Requerimientos técnicos de los sitios webs para el hospedaje:

- Los sitios deben estar desarrollados en versiones compatibles con las que se relacionan:

Plataforma UNIX:	**Plataforma Windows:**	**Base de Datos:** (independiente de la tecnología de páginas Webs)
Apache 2.4.6 PHP 7.2.10 PHP 5.6.25 Tomcat 7.0.54 Java 1.8.5 JavaScript Memcache 1.4.15 Redis 3.2.4 Postfix 2.10.1 (only localhost relay) ModSecurity 2.9.0 (habilitado) Selinux 3.13.1 (habilitado)	IIS 6.0 ASP 1.0 Framework ASP.NET 1.0 a 4.0 JavaScript VBScript IIS SMTP (only localhost relay) Componentes: aspSmartUpload 3.0 URLScan 3.1	MariaDB 10.0.20 (MySQL 5.6) PostgreSQL 9.4.6 MSSQL 2005 Access 2000+

- Los software para gestión de contenidos (CMS) utilizados por los clientes para desarrollar sus sitios deben estar en correspondencia con las versiones de lenguajes de programación que se soportan.
- En la plataforma de hospedaje web compartido corre PHP en modo seguro; por lo que se encuentran deshabilitadas algunas funciones que pueden comprometer la seguridad del sitio y permitirle a posibles atacantes inyectar comandos o ejecutar script desde sus sitios web al servidor, por ejemplo, pueden estar deshabilitan las funciones: cURL, proc_open y fsockopen. Algunas de estas funciones se deshabilitan como complemento de la restricción de acceso desde los servidores web hacia redes externas a la plataforma."
- Adicionalmente, a excepción de la mensajería, se inhabilita la realización de pasarelas de intercambios de datos y otros similares que faciliten la salida hacia otros servicios ubicados fuera del servidor donde se hospeda el sitio, que impliquen la interacción de este con otros sistemas y aplicaciones externos al servicio.
- En todos los casos siempre es aconsejable referirse al informe de compatibilidad que anuncia el fabricante. En este aspecto es importante tener presente que por lo general en las tecnologías Open Source y Software Libre se garantiza compatibilidad solamente entre diferentes releases dentro de una misma versión del núcleo. Por ejemplo, el fabricante garantiza compatibilidad entre todos los releases dentro de PHP5, no así entre PHP4, PHP5 o PHP7 ya que son versiones de núcleo diferente. Lo mismo sucede con MySQL o PostgreSQL.
- En los servidores web Apache corre el módulo de seguridad ModSecurity y la herramienta SELinux en modo enforcing, así como un módulo AntiDOS para asegurar el servicio y los sitios contra ataques e intrusiones malintencionadas. Es preciso que los sitios estén diseñados con los requerimientos establecidos para que puedan funcionar adecuadamente en un ambiente seguro.
- Se sugiere a clientes con sitios PHP Linux no usar funciones PHP inseguras y usar el módulo rewrite del apache y activar URLs limpias (amigables) y

mantener actualizados sus sitios para evitar problemas con el módulo de seguridad. El ModSecurity deniega las URL sucias que le resultan sospechosas.

- Se recomienda habilitar el uso de memcache o redis en la configuración del sitio para mejorar el rendimiento. Algunos tipos de CMS, LMS o Framework traen incorporada una opción para habilitar el uso de estas funcionalidades.
- En los servidores Web IIS se instala la herramienta URLScan para filtrar las cadenas de caracteres que se pasan al sitio a través de la URL y otras sentencias en el código de los mismos.

Otros aspectos a tener en cuenta:

- Las cuotas de espacio en disco se miden por el espacio real que ocupe el sitio y su base de datos una vez montado en el servidor en producción. Por lo que se debe tener en cuenta que los volúmenes de datos difieren según el sistema de archivos sobre el que se encuentren. En nuestro caso los sistemas de archivo utilizados son CIFS sobre NTFS para el hospedaje de sitios en Plataforma Windows y NFS sobre XFS para los de Plataforma UNIX, por lo que los valores obtenidos por el cliente en sistema de archivos Windows NTFS, Linux ext3 o ext4 u otro, durante la etapa de desarrollo, al calcular el peso del sitio, no es el espacio real que ocuparía una vez que se hospede en nuestros servidores. Cuando el cliente alcanza el límite fijado para su cuota de espacio en disco no podrá continuar con las actualizaciones por ninguna de las vías habilitadas (FTP, HTTP).
- Se ofrece acceso FTP Seguro para actualizar los sitios solo desde redes nacionales, con autentificación por SSL, por lo que el programa cliente FTP debe permitir protocolo SSL en la autentificación. Recomendamos Filezilla usando protocolo “FTPES –Ftp sobre TLS/SSL explícito”.
- Estadísticas de visitas al sitio disponibles en servicio web de utilidades.
- Salva semanal con 30 días de retención del sitio y la base de datos.
- HTML, preferiblemente se hospeda en la plataforma UNIX, aunque se tiene en cuenta lo que el cliente solicite considerando sus perspectivas de migración a tecnología dinámica.
- Para la mensajería del sitio, puede usar como from de los mensajes que se envían desde su sitio web una cuenta de correo bajo dominios enet.cu, nauta.cu, u otro de los manejados por el servidor de correo de ETECSA. Si desea usar otro from de correo de un dominio no gestionado por ETECSA, debe habilitar un registro SPF en dicho dominio para autorizar a los servidores de correo de ETECSA a enviar la mensajería con ese from. Debe informar siempre a ETECSA el from de correo que usará para autorizarlo en la configuración del sitio.
- Si su sitio Web posee una interface de gestión de contenidos para actualizar la información y administrar el sitio y desea asegurarlos habilitando HTTPS, debe ponerse en contacto con el servicio de Asistencia de Hosting de ETECSA y entregarles las URL/Directorios susceptibles de ser protegidos bajo este mecanismo de seguridad. El certificado es autogenerado por la plataforma, por lo que solo se usará para administrar, pero si posee un certificado oficial generado por una entidad certificadora internacional para el sitio también se acepta.
- Por políticas de seguridad del servicio, desde los servidores Web de Hospedaje Web de ETECSA, está deshabilitada la resolución DNS y no se permite la salida hacia las redes externas desde este servicio, a excepción de la mensajería.

Sobre las bases de datos:

- Para sitios con más de una base de datos, estas deberán ser de la misma tecnología y versión.
- La codificación de las bases de datos y el sitio Web debe ser UTF8.
- Por políticas de seguridad no se permite administración de bases de datos a través del servidor Web donde se hospeda el sitio. Para tal fin existe un manager Web (Ej. PhpMyAdmin) en un servidor independiente con todos los requerimientos de seguridad, con acceso restringido solo para los clientes que tengan hospedada una base de datos. Solicitamos a los clientes evitar instalar PhpMyAdmin, WebAdmin u otras herramientas web para gestionar sus bases de datos dentro de la estructura del sitio.
- Atendiendo a la política anterior, no se brinda el servicio de hospedaje de bases de datos como un servicio en si mismo, sino que estas siempre deberán estar asociadas a un sitio web.
- Se recomienda usar roles de privilegios para el acceso a las bases de datos separados, tales como db_datawriter, db_datareader y dbowner.