Cuestionario de seguridad

Las respuestas listas a las preguntas que hace el departamento de seguridad de una gran empresa antes de comprar. Dicen lo que Russet hace hoy; donde algo falta, pone «falta» y qué hace falta. Actualizado el 19 de noviembre de 2026.

¿Dónde están nuestros datos y quién los trata?

El servicio funciona en Alemania (netcup GmbH, ISO 27001 y 27701); las copias están en los Países Bajos (Backblaze, SOC 2 Tipo 2), cifradas antes de salir. Vuestros datos que van a la IA llegan solo a OpenAI (EE. UU. e Irlanda), sin los nombres de vuestros clientes; el trabajo interno del equipo de Russet, sin vuestros datos, también a Anthropic (EE. UU.). El correo de Russet está en Microsoft; los correos de servicio salen de Scaleway (Francia); la conexión con el banco, si la activáis, pasa por Enable Banking (Finlandia). Cada empresa tiene sus bases de datos en carpetas separadas.

¿Cómo se cifran los datos, en tránsito y en reposo?

En tránsito siempre HTTPS con HSTS. En reposo: secretos y copias cifrados con AES-256-GCM con claves solo en el servidor. Las bases de datos en el servidor no están cifradas a nivel de archivo: las protege el acceso al servidor y la separación por empresa.

Copias y restauración: ¿cada cuánto, dónde, probadas?

Una copia de cada empresa cada hora, cifrada, en un segundo centro de datos europeo, releída byte a byte. Cada copia vive 14 días y luego la borra Russet (la última de una empresa activa se queda). La restauración se prueba en una carpeta aparte. Falta la prueba completa programada en el servidor real.

¿Cómo se controlan los accesos de las personas?

Cuatro roles decididos por quien administra, con la matriz escrita en un solo lugar. Contraseña y segundo paso obligatorio para todos, impuesto por las páginas de acceso de Russet; titular y administradores con passkey o app. Acceso con la cuenta de empresa (Microsoft Entra ID o Google), bajo petición y por activar (hoy apagado en el servidor): entran las personas del grupo elegido, con su rol; quien sale del grupo ya no entra (SCIM 2.0). Quitar a una persona cierra sus sesiones.

¿Hay un registro de quién hizo qué?

Sí: cada acción es una línea con quién o qué, sobre qué datos, con qué regla, con qué resultado; se consulta en «Historial» con filtros y se descarga en CSV. Las líneas están en la cadena firmada de los datos de la empresa.

¿Qué subencargados tratan los datos y con qué garantías?

netcup, Backblaze, Scaleway, el servicio de acceso (ZITADEL), OpenAI, Stripe y los servicios de notificación del navegador, cada uno con acuerdo de tratamiento (art. 28); hacia EE. UU. las cláusulas contractuales tipo. Avisamos antes de añadir un proveedor.

¿Cómo y cuándo se borran nuestros datos?

En cualquier momento descargáis todo. Al terminar, 90 días para descargar; después borramos en 30 días (salvo lo que exige la ley), con un procedimiento de dos pasos registrado; Russet borra las copias, como muy tarde cuando vence el bloqueo contra el borrado (hasta 14 días).

¿Qué pasa en caso de incidente o violación?

El estado del servicio y los incidentes de 30 días son públicos en /estado. Si descubrimos una violación os avisamos en 48 horas como máximo. Falta un registro formal de incidentes con causa y lección.

Continuidad: ¿qué se pierde como máximo, en cuánto se recupera?

Como máximo una hora de trabajo. El servidor de reserva releva al principal con tiempos medidos; los procedimientos de emergencia están escritos. Russet hoy es una sola persona: la continuidad de las personas es el punto débil y debe constar en el contrato.

¿Cómo de seguro es vuestro desarrollo y despliegue?

Cada versión pasa cientos de pruebas automáticas, 26 archivos solo de seguridad; dependencias fijadas; paquete verificado por huella. Falta la revisión por una segunda persona y un test de intrusión de terceros.

¿Qué hacéis con la inteligencia artificial sobre nuestros datos?

Modelos de OpenAI por las interfaces de empresa: los datos no entrenan los modelos. Al modelo solo llega lo necesario: números y roles, nunca nombres. Cada llamada tiene tope de gasto y queda registrada.

¿Tenéis SOC 2 o ISO 27001?

No, todavía no, y no lo decimos. Los proveedores sí. Los controles de Russet están ordenados como piden SOC 2 e ISO 27001, con lo que falta escrito con honestidad: /seguridad/controlli. La certificación real llega después.

Controles SOC 2 e ISO 27001

16 controles están, 9 en parte, 2 faltan. Cada control como lo piden SOC 2 (Trust Services Criteria) e ISO/IEC 27001:2022 (Anexo A): dónde está en Russet, la prueba, el estado. Sin certificación: este es el mapa honesto para llegar, con la burocracia después.

- ORG-1 · Políticas de seguridad escritas y responsabilidades — en parte: Un documento único de política de seguridad aprobado y fechado, con revisión anual: hoy las reglas están escritas página a página, no reunidas y firmadas.
- ORG-2 · Evaluación de riesgos y amenazas — en parte: Un registro de riesgos con probabilidad, impacto, responsable y revisión periódica: hoy los riesgos se tratan como pruebas automáticas, no en un registro.
- ORG-3 · Proveedores: lista, función, país, acuerdos — está
- ORG-4 · Personas: verificación, confidencialidad, formación — falta: Russet hoy es una sola persona, sin empleados: con la primera harán falta contrato con confidencialidad, verificación y formación anual.
- ACC-1 · Roles y permisos por persona (cuatro roles, una matriz) — está
- ACC-2 · Acceso fuerte: contraseña y segundo paso para todos; passkeys y app de autenticación — está
- ACC-3 · Acceso con la cuenta de empresa (Microsoft Entra ID, Google) y personas del grupo (SCIM 2.0, lectura del grupo) — en parte: Bajo petición, por activar: hoy está apagado en el servidor. Probado con Microsoft y Google simulados que responden como los reales; se activa, y se prueba con un tenant real, cuando una empresa lo pide.
- ACC-4 · Quien sale ya no entra: baja, sesiones cerradas, revisión de accesos — en parte: La revisión periódica es automática solo para quien entra por el grupo; para los invitados a mano falta un recordatorio trimestral.
- ACC-5 · Sesiones: duración, dispositivos recordados, verificación antes de operaciones delicadas — está
- ACC-6 · Separación entre empresas: bases de datos separadas — está
- ACC-7 · Acceso de la asistencia solo con permiso del titular, con tiempo y motivo — está
- DAT-1 · Cifrado en tránsito (HTTPS, HSTS) y de los secretos en el servidor (AES-256-GCM) — está
- DAT-2 · Minimización: sin IP escritas, extracto leído y descartado, nombres nunca a la IA — está
- DAT-3 · Borrado y devolución: datos descargables siempre, 90 días tras el fin, borrados en 30; copias borradas por Russet

tras 14 — está

- DAT-4 · Antivirus en cada archivo guardado; los leídos no se guardan — está
- DAT-5 · Reglas del navegador en cada página: CSP, sin incrustación, sin caché, sin scripts de terceros — está
- OPS-1 · Copias cada hora, cifradas antes de salir, en un segundo centro de datos europeo; releídas y comparadas — está
- OPS-2 · Continuidad: restauración en carpeta aparte probada, escenarios escritos, relevo medido — en parte: La prueba de restauración completa en el servidor real debe repetirse con calendario (cada seis meses): hoy está probada en código y documentada, no programada.
- OPS-3 · Registro de cada acción (quién, datos, regla, resultado) en la cadena firmada; registro técnico sin IP ni contenidos — está
- OPS-4 · Monitorización: estado público minuto a minuto, alarmas en el teléfono, incidentes de 30 días — está
- OPS-5 · Incidentes: aviso a las empresas en 48 horas, procedimientos escritos, canal para avisar de una debilidad — en parte: Un registro de incidentes con causa, remedio y lección: hoy están en la página de estado y en el diario de trabajo.
- OPS-6 · Cambios: cada versión pasa las pruebas; el paquete instalado se comprueba con la huella de cada archivo; dependencias fijadas — en parte: La revisión del código por una segunda persona antes de instalar: hoy escribe e instala una sola persona.
- OPS-7 · Vulnerabilidades: pruebas de seguridad en cada versión; test de intrusión de terceros — en parte: Un test de intrusión de terceros con informe: nunca hecho; se hará tras el primer cliente.
- OPS-8 · Seguridad física y del servidor: centro de datos certificado ISO 27001; secretos legibles solo por el servicio — está
- OPS-9 · IA: tope de gasto por llamada, registrada; sin entrenamiento; nombres nunca al modelo; software generado aislado — está
- PRI-1 · RGPD: acuerdo art. 28, privacidad, solicitudes en un mes, proveedores con acuerdo — en parte: El texto del acuerdo art. 28 revisado por el abogado y firmado con el contrato: hoy no existe aún.
- PRI-2 · Certificación SOC 2 / ISO 27001 propia de Russet — falta: La certificación real llega después, con la burocracia: auditor acreditado, 6–12 meses. Los proveedores ya están certificados.