



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provkse@tse.go.cr

LICITACIÓN ABREVIADA 2015LA-000009-85002

“CONTRATACIÓN DEL SERVICIO DE ANALISIS DE SEGURIDAD DE LA PLATAFORMA TECNOLÓGICA DEL TRIBUNAL SUPREMO DE ELECCIONES”

CARTEL MODIFICADO

La Proveeduría Institucional del Tribunal Supremo de Elecciones, recibirá ofertas digitales hasta las **10:00 horas del día 02 de junio de 2015**, para la Licitación Abreviada denominada “**CONTRATACION DEL SERVICIO DE ANALISIS DE SEGURIDAD DE LA PLATAFORMA TECNOLÓGICA DEL TRIBUNAL SUPREMO DE ELECCIONES** “. La oferta deberá aportarse vía digital mediante el sistema Comprared y utilizando la “firma digital”. Procedimiento para la presentación de Oferta Digital de la Dirección General de Administración de Bienes y Contratación Administrativa.

<https://www.hacienda.go.cr/rp/manuales/Manual%20oferta%20digital%20-%20proveedor%20comercial.pdf>

Para consultas y aclaraciones llamar a los teléfonos: Proveeduría Institucional: 2287-5626, fax: 2287-5805., consultas técnicas al teléfono 2287-5789 con el Ing. Esteban Brenes Hernández.

I. DESCRIPCIÓN DEL SERVICIO

ITEM	DESCRIPCION DEL SERVICIO
1	<p>Servicio para el análisis de seguridad de la plataforma tecnológica del TSE mediante pruebas éticas de penetración.</p> <p>Objetivo General</p> <p>Realizar un análisis de seguridad de la plataforma tecnológica del TSE mediante pruebas de penetración con el fin de identificar la existencia de riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información del TSE.</p> <p>En el anexo 1 de este cartel se encuentran las especificaciones técnicas de este servicio.</p>



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provts@tse.go.cr

II. ADMISIBILIDAD

- a) La Administración verificará el día de la apertura, mediante los medios electrónicos dispuestos para este fin, que el oferente, sea persona física o jurídica, se encuentre inscrito como patrono o trabajador independiente y al día con el pago de las obligaciones de la Caja Costarricense de Seguro Social (CCSS), al día con el pago de FODESAF y del Impuesto a las Personas Jurídicas, en este último caso cuando se trate de sociedades.

En caso de presentarse morosidad o exista algún inconveniente con las páginas electrónicas de consulta, esta Administración prevendrá al oferente para que en el lapso de 3 días hábiles presente la certificación que pruebe su estado al día con dichas obligaciones. Si no atiende la prevención y persiste la morosidad se declarará inadmisibles las ofertas.

- b) No se admiten a concurso las ofertas que incumplan con las condiciones legales y las especificaciones técnicas solicitadas.
- c) Toda oferta deberá suministrar la información completa y suficiente del servicio ofrecido que permita su análisis y estudio comparativo para efectos de adjudicación, sin necesidad de reiterar la aceptación de las cláusulas invariables o condiciones obligatorias, cuyo cumplimiento se presume.
- d) Se consideran excluidas las ofertas que tengan una vigencia inferior al 80% del plazo fijado en este pliego (Arts. 67 y 81 inciso f RLCA), carezcan de firma, o no indiquen el plazo de entrega o la garantía del servicio.
- e) El oferente deberá adjuntar a su oferta económica el desglose del costo de cada una de las fases del análisis de seguridad que se indican en el anexo 1.
- f) El oferente debe presentar junto con su oferta un listado de las herramientas de seguridad que utilizará para ejecutar la contratación, dentro de las cuales deberá haber al menos una herramienta de uso comercial para análisis de seguridad de aplicaciones y esta deberá figurar en alguna de las 4 posiciones del cuadrante mágico de Gartner para test de seguridad de las aplicaciones del 2014.

El cuadrante mágico de Gartner para test de seguridad de las aplicaciones del 2014 puede ser consultado en el siguiente enlace:

http://info.hpenterprisesecurity.com/LP_398558_AP_AppSec_0614?src=hp

- g) El equipo de trabajo propuesto por el oferente deberá ser encabezado por un líder de proyecto, este deberá ser profesional en ciencias de la computación, para lo cual deberá acreditar mediante fotocopia certificada por notario público, del título académico.
- h) En conjunto el equipo de trabajo del oferente deberá tener las siguientes certificaciones:
- Al menos un miembro certificado CISSP del ISC2.



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provtse@tse.go.cr.

- Al menos un miembro certificado CISM de ISACA.
- Al menos un miembro certificado CISA de ISACA.
- Al menos un miembro certificado CRISC de ISACA.
- Al menos un miembro certificado ISO 27001:2013 del BSI o el PECB.
- Al menos un miembro certificado CEH de EC-COUNCIL.

III. CONDICIONES GENERALES DE LA OFERTA

- a) La oferta debe adjuntar comprobante de pago del **timbre** de **¢200,00** (doscientos colones exactos) del Colegio de Profesionales en Ciencias Económicas (Ley 7105) extendido a la cuenta electrónica del CPCE en el Banco de Costa Rica 001-0281016-6 en colones bajo la denominación "Pago de timbres CPCECR" y el **timbre** de **¢20,00** (veinte colones exactos) de la Ciudad de Las Niñas (Ley 6496) el cual deberá adjuntarlo a la oferta digital debidamente cancelado con el sello de la empresa oferente y debidamente identificado el número de la licitación, documento que de esta forma deberá escanear e incluir en la oferta digital.
- b) Los oferentes podrán concurrir a través de cualquiera de las formas de representación contenidas en el artículo 18 del R.L.C.A y cotizar cualquier ítem de su interés.
- c) **Vigencia de la oferta:** deberá ser igual ó mayor a **60 días hábiles** a partir de la apertura de las ofertas.
- d) **Plazo de ejecución:** El contratista cuenta con un máximo de **treinta y tres (33) días hábiles** a partir de la orden de inicio dada por escrito por el órgano fiscalizador para ejecutar y finalizar la contratación. Los 33 días se desglosan de la siguiente manera:
- **9 Días desde la orden de inicio para entregar el plan de proyecto aceptado por el órgano fiscalizador.**
 - **6 Días de la fase 1.**
 - **6 Días de la fase 2.**
 - **3 Días de la fase 3.**
 - **6 Días de la fase 4.**
 - **3 Días para el informe final ejecutivo.**
- e) **Lugar de prestación del servicio:** La ejecución de las **fases 1, 2 y 4** detalladas en el anexo 1 se llevará a cabo en las instalaciones del Tribunal Supremo de Elecciones, el cual se ubica en calle 15 avenidas 1 y 3. **La fase 3** se realizará en las siguientes oficinas regionales:
- Oficina Regional de Cartago, ubicada del Polideportivo 100 metros oeste y 100 metros sur, contiguo a la Clínica Asembis.



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provts@tse.go.cr

- Oficina Regional de Heredia, ubicada de la estación del tren, 100 metros sur y 50 metros al este.
 - Oficina Regional de Puriscal, ubicada al costado norte del Parque Central, Santiago, Puriscal, San José.
- f) El oferente en la cotización deberá adjuntar el desglose de los componentes de los costos de la oferta, debiendo presentar los precios unitarios y totales, ello según las disposiciones estipuladas en los artículos 25, 26, 27 y 52 del R.L.C.A. Con especial atención a la regulación del artículo 26 anterior, en cuanto a indicar la estructura porcentual del precio.
- g) Los precios deberán ser ciertos y definitivos, sin perjuicio de eventuales revisiones. Se cotizará la oferta libre de tributos, debiéndose indicar a la vez el monto total de la oferta, en números y letras coincidentes.
- h) El oferente deberá declarar, bajo fe de juramento y en el entendido de las sanciones con que la ley castiga los delitos de perjurio y falso testimonio (artículos 311 y 316 del Código Penal), sobre los siguientes aspectos:
- Que se encuentra al día con el pago de los impuestos nacionales y municipales;
 - Que no le afecta ninguna de las prohibiciones de los artículos 22 y 22bis de la Ley de Contratación Administrativa y
 - Que no se encuentra inhabilitado para contratar con la Administración Pública.
 - La capacidad de actuar de todo oferente se presume, por lo que esa condición solamente la deberá acreditar el adjudicatario.
- i) **Órgano Fiscalizador:** Le corresponde la fiscalización al funcionario Esteban Brenes Hernández correo electrónico: ebrenes@tse.go.cr o quien le sustituya.
- j) **Modalidad y Forma de Pago:** Usual de gobierno, según se brinden los servicios autorizados por el órgano fiscalizador. El tiempo máximo para el pago de facturas, mediante transferencia bancaria, será de TREINTA DÍAS NATURALES, de conformidad con la Directriz No 033-H del 4 de marzo de 2009, publicada en el Diario Oficial La Gaceta No. 64 del 1º de abril de 2009) a partir de la presentación de la factura y una vez recibido el servicio de manera definitiva y a satisfacción del Jefe de la Sección de Riesgos y Seguridad.
- k) **Solicitud de pedido:** Esta licitación abreviada se encuentra amparada en la siguiente solicitud de pedido: **4011520349**. Puede consultar el presupuesto disponible de estos documentos o del que eventualmente les sustituyan en la siguiente dirección: <https://www.hacienda.go.cr/rp/ca/consultaTramites.aspx>
- l) Toda notificación de esta contratación se realizará por medio del Sistema Informático Comprared, de conformidad con el plazo para cada uno de los actos que se realicen.



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provtsse@tse.go.cr

- m) No se permiten ofertas conjuntas, ni la cotización parcial de la línea ni el cobro separado del transporte o acarreo.
- n) El TSE se reserva el derecho de no adjudicar alguna de las fases del análisis de seguridad.

IV CONDICIONES ESPECÍFICAS

- a) El oferente deberá presentar una declaración jurada donde se compromete a reconocer que toda la información que obtenga del TSE debe clasificarla como confidencial y que no será divulgada, además del compromiso de que únicamente el equipo de trabajo que ejecutará la contratación tendrá acceso a la información confidencial del TSE.
- b) El oferente deberá gestionar la contratación de inicio a fin como un proyecto haciendo uso de una metodología eficiente y comprobada según estándares internacionales.
- c) El oferente deberá demostrar que posee experiencia en la ejecución de pruebas de penetración, debe haber ejecutado al menos 5 pruebas de penetración en los últimos 3 años, para demostrarlo deberá adjuntar las cartas de referencia emitidas por las organizaciones respectivas.
- d) El oferente deberá garantizar por escrito en la oferta que su equipo de trabajo cuenta con la experiencia en la ejecución de análisis de seguridad y ha participado en al menos 3 pruebas de penetración en los últimos 2 años.
- e) El oferente debe presentar junto con su oferta un plan de trabajo preliminar que incluya en detalle lo siguiente:

Plan de trabajo preliminar del oferente

- Detalle las herramientas a utilizar.
- Metodología que será empleada para la ejecución de la contratación según las mejores prácticas.
- Detalle de las actividades que realizarían durante el análisis de seguridad.
- Roles y responsabilidades de su equipo de trabajo.
- Cronograma preliminar de tiempo con el detalle de la programación de las actividades.
- Considerar que aquellas pruebas potencialmente peligrosas que podrían ocasionar una interrupción de los servicios deben ser ejecutadas en horario el que comprende entre las 22:00 horas y 4:00 horas del siguiente día.



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provtse@tse.go.cr.

V SISTEMA DE VALORACIÓN Y COMPARACIÓN DE OFERTAS

Con las ofertas admisibles para una eventual adjudicación, se procederá a realizar la calificación de cada oferta, aplicando la metodología de evaluación siguiente:

Precio 100%

El puntaje se calculará de acuerdo a la razón del precio menor dividido entre cada uno de los precios de las ofertas en estudio, multiplicado por 100.

$$\text{Puntaje} = \frac{\text{Menor precio}}{\text{Precio de la oferta en estudio}} \times 100$$

Notas:

- Las ofertas deberán cotizarse preferiblemente en colones, moneda de Costa Rica. Sin embargo, si la oferta se cotiza en dólares de los Estados Unidos, para efectos de comparación de las ofertas, la conversión a colones se realizará utilizando el tipo de cambio de venta oficial establecido por el Banco Central de Costa Rica al día de la apertura de las ofertas. Para efectos de cancelación de facturas de ofertas cotizadas en dólares se utilizará el tipo de cambio venta del colón con respecto al dólar calculado por el Banco Central de Costa Rica vigente a la fecha del pago efectivo.
- El precio se deberá cotizar y se entenderá para todos los efectos, libre de los impuestos. El oferente deberá indicar el desglose porcentual del factor precio en costos directos o indirectos que componen el precio cotizado, de manera que permita revisar y resolver en forma rápida y correcta las solicitudes de revisión del precio que eventualmente formule el contratista.

Criterio de desempate de las ofertas

De conformidad con el artículo 20 de la Ley 8262, se establece como mecanismo de desempate para la adjudicación de la oferta el siguiente:

- Se preferirán a la PYME de producción nacional.
- Cuando existan dos o más PYME nacionales participando en un mismo procedimiento de contratación administrativa, la Administración aplicará los criterios del artículo No. 55 bis del Reglamento a la Ley de Contratación Administrativa.
- De mantenerse la igualdad, la Proveeduría establecerá un **SISTEMA DE RIFA** entre las ofertas que se encuentren en esa condición en presencia del analista jurídico, el analista encargado y un representante de cada una de las empresas, previa convocatoria formulada –cuando menos- el día anterior. Ante la inasistencia de alguno de los representantes, un funcionario de la Proveeduría Institucional tomará su lugar en el sorteo, en el cual se utilizarán papelitos de igual tamaño, color y uno de ellos tendrá la palabra ganador. De todo ello se levantará un acta que será firmada por los presentes y agregada al expediente administrativo.



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provts@tse.go.cr

La no asistencia de las partes no impedirá la realización de la rifa. De lo actuado se levantará un acta que se incorporará al expediente.

VI ADJUDICACIÓN

- a) El Tribunal Supremo de Elecciones, resolverá este concurso en un plazo que no podrá ser superior al doble del plazo fijado para recibir ofertas; incluyendo las prórrogas que se den. (Artículo 87 y 95 R.L.C.A.).
- b) Será adjudicataria la oferta que presente el menor precio.

VII. DEL ADJUDICATARIO O CONTRATISTA.

Una vez en firme el acto de adjudicación se deberá tomar en cuenta lo siguiente:

- a) El contratista se sujetará a las disposiciones contempladas en la normativa que rige la materia de contratación administrativa, así como a las medidas de seguridad y políticas del TSE.
- b) El contratista tiene el deber ineludible de cumplir las obligaciones laborales y de seguridad social, incluido el pago de los salarios mínimos para sus trabajadores establecido por el Ministerio de Trabajo y Seguridad Social, durante todo el periodo de ejecución contractual. La omisión de esta estipulación se tomará como causal de incumplimiento de acuerdo a la Directriz No. 34 del Poder Ejecutivo publicada en La Gaceta No. 39 del 25 de febrero del 2002, haciéndose acreedor el contratista a las sanciones establecidas en la Ley de Contratación Administrativa y su Reglamento en éstos casos.
- c) La subcontratación se admitirá hasta en un 50% del monto cotizado, para lo cual deberá aportar un listado de las empresas físicas o jurídicas a subcontratar incluyendo su porcentaje de participación en el costo total de la oferta y aportará una certificación de los titulares del capital social y de los representantes legales, en el caso de personas jurídicas.
- d) Si el contratista incumple con alguna de las condiciones establecidas precedentemente, habrá incurrido, sin más, en causal de incumplimiento de contrato. En estas circunstancias, se procederá de acuerdo con lo establecido en la normativa en contratación administrativa vigente.

VIII. GARANTÍA DE CUMPLIMIENTO

Quien resulte adjudicatario rendirá una garantía de cumplimiento en la Contaduría del TSE, dentro de los cinco (5) días hábiles posteriores a la fecha en que hubiese recibido requerimiento por escrito de la Proveeduría del Tribunal Supremo de Elecciones. Esta garantía equivaldrá al 5% del monto total anual adjudicado y tendrá un término de validez durante las ejecuciones del contrato y sesenta (60) días naturales adicionales al vencimiento del contrato incluidas las prórrogas.



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provkse@tse.go.cr

En caso de rendir garantía de cumplimiento en efectivo, deberá aportar el número de licitación para que la Contaduría del TSE emita dos comprobantes, un original para el adjudicatario para que posteriormente solicite la devolución correspondiente, y una copia que el adjudicatario debe entregar en la Proveeduría. En el caso que sea en colones, puede hacer el depósito en la cuenta N° 001-0132062-9 del Banco de Costa Rica y cuando se trate de dólares, puede hacer el depósito en la cuenta No. 100-02-000-621441, del Banco Nacional, en cualquier caso, debe presentar el recibo emitido por el banco en la Contaduría (Área de Tesorería) para que esta a su vez emita los comprobantes indicados en este punto.

En el caso de aportar la garantía en una modalidad distinta al efectivo, deberá presentar el documento original y una fotocopia, la Contaduría emitirá dos comprobantes, el original es para el adjudicatario y una copia es para adjuntarle la fotocopia del documento de garantía para que el adjudicatario los entregue en la Proveeduría.

IX. OBLIGACIONES DEL TRIBUNAL:

El Tribunal por su parte se obliga a pagar el precio pactado, siguiendo para ello el trámite que al efecto tiene establecido la Administración. Además, facilitará el ingreso del personal del contratista al lugar para que pueda cumplir con su labor.

X. SANCIONES A PARTICULARES:

El Tribunal se reserva el derecho de no tramitar las facturas que el contratista presente a cobro, si éste hubiere incurrido en alguna forma de incumplimiento respecto de las prestaciones u obligaciones aquí contraídas; todo sin perjuicio de los apercibimientos o de las otras sanciones que con arreglo a la ley proceda.

Conforme lo establece el capítulo X de la Ley de Contratación Administrativa. El contratista que durante el curso del procedimiento de contratación, incurra en las causales previstas en dicho capítulo, serán sancionados con apercibimiento e inhabilitación, según corresponda, previo debido proceso, de conformidad con lo establecido en el artículo 215 del Reglamento a la Ley de Contratación Administrativa.

XI. CESIÓN DE LA CONTRATACIÓN:

Los derechos y obligaciones derivados de un contrato en ejecución o listo para iniciarse, podrán ser cedidos a un tercero, siempre y cuando no se trate de una obligación personalísima. En todo caso, la cesión debe ser autorizada por la administración mediante acto debidamente razonado. Cuando la cesión corresponda a más de un 50% del objeto del contrato, independientemente del avance en su ejecución, deberá ser autorizada por la Contraloría General de la República. (Art. 209 del R.L.C.A.).

XII. REAJUSTE DE PRECIOS

Para los precios cotizados en colones, el cálculo de las eventuales revisiones se realizará con base en la fórmula matemática recomendada por la Contraloría General de la República, publicada en el Diario Oficial La Gaceta No. 232 del 2 de diciembre de 1982, con el artículo No. 18 de la Ley de Contratación Directa y conforme al artículo 31 del Reglamento a la Ley de Contratación Administrativa, para lo cual se deberá indicar en la oferta el desglose porcentual del factor precio en mano de obra, insumos, gastos administrativos y utilidad ($P = MO + I + GA + U$) que componen el precio cotizado, de manera que permita revisar y resolver en forma rápida y correcta las solicitudes de reajuste que eventualmente formule el adjudicatario. El derecho a revisión de los precios rige desde la presentación de la oferta y podrá ser solicitado una vez que dé inicio la ejecución contractual, una vez aportada la documentación probatoria a satisfacción al Tribunal Supremo de Elecciones, de conformidad con el artículo 31 del Reglamento a la Ley de Contratación Administrativa. El oferente deberá indicar en su oferta los renglones con que trabajará para los Índices aplicables para las fórmulas de servicios para la mano de obra y los insumos, tal y como se indica en la siguiente fórmula:

$$PV = Pc \left[MO \left[\frac{iMOtm}{iMOtc} \right] + I \left[\frac{ilti}{iltc} \right] + GA \left[\frac{iGAtg}{iGAtc} \right] + U \right]$$

Donde:

PV =	Precio variado.
Pc =	Precio de cotización
MO =	Porcentaje costo de mano de obra sobre cotización total
I =	Porcentaje costo de insumo sobre cotización total
GA =	Porcentaje costo administrativo sobre cotización total
U =	Porcentaje utilidad en precio de cotización
iMOtm =	Índice costo de mano de obra en fecha de variación
iMOtc =	Índice costo de mano de obra en fecha de cotización
ilti =	Índice costo de insumos en fecha de variación
iltc =	Índice costo de insumo en fecha de cotización
iGAtg =	Índice de gastos administrativos en fecha de variación
iGAtc =	Índice de gastos administrativos en fecha de cotización

La información sobre cada uno de los Índices aplicables a la fórmula antes sugerida, deberá ser suministrada por los oferentes según renglón, nivel o capítulo, forma en



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provitse@tse.go.cr

que se combinaron renglones, si así corresponde (promedio simple o ponderado, etc) y la fuente para cada componente serán:

- 1-Decreto de Salarios Mínimos decretados por el Consejo Nacional de Salarios del Ministerio de Trabajo y Seguridad Social.
- 2-Banco Central de Costa Rica.
- 3-Instituto Nacional de Estadísticas y Censos.

En casos de que los índices sean propios de la empresa, éstos deberán ser certificados por un contador público autorizado y sometidos a consideración de la Administración.

XIII. PEDIDO Y TIMBRES FISCALES:

Para los proveedores registrados en el Registro de Proveedores de CompraRED, las notificaciones (incluida la orden de compra) se enviará a la dirección electrónica o número de fax que conste en dicho registro, como medio para recibir notificaciones, en caso de que no se pueda realizar la notificación por los medios señalados, operará la notificación automática en los términos establecidos en el Reglamento de Utilización del Sistema de Compras Gubernamentales CompraRED 2.0.

El adjudicatario deberá cancelar el pago de especies fiscales equivalente al 0,25% del monto adjudicado más el monto proporcional por concepto de reintegro sobre el monto adjudicado, según Directriz DGABCA-15-2012 de la Dirección General de Administración de Bienes y Contratación Administrativa, de previo a la firma del contrato y/ o a la emisión de la orden de compra con firma digital.

Lic. Allan Herrera Herrera
Proveedor Institucional

ANEXO 1

ESPECIFICACIONES

El contratista deberá revisar el estado general de la plataforma tecnológica de manera tal que se puedan identificar componentes que logren comprometer la seguridad de la información.

Toda reunión que se efectuó entre el contratista y el TSE deberá realizarse en las instalaciones del TSE. El contratista deberá elaborar la minuta de la misma.

El TSE proporcionará las facilidades de conectividad para la ejecución de las actividades desde su red interna. El equipamiento para realizar la evaluación (hardware y software) lo proporciona el contratista.

El contratista deberá utilizar tanto herramientas automáticas como manuales, de uso comercial y de uso libre, las cuales deberán estar actualizadas y contener las últimas firmas de detección. Las herramientas comerciales utilizadas deberán figurar en alguna de las 4 posiciones del cuadrante mágico de Gartner para test de seguridad de las aplicaciones del 2014.

Toda información que deba extraerse de la infraestructura del TSE para ser analizada deberá ser autorizada por el órgano fiscalizador.

La ejecución de las pruebas éticas de penetración debe realizarse de manera controlada y con previa aprobación del órgano fiscalizador, Jefe de la Sección de Riesgos y Seguridad.

Se debe evitar la afectación de la plataforma tecnológica, debe minimizarse el peligro de interrupciones no programadas. En caso de que se requiera ejecutar alguna prueba que podría afectar la plataforma el contratista requerirá de autorización expresa del órgano fiscalizador además dicha prueba deberá realizarse en horario que comprende entre las 22:00 horas y las 4:00 horas, estos casos deben ser previstos en el plan de proyecto que el contratista debe realizar.

Los análisis de vulnerabilidades y pruebas de penetración deberán ser ejecutados en un ambiente controlado.

Toda vulnerabilidad que sea descubierta deberá ser verificada manualmente con el fin de confirmarla y descartar un falso positivo.



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provitse@tse.go.cr.

Toda vulnerabilidad de nivel de criticidad alta que sea detectada deberá ser informada inmediatamente y el reporte deberá incluir las recomendaciones necesarias para su remediación.

En las aplicaciones web deberá categorizar las vulnerabilidades tomando como referente la guía OWASP top 10.

El contratista debe considerar que el horario de la jornada laboral ordinaria del TSE es de lunes a viernes desde las 8:00 horas y hasta las 16:00 horas, excluyendo los días de feriados oficiales de Costa Rica. En caso de que se requiera realizar alguna actividad fuera de este horario esta debe ser indicada en el plan de proyecto.

Los reportes que son generados por herramientas de seguridad utilizados durante el análisis se consideran únicamente como un anexo a los informes técnicos, bajo ninguna circunstancia un reporte de estos será considerado como un informe. Estos reportes deberán ser anexados a los informes respectivos.

El día hábil siguiente a la emisión la orden de inicio de la contratación, el contratista deberá asistir a una reunión con el órgano fiscalizador con el fin de que este le facilite toda la información necesaria para ejecutar la contratación.

El contratista deberá elaborar un plan de proyecto que será sujeto a aprobación del órgano fiscalizador en el que se describa la estrategia de dirección de la contratación, el detalle de los roles y responsabilidades de los participante, el detalle de las actividades a realizar y los resultados esperados de cada una, un cronograma de actividades y las herramientas que serán utilizadas durante la contratación, cada actividad deberá indicar los recursos materiales y humanos requeridos así como los responsables de su ejecución.

El contratista deberá entregar formalmente el plan de proyecto al órgano fiscalizador para su revisión y aceptación dentro de los 5 días hábiles posteriores a la orden de inicio de la contratación. En caso de que el plan deba ser corregido o modificado el contratista deberá asistir una sesión de trabajo que programará el órgano fiscalizador para la integración de las correcciones o modificaciones dado que estas son vinculantes. El plan de proyecto deberá estar aprobado a más tardar el séptimo día posterior a la orden de inicio de la contratación.

Las metodologías empleadas en los procedimientos ejecutados durante la contratación deberán ser reflejadas en todos sus entregables, el contratista deberá adjuntar cualquier tabla o gráfico que permita una medición a la seguridad analizada junto con la respectiva referencia que lo vincule a información validada por la industria mundial de la seguridad, así mismo la categorización del impacto en las vulnerabilidades encontradas.

El contratista en sus informes deberá realizar recomendaciones acerca de los afinamientos en la configuración de acuerdo con los hallazgos y resultados obtenidos.

El contratista deberá plasmar un documento de hallazgos por cada componente evaluado y que contenga las recomendaciones para fortalecer las políticas de seguridad, diseño o configuración recomendada.

El análisis de seguridad consta de 4 fases que se indican a continuación:

Fases del análisis de seguridad

1. Fase 1: Pruebas de penetración externas.
2. Fase 2: Pruebas de penetración internas.
3. Fase 3: Pruebas de penetración desde oficinas regionales.
4. Fase 4: Pruebas de penetración redes inalámbricas y red de telefonía IP.

La primera fase podrá iniciar hasta que el órgano fiscalizador haya aprobado el plan de proyecto que debe efectuar el contratista.

Las fases no podrán desarrollarse simultáneamente, es decir, tras iniciar la primera de las fases, la siguiente podrá iniciar hasta que su predecesora haya concluido.

El contratista deberá entregar un informe por cada una de las fases finalizadas, este deberá ser entregado dentro de los 3 días hábiles posteriores a la finalización de la ejecución de la fase y deberá contener como mínimo lo siguiente: Objetivo y alcance, escenarios de prueba, indicación de los activos que fueron objeto de análisis, indicación de las herramientas utilizadas para el análisis en general, detalle de la técnica empleada en el análisis que permita determinar la calidad de su ejecución, amplio detalle sobre los hallazgos, detalle de los riesgos agrupados según su nivel de criticidad y por tipo de dispositivo en el cual se encuentra presente, deberá indicarse el identificador CVE (clasificación internacional) cuando corresponda e indicar claramente en cuales equipos está presente, recomendaciones y pasos a seguir en el proceso de remediación de cada una de las vulnerabilidades, conclusiones y cualquier otro detalle que el contratista considere. Cada informe será entregado al órgano fiscalizador quien lo revisará para determinar si es aceptado.

Los informes deberán estar en idioma español y se presentarán en formato PDF, MS WORD e impreso. Los reportes de las herramientas automáticas que hayan sido utilizadas no se consideran un informe como tal, estos necesariamente deberán anexarse al informe como evidencia del trabajo realizado.

El contratista en cada una de las fases del análisis de seguridad deberá cumplir los requerimientos técnicos que se detallan en las siguientes tablas, se presenta una tabla para cada una de las fases con la indicación del plazo en cantidad de días hábiles en el que debe ser ejecutada.

Fase 1: Pruebas de penetración externas.
Plazo de ejecución: 6 días hábiles.
Requerimientos técnicos
<ul style="list-style-type: none"> • El contratista a través de internet debe evaluar vulnerabilidades en los activos de información que forman parte de esta fase e intentar explotarlas. • El contratista debe analizar y categorizar las vulnerabilidades explotables a través de internet basadas en su impacto potencial y posibilidad de ocurrencia. • El contratista debe realizar las pruebas de penetración externas con técnicas de hackeo ético con acceso no privilegiado. • El contratista debe brindar las recomendaciones necesarias para mitigar y/o eliminar las debilidades.
Activos de información que deben ser analizados en esta fase
<p>El contratista deberá ejecutar esta fase en los siguientes activos de información.</p> <ul style="list-style-type: none"> • Sitio web del TSE www.tse.go.cr. • Análisis a 9 direcciones IP públicas. • 2 Controladores VPN. • 2 Enrutadores.

Fase 2: Pruebas de penetración internas.
Plazo de ejecución: 6 días hábiles.
Requerimientos técnicos
<ul style="list-style-type: none"> • El contratista a través de la red interna del TSE debe evaluar vulnerabilidades en los activos de información e intentar explotarlas. • El contratista debe analizar y categorizar las vulnerabilidades explotables a través de la red interna basadas en su impacto potencial y posibilidad de ocurrencia. • El contratista debe realizar el análisis de seguridad interno haciendo uso de técnicas de hackeo ético tanto con acceso no privilegiado

<p>como con acceso privilegiado.</p> <ul style="list-style-type: none"> • El contratista debe brindar las recomendaciones necesarias para mitigar y/o eliminar las debilidades.
<p>Activos de información que deben ser analizados en esta fase</p>
<p>Activos de información para análisis de vulnerabilidades:</p> <ul style="list-style-type: none"> • Sitio web www.tse.go.cr. • 40 Servidores físicos. • 40 Servidores virtuales. • 5 Instancias de base de datos Oracle. • 5 Instancias de base de datos SQL. • 200 PC de escritorio. • 2 Firewall. • 2 Switch Core Cisco. • 12 Switches de acceso Cisco. <p>Activos de información en los que se deben efectuar pruebas de penetración:</p> <ul style="list-style-type: none"> • 30 Servidores. • 25 Equipos de escritorio. • 5 Aplicaciones. • Sitio web www.tse.go.cr.

<p>Fase 3: Pruebas de penetración desde oficinas regionales.</p>
<p>Plazo de ejecución: 3 días hábiles.</p>
<p>Un único día para cada oficina regional.</p>
<p>Requerimientos técnicos</p>
<ul style="list-style-type: none"> • El contratista deberá realizar esta fase del análisis de seguridad desde las siguientes oficinas regionales del TSE: <ul style="list-style-type: none"> ○ Cartago (cuenta con 12 equipos de escritorio). ○ Puriscal (cuenta con 5 equipos de escritorio). ○ Heredia (cuenta con 12 equipos de escritorio). • El contratista deberá realizar una inspección física a cada una de las 3 oficinas regionales. • El contratista debe evaluar vulnerabilidades en los activos de información de la oficina regional. • Desde cada una de las 3 oficinas regionales el contratista debe realizar una prueba de penetración sobre 5 equipos de escritorio de la red interna de las oficinas centrales del TSE.

- El contratista debe brindar las recomendaciones necesarias para mitigar y/o eliminar las debilidades.

Fase 4: Pruebas de penetración a redes inalámbricas y red de telefonía IP.

Plazo de ejecución: 6 días hábiles.

Requerimientos técnicos

El contratista debe cumplir los siguientes requerimientos relacionados al análisis de seguridad de la red inalámbrica.

- El contratista debe analizar los mecanismos de autenticación y cifrado.
- El contratista debe verificar rangos de cobertura de la red.
- El contratista debe verificar la disponibilidad
- El contratista debe realizar ataques de penetración contra clientes inalámbricos a través de 4 puntos de acceso.

El contratista debe cumplir los siguientes requerimientos relacionados al análisis de seguridad de la red de telefonía IP.

- El contratista a través de la red interna del TSE debe evaluar vulnerabilidades en los servidores, aplicaciones y protocolo de telefonía IP e intentar penetrar en el servicio.
- El contratista a través de internet debe analizar la seguridad del servicio y categorizar las vulnerabilidades explotables basadas en su impacto potencial y posibilidad de ocurrencia.
- El contratista deberá ejecutar las pruebas en ambientes tanto privilegiados como no privilegiados.

Activos de información que deben ser analizados en esta fase

Equipos de telefonía

- Una central telefónica IP distribuida en 3 servidores.
- Una dirección IP pública.

Equipos de la red inalámbrica

- 2 Wireless Lan Controller.
- 12 Access Point.

El contratista deberá presentar un informe final ejecutivo dentro de los 3 días hábiles posteriores a la finalización de las 4 fases del análisis de seguridad que abarque todas las fases ejecutadas y que contenga al menos la siguiente



TRIBUNAL SUPREMO DE ELECCIONES

PROVEEDURÍA INSTITUCIONAL

Teléfono 2287-5626 Fax: 2287-5805 Email: provts@tse.go.cr.

información: Objetivo y alcance, análisis de amenazas detectadas, breve resumen de la metodología utilizada durante el análisis de seguridad, descripción general de los dispositivos analizados, descripción general de los hallazgos, recomendaciones, conclusiones y resultados, el informe deberá presentarse en formato impreso y digital (PDF, MS WORD). Este informe final será entregado al órgano fiscalizador para que sea revisado y determine si es aceptado.

Una vez que el órgano fiscalizador haya aceptado el informe final ejecutivo el contratista deberá efectuar una presentación técnica detallada de los resultados de cada una de las fases del análisis de seguridad de esta contratación. El órgano fiscalizador será quien determine la audiencia de la presentación. Esta presentación no se contabiliza dentro de los 33 días hábiles otorgados al contratista para la ejecución de la contratación.”