Servicio de administración, supervisión de seguridad y mantenimiento de servidores LINUX

asplhosting.com

1.

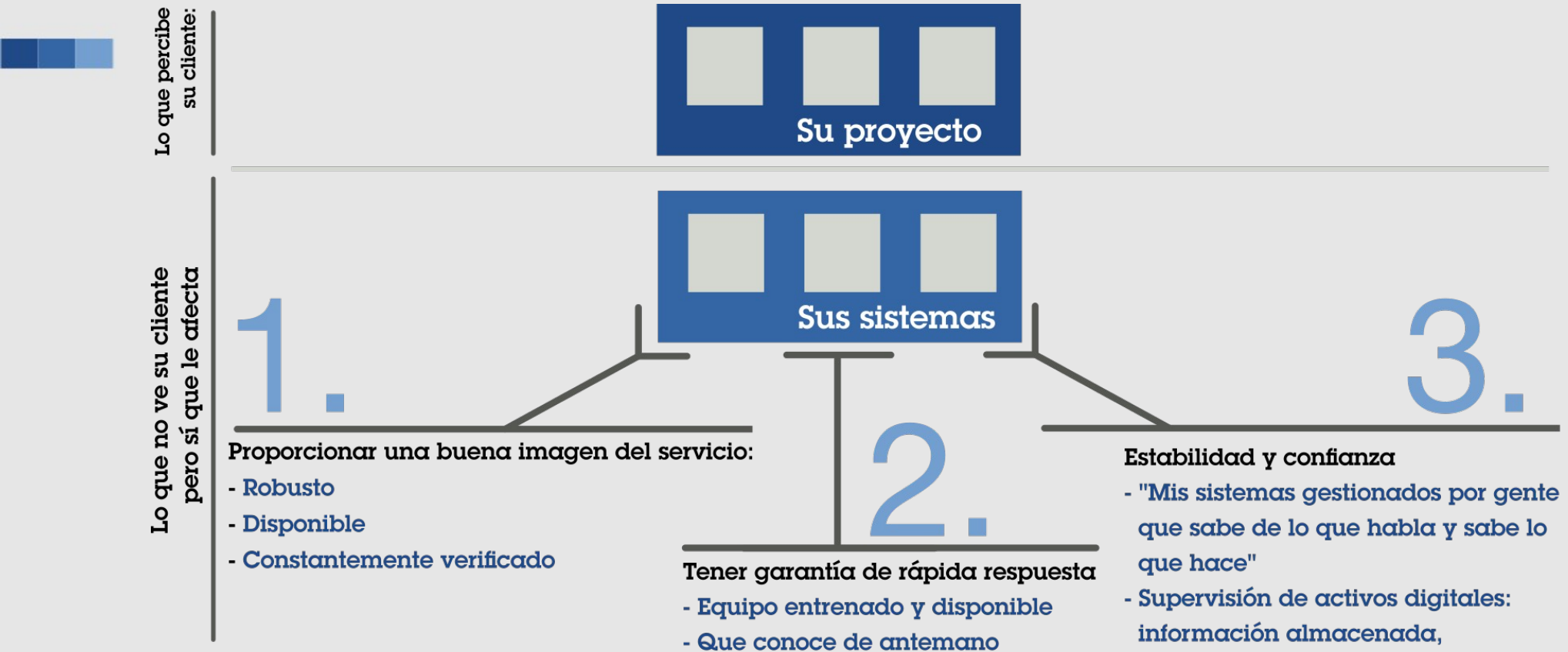
Qué valor aportamos:

Nuestro enfoque para la administración de sistemas Linux

Más que un servicio de administración

un grupo de expertos, una empresa y una cultura diseñada para mantener el sistema disponible y protegido en todas sus facetas

Servicio de administración, supervisión de seguridad y mantenimiento LINUX



La tranquilidad de estar cubierto todo el año

Soporte 24/7 BEST Effort con escalado interno siempre disponible

2.

Quienes somos y cómo trabajamos:

el equipo y las herramientas

Somos especialistas en administración y supervisión de seguridad de sistemas Linux

- ASPL fundada en el 2000 (20 años de exp. LINUX)

- Desarrollamos nuestras propias herramientas de administración de sistemas, comunicación segura, protocolos de comunicación

Core-Admin:

Plataforma de administración avanzada

https://core-admin.com

Valvula:

Servidor Open Source de políticas para postifx

https://aspl.es/valvula

noPoll:

Implementación Open Source WebSocket RFC6455

https://aspl.es/nopoll

Su proyecto: ¿sólo máquinas o es algo más?

Le presentamos nuestro **enfoque Cloud 360º**

Equipo entrenado y en constante formación interna

- Revisión de papers, artículos de seguridad, seguimiento de notificaciones DSA, Bugtrack..

- Formación continua del equipo técnico.

Varios niveles de escalado: siempre disponibles

- Equipo técnico dedicado a la administración y supervisión de sistemas:

  - **Ingenieros de sistemas senior** (20 años de experiencia)
  - **Ingenieros técnicos de sistemas senior** (8 años de experiencia)
  - **Técnicos de sistemas senior** (10 años de experiencia)
  - **Técnicos de sistemas junior** (menos de 3 años de experiencia)

Estamos especializados en plataforma **LINUX**

- Servicios Cloud para **distribuidores**, **empresas de desarrollo** y **marketing**

  (servidores cloud, servidores de correo, servidores para apps y webs, almacenamiento..)

- Servicio de administración, supervisión de seguridad

  (supervisión de sistemas linux)

- Cloud IoT (https://myqtthub.com):

  (nuestra propuesta de servicio basado en MQTT)

Capacitación técnica

3.

Infraestructura propia:

Despliegue de datacenter
Dónde estamos

Disponemos de infraestructura propia

- Datacenter Interxion Madrid
  (uno de los más prestigiosos)
- Racks totalmente gestionados por nuestro equipo
- Supervisión de red gestionada por ASPLhosting
  (somos RIPE LIR AS206102, con varios prefijos /22 publicados por BGP)
- Varios enlaces primarios replicados Gbps con operadores premium datacenter
  (Level3, Cogent, DE-CIX ...)

Infraestructura propio: nuestros fundamentos

- Despliegue usando **Nova, Neutron, Cinder, Glance...**
  (sistema cluster opensource para servidores cloud)
- Backend **Ceph**
  (almacenamiento de alto rendimiento SSD, triple replicación en tiempo real)
- Máquinas con gran capacidad I/O, óptimamente localizadas en Madrid
  (ideal para clientes ADSL telefónica, Jazztel, MasMóvil y similares...)

Protección de datos, **GDPR**

- Localización **Madrid (España)**

- Sin transferencia internacional de los datos

- Equipo, infraestructura y empresa: **cumplimiento normativa protección de datos**

- **Cuidamos tus datos y privacidad**

4.

En qué consiste nuestro servicio y hasta donde llegamos

Realizamos supervisión de todos los sistemas

- Core-Admin: plataforma de administración, supervisión, mantenimiento y seguimiento

- El promedio diario de ataques bloqueados gracias a Core-Admin es de:

20.000 Logins no autorizados (Wordpress, IMAP, Apps, ssh)	**7.000** Consultas no autorizadas (Remote command, Remote shell exec..)	**4.000** Incidentes de Inyección SQL	**3.000** Ataques SYN FLOOD o desbordamiento

Servicio proactivo: anticiparse es la clave

La constante supervisión que aplicamos, nos permite en muchos casos **anticiparnos al problema,** proporcionando un soporte superior.

- **Autoreparación**
- **Autodefensa**
- **Autodiagnóstico** constante
- **Core-Admin**

Trazado y supervisión de acceso a la máquina

Verificación constante de los accesos a la máquina:

- Registro y verificación de accesos ssh (ssh_login)
- Registro y notificación de aperturas de terminal (root_terminal_opened)

Asegurar estabilidad y coherencia interna de la máquina

- Trazado y corrección de la **hora del sistema**

- Seguimiento de configuración interna de hostname, ips asociadas, disponibilidad y reputación de las mismas.

Supervisar y asegurar los parámetros operativos del sistema

- **Memoria** disponible (configuración y rendimiento de la swap)
- Disponibilidad del **disco** (espacio suficiente, funcionamiento, signos de fallo del disco, comprobación estado de las controladoras, indicadores S.M.A.R.T.)
- Disponibilidad de **entrada/salida** al disco
- Supervisión de **carga excesiva** de CPU o I/O (entrada/salida)
- Revisión y supervisión de **kernel traces**
- Seguimiento de **OOM-Killer** (sistema sin memoria)

Supervisar y asegurar parámetros de ejecución del sistema

- Detectamos y trazamos **procesos sospechosos**
- **Puertos** que no deberían estar en uso
- Binarios con **variables de entorno no autorizadas**
- **Crons** de usuario ejecutados como root
- **Configuraciones problemáticas** (cerrado de /proc, sudo)

Supervisión disponibilidad IP y su reputación

- Comprobamos que todas las **IPS** en uso estén **limpias** (**RBLs**)
- Aseguramos que toda IP en ejecución está declarada
- Comprobamos que IP declaradas estén en ejecución

Supervisión integridad **certificados** y validez

- Comprobamos que todos los **certificados** SSL/TLS no estén caducados

- Que tengan una configuración correcta (permisos, cadena de certificados correcta, fallos de formato, duplicación de entradas...)

Supervisión del estado de la **copia de seguridad**

- Nos aseguramos de que la **copia de seguridad funcione correctamente** (revisión diaria)

- Fuera de datacenter ASPL, necesitamos hardware independiente donde almacenar la copia.

- Nos encargamos de configurar el sistema, retenciones y rotaciones de volumen para **disponer de los últimos 30 días de copia**.

5.

Cómo gestionamos los hackings y las amenazas de ciberseguridad

Respuesta ante **hackings**: amenazas habituales

- Equipo, cultura, formación y herramientas para responder a las amenazas de **ciberseguridad** actuales:

  - **Modificación no autorizada** de código (hacking php, hacking shell..)
  - **Ejecución** de procesos **no autorizados**
  - **Suplantación de identidad** SMTP (robo de contraseñas de correo)
  - **Inyección SQL** / remote command execution (subvertir el funcionamiento de la APP)
  - Desbordamiento de la APP por **exceso de tráfico** anómalo

Protocolo de respuesta ante **hackings**

En caso de presentarse un **incidente de ciberseguridad**:

- Medidas automatizadas o manuales de bloqueo o **mitigación**

- Generación de **informe al cliente** explicando las **medidas** adoptadas y las medidas que el cliente debe adoptar

- Realimentación de incidente para **resistir mejor** en siguiente ocasión (automatización, reglas de bloqueo IP, cierre de puertos, cierre de urls..)

Ciberseguridad, backups y supervisión

"**Supervisar** las máquinas, tenerlas **trazadas** y controladas es clave para **controlar la información** que hay en ellas, la imagen de servicio que proporcionan, pero sobre todo, proporcionar **certeza al cliente**: sistemas seguros como **cultura para la continuidad de negocio**"

6. Tareas habituales y soporte al desarrollo, despliegue de aplicaciones y migraciones

Asistencia al desarrollo y programación

Actuamos como el **equipo de administración** para el **equipo de desarrollo**:

- Desplegamos **paquetes**, **configuraciones**

- Revisamos porqué puede estar fallando una aplicación que estaba funcionando y en producción

- Hacemos recomendaciones de uso

Casos habituales de asistencia al desarrollo

- **Despliegue de paquetes y configuraciones**: “Necesitamos desplegar la base de datos X, estos paquetes Y con versiones Z y W, configurados de cierto modo”.

- **Revisión de fallos en producción**: “Nos ha dejado de un funcionar una aplicación, ¿podéis revisarlo para ver qué puede estar pasando?”

    - Revisión de logs
    - Revisión de configuraciones

- **Recomendaciones de uso**: “Queremos desplegar este software, ¿es posible en nuestras máquinas? ¿os podéis en encargar?”

asplhosting.com – aspl.es – myqtthub.com

ASPL – Advanced Software Production Line, S.L.
B-82827932
Av. Juan Carlos I°13, 2°C (Torre garena)
Alcalá de Henares (28806) Madrid