|  |
| --- |
| **ESPECIFICACIONES TÉCNICAS****SERVICIO DE TERCEROS PARA ANÁLISIS DE SEGURIDAD DE SISTEMAS INFORMÁTICOS (SEGUNDA VUELTA) - ELECCIONES SUBNACIONALES 2021** |
| 1. **JUSTIFICACIÓN y alcance del servicio**
 |
| 1. **JUSTIFICACIÓN**
 |
| Durante la gestión 2020 y del proceso electoral llevado a cabo en dicha gestión, el Órgano Electoral Plurinacional (OEP), encaró un proceso de renovación tecnológica integral que incluye infraestructura física de comunicaciones y almacenamiento bajo un esquema de aseguramiento de datos, así como el ajuste de los sistemas electorales y la optimización de procedimientos y protocolos.En el marco de las buenas prácticas de seguridad de información, se requiere contratar un **PROVEEDOR** que realice un análisis de vulnerabilidades 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 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.
* Soporte en la corrección de vulnerabilidades detectadas.
* Evaluación de cumplimiento en aplicación de medidas de gestión de vulnerabilidades detectadas.
 |
| 1. **ALCANCE DEL SERVICIO**
 |
| Las Actividades del **PROVEEDOR** deberá abarcar la siguiente infraestructura tecnológica: * Servidores de cómputo oficial (red local para procesamiento y red en nube para publicación de resultados), mínimamente:
	+ 12 controladores de dominio
	+ 1 emisor de certificados
	+ 2 servidor SCCM
	+ 2 servidor antivirus abarcar
	+ 1 servidor de monitoreo
	+ 2 servidores de cómputo
	+ 2 servidores de resultados
	+ 10 servidores de imágenes
	+ 2 servidores de publicación de servicios
* Bases de datos de cómputo
* Aplicación de escritorio de cómputo
* Aplicaciones web de resultados de cómputo
* Repositorio de imágenes
* Páginas web de publicación de resultados de cómputo oficial
* 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
* Otro hardware y software
 |
| 1. **CARACTERÍSTICAS GENERALES DEL (LOS) SERVICIO(S)**
 |
| 1. **Requisitos del servicio**
 |
| **Ítem** | **Características Técnicas** |
| 1 | **PRUEBAS DE PENETRACIÓN INTERNA Y EXTERNA** **ACTIVIDADES A REALIZAR:****Pruebas de Penetración Externas**Pruebas de penetración desde Internet, simulando ser un atacante externo, realizando las siguientes actividades:• Ataques de denegación de servicios• Ataques basados en secuestro de sesiones• Ataques de tipo 'Cross-Site Scripting'• Ataques de tipo 'Spoofing'• Ataques de tipo Inyección de SQL• Ataques de tipo Inyección de Código• Ataques de desbordamiento de memoria• Ataques basados en interceptación Remota• Ataques basados en escalada de privilegio• Ataques a dispositivos de Red y Protocolos• Evasión de protecciones perimetrales• 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.• Detección de Vulnerabilidades en la gestión de contraseñas• Otros (Propuestos Por El Proveedor)**Pruebas de Penetración Internas**Pruebas de penetración desde la red interna del OEP, realizando las siguientes actividades de tipo caja gris:• 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 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 en la gestión de contraseñas• Otros (Propuestos por el proveedor) |
| 2 | **CORRECCIÓN DE VULNERABILIDADES Y RETEST****ACTIVIDADES A REALIZAR:*** 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
* Otras recomendaciones planteadas por el **PROVEEDOR**
 |
| * Presentación de Informe Final y Conclusivo
 |
| 1. **CONDICIONES COMPLEMENTARIAS**
 |
| **PROPUESTA TÉCNICA Y ECONÓMICA:**El **PROVEEDOR** debe presentar su propuesta técnica y económica de acuerdo a las características Generales del Servicio numeral II y el inciso A columna características técnicas, descritas por la Unidad Solicitante, donde deberá contener mínimamente: objetivos, alcance, plan y cronograma de trabajo u otros que se considere necesario.**RECURSOS TÉCNICOS:**El **PROVEEDOR** deberá 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 11 de abril de 2021. 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, estaciones de trabajo, bases de datos y aplicaciones de la Institución a ser utilizados en el proceso electoral mencionado.El **PROVEEDOR** deberá brindar las herramientas necesarias para realizar el servicio, sin que este implique costo adicional para el OEP.El **PROVEEDOR** debe garantizar que el análisis de seguridad no comprometa la integridad, disponibilidad y confidencialidad de la información, ni de los servicios tecnológicos proporcionados durante el proceso electoral. |
| 1. **EXPERIENCIA Y PERSONAL TÉCNICO DEL PROVEEDOR**
 |
| 1. **EXPERIENCIA GENERAL**
 |
| El **PROVEEDOR** 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 ser validada por documentación en fotocopia simple legible, de alta resolución y tamaño original de alguno de los siguientes documentos: certificados de cumplimiento de contrato o contratos u órdenes de servicio o actas de conformidad o facturas o documentos equivalentes donde se mencione el servicio realizado).** |
| 1. **EXPERIENCIA ESPECIFICA**
 |
| El **PROVEEDOR** deberá 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 ser validada por documentación en fotocopia simple legible, de alta resolución y tamaño original de alguno de los siguientes documentos: certificados de cumplimiento de contrato o contratos u órdenes de servicio o actas de conformidad o facturas o documentos equivalentes donde se mencione el servicio realizado).** |
| 1. **PERSONAL TÉCNICO**
 |
| El **PROVEEDOR** debe presentar como **GERENTE DE PROYECTO** una (1) persona que cumpla con los siguientes requisitos:**Formación y/o conocimientos.*** Licenciatura o estudios superiores en informática o ingeniería de sistemas o ramas afines. (Nacional o Internacional).
* Contar con al menos un (1) postgrado o especialización en Tecnologías de la Información y Comunicación (TICs) o ramas afines (Nacional o Internacional).
* Contar mínimamente con un (1) curso o certificación en el área de Gestión de Proyectos o Auditoria de Sistemas o seguridad de la información o ethical hacking o ciberseguridad o ramas afines (Nacional o Internacional).

**(Presentar documentación de respaldo en fotocopia simple legible, de alta resolución y tamaño original de la formación y certificaciones requeridas).****Experiencia General.*** Más de tres (3) años de experiencia general en Tecnologías de la Información y Comunicación (TICs) o ramas afines

**(La misma podrá ser respaldada con fotocopias simples legibles, de alta resolución y tamaño original de: certificados de trabajo u órdenes de servicio o memorándums o contratos u otro documento similar).****Experiencia Específica:*** Más de dos (2) años de experiencia especifica en Gerenciamiento de Proyectos de tecnología o auditoria informática o Seguridad Informática u otro equivalente.

 **(La misma podrá ser respaldada con fotocopias simples legibles, de alta resolución y tamaño original de: certificados de trabajo u órdenes de servicio o memorándums o contratos u otro documento equivalente).**El **PROVEEDOR** debe presentar como **PERSONAL TÉCNICO** a dos (2) personas, cada una deberá cumplir con los siguientes requisitos:**Formación y/o conocimientos.** * Licenciatura o estudios superiores en informática o ingeniería de sistemas o ramas afines (Nacional o Internacional)
* Contar mínimamente con 2 cursos o certificaciones en el área de auditoría de sistemas o seguridad de la información o ethical hacking o ciberseguridad o ramas afines. (Nacional o Internacional)

**(Presentar documentación de respaldo en fotocopia simple legible, de alta resolución y tamaña original de la formación y certificaciones requeridas).****Experiencia General.*** Más de tres (3) años de experiencia general en Tecnologías de la Información y Comunicación (TICs) o ramas afines.

**(La misma podrá ser respaldada con fotocopias simples legibles, de alta resolución y tamaño original de: certificados de trabajo u órdenes de servicio o memorándums o contratos u otro documento equivalente).****Experiencia Específica.** * Un (1) año o más de experiencia especifica en seguridad de la información o auditoría de sistemas o ethical hacking o ciberseguridad u otro equivalente.

**(La misma podrá ser respaldada con fotocopias simples legibles, de alta resolución y tamaño original de: certificados de trabajo u órdenes de servicio o memorándums o contratos u otro documento equivalente).** |
|
|
|
|
| 1. **PRESENTACIÓN DE PROPUESTA**
 |
| La propuesta deberá ser entregada en sobre cerrado 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 la Certificación Electrónica del NIT (estado activo)
* Fotocopia simple Registro FUNDEMPRESA (vigente)
 |
| 1. **CONDICIONES DEL SERVICIO**
 |
| 1. **FORMALIZACIÓN**
 |
| La contratación se formalizara mediante la suscripción de CONTRATO.  |
| 1. **LUGAR DE PRESTACIÓN DEL SERVICIO**
 |
| El servicio se realizara en oficinas de la DNTIC ubicada en la Av. Aniceto Arce N° 2985 – Zona San Jorge, ciudad de La Paz del Tribunal Supremo Electoral u otros ambientes establecidos por la entidad o brindar el servicio en modalidad teletrabajo de acuerdo a la necesidad del servicio en días y horarios establecidos en coordinación con el Responsable o Comisión de Recepción con el fin de alcanzar los objetivos del objeto de contratación. |
| 1. **PLAZO DEL SERVICIO**
 |
| Diez (10) días calendario, computable a partir de la emisión de la orden de proceder que será entregada al PROVEEDOR adjudicado por parte de la Unidad Solicitante.El **PROVEEDOR** prestará el SERVICIO en estricto cumplimiento con la propuesta adjudicada, las Especificaciones Técnicas y el contrato, de acuerdo a siguiente tabla:

|  |  |  |
| --- | --- | --- |
| **ITEM** | **PLAZO DE EJECUCIÓN DEL SERVICIO (computable a partir de la emisión de la orden de proceder)** | **FUENTE DE VERIFICACIÓN** |
| PRIMER SERVICIO | Hasta 4 días calendario  | 1. Informe técnico de hallazgos por tipo de intrusión que incluya:
* Tipo de ataque o análisis
* Detalle de hallazgos.
* Detalle de vulnerabilidades
* Descripción de hallazgos
* Indicadores de riesgo (impacto, probabilidad, criticidad)
* Recomendaciones de solución
1. Resumen ejecutivo
 |
| SEGUNDO SERVICIO | Hasta 10 días calendario | 1. Informe de soporte de corrección de vulnerabilidades, que incluya:
* Detalle de hallazgos corregidos.
* Descripción de soluciones
* Descripción de soporte proporcionado
1. Resumen ejecutivo
 |
| 1. Informe final de resultados consolidados de todo el servicio brindado.
2. Resumen ejecutivo conclusivo de todo el servicio brindado.
 |

El **PROVEEDOR** debe enviar los informes y resúmenes ejecutivos dirigidos al Responsable y/o Comisión de Recepción del TSE por cada servicio realizado.Por aspectos de seguridad y confidencialidad, a fin de evitar fuga de información sensible, la presentación de informes y resúmenes ejecutivos del primer y segundo servicio, deberá ser en medio óptico y éstos deberán ser protegidos por contraseña proporcionada al Responsable o Comisión de Recepción. |
| 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.La retención de la garantía de cumplimiento de contrato será devuelta previa presentación de:* Informe final de resultados consolidados de todo el servicio brindado.
 |
| 1. **ANTICIPO**
 |
| NO se otorgará anticipo. |
| 1. **RÉGIMEN DE MULTAS**
 |
| El PROVEEDOR adjudicado debe cumplir con los plazos de entrega de los 2 Items, 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, el PROVEEDOR adjudicado 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. **RESOLUCIÓN**
 |
| Por suspensión del SERVICIO sin justificación alguna, por el lapso de 3 días calendario continuos, sin autorización escrita de la CONTRAPARTE. |
| 1. **RESPONSABLE O COMISIÓN DE RECEPCIÓN**
 |
| El Responsable o Comisión de Recepción será designado por el Responsable de Proceso de Contratación Directa y se encargará de realizar el seguimiento al servicio contratado, a cuyo efecto realizará las siguientes funciones:* Efectuar la recepción del servicio y dar su conformidad verificando el cumplimiento de las especificaciones técnicas.
* Emitir el informe de conformidad, cuando corresponda.
* Emitir el informe de disconformidad, cuando corresponda.
* Emitir el informe final de conformidad donde deberá solicitar la devolución de la garantía de cumplimiento de contrato del 7 % (si corresponde)
 |
| 1. **CONFIDENCIALIDAD**
 |
| La documentación producida por el **PROVEEDOR**, así como la información a la que la tuviese acceso durante o después de la ejecución del presente **SERVICIO,** 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 el **PROVEEDOR** reconoce que la **ENTIDAD** es el único propietario de la información y documentos producidos en el **SERVICIO.** |
| 1. **MONTO, MONEDA Y FORMA DE PAGO**
 |
| Los pagos se realizarán vía SIGEP, a la presentación de informes y resumen ejecutivo (medio óptico) según lo establecido en el Punto C Plazo del Servicio e informe de conformidad (emitido por el Responsable/Comisión de Recepción), y remisión de factura.El monto total por el servicio es de **Bs 130.239,43 (Ciento Treinta Mil Doscientos Treinta y Nueve 43/100 Bolivianos)**, de acuerdo al siguiente detalle:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N° DE PAGO** | **SERVICIO** | **PLAZO DEL SERVICIO (computable a partir de la emisión de la orden de proceder)** | **CANTIDAD** | **PAGO UNITARIO REFERENCIAL****(Bs.)** | **PAGO TOTAL REFERENCIAL****(Bs.)** |
| PRIMER PAGO | ÍTEM 1 | A LOS 4 DÍAS CALENDARIO | 1 | 73.948,38 | 73.948,38 |
| SEGUNDO PAGO | ÍTEM 2 | A LOS 10 DÍAS CALENDARIO | 1 | 56.291,05 | 56.291,05 |
| **Son: Ciento treinta mil doscientos treinta y nueve 43/100 bolivianos** | **130.239,43** |

 |