraestructura VPS	El proveedor declara ISO/IEC 27001:2022, supervisión de servidores, equipo de seguridad y prácticas de gestión de vulnerabilidades. [1]	Base de alojamiento respaldada por controles de infraestructura. Su aplicación depende del servicio contratado y de la responsabilidad de administración del VPS.
Servicios gestionados de datos	El proveedor declara ISO/IEC 27001:2022, SOC 2 Type 2, cifrado en reposo y tránsito y copias diarias de las bases de datos de pago. [2, 3]	Protección de la capa gestionada de datos, complementada por permisos de aplicación y custodia de credenciales.
Entorno Daytona	Su centro de confianza publica referencias a ISO/IEC 27001 y SOC 2, controles de seguridad y documentación para evaluación. [4]	Entorno especializado de ejecución con un expediente de seguridad propio que debe revisarse para la modalidad utilizada.
Aplicación Hub Bot	MFA obligatorio, comprobaciones de empresa y recursos, capacidades por ejecución y registros.	Control del uso que personas y agentes hacen de la tecnología integrada.

Cómo se aprovechan los controles del proveedor

Cuando un componente gestionado aplica una medida de protección, el servicio que utiliza ese componente se beneficia de ella dentro de su alcance. Por ejemplo, el cifrado de la base de datos gestionada protege la información alojada en esa capa; Hub Bot añade las decisiones sobre quién puede acceder a ella y con qué finalidad.

La protección de infraestructura y la protección de aplicación se complementan. El cliente recibe un servicio construido sobre ambas capas.

Las certificaciones corresponden a la entidad y al alcance evaluados. Se aportan como evidencias de la cadena de suministro, sin convertirlas en una certificación propia de Hub Bot. Las referencias públicas no sustituyen la revisión de vigencia, alcance y configuración contratada.

07 / GARANTÍA Y EVOLUCIÓN

Controles respaldados por evidencias

La revisión técnica recoge pruebas de autenticación, autorizaciones seleccionadas y publicación. Las evidencias permiten concretar qué comportamiento se comprobó y bajo qué alcance.

EVIDENCIA DOCUMENTADA	RESULTADO	ALCANCE
Regresión seleccionada	221/221	MFA, identidad/aislamiento y base de integración seleccionados.
Interfaz de autenticación	5 pruebas	Recorridos cubiertos de alta, verificación y recuperación.
Comprobación con base real	18 controles	Cuenta sintética, cifrado persistente, TOTP, recuperación, revocación y limpieza.
Validación por HTTPS público	18/18	24/09/2026 a las 14:41:50 UTC; incluye rechazo de cookie anterior y revocación.
Validación del frontal	14/14	Pruebas del comprobador de entrada y arranque JavaScript.
Recorrido manual	Confirmado	Alta en Google Authenticator y acceso correcto por el propietario.

Resultados de grupos seleccionados; no se suman como una auditoría total. Esta edición sintetiza el estudio interno y no constituye un pentest ni una nueva comprobación del estado de producción.

Cambios y operación

El despliegue documentado incluyó respaldos recuperables de los cambios, comprobación de artefactos y mecanismos de reversión. Los registros MFA y de autorización aportan trazabilidad operativa; se describen como registros de aplicación, sin atribuirles inmutabilidad o captura garantizada de todos los eventos.

Compromiso de mejora y certificación

Iluzona SL dedica recursos a la evaluación de su seguridad, la mejora interna y la preparación de certificaciones propias, con contactos iniciales con AENOR orientados a ISO/IEC 27001.

Esta línea de trabajo, comunicada por la dirección, acompaña la evolución de Hub Bot y refuerza su compromiso con la confianza empresarial. La certificación propia se encuentra en fase de preparación, sin certificado emitido.

Los objetivos de continuidad, soporte y respuesta aplicables a cada servicio se concretan en la contratación. Los respaldos del despliegue no equivalen por sí solos a una restauración integral validada.

08 / EVALUACIÓN EMPRESARIAL

Un dossier para su equipo de seguridad

Este documento facilita la evaluación de Hub Bot por dirección, compras y responsables de seguridad, incluidas organizaciones que gestionan sus procesos conforme a ISO/IEC 27001.

ÁMBITO DE EVALUACIÓN	BASE PARA LA REVISIÓN DEL CLIENTE
Identidad y permisos	Controles de MFA, sesiones, roles, pertenencia y acceso a recursos descritos en las páginas 4 y 5.
Uso de agentes IA	Herramientas habilitadas, alcance de las tareas, conexiones autorizadas y política de aprobación de acciones sensibles.
Datos y proveedores	Mapa de tratamiento, proveedores por función y documentación contractual aplicable a la implantación.
Infraestructura y evidencias	Referencias de seguridad de los proveedores y resultados de validación con su alcance identificado.
Puesta en servicio	Casos de uso, permisos mínimos, pruebas de acceso y denegación, interlocutores y condiciones de soporte acordadas.

La aceptación del proveedor corresponde a los criterios y al análisis de riesgos de la organización cliente. Este dossier aporta una base técnica para esa decisión; la aprobación se completa con la documentación y las condiciones exigidas para el servicio concreto.

Referencias y control documental

Fuente técnica: estudio interno “Seguridad de Hub Bot. Arquitectura, controles, responsabilidad y hoja de ruta”, 24/09/2026. Base de los controles y pruebas de aplicación descritos. Información sobre AENOR comunicada por la dirección.

Referencias públicas consultadas el 24/09/2026. Los enlaces permiten revisar el emisor y el alcance de cada declaración:

- [1] [Infraestructura VPS: medidas de seguridad y certificación](#)
- [2] [Servicios gestionados de datos: seguridad y protección de datos](#)
- [3] [Servicios gestionados de datos: alcance ISO/IEC 27001:2022](#)
- [4] [Daytona: centro de confianza y documentación de seguridad](#)
- [5] [ISO: descripción de ISO/IEC 27001 y su sistema de gestión](#)

Iluzona SL · CIF B75648386

HB-SEG-2026-09 · Versión 2.0 · Fecha de referencia: 24/09/2026
[iabot.io](#) · [hub.iabot.io](#)

Edición corporativa para distribución empresarial. Las afirmaciones se refieren al alcance descrito y a su fecha de referencia. Los compromisos de servicio y tratamiento se recogen en la contratación aplicable.