**TÉRMINOS DE REFERENCIA**

**SERVICIO DE CONSULTORÍA POR PRODUCTO PARA ANALISIS DE SEGURIDAD DE SISTEMAS INFORMÁTICOS PARA LAS ELECCIONES GENERALES 2020**

|  |
| --- |
| **REQUISITOS NECESARIOS DE LA CONSULTORÍA** |
| 1. **JUSTIFICACIÓN Y ALCANCE DE LA CONSULTORÍA** |
| 1. **JUSTIFICACIÓN** |
| En atención a las observaciones de auditoría de la Organización de Estados Americanos (OEA), en relación al reciente proceso electoral presidencial, llevado a cabo en el mes de octubre de 2019 y de cara al nuevo proceso electoral a llevarse a cabo en fecha 18 de octubre de 2020, El Órgano Electoral Plurinacional (OEP), encara un proceso de renovación tecnológica integral que incluye infraestructura física de comunicaciones y almacenamiento bajo un esquema de aseguramiento de datos, así como el aprovisionamiento de nuevos sistemas electorales y la optimización de procedimientos y protocolos  Por lo mencionado, se requiere contratar una empresa Consultora que realice un análisis de seguridad informática y que provea resultados para determinar el nivel de riesgo asociado a la infraestructura tecnológica y entorno reglamentario, debiendo realizar tareas de:   * Análisis de las vulnerabilidades en el marco de: gestión documental de seguridad de la información, gestión de seguridad física y lógica, gestión de base de datos, gestión de sistemas informáticos, gestión de redes y comunicaciones. * Identificación de todas las vulnerabilidades reales, de alto, mediano y pequeño impacto. * Identificación de componentes sensibles de mejora. * Identificación de un plan de acción para la gestión de riesgos en base a las vulnerabilidades detectadas. * Evaluación de cumplimiento en aplicación de medidas de gestión de vulnerabilidades detectadas. * Soporte en la corrección de vulnerabilidades detectadas. |
| 1. **ALCANCE DE LA CONSULTORÍA** |
| El alcance de la consultoría consiste en detectar posibles vulnerabilidades y la exposición de riesgo en la infraestructura tecnológica implementada por el OEP para la ejecución del proceso electoral a llevarse a cabo el 18 de octubre de 2020. Este proceso deberá enmarcarse en la ejecución hacking ético a través de pruebas de intrusión externas e internas de tipo caja negra y/o caja gris, en un entorno asegurado y definido por el OEP, identificando la existencia de vulnerabilidades que pudiesen ser explotadas para comprometer la seguridad de los sistemas, acceder a información sensible, alterar datos remotamente, hasta llegar a comprometer los distintos equipos de redes y comunicación, servidores, bases de datos y aplicaciones de la Institución a ser utilizados en el proceso electoral mencionado (sistema de difusión rápida de resultados y sistema de cómputo oficial de resultados).  La consultoría abarcará la siguiente infraestructura tecnológica:   * Servidores de difusión de resultados preliminares (red en nube), mínimamente: * 1 servidor controlador de dominio * 1 servidor de Base de Datos * 1 granja de servidores de aplicación (2 nodos inicialmente) * Servidores de cómputo oficial (red segmentada y red en nube), mínimamente: * 9 servidores controladores de dominio * 1 servidor de certificados * 1 servidor SCCM * 1 servidor antivirus * 11 servidores de imágenes * 2 servidores de cómputo * 1 servidor de aplicación * Bases de datos de difusión de resultados preliminares y cómputo * Aplicación web de difusión de resultados preliminares y cómputo * Aplicación móvil de captura de datos y difusión de resultados preliminares * Páginas Web de publicación de resultados preliminares y cómputo oficial (entorno externo) * Páginas web institucionales (oep, yoparticipo) * Dispositivos de comunicación, firewalls y otros dispositivos que intervienen en el cómputo * Aproximadamente 450 terminales de transcripción y verificación para proceso de cómputo * Enlaces de comunicación entre TSE y Tribunales Departamentales   El proponente deberá brindar las herramientas necesarias para realizar la consultoría, sin que este implique costo adicional para el OEP. |
| 1. **CARACTERÍSTICAS DE LA CONSULTORÍA** |
| 1. **PRODUCTOS ESPERADOS** |
| |  |  |  |  | | --- | --- | --- | --- | | **PRODUCTO N°** | **DESCRIPCIÓN DEL PRODUCTO** | **ACTIVIDADES A REALIZAR DENTRO DEL PRODUCTO** | **FUENTE DE VERIFICACIÓN** | | 1 | Pruebas de penetración interna, externa y en aplicación móvil | **PRUEBAS DE PENETRACION EXTERNAS**  Pruebas de penetración desde internet, simulando ser un atacante externo, con conocimientos de las aplicaciones objetivo del cliente. Se realizarán los siguientes trabajos:   * Detección de vulnerabilidades de tipo 'deface' * Ataques de tipo 'cross-site scripting' * Ataques de tipo 'spoofing' * Ataques de tipo inyección de SQL * Ataques de tipo inyección de código * Ataques derivados de la validación de E/S * Ataques derivados del análisis de tiempos * Evasión de protecciones perimetrales * Ataques de desbordamiento de memoria * Ataques basados en secuestro de sesiones * Detección de vulnerabilidades en las Bases de Datos y SO * Detección de vulnerabilidades de infraestructura de redes y almacenamiento * Detección de Vulnerabilidades en Firewalls, IDS, IPS, WAF, AD, Antivirus, etc. * Ataques basados en interceptación remota * Ataques basados en escalada de privilegio * Ataques en la gestión de contraseñas. * Inyección de código * Ataques de denegación de servicios * Autenticación incompleta y gestión de sesiones * Ataques a dispositivos de red y protocolos * Ataques criptográficos. * Otros (propuestos por la empresa consultora)   **PRUEBAS DE PENETRACION INTERNAS**  Pruebas de penetración desde la red interna de OEP.  Se realizarán las siguientes tareas:   * Ataques de arquitectura de las Aplicaciones Internas e Intranets * Ataques de arquitectura a los Servidores y estaciones de trabajo * Ataques de arquitectura a las Bases de Datos * Explotación de servicios vulnerables * Detección de vulnerabilidades de abuso contra interfaces de programación de aplicaciones * Detección de vulnerabilidades de calidad de código * Detección de vulnerabilidades derivadas de la configuración de los Servidores * Detección de vulnerabilidades en la conexión a las Bases de Datos * Detección de Vulnerabilidades en los protocolos de red * Detección de Vulnerabilidades Criptográficas * Detección de Vulnerabilidades en la gestión de contraseñas * Ataques a nivel de entropía. * Otros (propuestos por la empresa consultora)   **PRUEBAS DE PENETRACION EN APLICACIÓN MÓVIL**  Pruebas de penetración a la infraestructura relacionada y aplicativo móvil.  Se deben realizar las siguientes tareas:   * Ingeniería inversa para detección de código fuente * Pruebas remotas a nivel aplicación y servicios * Análisis de sistema de configuración * Análisis de sistema de archivos * Análisis de manejo de sesiones * Pruebas de capa de transporte * Pruebas de autenticación * Pruebas de autorización * Pruebas de validación de datos * Pruebas de servicios web * Pruebas AJAX * Ataques server-side * Análisis de dependencias de servicio remoto} * Análisis de comunicación entre procesos * Otros (propuestos por la empresa consultora) | 1. Resumen ejecutivo 2. Informe técnico de hallazgos por tipo de intrusión que incluya:  * Detalle de hallazgos. * Detalle de vulnerabilidades * Descripción de hallazgos * Indicadores de riesgo * Recomendaciones de solución | | 2 | Corrección de vulnerabilidades (RETEST) | **CORRECCION DE VULNERABILIDADES**  Deberá consistir en:   * Acceso a procedimientos de corrección * Soporte y acompañamiento en implementación de soluciones recomendadas para corrección de vulnerabilidades * Visibilidad de avance en línea. * Verificación de implementación de correcciones | Informe de soporte de corrección de vulnerabilidades, que incluya:   * Detalle de hallazgos corregidos. * Descripción de soluciones * Descripción de soporte proporcionado | |
| 1. **PROPUESTA TÉCNICA, ECONÓMICA Y CURRICULUM VITAE** |
| * La empresa proponente debe presentar su propuesta técnica y económica de acuerdo a los productos esperados y las actividades descritas por la Unidad Solicitante, y deberá contener mínimamente: objetivos, alcance, plan y cronograma de trabajo u otros que se considere necesario. * La empresa proponente debe presentar curriculum vitae del personal técnico de acuerdo al siguiente detalle:   El Proponente debe presentar como personal técnico a dos (2) personas, cada una deberá cumplir con los siguientes requisitos:   1. **Formación y/o conocimientos.**  * Licenciatura en informática, ingeniería de sistemas o ramas afines. * **C**ontar mínimamente con 2 certificaciones en el área de auditoría de sistemas, seguridad de la información, ethical hacking, ciberseguridad o ramas afines.   **(Presentar documentación de respaldo en fotocopia simple, que acredite la formación y conocimiento requerido)**.   1. **Experiencia General.**   Más de tres (3) años de experiencia general en el área de sistemas Informáticos o ramas afines, a partir de la emisión de título profesional.  **(La misma podrá ser respaldada con fotocopias simples de certificados de trabajo, órdenes de servicio, memorándums, contratos u otro documento equivalente).**   1. **Experiencia Específica.**   Más de un (1) año de experiencia en seguridad de la información, auditoría de sistemas, ethical hacking, ciberseguridad u otro equivalente, a partir de la emisión de título de certificación.  **(La misma podrá ser respaldada con fotocopias simples de certificados de trabajo, órdenes de servicio, memorándums, contratos u otro documento equivalente).**  El Proponente debe presentar como gerente de proyecto una (1) persona que cumpla con los siguientes requisitos:   1. **Formación y/o conocimientos.**  * Licenciatura en informática, ingeniería de sistemas o ramas afines. * Contar con al menos un postgrado en el área informática.   **(Presentar documentación de respaldo en fotocopia simple, que acredite la formación y conocimiento requerido)**   1. **Experiencia General.**   Más de cinco (5) años a partir de la emisión de título profesional, en el área de sistemas Informáticos o ramas afines. **(La misma podrá ser respaldada con fotocopias simples de Certificados de trabajo, órdenes de servicio, memorándums, contratos u otro documento equivalente)**   1. **Experiencia Específica.**   Más de tres (3) años de experiencia en seguridad de la información, ethical hacking, ciberseguridad u otro equivalente. **(La misma podrá ser respaldada con fotocopias simples de Certificados de trabajo, órdenes de servicio, memorándums, contratos u otro documento equivalente).** |
| 1. **PRESENTACIÓN DE PROPUESTA** |
| La propuesta deberá ser entregada en sobre cerrado, debidamente foliado de acuerdo al siguiente formato:  **OBJETO DE CONTRATACIÓN:**  **NOMBRE DEL PROVEEDOR:**  **TELÉFONO:**  **FECHA:**  **El proponente deberá adjuntar a su propuesta la siguiente documentación:**   * Fotocopia simple de Número de Identificación Tributaria (activa) * Fotocopia simple de Registro FUNDEMPRESA (válida y activa) |
| 1. **CARACTERÍSTICAS DE LA EMPRESA CONSULTORA A SER CONTRATADA** |
| 1. **PERFIL DE LA EMPRESA CONSULTORA** |
| 1. **Experiencia General:** La empresa deberá contar con un mínimo de tres (3) trabajos en el rubro de Tecnologías de la Información, durante los últimos 2 años. (Dicha experiencia podrá estar acreditada por documentación en fotocopia simple de: certificados de cumplimiento de contrato, contratos, órdenes de servicio, actas de conformidad o facturas donde mencione el servicio realizado). |
| 1. **Experiencia Específica:** La empresa debe de haber realizado por lo menos dos (2) trabajos referentes a Ciberseguridad o Ethical Hacking o seguridad de la información u otros relacionados a seguridad de la información en empresas públicas o privadas, durante los últimos 2 años. (Dicha experiencia podrá estar acreditada por documentación en fotocopia simple de: certificados de cumplimiento de contrato, contratos, órdenes de servicio, actas de conformidad o facturas donde mencione el servicio realizado). |
| 1. **CONDICIONES DE LA CONSULTORÍA** |
| 1. **PLAZO** |
| El plazo será de (20) días calendario a partir de la emisión de la orden de proceder que será entregada a la empresa consultora por parte de la Unidad Solicitante, dentro de los plazos incluye el siguiente cronograma de presentación de cada producto:   |  |  |  | | --- | --- | --- | | **PRODUCTO N°** | **DESCRIPCIÓN DEL PRODUCTO** | **PLAZO (A partir de la emisión de la Orden de proceder)** | | 1 | Pruebas de penetración interna, externa y en aplicación móvil | Hasta 8 días calendario | | 2 | Corrección de vulnerabilidades (RETEST) | Hasta 20 días calendario | |  | Presentación de Informe Final | Hasta 20 días calendario | |
| 1. **GARANTÍAS** |
| **CUMPLIMIENTO DE CONTRATO** |
| La entidad convocante solicitará la Garantía de Cumplimiento de Contrato, equivalente al siete por ciento (7%) del monto del contrato. Cuando se tengan programados pagos parciales, en sustitución de la Garantía de Cumplimiento de Contrato, se podrá prever una retención del siete por ciento (7%) de cada pago. |
| 1. **ANTICIPO** |
| NO se otorgará anticipo. |
| 1. **RÉGIMEN DE MULTAS** |
| La empresa adjudicada debe cumplir con los plazos de entrega de los productos, caso contrario se le aplicará una multa del 1 % del monto total del contratopor cada día calendario de retraso o incumplimiento en la prestación del servicio.  La suma de las multas no podrá exceder en ningún caso el 20% del monto total del contrato, sin perjuicio de resolver el mismo.  \*En casos de fuerza mayor o casos fortuitos, la empresa adjudicada deberá enviar un informe documentado del hecho al Responsable o Comisión de Recepción en un plazo no mayor a las 48 horas de sucedido el imprevisto. Esto para evitar multas por incumplimiento del servicio y pagos que no correspondan. |
| 1. **RESPONSABLE O COMISIÓN DE RECEPCIÓN** |
| El Responsable o Comisión de Recepción se encargará de realizar el seguimiento al servicio contratado, a cuyo efecto realizará las siguientes funciones:   * Deberá dar su conformidad, supervisará, aprobará y solicitará expresamente el pago de cada producto. * Verificará el cumplimiento de lo establecido en el contrato. * En el informe final de conformidad (conclusiones) deberá solicitar la devolución de la garantía de cumplimiento de contrato del 7 % (si corresponde) |
| 1. **RESOLUCIÓN** |
| Por suspensión del SERVICIO sin justificación alguna, por el lapso de 3 días calendario continuos, sin autorización escrita de la CONTRAPARTE. |
| 1. **MONTO Y FORMA DE PAGO** |
| El monto total para la ejecución de la CONSULTORÍA es de Bs211.091,43 (Doscientos Once Mil Noventa y Uno 43/100 Bolivianos)   |  |  |  |  | | --- | --- | --- | --- | | **PRODUCTO N°** | **DESCRIPCIÓN DEL PRODUCTO** | **PORCENTAJE** | **MONTO** | | 1 | Pruebas de penetración interna, externa y en aplicación móvil | 62,50% | 131.932,14 | | 2 | Corrección de vulnerabilidades (RETEST) | 37,50% | 79.159,29 |   La **CONTRAPARTE** de la consultoría será el Responsable o Comisión de Recepción quien una vez recibidos los productos de la empresa, revisará cada uno de éstos de forma completa, así como otros documentos que emanen de la **CONSULTORÍA** y hará conocer a la **EMPRESA** la aprobación de los mismos o en su defecto comunicará sus observaciones. En ambos casos la **CONTRAPARTE** deberá comunicar su decisión a la **EMPRESA** respecto al informe en el plazo máximo de tres (3) días calendario computados a partir de la fecha de recepción de los productos. Si dentro del plazo señalado precedentemente, la **CONTRAPARTE** no se pronunciara respecto a los productos presentados, se aplicará el silencio administrativo positivo a favor de la **EMPRESA**.  La **EMPRESA** tiene la obligación de responder a las observaciones hechas por el Responsable o Comisión de Recepción dentro del plazo máximo de dos (2) días calendario computados a partir de la recepción de las demandas de aclaración o complementación requeridas.  Por la dinámica de la **CONSULTORÌA**, la comunicación con la **EMPRESA** será a través de notas escritas o vía correo electrónico. |
| 1. **INSTALACIONES EN LAS QUE SE EFECTUARA LA CONSULTORÍA** |
| La Empresa Consultora desarrollará las actividades de esta consultoría en instalaciones de la Dirección Nacional de Tecnologías de la Información y la Comunicación ubicada en la Av. Aniceto Arce N° 2985 – Zona San Jorge, ciudad de La Paz del Tribunal Supremo Electoral, en coordinación directa con el Responsable o Comisión de Recepción; podrá recibir apoyo remoto y realizar pruebas desde fuera, cuando la naturaleza del servicio así lo requiera. |
| 1. **CONFIDENCIALIDAD** |
| Los productos y la documentación producida por la **EMPRESA** en el marco de la **CONSULTORÌA**, así como la información a la que la **EMPRESA** tuviese acceso durante o después de la ejecución de la **CONSULTORÍA**, tendrá carácter confidencial, quedando expresamente prohibida su divulgación a terceros, exceptuando los casos en que la **ENTIDAD** emita un pronunciamiento escrito estableciendo lo contrario.  Así mismo la **EMPRESA** reconoce que la **ENTIDAD** es el único propietario de los productos y documentos producidos en la **CONSULTORÍA.** |