

NORMATIVA DEL SERVICIO DE ALOJAMIENTO DE INFRAESTRUCTURA DE LA UNIVERSIDAD DE SEVILLA

Características generales.-

La Universidad de Sevilla (US), a través del Servicio de Informática y Comunicaciones (SIC), pone a disposición del Personal Docente e Investigador y de los Servicios y Unidades Administrativas de la Universidad de Sevilla el Servicio de Alojamiento de Infraestructura, para facilitar las tareas relacionadas directamente con investigación (nunca para docencia) y la prestación de servicios. A diferencia de un servidor tradicional, el responsable podrá acceder a un espacio virtual dedicado, que podrá escalarse de forma casi instantánea, dependiendo de las necesidades de hardware.

De esta manera, se podrá albergar una amplia gama de aplicaciones de alto nivel utilizando los sistemas operativos Linux o Windows en sus últimas versiones.

Este servicio se ofrece en modo IaaS y PaaS:

IaaS: El solicitante dispondrá de una máquina virtual con sistema operativo Windows o Linux en el entorno de virtualización del área de infraestructuras del SIC, monitorizado, en alta disponibilidad y con copias de seguridad. Se facilitarán las credenciales de administración para que se pueda realizar la correcta administración del sistema, que siempre recaerá sobre el propio solicitante o la persona/empresa en quien delegue.

PaaS: A través de este modo de servicio, el solicitante podrá disponer de una base de datos Oracle o MySQL para su uso y necesidades específicas. Se facilitarán las credenciales para la administración de la citada base de datos. Las labores de monitorización y copias de seguridad de la misma, las realizará el área de infraestructuras del SIC.

Con el fin de asegurar la calidad de servicio, la solución permite adaptar la capacidad de cada uno de los principales dispositivos virtuales -almacenamiento en disco, procesador, memoria y conectividad- según las necesidades particulares, independientemente del sistema operativo elegido.

Características Técnicas:

1. Diseños a medida:

- Máquina Virtual básica con sistema operativo windows o linux (IaaS).

2. Hasta 4 procesadores x64

3. Conectividad a Internet.

4. Arquitectura en Alta Disponibilidad sin necesidad de duplicar hardware gracias a la tecnología VMware HA®.

Operativa de funcionamiento.-

La máquina virtual con las características solicitadas se pondrá a disposición del responsable en el plazo de una semana, siempre y cuando, éste haya cumplimentado todos los requisitos que se le hayan solicitado desde el Servicio de Informática y Comunicaciones.

La operativa de puesta en marcha de la infraestructura solicitada será la siguiente:

Se creará una máquina virtual con los requerimientos señalados y se pondrá a disposición del responsable tanto los accesos a la misma como las credenciales para administrarla.

Desde ese momento la responsabilidad del sistema recae directamente en la persona que ha solicitado el servicio y estará obligado a gestionar el mismo atendiendo al conjunto de buenas prácticas que se detallan en este documento.

Las máquinas apagadas se borrarán pasado un mes. El responsable, podrá solicitar durante ese mes una copia de la máquina virtual, facilitando al SIC un soporte para depositarla.

Condiciones de Uso del software a instalar.-

Tanto los sistemas Operativos como los programas específicos a instalar serán responsabilidad del peticionario del Servicio, debiendo contar los mismos con licencia para su uso (ya sea en modo software libre, freeware, software comercial adquirido, o cualquier tipo de licencia que faculte su uso al peticionario).

El peticionario puede dirigirse al SIC a la dirección de correo equipainfor@us.es para solicitar asesoramiento de software o realizar la adquisición de sistemas operativos (Windows / Linux RedHat) o programas específicos a través de acuerdos establecidos.

Servicios prestados.

1. Servicios de consultoría.

El SIC realizará labores de consultoría de sistemas para los usuarios del servicio que así lo soliciten. Con esto se pretende ayudar a definir el entorno óptimo para las aplicaciones o servicios en hosting.

2. Servicios de Administración y mantenimiento de los sistemas.

En el caso de servicios IaaS, esta responsabilidad recaerá sobre el responsable del servicio.

Es responsabilidad del SIC la administración de la infraestructura hardware que sostiene este servicio.

3. Servicio de copias de seguridad.

Se realizarán copias de seguridad semanalmente de todas las máquinas virtuales asociadas al servicio de hosting.

El responsable podrá solicitar una recuperación del sistema completo pero nunca se recuperarán ficheros o carpetas por separado.

Se mantendrán copias de seguridad por un periodo de 21 días y pasado ese tiempo, se irá borrando la información relativa a las mismas.

4. Servicio de Monitorización de todos los sistemas integrantes de la plataforma de hosting.

El SIC mantendrá sistemas de monitorización de todas las máquinas virtuales integrantes del servicio de hosting, así como de las aplicaciones críticas dentro de estos nodos.

Los responsables del hosting recibirán por correo notificaciones de eventos al igual que los administradores del SIC.

Igualmente se monitorizará toda la infraestructura que soporta el servicio de hosting.

5. Servicios de seguridad perimetral.

El SIC se hace responsable del correcto funcionamiento de accesos a los

sistemas virtualizados, así como de la seguridad perimetral de los mismos.

Se permitirán los accesos sólo y exclusivamente a los servicios que sean estrictamente necesarios y a ningún otro.

6. Servicios de conexión a través de VPN.

El responsable o la persona que él decida a tal efecto, tendrá la posibilidad de trabajar en remoto a través de una VPN que el SIC pondrá a su disposición.

7. Lista de distribución.

Existe una lista de distribución autogestionable consultahosting@listas.us.es (que mantendrá y administrará el SIC) donde estarán dados de alta todos y cada uno de los responsables que hayan solicitado un servicio de hosting, para facilitar así cualquier incidencia o comunicación que haya que hacer al respecto.

Contenidos. Denegación o baja de los servicios.-

Los servicios de hosting deben ser utilizados exclusivamente con fines lícitos.

Queda estrictamente prohibido el uso de cualquier servicio que viole cualquier ley local, nacional o internacional.

No se podrá divulgar o transmitir información ilegal, abusiva, difamatoria, racista, ofensiva, o cualquier otro tipo de información susceptible de objeción, ya sea mediante fotografías, textos, banners publicitarios o enlaces a páginas externas, así como publicar, transmitir, reproducir, distribuir o explotar cualquier información o software que contenga virus o cualquier otro componente dañino, software u otro material que no sea original (pirata), infringir derechos de propiedad intelectual, publicar o facilitar material o recursos sobre hacking, cracking, cualquier otra información que el SIC considere inapropiada.

Cualquier uso del sistema para fines ilícitos autorizará al SIC a suspender los servicios solicitados sin previo aviso.

El SIC se reserva el derecho a denegar o cancelar los servicios solicitados, con o sin notificación previa, si se incurre en cualquier conducta o actividad que se considere abuso o violación de alguno de los términos, normas y condiciones aquí expuestas.

Conjunto de buenas prácticas a la hora de administrar un

sistema.-

1. El Sistema Operativo debe mantenerse en todo momento actualizado y al último nivel de parches disponibles para el mismo, con el objeto de que quede exento ante cualquier vulnerabilidad que pudiera presentar el sistema.
2. Las aplicaciones instaladas en el servidor deben mantenerse en todo momento actualizadas en las últimas versiones estables disponibles, con el objetivo que queden exentas de cualquier vulnerabilidad que pudieran presentar.
3. El administrador del sistema IaaS debe estar dado de alta en las listas de distribución relacionadas con el sistema operativo que gestiona, así como en las de las aplicaciones que tenga instaladas en el sistema. De esta manera, estará permanentemente informado de las actualizaciones disponibles, así como de las posibles vulnerabilidades de seguridad que se pudieran presentar en cada momento en su sistema y/o aplicaciones instaladas¹.
4. Las contraseñas utilizadas en el sistema IaaS deben ser claves fuertes para impedir así el acceso al sistema utilizando mecanismos reiterativos.
5. El mantenimiento y revisión de los ficheros de logs de forma periódica constituyen una buena práctica para gestionar correctamente un sistema y así estar en todo momento informado de los accesos y actividad en el mismo.
6. Es recomendable seguir el conjunto de buenas prácticas recomendadas por los distintos fabricantes², tanto de sistema operativo como de las distintas aplicaciones que se encuentren instaladas
7. Seguir el principio de “mínimo privilegio”. Las aplicaciones deben contar con la cantidad mínima de permisos para ejecutar su tarea. A su vez, se deben desactivar todos aquellos servicios innecesarios así como desinstalar todo aquel software que no se vaya a utilizar.

¹Ejemplos de listas de distribución

<http://www.redhat.com/mailman/listinfo/rhsa-announce>

<http://lists.centos.org/mailman/listinfo/centos-announce>

[https://profile.microsoft.com/RegSysProfileCenter/subscriptionwizard.aspx?wizid=5a2a311b-5189-4c9b-](https://profile.microsoft.com/RegSysProfileCenter/subscriptionwizard.aspx?wizid=5a2a311b-5189-4c9b-9f1a-d5e913a26c2e&lcid=1033)

[9f1a-d5e913a26c2e&lcid=1033](https://profile.microsoft.com/RegSysProfileCenter/subscriptionwizard.aspx?wizid=5a2a311b-5189-4c9b-9f1a-d5e913a26c2e&lcid=1033)

² En el caso de Red Hat o Microsoft

[https://access.redhat.com/knowledge/docs/en-](https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/index.html)

[US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/index.html](https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/index.html)

<http://technet.microsoft.com/en-us/library/ff817650%28v=ws.10%29.aspx>

8. En lo posible, emplear protocolos seguros de acceso a la información (ej: sftp en vez de ftp, https en vez de http) y en caso de almacenar información sensible (ej: información médica o personal), cifrar adecuadamente la misma para que en caso de un posible compromiso dicha información no esté accesible para el atacante.

Medidas a tomar ante el incumplimiento de las obligaciones.-

El SIC periódicamente revisará las actualizaciones pendientes de los sistemas y enviará un correo a la lista de distribución consultahosting@listas.us.es, donde están todos los responsables de los servicios de hosting ofrecidos, indicando un periodo de actualización de sistemas. Pasados el plazo establecido de actualización, y en función de la gravedad de la misma, el SIC se reserva el derecho a dejar de prestar servicio o cancelar temporalmente un sistema comprometido o altamente vulnerable.

Con estas medidas preventivas el SIC pretende proteger y no comprometer el resto de servidores de hosting dado que al estar todos en la misma subred las posibilidades de ataques una vez que se ha producido el primero son mucho mayores.

Soporte.-

El soporte técnico se realizará a través del Servicio de Operaciones y Sistemas (SOS) vía telefónica (954554444), correo electrónico (sos@us.es) o el formulario vía web dedicado a tal efecto (<https://sicremedy.us.es/arsys>). APLICACIONES –APOYO A LA DOCENCIA E INVESTIGACION - HOSPEDAJE DE SOFTWARE – INCIDENCIAS CON HOSPEDAJE DE SOFTWARE.