**TERMINOS DE REFERENCIA**

**SERVICIO DE CONSULTORÍA POR PRODUCTO PARA FORTALECIMIENTO Y MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA – ELECCIONES SUBNACIONALES 2021**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **REQUISITOS NECESARIOS DE LA CONSULTORÍA** | | | | | | |
| 1. **JUSTIFICACIÓN Y ALCANCE DE LA CONSULTORÍA** | | | | | | |
| 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.  Asimismo, en atención a las observaciones de auditoría de la Organización de Estados Americanos (OEA), 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.   Adicionalmente y en el marco de protección de datos y de la infraestructura tecnológica a ser utilizada el día de las elecciones y durante el cómputo oficial de resultados, se deben efectuar las tareas de:   * Fortalecimiento de la infraestructura tecnológica * Monitoreo de la infraestructura tecnológica | | | | | | |
| 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 07 de marzo 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, bases de datos y aplicaciones de la Institución a ser utilizados en el proceso electoral mencionado.  La consultoría abarcará 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 * 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   El proponente deberá brindar las herramientas necesarias para realizar la consultoría, sin que este implique costo adicional para el OEP. | | | | | | |
|  | | | | | | |
| 1. **ALCANCE DE LA CONSULTORÍA** | | | | | | |
| 1. **PRODUCTOS ESPERADOS** | | | | | | |
| **PRODUCTO N°** | | **DESCRIPCIÓN DEL PRODUCTO** | | **ACTIVIDADES A REALIZAR DENTRO DEL PRODUCTO** | **FUENTE DE VERIFICACIÓN** | |
| 1 | | Análisis de intrusión interna, externa a la infraestructura de Cómputo Oficial | | **ANÁLISIS DE INTRUSIÓN EXTERNA**  Análisis de intrusión 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 la empresa consultora)   **ANÁLISIS DE INTRUSIÓN INTERNA**  Análisis de intrusión desde la red interna del OEP, realizando las siguientes actividades 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 la empresa consultora) | 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 | |
| 2 | Corrección de vulnerabilidades y 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 | | 1. Informe de soporte de corrección de vulnerabilidades, que incluya:  * Detalle de hallazgos corregidos. * Descripción de soluciones * Descripción de soporte proporcionado  1. Resumen ejecutivo | |
| 3 | Fortalecimiento de infraestructura tecnológica (Hardening) | | **HARDENING**  Deberá consistir en:   * Identificación de procesos y servicios en ejecución * Identificación de cuentas de usuario * Revisión de reglas de filtrado y lista de control de accesos * Protección frente a ataques físicos o de hardware * Configuración de contraseñas * Protección de cuentas de administración * Fortalecimiento de credenciales de usuarios * Restricción de instalación de software y hardware en base a políticas de seguridad * Habilitación de sistemas de auditoría y monitoreo de logs de servidores y equipo perimetral * Aseguramiento de consolas de administración, pantallas de logueo y accesos remotos * Administración de paquetes de instalación, parches de seguridad en servidores y equipos * Aseguramiento de código fuente y software * Configuración y afinamiento de reglas en firewalls y software de seguridad * Implementación de esquemas de seguridad DMZ en base a infraestructura del OEP. * Otros (propuestos por la empresa consultora) | | 1. Informe de fortalecimiento de infraestructura tecnológica 2. Resumen ejecutivo | |
| 4 | Monitoreo y seguridad persistente | | **MONITOREO Y SEGURIDAD PERSISTENTE**  Plataforma de seguridad implementada por la empresa para monitoreo persistente 24/7 y defensa ante ataques a la infraestructura tecnológica utilizada el cómputo oficial de resultados. Dicho monitoreo debe ser ejecutado durante el proceso electoral hasta su conclusión y confirmación del OEP. Se deben ejecutar las siguientes actividades:   * Instalación de software de monitoreo y defensa. * Instalación de agentes para monitoreo y defensa, remotos. * Configuración de logs de eventos de sistema operativo, servicios web, dispositivos de red, antivirus, firewalls, active directory, etc. * Identificación de puertos y servicios de forma pasiva y activa. * Identificación de tecnologías vulnerables. * Identificación de vulnerabilidades web. * Identificación de correos electrónicos comprometidos. * Identificación de redes sociales comprometidas. * Despliegue gráfico de infraestructura externa e interna * Despliegue de tableros de monitoreo de infraestructura y eventos. * Monitoreo, alertas y defensa persistente (24/7) durante el proceso electoral, cómputo oficial de resultados, hasta su conclusión. * Capacitación al personal del OEP para acceso y consulta a la plataforma de monitoreo * Otros (propuestos por la empresa consultora)   El monitoreo no debe comprometer la integridad, disponibilidad y confidencialidad de la información y los servicios proporcionados durante el proceso electoral. | | 1. Informe de monitoreo y seguridad persistente, que incluya:  * Detalle cronológico de monitoreo * Detalle de incidentes. * Descripción de soluciones * Reportes SOC * Otros (propuestos por la empresa consultora)  1. Resumen ejecutivo | |
| * Presentación de Informe Final y Conclusivo | | 1. Informe final de resultados consolidados de la consultoría 2. Resumen ejecutivo conclusivo de la consultoría. | |
| Por aspectos de seguridad y confidencialidad, a fin de evitar fuga de información sensible, la presentación de informes y resúmenes ejecutivos de cada producto, deberá ser en medio óptico y éstos deberán ser protegidos por contraseña proporcionada al responsable o Comisión de Recepción. | | | | | |
| **B. 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 deberá presentar un listado del personal que ejecutara la presente consultoria por producto. Identificando sus roles (Tecnico – Gerente) y experiencia (años).   La empresa proponente 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.   **(Presentar documentación de respaldo en fotocopia simple de la formación y**  **certificaciones requeridas)**.  **Experiencia General.**   * + Más de tres (3) años de experiencia general en el área de sistemas Informáticos o ramas afines   **(La misma podrá ser respaldada con fotocopias simples 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 de: certificados de trabajo u**  **órdenes de servicio o memorándums o contratos u otro documento equivalente).**  El Proponente 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 el área de sistemas Informáticos o ramas afines (Nacional o Internacional).   + Contar minimamente 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.   **(Presentar documentación de respaldo en fotocopia simple de la formación y**  **certificaciones requeridas)**.  **Experiencia General.**   * + Más de tres (3) años de experiencia general en el área de sistemas Informáticos o ramas afines   **(La misma podrá ser respaldada con fotocopias simples de: certificados de trabajo u**  **órdenes de servicio o memorándums o contratos u otro documento equivalente).**  **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 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 en fotocopia simple:**   * Fotocopia simple de Número de Identificación Tributaria (NIT) y Certificación Electrónica (estado activo) * Fotocopia simple Registro FUNDEMPRESA (vigente)   (La actividad del NIT y FUNDEMPRESA debe estar asociada al servicio) | | | | | |
| 1. **CARACTERÍSTICAS DE LA EMPRESA CONSULTORA A SER CONTRATADA** | | | | | |
| 1. **PERFIL DE LA EMPRESA CONSULTORA** | | | | | |
| 1. Experiencia General: La empresa proponente deberá contar con un mínimo de tres (3) trabajos en el rubro de Tecnologías de la Información y/o Comunicación, y al menos un (1) trabajo en Seguridad de la Informacion, durante los últimos 5 años. **(Dicha experiencia podrá ser validada por documentación en fotocopia simple de alguno de los siguientes documentos: certificados de cumplimiento de contrato o contratos u órdenes de servicio u ordenes de compra o actas de conformidad o facturas o documentos equivalentes donde se mencione el servicio realizado).** | | | | | |
| 1. Experiencia Específica: La empresa proponente deberá demostrar haber realizado por lo menos tres (3) 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, incluyendo experiencia en asociaciones accidentales, acuerdos o contratos de canal o representaciones de partnership, durante los últimos 5 años. **(Dicha experiencia podrá ser validada por documentación en fotocopia simple de alguno de los siguientes documentos: asociaciones accidentales, acuerdos o contratos de canal o representaciones de partnership o 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. **CONDICIONES DE LA CONSULTORÍA** | | | | | |
| 1. **PLAZO** | | | | | |
| El plazo será de treinta (30) 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 | Análisis de intrusión interna, externa a la infraestructura de Cómputo Oficial | Hasta 7 días calendario | | 2 | Corrección de vulnerabilidades y RETEST | Hasta 14 días calendario | | 3 | Fortalecimiento de infraestructura tecnológica (Hardening) | Hasta 21 días calendario | | 4 | Monitoreo y seguridad persistente | Hasta 30 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.  La retención de la garantía de cumplimiento de contrato será devuelta previa presentación de un informe final realizado por el adjudicado  el mismo deberá contener las actividades realizadas durante la duración del contrato. | | | | | |
| 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 pago se realizará vía SIGEP, el monto total para la ejecución de la CONSULTORÍA es de Bs 589.669,93 (Quinientos Ochenta y Nueve Mil Seiscientos Sesenta y Nueve 93/100 Bolivianos)   |  |  |  | | --- | --- | --- | | **PRODUCTO N°** | **DESCRIPCIÓN DEL PRODUCTO** | **MONTO (Bs.)** | | 1 | Análisis de intrusión interna, externa a la infraestructura de Cómputo Oficial | 119.488,72 | | 2 | Corrección de vulnerabilidades y RETEST | 118.799,43 | | 3 | Fortalecimiento de infraestructura tecnológica (Hardening) | 141.518,74 | | 4 | Monitoreo y seguridad persistente | 209.863,04 |   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.** | | | | | |