

CONDICIONES DE ALOJAMIENTO DE LA  
APLICACIÓN GANDIA INTEGRADA EN EL  
SERVIDOR DE *TESI* S.L.

## Índice

---

1. Introducción .....	3
2. Descripción del servicio .....	4
3. Especificaciones técnicas.....	6
3.1. Alojamiento .....	6
3.2. Seguridad del servidor .....	6
3.3. Control de tráfico.....	7
3.4. Acceso a los servidores .....	7
3.4.1. Acceso Físico .....	7
3.4.2. Acceso remoto.....	7
3.5. Operación y administración .....	7
3.6. Monitorización .....	7
3.6.1. Monitorización externa .....	7
3.6.2. Monitorización interna .....	7
3.7. Backup .....	8
3.8. Control eléctrico, de temperatura y de humedad.....	8
3.9. Protección contra incendios.....	8
3.10. Seguridad.....	8
4. Calidad del servicio.....	9
4.1. SLA (Service Level Agreement).....	9
4.2. Disponibilidad de Red .....	9
4.3. Condiciones generales de prestación.....	10

## 1. Introducción

La empresa **TESI, SL** (en adelante **TESI**), ofrece a sus clientes la posibilidad de alojamiento de su aplicación Gandia Integra en un servidor propio ubicado en CATNIX en modo **colocation** (Housing) y gestionado el alojamiento por la empresa **EUROVIA SERVICIOS TELEMATICOS, SL.** (en adelante **EUROVIA**). El servidor alojado en el CATNIX es mantenido a nivel de software por la empresa **EUROGARAN**.

## 2.Descripción del servicio

El servicio de **Colocation** (Housing) de **EUROVIA** implica el Alojamiento, Conexión, Gestión y Administración (a diversos niveles) de equipos informáticos, ya sean adquiridos por **EUROVIA** Servicios Telemáticos (en adelante **EUROVIA**) o por *Eurogaran* (en adelante el *Cliente*), en instalaciones de **EUROVIA**, operados, explotados y mantenidos por personal propio y/o del *Cliente*, con el fin de desarrollar y explotar servicios avanzados de telecomunicaciones según las necesidades y requerimientos del *Cliente*. Un servicio orientado a empresas que permite obtener la máxima eficiencia de las máquinas y prestar servicios de conectividad al ser integradas en la avanzada arquitectura tecnológica de **EUROVIA** y gestionadas por un experto grupo de profesionales. Los servicios de **Colocation** permiten tener alojado en régimen de outsourcing uno o varios servidores en la infraestructura de **EUROVIA**, quien se encargará de alojar, conectar y mantener estos servidores de una forma eficiente, con multitud de opciones, **EUROVIA** se adaptará a las necesidades de su empresa, cualquiera que sea su tamaño y alcance. [...]

El servicio de **Colocation** (housing) ofrece un espacio dedicado para alojar sus servidores en nuestro entorno controlado dentro del CATNIX (nodo independiente de intercambio de tráfico IP internacional en Cataluña). Sus servidores ocuparán un área dedicada en nuestros racks. Se permitirá el acceso a nuestras instalaciones a cualquier persona designada por el *Cliente*. Cualquier modificación en el emplazamiento físico de la máquina precisará de aprobación por parte del *Cliente*. Los servidores pueden ser de propiedad del *Cliente* o alquilados o financiados por **EUROVIA** y en ellos podrá residir cualquier software/hardware que se quiera instalar, siempre bajo responsabilidad del *Cliente*. Cada espacio tiene su alimentación de energía dedicada proveniente de una distribución de energía compartida. Nuestro Data Center cuenta con infraestructuras redundantes que nos permiten garantizar una total seguridad en el servicio. También puede contratar un armario (rack) entero o divisiones de un armario si necesita más espacio o independencia física. **EUROVIA** se compromete a proporcionar y controlar el caudal Internet contratado y al correcto funcionamiento de toda la infraestructura de acceso a Internet. Además, prestará soporte y asesoramiento técnico y realizará aquellas pequeñas intervenciones que sean necesarias para el correcto funcionamiento de su servidor.

La garantía de servicio está detallada en el apartado SLA "calidad del servicio de housing" (véase más adelante).

El servicio de housing incluye:

- Alojamiento del servidor
- Mantenimiento hardware/software del servidor (contratación especial)
- Firewall
- Servicio de alimentación ininterrumpida
- Sala de housing refrigerada
- Control remoto del servidor
- Estadísticas de consumo
- Seguridad

Las principales ventajas del servicio de **Colocation** son:

- Infraestructura propia para el desarrollo de los servicios: espacio físico para albergar los equipos, conexión a Internet y software necesario para proporcionar el nivel de servicio requerido.
- Gestión de los servicios: administración, soporte técnico para la plataforma tecnológica, comunicaciones, operaciones y explotación de la plataforma, y seguimiento y control del servicio.
- Procedimientos de Seguridad del Centro de Datos: mantenimiento y cumplimiento de procedimientos de seguridad física para la prestación de los servicios al *Cliente*.

CONDICIONES DE ALOJAMIENTO DE LA APLICACIÓN GANDIA INTEGRADA EN EL  
SERVIDOR DE **TESI**S.L.

- El personal que forma parte del equipo de trabajo destinado por **EUROVIA** al desarrollo de las actividades objeto del servicio prestado estará vinculado directamente a **EUROVIA**.

**EUROVIA** garantiza en todo momento el mantenimiento del nivel adecuado de competencia del equipo humano asignado a los Servicios, ante posibles nuevas condiciones tecnológicas que se incorporen consecuencia de la evolución de los servicios incluidos bajo el Contrato de prestación de servicios.

- Seguimiento del servicio: reuniones, revisiones, control de informes de seguimiento del servicio, análisis de los niveles de servicio para los indicadores prefijados, notificación de penalizaciones.
- Indicadores de calidad del servicio.
- Suministro del servicio: los incrementos de recursos debidos a la variación en la prestación del servicio se fundamentarán en informes que justifiquen tales extremos; de la misma forma serán justificados los términos económicos, las condiciones técnicas de la implantación y la planificación de la instalación.
- Seguridad.
- Estadísticas.
- Servicios de soporte a usuarios: CAU (Centro de Atención al Usuario).
- Conectividad directa (líneas exclusivas SHDSL, punto a punto, etc.) y garantizada al 100% desde el domicilio del cliente hasta nuestro Data Center en el Catnix.

## 3. Especificaciones técnicas

### 3.1. Alojamiento

El servicio se ha materializado utilizando un servidor con las siguientes características:

- Servidor Fujitsu Siemens PY RX300S3 E5310
- 2x Xeon 1.60 GHz
- 4 GB RAM ECC 1.66 MHz
- RAID KEY SAS LSI
- 3 discos 160 GB
- Fuente de alimentación redundante

### 3.2. Seguridad del servidor

El servidor alojado por TESI dispone de las medidas de seguridad típicas de un servidor web, a saber:

- Denegación de todas las conexiones vía firewall excepto las que se realizan al servidor web (puerto 80), DNS (udp 53) y ssh (tcp 22).
- Firewall basado en estados. No se tienen abiertos tampoco los puertos de usuario (1025-65535) como en cortafuegos menos potentes. Se dispone de denegación predeterminada además de una regla de denegación específica por tabla (doble seguridad), por lo que es impensable un error en la configuración que deje abiertos puertos no intencionadamente. Dicho firewall, a su vez, cuenta con controles especiales para situaciones que no deberían de suceder, ciertos tipos de ataque comunes y paquetes incorrectos, anómalos o provenientes de direcciones de red que no deberían de utilizarse (direcciones de broadcast, reservadas o que no cumplan la especificación del protocolo IP).
- Seguridad secundaria vía ACLs en algunos servicios y mediante la utilización de TCP - Wrappers.
- Servidor web lo tenemos actualizado mediante las políticas de seguridad de Debian, de manera que cualquier vulnerabilidad de seguridad que se descubriera es reparada en la siguiente actualización. Las vulnerabilidades de seguridad del software servidor web Apache se suelen dar (al menos en los últimos años) en servicios que actualmente no están activados en la máquina, por lo que el nivel de seguridad es muy alto. Además el apache se ejecuta con un usuario sin privilegios, por lo que no se pueden ni modificar los ficheros de la web utilizando una posible vulnerabilidad.
- DNS muy limitado y ejecutado por un usuario sin privilegios, por lo que, incluso atacándolo con éxito, lo único que se podría hacer es detener el servicio DNS.
- Las conexiones SSH utilizan encriptación de 1024 bits, y la clave negociada tiene una duración muy breve, por lo que no supone un peligro. Ni siquiera es posible interceptar datos de la conexión con un ataque "*man in the middle*", puesto que la clave de sesión es muy larga y se renegocia constantemente.
- Servicio SSH solo utiliza el usuario administrador en determinados trozos de código para los cuales es imprescindible, como la apertura del puerto 22 (por ser menor de 1024). El resto del código se ejecuta como usuario restringido.
- Existen muy pocas cuentas de usuario válidas para el servicio SSH, además de estar desactivada para este servicio la cuenta de administrador. Si se intenta hacer un ataque a fuerza bruta se produce un tiempo de espera considerable entre intentos, por lo que no se puede realizar dicho ataque con éxito. Suponiendo que se acertara la contraseña a la primera, nos encontramos en un sistema que no nos deja hacer prácticamente nada, y requeriríamos un ataque a la cuenta de administrador, muy difícil

## CONDICIONES DE ALOJAMIENTO DE LA APLICACIÓN GANDIA INTEGRADA EN EL SERVIDOR DE **TESI** S.L.

debido a los pocos servicios que corren en la máquina, además del almacenamiento de las contraseñas en el fichero shadow, no accesible para usuarios corrientes.

- La base de datos tiene su sistema interno de seguridad, que añade un impedimento más al acceso a los datos. Se permiten conexiones directas a la base de datos pero solo desde las direcciones IP de Tesi o Eurogarán.
- Seguridad extra en las conexiones salientes (desde la propia máquina), solo permitiendo conectar desde la misma por puertos 22 (ssh), 25 (smtp, envío de correo), 53 (DNS), 80 (web, para actualizaciones de sistema), 953 (control de servidor de nombres) y 110 (POP3).
- Puesto que se dispone de un ancho de banda de seguridad de 10 mbit/s, un ataque de denegación de servicio se hace también muy complicado, además de tener un impacto mínimo sobre la plataforma.
- Seguridad básica de Linux, en estado muy maduro, reforzada en distribuciones Debian utilizadas.
- Por último, la aplicación Gandia Integra mantiene una seguridad básica con autenticación de usuarios con claves encriptadas (login y password) y niveles de acceso diferenciados a personas.

### **3.3. Control de tráfico**

La solución seleccionada por TESI es la de no limitar el ancho de banda que es dirigido a clientes con picos de tráfico y que deseen ofrecer el mismo nivel de servicio en todo momento, sin limitar su ancho de banda. **EUROVIA** absorberá los picos de tráfico y facturará al *Cliente* por el consumo medio de tráfico mensual.

### **3.4. Acceso a los servidores**

#### **3.4.1. Acceso Físico**

Acceda a nuestro Data Center cuando lo necesite con la autorización pertinente por parte de **EUROVIA** y **TESI**.

#### **3.4.2. Acceso remoto**

Acceso remoto por red IP: VPN directo, RTB, RDSI, ADSL, ATM / Frame Relay, punto a punto, radio enlace, LMDS, etc.

### **3.5. Operación y administración**

Nuestro servicio de **Colocation** ofrece una amplia gama de posibilidades que abarca desde una operación básica que incluye reinicio de servidores, soporte de backup y chequeos externos de los equipos, hasta una administración total en función del hardware y software utilizados.

### **3.6. Monitorización**

#### **3.6.1. Monitorización externa**

Vigila el estado de la red y de su máquina (servicios Web, FTP, IP, etc.).

#### **3.6.2. Monitorización interna**

**EUROVIA** puede gestionar la instalación de agentes de vigilancia internos que permitan visualizar en todo momento el estado de sus sistemas y aplicaciones.

## CONDICIONES DE ALOJAMIENTO DE LA APLICACIÓN GANDIA INTEGRADA EN EL SERVIDOR DE **TESI**S.L.

### ***3.7.Backup***

Diariamente y de forma automática y transparente a los usuarios de las aplicaciones, se realizan copias de seguridad de las bases de datos de los diferentes clientes y estudios alojados en el sistema. De forma periódica, las copias de seguridad son remitidas por ssh a un servidor externo al Data Center.

### ***3.8.Control eléctrico, de temperatura y de humedad***

Entorno controlado preparado para el alojamiento de equipos de telecomunicaciones. El potencial eléctrico por metro cuadrado es de 400 vatios. Proporciona redundancia N+1. Disponemos de dos generadores diesel de backup conectados a un transfer switch (ATS) que se pone en funcionamiento de forma automática a los 30 segundos de la caída eléctrica. La temperatura se mantiene en la franja de los 18 y los 25° C. La humedad relativa se mantiene entre el 10 y el 80%.

### ***3.9.Protección contra incendios***

Los racks están equipados con sistemas de detección de humo como primera línea de defensa en caso de incendio.

### ***3.10.Seguridad***

La seguridad es tan importante para nosotros como lo es para usted. Por ello, todas las instalaciones del Data Center de alojamiento han implementado medidas para proteger sus activos. Para ello se contempla:

- El control de acceso seguro 24x7
- Personal de seguridad 24x7
- Vigilancia de sala a través de cámaras CCTV
- Servicios de Monitorización, Operación y Soporte 24x7

## 4. Calidad del servicio

### 4.1. SLA (Service Level Agreement)

Un SLA (Service Level Agreement) representa un contrato entre **EUROVIA** y el *Cliente* que define los términos de responsabilidad de **EUROVIA** hacia el *Cliente* y el tipo y extensión de la penalización en caso de incumplimiento. Los niveles de disponibilidad y de penalizaciones se calculan de forma mensual y de manera individualizada para cada *Cliente*. Las disponibilidades, así como las penalizaciones, se muestran en %; las disponibilidades definen el % del servicio y las penalizaciones se refieren al % de descuento a realizar, de forma automática, en la factura correspondiente al mes siguiente. La disponibilidad se calcula de la siguiente forma  $\text{Tiempo periodo} - \text{Tiempo sin servicio} \times 100 / \text{Tiempo periodo}$  Donde "Tiempo sin servicio" es el periodo durante el que, por cualquier causa, no existe conectividad desde el router del centro de datos hasta la boca LAN asignada a la máquina del *Cliente*. Quedan excluidos del cálculo los tiempos coincidentes con los periodos de inactividad planificados, que son ventanas programadas para la realización de actividades que tendrán como objetivo el mantenimiento de la disponibilidad acordada. Los tiempos de inactividad planificados estarán predefinidos por **EUROVIA** y serán avisados con al menos 48 horas de anticipación, efectuándose en el horario que menor impacto tenga para el *Cliente*, siendo el número de paradas realizadas al año no superior a 6. Quedarán también excluidas de este cálculo las interrupciones del servicio que pudieran producirse por causas imputables al *Cliente*, así como aquellas debidas a causas de fuerza mayor y desastres naturales.

### 4.2. Disponibilidad de Red

**EUROVIA** garantiza una disponibilidad del 100 % de la Red, aplicando la siguiente tabla de penalizaciones en caso de incumplimiento.

Disponibilidad de Red	
% Disponibilidad	% Penalización
100,00%	SLA
99,90%	5%
99,80%	10%
99,70%	15%

### 3.3. Alimentación ininterrumpida

**EUROVIA** garantiza una disponibilidad del 100 % en el suministro eléctrico, aplicando la siguiente tabla de penalizaciones en caso de incumplimiento.

Alimentación ininterrumpida	
% Disponibilidad	% Penalización
100,00%	SLA
99,95%	5%
99,85%	10%
99,75%	15%
99,65%	20%

CONDICIONES DE ALOJAMIENTO DE LA APLICACIÓN GANDIA INTEGRADA EN EL  
SERVIDOR DE **TESI** S.L.

99,55%	25%
99,45%	30%
99,35%	35%
99,25%	40%
99,15%	45%
99,05%	50%

**4.3. Condiciones generales de prestación**

Durante la fase de prestación del servicio estará a disposición del *Cliente* un número de teléfono del Help Desk de **TESI** y de éste con **EUROVIA**, operativo en horario de oficina (9 a 14h y de 16 a 19h). Para días festivos y horarios diferentes a los de oficina se facilitarán una serie de posibilidades de atención que serán presupuestadas de forma individual. Cuando se detecte un problema que afecta al buen funcionamiento del servicio, bien por aviso de TESI o bien por los procedimientos de supervisión que forman parte de la gestión propia del servicio, desde ese momento se desencadenan las actuaciones previstas para el tratamiento y resolución de incidencias. A través del Protocolo de Mantenimiento que deberá ser consensuado por ambas partes, se establecerán todas las particularidades que se consideren necesarias, así como los mecanismos concretos de notificación de incidencias a las personas de contacto.