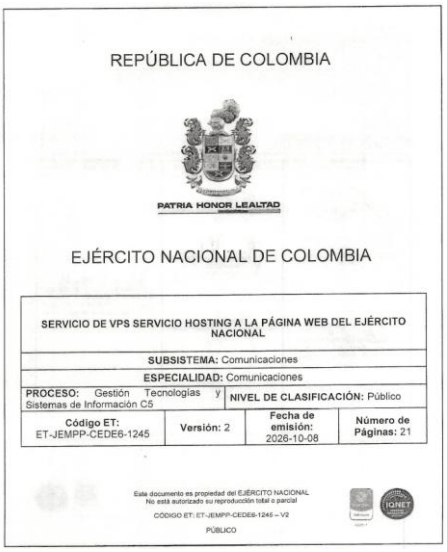
ANEXO ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

Facatativá XX de XXXXX de 2026

Las condiciones técnicas del presente proceso, se dará aplicación a la Especificación técnica "SERVICIO DE VPS SERVICIO HOSTING A LA PÁGINA WEB DEL EJÉRCITO NACIONAL" No. ET-JEMPP-CEDE6-1245 Version 2 y las ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO PARA EL SERVICIO VPS - HOSTING DEDICADO PARA LA PAGINA WEB Y SUBSITIOS DEL EJÉRCITO NACIONAL, A EJECUTAR EN LA VIGENCIA 2026-2027, las cuales contienen los parámetros técnicos que deben cumplir los oferentes en la acreditación del servicio, así mismo, el contenido es el mismo del ANEXO ESPECIFICACIONES TÉCNICAS, los cuales se describen a continuación:



REPÚBLICA DE COLOMBIA

PATRIA HONOR LEALTAD

EJÉRCITO NACIONAL DE COLOMBIA

SERVICIO DE VPS SERVICIO HOSTING A LA PÁGINA WEB DEL EJÉRCITO NACIONAL			
SUBSISTEMA: Comunicaciones			
ESPECIALIDAD: Comunicaciones			
PROCESO: Gestión Tecnologías y Sistemas de Información C5		**NIVEL DE CLASIFICACIÓN:** Público	
Código ET: ET-JEMPP-CEDE6-1245	**Versión:** 2	**Fecha de emisión:** 2026-10-08	**Número de Páginas:** 21

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial
CÓDIGO ET: ET-JEMPP-CEDE6-1245 – V2
PÚBLICO



Elaboró	Revisó	Aprobó
TA1S. PEÑA JIMÉNEZ JUAN CAMILO Técnico para Apoyo y Defensa - DICOE	TE. BONILLA ACUNA WALTER JOSE Asesor Jurídico - DICOE	TC. MANUEL FELIPE CESPEDES RAMOS Director Comunicaciones Estratégicas del Ejército Nacional
SV. SALAZAR GOMEZ NELSON ANDRES Suboficial Producción Informativa - DICOE	CT. DEVIA PEREZ JINNA MARCELA Oficial De Políticas Y Planificación CEDE6	
	CT. SÁNCHEZ REYES YAKELLINE Oficial de Políticas y Planificación C5 CEDE6	
	MY. EYMER RICARDO PANTOJA ERAZO Oficial Proyectos – DICOE	

REQUISITOS GENERALES

Servicio de Hosting Dedicado, Colocación, Hardware dedicado, Conectividad a Internet y demás servicios asociados a un Data Center Externo para alojar la página web del Ejército Nacional, que permita garantizar la disponibilidad y seguridad de la información, siguiendo los requerimientos definidos por la Entidad para el cabal cumplimiento de sus funciones.

Tabla 1. Requisitos Generales para servicio de VPS servicio HOSTING a la página web del Ejército Nacional.

ITEM	DESCRIPCIÓN REQUISITOS
1	Se debe prestar el servicio de VPS y servicios de hosting, con funcionamiento y monitoreo 7x24x365 (siete días a la semana, 24 horas al día, 365 días del año) y una disponibilidad mínima del 99,995% (TIER IV).
2	Se debe garantizar que los equipos empleados para la prestación del servicio de VPS y servicios de hosting sean de su propiedad o que posea una relación comercial si es tercerizado. Adicionalmente, debe aceptar que el Ejército Nacional pueda verificar, revisar o mejorar el servicio de VPS y servicios de hosting.
3	Se debe garantizar acceso y administración total al VPS y servicios de hosting, (usuario root), base de datos, SSH, FTP, Analytics y demás elementos de hardware y software que esté utilizando.
4	Se debe suministrar el servicio de streaming de audio para que funcione en las páginas web del Ejército Nacional, permitiendo la distribución de la señal de la emisora del Ejército Nacional para un mínimo de diez mil (10000) usuarios simultáneamente durante la vigencia del contrato.

5	Se debe proveer un servicio de alertas mediante mensajes de texto y correos electrónicos a los funcionarios designados por el supervisor del contrato, con el fin de notificar caídas y tiempos fuera de servicio del VPS, los servicios de hosting y el streaming de audio.
6	Se compromete a prestar el servicio de VPS y servicios de hosting conforme a todos los ítems de la presente especificación técnica, durante la ejecución del contrato y una vez cumplidas las obligaciones contractuales, deberá: - Entregar informes mensuales, trimestrales y anuales en los formatos requeridos por el personal designado por la Fuerza. - En caso que las instalaciones del servidor estén en Colombia, se debe permitir el acceso a las instalaciones, para previa verificación de la implementación de las medidas de seguridad del mismo. Esta visita se deberá realizar bajo los protocolos de seguridad establecido por la empresa. - Brindar soporte técnico al servidor y atender todas las solicitudes que requieran el supervisor del contrato y su equipo de trabajo. Esto se debe realizar con el objetivo de facilitar la migración de la información, bases de datos, aplicativos, copias de seguridad y demás servicios que proporcionen al Ejército Nacional (servidores, hosting, bases de datos, accesos SSH, entre otros), con el fin de mantener el servicio activo y sin interrupciones durante el proceso de adjudicación para futuras vigencias. Lo anterior no generará costos adicionales para el Ejército Nacional.
7	Se debe, por razones de seguridad, proporcionar la ubicación del datacenter donde esté alojado el VPS y el servicio de hosting, el cual puede estar en Colombia, Estados Unidos o Canadá, con el propósito de mantener la información institucional en ubicaciones geográficas previamente definidas y controladas, reducir riesgos asociados al almacenamiento y procesamiento de datos en otras jurisdicciones y garantizar condiciones adecuadas de seguridad, disponibilidad y continuidad del servicio.

1.1 REQUISITOS ESPECIFICOS

Tabla 2. Requisitos Especifico para servicio de VPS servicio HOSTING a la página web del Ejército Nacional

ITEM	DESCRIPCIÓN REQUISITOS
1	Se debe cumplir con las condiciones técnicas del VPS y servicio de hosting, parametrizando la arquitectura de la siguiente manera: - El entorno de producción para el dominio ejercito.mil.co debe funcionar, como mínimo, en dos (2) servidores con las siguientes características: • Servidor Front de Producción: 24 vCPU Intel Xeon (versión mínima Intel Xeon GOLD 6542Y — 24 vCPU por servidor). Debe contar con mínimo 128GB DDR5 ECC Registeredy almacenamiento especializado SAN-FC o Cloud Storage con 4500 IOPS, de 2TB NVMe Enterprise en RAID-10 con IOPS garantizados >30,000. • Servidor de Base de Datos de Producción: 20 vCPU Intel Xeon (versión mínima GOLD Intel Xeon GOLD 6542Y). Debe contar con mínimo 64GB DDR5 ECC Registered de memoria RAM y almacenamiento especializado SAN-FC o Cloud Storage con 4500 IOPS, de 500GB NVMe Enterprise en RAID-10 con IOPS garantizados >30,000. - El entorno de producción para el dominio pqr.mil.co debe funcionar, como mínimo, en dos (2) servidores con las siguientes características: • Servidor Front de Producción: 24 vCPU Intel Xeon (versión mínima Intel Xeon GOLD 6542Y — 24 vCPU por servidor). Debe contar con mínimo 128GB DDR5 ECC Registered y almacenamiento especializado SAN-FC o Cloud Storage con 4500 IOPS, de 2TB NVMe Enterprise en RAID-10 con IOPS garantizados >30,000. • Servidor de Base de Datos de Producción: 20 vCPU Intel Xeon (versión mínima GOLD

	Intel Xeon GOLD 6542Y). Debe contar con mínimo 64GB DDR5 ECC Registered de memoria RAM y almacenamiento especializado SAN-FC o Cloud Storage con 4500 IOPS, de 500GB NVMe Enterprise en RAID-10 con IOPS garantizados >30,000. - Se deberá crear una máquina virtual dedicada para almacenar aplicaciones que el Ejército Nacional requiera, configurada de la siguiente manera: • Servidor Máquina Virtual: 12 vCPU Intel Xeon (versión mínima Intel Xeon GOLD 6542Y). Debe contar con mínimo 64GB DDR5 ECC y almacenamiento especializado SAN-FC o Cloud Storage con 4500 IOPS, 500GB NVMe Enterprise en RAID-10. Todos los servidores deben incluir: - Esquema de alta disponibilidad con clúster redundante de almacenamiento y procesamiento. - Red de interconexión de los servidores de mínimo 10 Gb. - Sistema operativo Alma Linux, o Cloud Linux. - Base de datos MySQL o MariaDB en su última versión estable. - Lenguaje de programación PHP en su última versión estable. - Capa media Apache en su última versión estable. - Acceso root vía SSH y Analytics. - 01 firewall Avanzado UTM con protección WAF, CDN, DOS, DDOS e IPS para los servidores de producción. - 01 clúster de alta disponibilidad para todos los servidores, servicios e información. - 01 Certificado de seguridad SSL Wildcard. - Servicio de hacking ético. - Canal de internet. - WHM y cPanel para la configuración de los servidores, con dos licencias, cada una con 5 usuarios.
2	Se debe cumplir con las siguientes condiciones para aplicaciones que se van a alojar en el VPS y servicio de hosting, deben ser de la siguiente manera: - Dominios: • ejercito.mil.co. • pqr.mil.co. • otros dominios del Ejército (máximo 70). - Características de las Aplicación • Ancho de banda consumido: Se debe garantizar que los tiempos de carga de las páginas deben ser acordes a las diferentes conexiones y ancho de banda. • Espacio en disco duro requerido: 02 Terabyte o según volumetría. • Visitas mensuales promedio: 3.000.000. • Visitas diarias pico: 300.000. • Páginas de la aplicación: 1.000.000. • Portales a alojar: Mínimo 100. • Velocidad de consulta mínima: 10.000 megas. Debe ser distribuidor oficial de cPanel, demostrarlo a través de una Certificación directamente por cPanel o a través de la verificación de licencias https://verify.cpanel.net/ que evidencie su condición de Partner NOC, asociada a la razón social
3	Se debe realizar las siguientes actividades: - Backup en base de datos y imagen del sistema o servidor

	• Cada mes se debe generar automáticamente una copia de backup completa de la base de datos y del servidor en las horas establecidas por el Ejército Nacional. Al finalizar el proceso de backup, los archivos deben ser copiados a un servidor o ubicación diferente al servidor de producción, utilizando SSH (comunicación encriptada y segura). Se deben mantener las copias de backup de los últimos 90 días, eliminando las copias que superen este período. - Backups en archivos de usuario y de la aplicación • Generar automáticamente una copia de backup diaria diferencial de todos los archivos del sistema. Al finalizar el proceso de backup, los archivos deben ser copiados a un servidor diferente al servidor dedicado y compartido. - Pruebas trimestrales de backups y Hacking Ético • Se debe junto con el supervisor del contrato y su equipo de trabajo, realizar una restauración de los backups para comprobar la eficacia de los mismos. • Se debe realizar pruebas de vulnerabilidad, seguridad y hacking ético sobre el VPS y los servicios de hosting, utilizando su departamento de testing o de seguridad informática, Las anteriores actividades se deben realizar durante la ejecución del contrato y no generará costos adicionales para el Ejército Nacional.
4	Se deberá brindar servicio de soporte técnico durante la ejecución del contrato con disponibilidad 7x24,y garantizar los medios de comunicación a través de línea comercial, celular, correo electrónico o de forma presencial, con el fin de resolver los requerimientos presentados por el supervisor del contrato y su equipo de trabajo.
5	Se deberá, durante la ejecución del contrato entregar: - Informe mensual del UPTIME del VPS y servicio de hosting. - Informe mensual de los backups realizados. - Informe trimestral del hacking ético. - Informe trimestral de la prueba de restauración del backup. Para la entrega de estos informes, se debe elaborar un cronograma de actividades que estipule las fechas de estos entregables.
6	Se debe contar con un sistema de seguridad físico y lógico implementado, habilitado, configurado y en funcionamiento que garantice la integridad, confiabilidad y disponibilidad de la información. Este sistema debe incluir, como mínimo, lo siguiente: - Firewall: Un firewall de hardware y software que soporte el sistema descrito en los numerales anteriores y asegure la disponibilidad del sitio. - Sistema de Prevención de Intrusos (IPS): Un IPS que monitoreé permanentemente el canal y generé estadísticas de intentos de intrusión. Una vez que este reporte haya sido analizado en coordinación con el supervisor del contrato, se informará sobre las firmas que deben ser bloqueadas. - Certificado SSL Wildcard: Un certificado SSL wildcard para el dominio principal de*.ejército.mil.co. Cuando el Ejército Nacional utilice la máquina virtual, los aplicativos que se utilicen en este servidor virtual deberán tener certificado SSL. Este certificado debe contener el protocolo de seguridad (SSL 3.0 con cifrado de 256 bits y RSA con intercambio de 2048 bits) y ser emitido por una entidad de certificación abierta, lo cual es esencial para todas las transacciones de administración que impliquen la adición, modificación y/o eliminación de archivos. Asimismo, debe implementarse en los webs services que tenga el Ejército Nacional. Todas estas transacciones o sesiones deberán ser autenticadas con

	usuario y contraseña. Este certificado debe aplicarse desde el inicio del contrato, durante la ejecución, garantía técnica y tiempos de reposición; su costo no generará costos adicionales para el Ejército Nacional. - Aseguramiento de Parámetros de Configuración: Aseguramiento de los parámetros de configuración del lenguaje en que se desarrolla el portal. - Prevención de Indexación: Asegurar el servidor de tal forma que evite la indexación de carpetas, generando errores por defecto para evitar el escaneo de carpetas y/o usuarios. - Opciones de Ocultación de Información: La opción de ocultar información sobre el lenguaje, el servidor y el sistema operativo. - Deshabilitación de Métodos Trace: Deshabilitar métodos Trace en los servidores para prevenir ataques de cross-site scripting (XSS). - Limpieza de Parámetros: El portal debe realizar la limpieza de todos los parámetros GET, POST, Cookies, etc., para evitar ataques de SQL Injection. - Gestión de Logs: Configurar un gestor de logs para análisis y revisión de registros en el servidor. - Validación de Cookies: Si se utilizan cookies, validar que pertenezcan a una única IP para evitar el robo o la alteración de sesiones. - Protocolo de Transferencia: No utilizar el protocolo FTP (protocolo de transferencia de archivos) para transacciones con el servidor. Utilizar SSH para transacciones con el servidor, restringiendo el acceso por IP y evitando el acceso directo al usuario súper administrador. - Transacciones Sensibles: Tener instalado y configurado el protocolo de seguridad SSL para transacciones que involucren información sensible, como contraseñas. - Acceso Administrativo: Ingresar al área administrativa a través de protocolo SSL. - Control de Conexiones Concurrentes: Se debe conocer el número de conexiones concurrentes que soporta el servidor web, con el fin de establecer en el firewall umbrales que permitan bloquear direcciones IP y, de igual forma, establecer umbrales en los que el firewall comience a bloquear el tráfico para prevenir hackeos al servidor web. - Bloqueo de Direcciones IP: Se debe estar en capacidad de bloquear direcciones IP que el Ejército considere maliciosas, de acuerdo con el número de eventos detectados. - Acceso Administrativo Seguro: El acceso administrativo vía SSH o RDP para los administradores de sistemas solo debe permitirse a través de conexiones encriptadas, asegurando el máximo nivel de encapsulación de la información y de las credenciales de acceso. - Medidas de Seguridad Continuas: Implementar medidas de seguridad continuas a los servidores a nivel de sistema operativo y a nivel del servicio web (IIS, Apache, NGINX), tales como instalación de parches, actualizaciones, aseguramiento de protocolos, eliminación de instalaciones por defecto y desarrollos seguros. - Puertos de Comunicación: Permitir solamente los siguientes puertos de comunicación TCP para el WEB SERVER: TCP 80, TCP 443, UDP 53.
7	En caso de presentarse una falla técnica en el datacenter donde se encuentra alojado el VPS y servicio hosting o un ataque hacking a cualquiera de las páginas web del Ejército Nacional que estén alojadas en el VPS y servicio hosting, se debe garantizar la restauración del servicio en un tiempo máximo una (01) hora.

ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

SERVICIO VPS - HOSTING DEDICADO PARA LA PAGINA WEB Y SUBSITIOS DEL EJÉRCITO NACIONAL ET-JEMPP-CEDE6-1245	
ITEM	**DESCRIPCIÓN REQUISITOS**
1	El oferente deberá anexar una certificación comercial o documento equivalente que acredite su relación contractual o comercial con el centro de datos donde se alojará la infraestructura tecnológica contratada. El centro de datos deberá contar con certificación Tier IV – Tier Certification of Constructed Facility (TCCF), expedida por el Uptime Institute, la cual será verificada mediante los mecanismos

	oficiales de consulta de dicha organización. Adicionalmente, el oferente deberá aportar los certificados vigentes ISO 9001 (Sistema de Gestión de Calidad), ISO 14001 (Sistema de Gestión Ambiental), ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información) e ISO 45001 (Sistema de Gestión de Seguridad y Salud en el Trabajo), correspondientes al operador del centro de datos propuesto, cuyo alcance deberá comprender las actividades relacionadas con su operación y prestación de servicios de alojamiento tecnológico. Las certificaciones deberán encontrarse vigentes, ser verificables y haber sido expedidas por organismos de certificación competentes.
2	El contratista se compromete a no divulgar y reproducir el software, hardware y la información que actualmente tiene el Ministerio de Defensa Nacional – Ejército Nacional, a los que se ve obligado a conocer como producto de la ejecución.
3	El contratista debe estar dispuesto a firmar los acuerdos de confidencialidad de la información suministrada y relacionada con la Fuerza, relacionados en el acta de inicio del contrato. Así mismo, debe aceptar y permitir que el Ejército Nacional efectúe un Estudio de Seguridad Personal (ESP) a los funcionarios designados para la ejecución del contrato, a fin de comprobar datos y establecer antecedentes disciplinarios que garanticen la seguridad de la infraestructura computacional e información del Ejército Nacional.
4	El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial.
5	El contratista se obliga a que todos los miembros del equipo de trabajo objeto del presente proceso, deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización
6	El contratista se obliga a que todos los miembros del equipo de trabajo deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento.
7	El oferente deberá acreditar, con la presentación de su oferta, un (1) profesional que cuente con uno de los siguientes títulos: Ingeniería de Sistemas, Ingeniería de Telecomunicaciones, Ingeniería Informática, Ingeniería de Sistemas y Computación o un programa académico relacionado con las tecnologías de la información y las comunicaciones, reconocido por el Ministerio de Educación Nacional y verificable mediante el Sistema Nacional de Información de la Educación Superior (SNIES). No se exige acreditar más de una de las profesiones enunciadas. Para ello aportará copia del diploma o acta de grado y, cuando aplique conforme a la Ley 842 de 2003, de la matrícula profesional y su certificado de vigencia; los títulos obtenidos en el exterior deberán estar convalidados ante el Ministerio de Educación Nacional. El contratista deberá garantizar que dicho profesional esté asignado a la administración, operación, mantenimiento y soporte de la infraestructura tecnológica contratada. Adicionalmente, el profesional acreditado deberá acreditar, de manera individual, las certificaciones o formaciones técnicas señaladas en los numerales 1, 2, 4 y 5 siguientes, de acuerdo con las funciones y responsabilidades asignadas: 1. Certificación o formación acreditada en Seguridad y Privacidad de la Información.

	2. Diplomado, certificación técnica o formación equivalente en Administración de Sistemas Operativos Linux. 3. Condición cPanel: se exige a la persona jurídica oferente y no al profesional, y se acredita conforme a lo establecido en el ítem 8 de las presentes especificaciones. 4. Certificación Lead Cybersecurity Professional Certification (LCSPC), Ethical Hacking Professional Certification (CEHPC) o certificación equivalente en ciberseguridad. Esta certificación podrá satisfacer simultáneamente lo exigido en el ítem 10, cuando sea equivalente. 5. Certificación Acronis Tech Associate, en una especialidad relacionada con protección y respaldo de información, o certificación técnica equivalente en administración de soluciones de copias de seguridad y recuperación de datos. Las certificaciones y acreditaciones deberán ser expedidas por instituciones educativas, fabricantes u organismos de formación o certificación competentes, y deberán ser verificables. El oferente deberá aportar, además, documento que acredite la vinculación o disponibilidad del profesional para la ejecución del contrato, mediante contrato laboral, contrato de prestación de servicios o carta de compromiso suscrita por el profesional y el oferente. Para el presente proceso, la solución tecnológica contratada contempla expresamente las plataformas cPanel/WHM y Acronis; en consecuencia, los requisitos específicos de formación y certificación relacionados con dichas tecnologías son de obligatorio cumplimiento. Durante la ejecución del contrato, el contratista garantizará la disponibilidad del profesional acreditado. Podrá disponer de personal adicional cuando lo considere necesario, sin que ello genere costos adicionales para la Entidad ni modifique las condiciones económicas pactadas. En caso de sustitución del profesional acreditado, el reemplazante deberá cumplir la totalidad de los requisitos exigidos, acreditarlos por escrito y contar con la verificación previa del supervisor del contrato. Todo el personal estará sujeto a los acuerdos de confidencialidad y al Estudio de Seguridad Personal previstos en los ítems 3, 5 y 6. El personal del contratista no tendrá vínculo laboral con el Ministerio de Defensa Nacional – Ejército Nacional. El contratista será responsable de garantizar que el personal dispuesto para la ejecución del contrato cumpla las especificaciones técnicas de obligatorio cumplimiento, las especificaciones técnicas adicionales aplicables y las demás condiciones y obligaciones contractuales, asegurando la adecuada prestación del servicio de alojamiento, administración, mantenimiento y soporte de la infraestructura tecnológica contratada.
8	El oferente deberá acreditar su condición de Partner o Distribuidor Autorizado de cPanel, con una antigüedad mínima de un (1) año, mediante certificación o documento vigente a la fecha de cierre, expedido directamente por el fabricante, en el cual se evidencie que dicha condición corresponde a la persona jurídica que presenta la oferta (razón social y NIT) y que cumple la antigüedad exigida. La verificación de licencias en https://verify.cpanel.net/ que evidencie su condición de Partner NOC, asociada a la razón social del oferente, servirá como constatación complementaria, sin reemplazar el documento expedido por el fabricante. Los documentos en idioma extranjero deberán acompañarse de traducción simple. En oferta plural, esta condición deberá ser acreditada por [al menos uno de sus integrantes, que asumirá la prestación del servicio de hosting]. Esta acreditación constituye requisito habilitante dentro del proceso de selección. En caso de resultar adjudicataria, la empresa contratista deberá mantener vigente su condición de Partner o Distribuidor Autorizado de cPanel durante toda la ejecución del contrato, lo cual constituye una obligación contractual; la pérdida o suspensión de dicha condición deberá informarse al supervisor dentro de los [tres (3)] días hábiles siguientes.
9	El contratista o el oferente debe anexar la carta de compromiso para prestar el servicio de VPS Y servicios Hosting de acuerdo a lo estipulado en el pliego de condiciones
10	El contratista o el oferente debe anexar una certificación en CEH, ECSA, ISEQ+, o en una especialidad compatible en temas de seguridad informática, la cual podrá corresponder a la acreditada por el profesional en el numeral 4 del ítem 7, cuando sea equivalente.

11	El contratista o el oferente deberán entregar el mecanismo de contingencia previsto, para que en caso de llegar a presentarse alguna falla con en el VPS y servicio hosting donde se alojarán todas las páginas Web del Ejército, el servicio pueda restablecerse máximo en una (1) hora. Debe especificar en documento independiente y el contratista entregará copia impresa de la contingencia al supervisor del contrato una vez iniciado el contrato.

Cordialmente,

(Firma – posfirma representante legal o apoderado)
Proponente:
Documento de Identidad: