DESARROLLADORES

Paquete de evaluación de seguridad

Este paquete describe cómo las integraciones de Masnet (webhooks y API de datos) protegen los datos de la empresa. Está redactado para quien evalúa el riesgo de conectar Masnet a sus sistemas. Lo no cubierto aquí se remite a los documentos legales publicados.

Contrato 1.7.0 (`sha256:18057f386936`), verificado contra el código de api-daas en la revisión 5d30fed45e8f.

Alcance y estado

- Cubre el envío de eventos por webhook, la API de datos de lectura y el registro de eventos, descritos en esta documentación.
- Los hechos técnicos se verificaron contra el código de la plataforma en la revisión `5d30fed45e8f` de api-daas; los plazos de retención y los objetivos de diseño provienen del diseño técnico de la plataforma y se indican como tales.
- Este paquete no declara certificaciones de seguridad ni auditorías de terceros.
- Las condiciones contractuales (nivel de servicio, subencargados, tratamiento de datos, divulgación de vulnerabilidades) están en los Anexos complementarios y en la Política de Privacidad; esta página los cita y no los reemplaza.

Arquitectura y flujo de datos

Un hecho de negocio (por ejemplo, un contrato que cambia de estado) se captura dentro de la misma transacción de la base de datos de negocio y se deja en una bandeja de salida. Un relay lo copia al registro de eventos, que vive en una base de datos separada y aislada por empresa. Un único proceso, sin acceso desde internet, toma las entregas pendientes y las envía al destino HTTPS de la empresa. Ese proceso es el único con salida a internet y el único que posee las claves privadas con que se descifran las credenciales de los destinos.

Flujo de un evento

```
Acción en Masnet
  -> captura transaccional (base de datos de negocio) -> bandeja de salida
  -> relay -> registro de eventos (base aislada, filas separadas por empresa)
  -> planificador de entregas -> proceso de envío (único con salida a internet)
  -> HTTPS (TLS) -> destino de la empresa cliente
```

- Cada entrega se proyecta, en el momento del envío, con los grupos de campos que el destino tiene otorgados; antes de cada intento se vuelven a comprobar el estado de la integración y del destino y los permisos vigentes.
- Los pods de la API solo cifran las credenciales de un destino con una clave pública: una API comprometida puede crear material pero no leerlo.
- Una integración nunca administra integraciones: sus credenciales no sirven para cambiar la configuración.
- La API de datos siempre se limita a la empresa de la credencial; la empresa nunca es un parámetro y un objeto ajeno responde como inexistente.

Datos que salen, por dominio y grupo

La empresa otorga a cada integración un permiso por dominio y por grupo de campos. `public` y `business` salen al otorgar el dominio; `confidential` y `people` solo con una confirmación explícita del administrador. La tabla cuenta, por objeto, los campos de primer nivel de `data.object` que pertenecen a cada grupo según los esquemas publicados; un objeto anidado cuenta como un campo.

Objeto	Dominio	public	business	confidential	people
`bid`	`bids`	1	13	0	0
`award`	`awards`	1	14	0	0
`contract`	`contracts`	3	18	0	0
`purchase_order`	`contracts`	4	11	0	0

Objeto	Dominio	public	business	confidential	people
guarantee	guarantees	1	20	0	0
opportunity	opportunities	1	11	1	2
tender	tenders	11	2	0	0
milestone	contracts	0	11	0	0
deadline	deadlines	1	12	0	0
audit	audit	0	14	0	3
document	documents	0	4	0	2
catalog_item	catalog	0	21	3	0
price_rule	prices	0	6	12	0
export	exports	0	12	0	1
communication	communications	0	11	0	0
survey	surveys	0	11	0	0
price_request	price_requests	0	15	0	0
framework_agreement_price_request	price_requests	0	17	0	0
client	clients	1	16	0	1
client_group	clients	0	18	0	1
sales_portfolio	sales_portfolios	0	12	0	3
sales_scope	sales_portfolios	0	6	0	2
client_assignment	sales_portfolios	0	5	0	2
product_group	catalog	0	15	0	0
competitor_mark	catalog	2	12	0	2
business_line	business_lines	0	14	0	4

Lo que nunca se exporta

- Texto libre de comentarios, notas, conversaciones, justificaciones y glosas internas.
- Contenido de archivos y URL firmadas.
- Datos de KIM, indicaciones y respuestas de inteligencia artificial.
- Marcas personales (destacar, seguir, leído, archivar, descartar, flags, prioridad y carpetas), etiquetas y checklists privadas, borradores y tareas privadas.
- Secretos y credenciales, telemetría y navegación.

El registro de acciones de usuarios exporta el hecho de cada acción, nunca su contenido. Nombre, correo, IP y agente de usuario requieren además el grupo `people`, y la lectura exige que el administrador declare que la empresa informó el control a sus usuarios.

Cifrado y firma

Superficie	Mecanismo
En tránsito	TLS. Objetivo de diseño: TLS 1.2 como mínimo y TLS 1.3 preferido. Los destinos deben ser HTTPS en el puerto 443 u 8443.
Integridad y autenticidad del envío	HMAC-SHA256 según Standard Webhooks, con un secreto por destino generado por Masnet y mostrado una sola vez. Rotación con dos firmas durante 24 horas.
Material del destino en reposo (URL, credenciales y secretos de firma)	Sobre sellado con X25519, HKDF-SHA256 y AES-256-GCM. Cada parte lleva datos autenticados que la ligan a la empresa, la integración y el destino.
Claves de cliente de la API	Se almacenan solo como hash SHA-256 y se comparan en tiempo constante.
Tokens de acceso	JWT de 15 minutos firmados con un llavero propio, con identificador de clave, emisor y audiencia fijos y rotación.

Salida de red y direcciones IP

Masnet no publica direcciones IP de salida fijas. Las entregas salen desde direcciones compartidas entre empresas, por lo que la IP no autentica: el receptor debe verificar la firma o la credencial. Un receptor cuyo cortafuegos exija una lista de IP de origen usa el modo pull (API de datos y registro de eventos), que se consulta desde su red; si una empresa exige además recibir webhooks desde direcciones IP conocidas, se acuerda con ella.

- Cada intento resuelve el nombre DNS, rechaza cualquier dirección no pública y fija la conexión a las direcciones validadas.
- No se siguen redirecciones y la respuesta se lee solo hasta 2 KiB.
- La dirección del servidor de autorización de OAuth pasa por las mismas defensas.
- La URL del destino, que puede incluir una firma en la query, se trata como una credencial: se cifra, se muestra enmascarada y no se registra.

Retención

Valores del diseño técnico de la plataforma:

Dato	Retención
Eventos con su contenido (registro y reenvío)	30 días
Entregas, intentos y extracto de respuesta	30 días
Marca de deduplicación	45 días
Auditoría de configuración y de permisos	365 días
Registro de acciones de usuarios (API de lectura)	365 días

Los eventos se particionan por día y se eliminan por partición. Una solicitud de supresión de datos personales purga el contenido afectado. Para los datos de la cuenta al término del contrato, véanse la sección 9 de la Política de Privacidad y el Anexo F.9 de los Anexos.

Auditoría

- La emisión de tokens, los fallos de autenticación y las lecturas del registro de eventos y de acciones quedan registrados por integración, con el identificador de solicitud.
- Diez fallos de autenticación de un cliente en 15 minutos generan un aviso al administrador de la integración. Los fallos repetidos desde una misma IP aumentan el retraso y pueden bloquearla; por cliente solo hay retraso, nunca bloqueo, para que un tercero no deje sin acceso a un cliente legítimo.
- Los cambios de configuración (destinos, permisos, credenciales, declaraciones) se registran y pueden recibirse como el evento `audit.integration_changed`, que nunca incluye valores secretos.
- Cada entrega conserva su historial: intentos, códigos, duración y la huella SHA-256 del cuerpo enviado para conciliar con el receptor.

Gestión de secretos

- Los secretos de firma, claves de API y secretos de cliente se muestran una sola vez y no se pueden leer después.
- Las claves de API vencen por omisión a los 365 días y cada cliente admite dos secretos vigentes para rotar sin interrupción; la revocación es inmediata.
- Los extractos de respuesta del receptor se depuran: no conservan las credenciales que se le enviaron.

Respuesta a incidentes

Plazo de notificación publicado: la sección 10 de la Política de Privacidad establece que, ante incidentes de seguridad que afecten datos personales, Masnet evaluará el riesgo y notificará al Cliente o a los titulares afectados dentro de las 72 horas siguientes a la confirmación del incidente. El Anexo F.7 de los Anexos agrega que la notificación se hace sin demora indebida y con cooperación en la evaluación. Los reportes de vulnerabilidades se envían a seguridad@masnet.com; la política de divulgación responsable es el Anexo B.

Subencargados y tratamiento de datos

- Roles: la empresa cliente es la responsable del tratamiento y Masnet, la encargada (Anexo F.2).
- Subencargados: el Anexo D describe sus categorías y obligaciones, y las secciones 7 y 8 de la Política de Privacidad identifican a los proveedores y las transferencias internacionales. La información detallada se entrega a solicitud en legal@masnet.com o privacidad@masnet.com.
- Ley 21.719: la Política de Privacidad describe la transición normativa. Para un Data Processing Addendum detallado, el Anexo F.10 indica solicitarlo a legal@masnet.com.
- Medidas de diseño de las integraciones: minimización por omisión (`people` excluido), registro de cada envío, revocación inmediata y retención acotada.
- Disponibilidad: el Anexo A fija la disponibilidad mensual de la Plataforma.

> Esta página no sustituye los documentos contractuales. Ante cualquier diferencia, prevalecen los Términos de Servicio, la Política de Privacidad y los Anexos vigentes.

Prueba de penetración externa

La prueba de penetración externa previa a la disponibilidad general **todavía no se ha realizado**. Sus resultados se publicarán en esta página cuando exista.