



TNote Ficha Técnica

RESUMEN

Nombre	TNote
Descripción	Gestor de incidencias y actividades.
Características	Se basa en los requisitos de gestión de incidencias o actividades de la certificación del "Operador Económico Autorizado". Incorpora la gestión de incidencias como un flujo de trabajo. Crea y gestiona alertas. Clasifica las solicitudes en base a la política de usuarios y la organización interna de la empresa. Ofrece trazabilidad, análisis e informes.
Parámetros de comercialización	Usuarios concurrentes y volumen de almacenamiento.
Lanzamiento	Año 2014

ARQUITECTURA

Género	Aplicación web
Base de Datos	PostgreSQL
Sistema operativo	Cualquiera
Modelo de implementación	Privado: SaaS sobre Infraestructura basada en GNU/Linux con servicio de cliente multi-tenant. Público: URL accesible.
Dependencia	Software: Navegadores Google Chrome, Mozilla Firefox o Internet Explorer 10 o superior. Hardware: N/A
Customización y parametrización	Política de usuarios, tipología de incidencias, organización de las delegaciones, suscripción a tipologías de incidencias e integración con otras aplicaciones (Taric y externas).
Módulos adicionales Taric, S.A.U.	N/A
Idiomas	Interfaz de usuario en castellano.
Entornos de trabajo	Las actualizaciones de aplicación y entorno de cliente se validan en plataformas diferenciadas de pruebas y pre-producción.
Actualización	Aplicación e infraestructura con actualización periódica automática.
Panel de Control	Administración, monitorización y provisionamiento del servicio con herramientas internas Taric y proceso gestionados por equipo soporte Taric.
Tipo provisionamiento	Gestión de la capacidad con escalado horizontal basado máquinas redundantes geográficamente dispersas. Funcionalidades software y configuración gestionada por el cliente con la asistencia del equipo de Soporte Taric. Alta y gestión de usuarios por el operador con perfil de administrador desde la aplicación.

INTEGRACIONES CON OTRAS APLICACIONES

Aplicaciones Taric, S.A.U.	Gestión de declaraciones aduaneras (TDua), gestión aduanera de depósitos (TDepo).
Tipos de API	Api REST via HTTPS
Puertos necesarios	TCP/443

LEGAL

Normativo y regulatorio	El servicio cumple con los requisitos exigidos por la LOPD y los principios de Safe Harbor.
Propiedad intelectual	Taric, S.A.U.
País CPD principal	España, Barcelona
País CPD respaldo	España, Madrid
Subcontratación	Todos los subcontratistas del servicio pertenecen a la Unión Europea.

SOPORTE Y NIVEL DE SERVICIO

Criterios de atención/ resolución	Soporte propio de Taric, S.A.U.: Gestión de incidencias en herramienta interna (CRM). Soporte remoto (Team Viewer).
Nivel soporte funcional	Soporte funcional lunes a viernes de 08:00 a 18:30 horas. Excepto festivos nacionales.
Nivel soporte técnico	Configuración inicial, apoyo al uso, reporte de errores y mantenimiento correctivo.
Mecanismos comunicación soporte	Atención telefónica y por correo electrónico.
Idiomas soporte	Castellano
Interrupciones de mantenimiento	Planificadas y notificadas al usuario.
Actualizaciones	Periódicas y automáticas.

SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN

Mecanismo de autenticación	Contraseña almacenada con cifrado no reversible (non-reversible encryption salted hash). Acceso a servicio vía HTTPS. Servidor con certificado SSL/TLS.
Mecanismo de control de acceso	Lista de usuarios mantenida por la propia aplicación.
Limitación de acceso	Se definen límites de tiempo a sesión de usuario inactiva.
Acceso a la información	Usuario tiene acceso a funcionalidad de exportación de entidades principales de datos de la aplicación en diferentes formatos CSV/Excel/JSON.
Plan de Recuperación ante Desastres	Se mantiene réplica asíncrona del servicio del cliente en centro de datos separado geográficamente del principal.
Nivel de aislamiento	A nivel de aplicación: Autenticación vía usuario + contraseña u OAuth2. A nivel de plataforma: Ubuntu GNU/Linux LTS. A nivel de virtualización: VMware vSphere con vCloud Networking and Security. A nivel físico: Centro de procedo de datos (CPD) con controles de acceso al edificio, CCTV, alarmas, puerta blindada, cortafuegos, guardias 24/7/365, climatización y acceso mediante lector biométrico de huellas digitales y tarjeta.
Cifrado de datos almacenados	No
Cifrado de datos de backup	Cifrado AES de 256 bits.
Cifrado de datos en tránsito	Cifrado RC4 de 128 bits.
Seguridad perimetral	VMware vShield Edge del centro de proceso de datos (CPD). Se puede restringir acceso a servicio habilitando únicamente direccionamiento IPv4 del cliente.
Gestión de backup	Backup de instancia virtual diaria, con retención mínima de 7 días (configurable). Backup de aplicación y datos de aplicación diaria, con retención mínima de 1 hora. Replicación asíncrono entre centro de datos con periodicidad inferior a 2 horas.
Baja del Servicio	Existe un proceso estandarizado para la retirada del servicio en caso de migración o baja del mismo. El proceso implica la entrega de todos los datos asociados.