Requerimientos técnicos de los sitios webs para el hospedaje:

Los sitios deben estar desarrollados en versiones compatibles con las tecnologías que se relacionan a continuación soportadas exclusivamente sobre sistema operativo UNIX/Linux:

1. Servidor Web Apache 2.4.6 con
   PHP (versiones 7.3.11, 7.2.10, 5.6.25)
   JavaScript (NodeJS 12.10.0, npm 6.10.3)
   Memcache 1.4.15
   Redis 3.2.4

2. Servidor Web Apache 2.4.6 con Tomcat 7.0.54
   Java 1.8.5

Base de Datos:
MariaDB 10.3.27 (MySQL 8.0)
PostgreSQL 9.4.6

Postfix 2.10.1 (only localhost relay)
ModSecurity 2.9.0 (habilitado)
Selinux 3.13.1 (habilitado)

Por criterios de diseño, optimización y rendimiento, orientados a mantener la compatibilidad funcional, los sitios cuyas páginas se basan en tecnología JAVA se separan de los que utilizan PHP en servidores diferentes.

Los softwares 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 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 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 permitirles a posibles atacantes inyectar comandos o ejecutar script desde sus sitios web al servidor. Las funciones deshabilitadas en su mayoría son las recomendadas en este enlace *https://www.php.net/manual/es/features.safe-mode.functions.php*.

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, usar el módulo rewrite del apache para activar URLs limpias (amigables) y mantener

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

Se recomienda habilitar el uso de memcached 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.

Sobre la aplicación JavaScript NodeJS:

Por las limitaciones que conlleva el servicio en el entorno compartido en cuanto a la asignación de puertos TCP por aplicación en los sitios, la aplicación JavaScript será alcanzable solamente en el entorno local mediante TCP ***localhost:puerto***. El acceso remoto sería a través de la URL del sitio ***http://www.nombresitio.[nat][co].cu/node/<mynodejsapp_dir>/***. Para evitar la necesidad de asignación de más de un puerto TCP, Ud. debe implementar todas las funcionalidades JavaScript NodeJS que requiere su sitio en una única aplicación, cumpliendo con las condiciones que se relacionan abajo. Además, debe mantener siempre el mismo directorio de trabajo y fichero inicial de carga de la aplicación para no tener que modificar la configuración inicial habilitada.

Para habilitar la aplicación en NodeJS, debe observar las siguientes premisas que debe cumplir obligatoriamente.

- ✓ El límite en cantidad de aplicaciones JavaScript NodeJS por sitio será una sola. Debe implementarla de modo que incluya todas las funcionalidades necesarias para el sitio.
- ✓ Para correr la aplicación JavaScript NodeJS se le asignará un puerto TCP, que es obligatorio, para evitar conflictos con otras aplicaciones. Tenga en cuenta que se trata de un entorno compartido.
- ✓ Configure el parámetro family de la aplicación para IPv4.
- ✓ Debe colocar su directorio de aplicación JavaScript dentro de la estructura de directorio ***htdocs/node/*** pues en la configuración del sitio se define una re-dirección de tipo ***ProxyPass /node/*** apuntando a *localhost* por el puerto TCP que le asignamos. Por ejemplo, supongamos que su aplicación se encuentra en el directorio ***mynodejsapp_dir/***. Este directorio debe estar ubicado en ***htdocs/node/<mynodejsapp_dir>/***.
- ✓ Debe informar al soporte técnico el fichero inicial de carga, por ejemplo, index.js, server.js, app.js, etc.
- ✓ Una vez que coloque su aplicación JavaScript en un directorio dentro de ***htdocs/node/***, y hayamos comprobado que ha sido configurada por el puerto TCP que le asignamos, compilaríamos la aplicación y la habilitaríamos en la plataforma web. Asegúrese de que su aplicación no contenga otros puertos configurados en diferentes ficheros.
- ✓ Cada vez que realice cambios a su aplicación JavaScript, debe informarlo al soporte técnico para que detenga el servicio y proceda a re-compilar y levantar la aplicación nuevamente.
- ✓ Preferentemente, mantener la aplicación JavaScript siempre en el mismo directorio.
- ✓ Si cambia el nombre del directorio que contiene la aplicación o el fichero inicial de carga debe informarnos pues debemos actualizarlo en la configuración de su servicio javascript nodejs, re-compilarlo y reiniciarlo.
- ✓ Implementar todas las funcionalidades JavaScript NodeJS que requiere su sitio en una única aplicación.
- ✓ No se permitirá acceso remoto por protocolo TCP a la aplicación JavaScript.

Conexión a servicios externos o de terceros:

Se permite la conexión a servicios externos o de terceros, facilitando 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, ya sean servicios nacionales (cubanos) o en Internet (fuera de Cuba), que cumplan determinadas características, entre los que se encuentran:

- ✓ Acceso a la pasarela de pago de XETID.
- ✓ Acceso a canales RSS. Sindicación de contenidos.
- ✓ Registro a través de cuentas de redes sociales.
- ✓ Acceso a repositorio de actualizaciones, extensiones y conectores de CMS y Framework más populares.

Ante la demanda de los clientes, la inclusión del acceso a nuevas APIs, canales RSS o repositorios de actualizaciones, será valorada por las áreas técnicas y comerciales correspondientes.

Los accesos a servicios externos se limitan fundamentalmente por razones de seguridad y puede darse el caso que el acceso al repositorio de algunos de los componentes no esté autorizado.

Los tipos de accesos a elementos externos autorizados no contemplan todos los tipos de componentes, pero si el cliente envía al servicio de Asistencia de Hospedaje Web 24 horas la FQDN o la URL de acceso a la página web del fabricante de cada componente que desea instalar, o a la API, se realizará el análisis correspondiente por las áreas implicadas (técnica, comercial y de seguridad). De ser factible la solicitud realizada, al no entrar en conflicto con las premisas establecidas para la seguridad y la calidad del servicio, se permitirá el acceso online desde la plataforma web.

Es importante que los clientes conozcan que autorizar el acceso al repositorio de tecnologías web, extensiones y componentes de manera online, en los casos que el componente o extensión, una vez desplegado, dependa de conexiones a servicios de terceros para su funcionamiento, no garantiza su usabilidad una vez desplegado ya que este acceso no será autorizado.

Ejemplo: Un sitio web pudiera habilitar un plugin para la seguridad antispam en los formularios web, pero este plugin realiza esta función utilizando una conexión al sitio del fabricante, o a otros, para el control mediante consultas en listas negras de diferentes compañías de seguridad. Este tipo de acceso no se autorizaría, entre otras razones porque la funcionalidad web antispam tiene muchas maneras de ser controlada mediante la habilitación de captcha, técnicas honeypot por marca de tiempo, o determinados tipos de componentes que no dependen de enlaces externos. Además, porque el módulo de seguridad de la plataforma web y el componente IDS del firewall del Centro de Datos contemplan este tipo de funcionalidad. Adicionar componentes que realicen esta tarea dependiendo de conexiones a servicios externos solo incrementaría la carga de procesamiento y congestiones de tráfico innecesarios en el servicio, que en definitiva redundarían en lentitud de la carga de los sitios, teniendo en cuenta que se trata de un entorno web compartido.

En el caso de presentar dificultades con la instalación o actualización del sitio y sus componentes de manera online, sugerimos que primero despliegue el sitio web en un entorno local y después lo suba al servidor de producción ya funcional. En segunda instancia, descargue los componentes y los despliegue manualmente.

Si se requiere habilitar el acceso al repositorio de algún tipo de componente o plugin de otro fabricante distinto, no incluido en el repositorio oficial del tipo de tecnología base de su sitio web (CMS, LMS o FrameWork), sugerimos al cliente que descargue los componentes y lo despliegue manualmente.

Otros aspectos a tener en cuenta:

- ✓ **La mensajería permitida es solo SMTP relay** desde el servidor local donde se hospeda el sitio. Para esto, 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 del Servicio de Hospedaje Web de ETECSA a enviar la mensajería con ese *from*. Debe informar siempre al soporte técnico el *from* de correo que usará para autorizarlo en la configuración del sitio.

- ✓ Se recomienda **habilitar verificación contra manipulación no humana** en todos los formularios de captación de datos, como el registro de usuarios o formularios de restablecimiento de contraseñas, formularios web, formularios de contacto, formularios de nodos y formularios de comentarios. Para esto puede usar CAPTCHA o un sistema invisible que utilice métodos *honeypot* por marca de tiempo para evitar que los robots de spam completen formularios en su sitio.

- ✓ **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 el sistema de archivos utilizado es NFS sobre XFS en una plataforma UNIX/Linux, por lo que los valores obtenidos por el cliente en sistema de archivos diferente, como Windows NTFS, Linux ext3 o ext4 u otro, durante la etapa de desarrollo al calcular el peso del sitio no será 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”. Se sugiere habilitar HTTPS SSL y realizar las actualizaciones de contenidos desde redes internacionales vía web a través de dicho protocolo.

- ✓ **Estadísticas de visitas** al sitio disponibles en servicio web de utilidades.

- ✓ **Salva semanal** del sitio y la base de datos con 30 días de retención.

- ✓ Si su sitio Web posee una **interface de gestión de contenidos** para actualizar la información y administración vía web y desea asegurarlos habilitando HTTPS, debe ponerse en contacto con el soporte técnico y entregarles las URL/Directorios susceptibles de ser protegidos bajo este mecanismo de seguridad. El certificado es autofirmado por la plataforma, por lo que solo se usará para administrar, pero si posee un certificado oficial para el sitio, generado por una entidad certificadora internacional, también se acepta.

Sobre las bases de datos:

Para sitios con más de una base de datos, estas deberán ser de la misma tecnología y versión y estar asociada al tipo de plataforma contratada, según la tabla con tecnologías disponibles por plataforma de la primera página de este documento.

La codificación de las bases de datos y el sitio web debe ser UTF8, usando preferentemente el charset utf8mb4 para la creación de las tablas. En el caso de bases MySQL, el motor de las tablas debe ser InnoDB y habilitar preferentemente el formato dinámico. Le sugerimos editar el script con las instrucciones para la creación de la estructura de la base de datos y cambiar en las instrucciones CREATE TABLE, ENGINE=MySAM por ENGINE=InnoDB, y agregar el parámetro ROW_FORMAT=DYNAMIC a cada tabla. Tener en cuenta la longitud máxima de los datos de tipo varchar respecto al charset seleccionado. Consulte estos enlaces https://mariadb.com/kb/en/troubleshooting-row-size-too-large-errors-with-innodb/, https://mariadb.com/kb/en/innodb-row-formats-overview/. Una vez hecho el cambio, podrá inyectar sus tablas en el servidor de producción.

La razón de que sea obligado el tipo de motor o ENGINE InnoDB, es que su base de datos se aloja en un esquema de servidores distribuidos en alta disponibilidad, en un cluster de MariaDB, y este requerimiento permite garantizar la integridad de las tablas en esquemas de alta disponibilidad. El motor MyISAM es más ligero, pero no permite los mecanismos de control requeridos en este esquema. Consulte también los siguientes enlaces para una mejor comprensión https://mariadb.com/kb/en/converting-tables-from-myisam-to-innodb/, https://mariadb.com/kb/en/choosing-the-right-storage-engine/.

Otro aspecto importante a tener en cuenta es que en el cluster de MariaDB todos los nodos pueden escribir datos en las tablas, es decir, se ejecuta una réplica multi-master. Imagine una situación en la que todos los nodos del clúster intentan insertar filas en la misma tabla al mismo tiempo. El resultado podría ser valores duplicados para cualquier columna que use auto_increment. Para evitar tales conflictos, el cluster incrementa los valores de las columnas en función del número de nodos del clúster. En los nodos miembros se establece el parámetro 'wsrep_auto_increment_control' en 'ON', para indicar que cambie el valor de 'auto_increment_increment' y auto_increment_offset' de MariaDB automáticamente. Esto evitará errores de 'entrada duplicada'. Se recomienda no modificar estas variables para garantizar la integridad de la réplica multi-master. Puede consultar más información al respecto en estos enlaces https://mariadb.org/auto-increments-in-galera/, https://galeracluster.com/library/kb/auto-increment-multiples.html.

Por políticas de seguridad no se permite la 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, PGAdmin, Adminer 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 sí mismo, sino que estas siempre deberán estar asociadas a un sitio web contratado.

Siempre que la aplicación web lo permita, se recomienda usar roles de privilegios para el acceso a las bases de datos, tales como db_datawriter, db_datareader y dbowner.

Sobre la habilitación del Protocolo HTTPS:

En la configuración inicial se habilita SSL a los sitios hospedados en la plataforma web usando un certificado autoafirmado por ETECSA solamente para el acceso a los directorios de administración del sitio. Debido a que el certificado es autofirmado, el cliente no podrá utilizar este para habilitar HTTPS SSL a todo el contenido del sitio. Para ello debe obtener un certificado oficial emitido por una entidad certificadora y hacerlo llegar a través del soporte del servicio.

Para cumplir lo que se establece en cuanto a garantizar la debida seguridad y el correcto funcionamiento de los sitios, los clientes deben implementar los siguientes requerimientos:

1. Se debe utilizar protocolo TLS, sólo se permiten las versiones v1.2 y v1.3., estableciendo por defecto y como protocolo principal TLS v1.3.
2. Configurar el servidor SSL/TLS de forma que seleccione adecuadamente la combinación de algoritmos criptográficos, que serán:
   - ✓ ECDHE-RSA-AES256-GCM-SHA384
   - ✓ DHE-RSA-AES256-GCM-SHA384
   - ✓ ECDHE-RSA-AES128-GCM-SHA256
   - ✓ DHE-RSA-AES128-GCM-SHA256
3. La autenticación se realizará utilizando el protcolo de acuerdo de Llaves Diffie-Hellman, generado utilizando OpenSSL v1.1.1b, con valor igual a 4096bits.
4. Habilitar la opción Forward Secrecy.
5. Deshabilitar mecanismo de renegociación de TLS, que puede ser iniciado por el cliente.
6. Deshabilitar la compresión en TLS.
7. Habilitar la persistencia en las conexiones HTTP.
8. Habilitar el uso de OCSP Stapling.
9. Hacer uso de una redirección de tipo 301 de HTTP hacia HTTPS, forzando el uso (por defecto) de HTTPS.
10. Habilitar en el servidor web la opción TLS Fallback Signaling Cipher Suite Value (SCSV).
11. Habilitar la directiva Secure en todas las cookies empleadas por la aplicación web.
12. Habilitar HSTS (HTTP Strict Transport Security). Emplear un valor de "max-age" de al menos 10886400 (18 semanas) y preferiblemente de 6 ó 12 meses ("31536000").

Le recomendamos además lo siguiente:

- ✓ La aplicación web hospedada en la plataforma web UNIX/Linux tenga habilitado el protocolo seguro HTTPS mediante una redirección completa hacia HTTPS.
- ✓ Revisar las cabeceras http que pudiera estar enviando el sitio de forma no segura y solucionar este problema cuanto antes. Al mismo tiempo le sugerimos consultar las recomendaciones de seguridad que proporcionan las siguientes herramientas de verificación en línea:
  https://letsdebug.net/ (by Alex Zorin)
  https://check-your-website.server-daten.de/ (by Jürgen Auer)
  https://whynopadlock.com/ (by LexiConn)
  https://www.ssllabs.com/ssltest/ (by Qualys)
  https://securityheaders.com/ (by Probely)

ETECSA, en la configuración del servicio, aplica la redirección de tipo 301 de HTTP a HTTPS solamente para los directorios y páginas de administración conocidos, según la tecnología de gestión de contenido web utilizado por el sitio, por lo cual, el cliente es responsable de habilitarlo para todo el sitio web.

Sobre http/2.

Para reforzar la seguridad y mejorar las prestaciones tecnológicas del protocolo HTTPS, en la plataforma de Hospedaje Web compartida se activa el protocolo http/2.

Para evitar errores que se pueden presentar al ejecutar ciertas funcionalidades de las páginas web cuando el navegador utilizado no soporta esta versión del protocolo http, se sugiere a los dueños de sitios web que habiliten HTTPS, e informar a sus usuarios que deben contar con navegadores que soporten el protocolo http/2, como Opera, Firefox o Chrome en sus versiones más actualizadas.

Sobre la obtención de Certificados SSL.

La oferta de servicio de hospedaje web no incluye certificado SSL. Nuestra empresa no está autorizada a emitir estos certificados por la autoridad competente en Cuba. Debido a regulaciones impuestas por las leyes del bloqueo económico, comercial, tecnológico y financiero de los Estados Unidos contra Cuba, no existe una entidad certificadora en nuestro país que pueda emitir certificados reconocidos por los navegadores web más populares.

El cliente debe obtener sus certificados con alguna de las entidades certificadoras internacionales. Utilizando **siempre** un canal seguro debe subirlo a la plataforma y notificar al servicio de Asistencia de Hospedaje Web 24 horas.

Se ha habilitado el directorio pki/ fuera de la estructura raíz del sitio para que el cliente deposite el certificado vía TLS/SSL por ftp. **Nunca debe enviarlo por correo electrónico.**

Para la generación de certificados SSL para su sitio con terceros, la entidad certificadora requiere verificar la autenticidad del dominio y su pertenencia. Existen varias maneras o retos para verificar el dominio:

1. Enviando un mail al dominio en este caso (@nombresitio.nat.cu).
2. DNS (CNAME), insertando un record en el registro de dominio (usualmente en CPANNEL etc).
3. HTTP/HTTPS file upload, subiendo un txt a la raíz del sitio.

La variante que podemos garantizar y sugerimos actualmente es la tercera, ***HTTP/HTPS file upload,*** y funciona perfectamente, pero para que esta variante funcione el cliente debe crear en la raíz del sitio un directorio llamado "*.well-known*", u otro nombre, algo que puede hacer vía ftp. Pero si el sitio tiene habilitado https con el certificado vencido o uno auto-firmado, o tiene habilitado filtrado IP para que sea visible solo desde determinado origen que no incluye la IP de la entidad certificadora, esta verificación no podrá funcionar.

Para realizar la generación de certificados por el método ***HTTP/HTTPS file upload*** se deben cumplir tres condiciones importantes:

1. El cliente debe crear un directorio oculto de verificación, generalmente de nombre "*.well-known*", con el punto delante y con permisos lectura para el usuario con que corre el sitio, en nuestro caso el propio usuario ftp del cliente, y colocar los ficheros con la información de validación que la entidad certificadora requiere durante la validación del dominio.
2. El sitio debe ser accesible por la entidad certificadora en el momento de la generación vía http o https. Es importante que el sitio no tenga habilitado un filtrado IP.
3. Si la verificación ocurre vía https, el certificado SSL habilitado en el sitio debe ser válido al momento de la generación del nuevo certificado, de lo contrario, el cliente debe deshabilitar https temporalmente. Es aconsejable que los clientes no esperen a que expire el certificado anterior para que puedan hacer esto vía https.

Al tratarse de un servicio de terceros, no podemos hacernos responsables si presentara alguna dificultad durante la obtención del certificado SSL. Consulte siempre la documentación del proveedor.

Cambio de contraseñas de la cuenta FTP y del usuario de Base de Datos.

Para el **cambio de contraseñas** está habilitado el sitio web del portal de utilidades del servicio, donde usted podrá actualizarla cada vez que lo desee.

En este sitio, si usted **conoce la contraseña anterior**, dispone de 5 intentos para realizar el cambio. Si agota los 5 intentos y no logra cambiar la contraseña, puede solicitar el cambio al servicio de Asistencia de Hospedaje Web 24 horas mediante correo electrónico a la dirección hosting@enet.cu.

La solicitud se aceptará si se realiza a través de la dirección de correo electrónico perteneciente al dueño del sitio web (titular del contrato), declarado como parte de los datos de contacto requeridos en el proceso de contratación, debiendo suministrar, en el cuerpo del correo, los siguientes datos, que son obligatorios:

- ✓ Nombre del sitio.
- ✓ Número de Contrato.
- ✓ Nombre y Apellidos de persona responsable del sitio (titular del contrato).

Con esta información el servicio de Asistencia de Hospedaje Web 24 horas procederá a realizar la solicitud y le informará el cambio realizado.

En el mismo sitio de utilidades puede **actualizar sus datos de contacto,** teléfono y correo electrónico, para garantizar que le lleguen las notificaciones de caducidad de contraseña a la dirección correcta.

Una vez que la **contraseña caduca** y agota los 5 intentos para obtener una nueva, **o en caso de olvido**, puede solicitar el cambio al servicio de Asistencia de Hospedaje Web 24 horas mediante correo electrónico a la dirección hosting@enet.cu. como se describe anteriormente.

Recuerde que, para una mayor seguridad, debe cambiar la contraseña cada cierto tiempo, o cuando detecte un uso inapropiado de su servicio por parte de otras personas.

Requisitos que deben tener las contraseñas de la cuenta FTP y del usuario de Base de Datos.

La contraseña debe cumplir y contener los siguientes requisitos:

- Longitud entre 8 y 15 caracteres.
- Letras minúsculas y mayúsculas.
- Caracteres numéricos y símbolos.
- No repetir las últimas 5 contraseñas.

Tiempo de caducidad.

La contraseña tiene una validez de 300 días. Si la dirección de correo electrónico aportada por el cliente es válida, le debe llegar una notificación de manera automática cuando la contraseña está próxima a caducar, una vez caducada, también se le envía la notificación que caducó la contraseña para que la actualice a través del sitio del portal utilidades del servicio.