Operadora de Pensiones Complementarias y de Capitalización Laboral de la Caja Costarricense del Seguro Social
Teléfono 2522-3643

INVITA A PARTICIPAR EN LA

CONTRATACIÓN DIRECTA

TÉRMINOS DE REFERENCIA

"ESTUDIO POR PARTE DE UNA EMPRESA ESPECIALIZADA EN LA DETECCIÓN DE VULNERABILIDADES DE LA PLATAFORMA DE TELECOMUNICACIONES PARA LA OPERADORA DE PENSIONES COMPLEMENTARIAS DE LA CCSS"

Artículo 144 RLCA Escasa Cuantía

Contenido

1. ACLARACIONES

La Unidad de Proveeduría de la Operadora de Pensiones Complementarias de la CCSS – OPC CCSS, tendrá a su cargo el presente proceso de Contratación, donde pueden solicitar toda la información adicional que requieran al teléfono 2522-3643 o al correo proveeduria@opcccss.fi.cr con Alejandra Zúñiga Angulo.

Todas las consultas técnicas sobre este cartel, deberán presentarse al correo electrónico proveeduria@opcccss.fi.cr con copia al correo electrónico lfvargas@opcccss.fi.cr; no se permite que el oferente realice ningún tipo de consulta vía telefónica o en forma directa al responsable indicado.

2. OBJETO DE LA CONTRATACIÓN

Elaborar un análisis de vulnerabilidades de la plataforma tecnológica que utiliza la OPC CCSS mediante un estudio de penetración de seguridad, tomando en cuenta seis direcciones IP públicas configuradas en dispositivos de red, servicios y conexiones tanto a nivel del perímetro de red de la organización como en servicios de proveedores que se utilizan considerando inicialmente solo los expuestos a Internet.

3. REFERENCIA DEL COSTO ESTIMADO

El costo total estimado para esta contratación es de ¢5 000 000 (cinco millones de colones).

El estrato del límite económico en el cual la OPC CCSS se encuentra en el F, según lo indicado en la resolución R-DC-15-2018 emitido por la Contraloría General de la República.

4. CONDICIONES GENERALES

La oferta debe contener:

- Nombre de la persona física o jurídica del oferente.
- Número cédula de la persona física o cédula jurídica.
- Escaneada la cédula de identidad. En caso de ser una sociedad mercantil adjuntar la personería jurídica.
- Dirección exacta, número de teléfono, número de fax, dirección postal y correo electrónico.
- Contacto del encargado del proyecto: número de teléfono, nombre completo y correo electrónico.

5. CONDICIONES DE ADMISIBILIDAD

El oferente como empresa, debe dedicarse a la seguridad en tecnología y tener como parte de sus servicios permanentes análisis de seguridad y pruebas de penetración. Para validar este aspecto, el proveedor deberá adjuntar un brochure o copia de su página web en donde se ofrezcan este tipo de servicios.

El oferente deberá demostrar su experiencia en los últimos tres años, a partir de la fecha de la apertura, para la prestación de servicios en temas relacionados con seguridad informática, ya sea en consultoría, escaneo de equipos y/o análisis de vulnerabilidades con iguales, similares o superiores características como las solicitadas en el presente cartel. Para la atención de este punto, el oferente deberá adjuntar en su oferta una declaración jurada de los servicios brindados, para esto deberá aportar al menos cuatro cartas de referencia emitidas por clientes que incluyan: tipo de servicio realizado, periodo en el cual se ejecutó el trabajo (fecha inicio-fecha final), descripción detallada del servicio proporcionado (alcance), nombre del representante de la empresa que recibió el servicio y grado de satisfacción de la empresa donde se brindaron los servicios, teléfono y correo electrónico donde contactar al representante de la empresa que haya recibido el servicio. A través de la información emitida en la declaración mencionada la OPC CCSS, si lo considera, podrá corroborar dicha información.

El oferente debe asignar al proyecto el personal técnico mínimo que se detalla a continuación, el cual estará a cargo de la ejecución del servicio. Es indispensable que se presenten los currículos que acreditan al personal y su experiencia, así como copia de los certificados válidos en la fecha de la apertura del concurso o en su defecto prueba de la entidad certificadora que acredite las certificaciones como válidas. Debe indicarse o poder visualizar en el certificado el número de certificación, el cual podrá ser validado por la OPC CCSS directamente con la entidad certificadora.

Para la atención de este punto, la empresa deberá facilitar la documentación respectiva, suficiente y contundente, que sustente la experiencia técnica del personal que conformará el equipo de trabajo, así como una **tabla con los siguientes campos para efectos comparativos de ofertas:** número de identificación, nombre completo del funcionario, cantidad de años de experiencia y rol que ejecutará durante el servicio. Cabe destacar que una misma persona solamente podrá asumir uno de los roles citados a continuación.

El oferente deberá contar con al menos un ingeniero (grado académico mínimo de bachiller universitario en alguno de los siguientes enfoques: telemática, electrónica o informática) especializado en Seguridad en Tecnología, con experiencia mínima de cinco años en la dirección de al menos cinco proyectos, de complejidad similar al objeto de esta contratación. Para esto, el oferente deberá aportar el currículo, en el cual deberá obligatoriamente ostentar la certificación Computer Hacking Forensic Investigator (CHFI) válida y vigente a la fecha de la apertura de la oferta. El profesional mencionado deberá ser asignado al proyecto en el rol de Líder Técnico para su implementación.

El oferente deberá contar con al menos dos profesionales especializados en Seguridad en Tecnología, que figuren en el rol técnico los cuales deben tener mínimo tres años de experiencia cada uno, capacitados en la detección de vulnerabilidades y ejecución de pruebas de penetración a redes y con participación en al menos tres proyectos similares o iguales. La demostración de lo solicitado podrá realizarse mediante declaración jurada o cartas de las empresas receptoras del servicio. Adicionalmente los profesionales propuestos deberán contar con al menos la certificación EC-Council Certified Ethical Hacker (EC-CEH).

El oferente deberá aportar los currículos de los profesionales propuestos para realizar el proyecto, en los cuales se encuentre la lista de certificaciones, así como la cantidad de años de experiencia de cada uno.

6. CONDICIONES ESPECÍFICAS

6.1 Sobre la adjudicación

Los renglones o líneas definidas en las especificaciones técnicas, así como los ítems contenidos en las mismas para la presente compra, serán adjudicados en su totalidad a una sola empresa debido a la necesidad institucional de realizar el proceso de análisis para la OPC CCSS de forma atómica o unificada e integrada, por tal motivo, no se aceptarán propuestas que consideren solamente una de las líneas o renglones del cartel.

6.2 Vigencia de la oferta

En la oferta se debe indicar el plazo de vigencia de esta, el cual no podrá ser menor de 45 (cuarenta y cinco) días hábiles contados a partir de la fecha de apertura de las ofertas.

6.3 Precio

El precio debe contemplar todos los impuestos, tomar en cuenta que la OPC CCSS no es exenta de impuestos.

De acuerdo con el artículo 26 del Reglamento de Contratación Administrativa se deberá detallar con el precio cotizado una estructura porcentual del precio (precio=%MO+%I+%GA+%U) y el presupuesto detallado.

El oferente debe incluir dentro de la cotización todos los costos necesarios para realizar correctamente el servicio solicitado, cualquier dispositivo adicional, ya sea de software o hardware, o cualquier otro componente necesario para el correcto funcionamiento del servicio debe ser cotizado por el oferente.

6.4 Mejoras al precio

La administración se reserva la posibilidad de solicitar una mejora al precio ofertado dentro de los cinco días posteriores a la apertura, para lo cual hará llegar una comunicación formal en la cual definirá el día y la hora en la cual los participantes podrán hacer llegar la mejora al precio.

6.5 Plazo de entrega

El oferente debe indicar en forma escrita como parte de la oferta, el plazo de entrega en días hábiles del objeto ofertado, así como del mismo operando conforme los alcances y condiciones definidas en el cartel, funcionando a entera satisfacción por parte del responsable técnico de la contratación.

La entrega, informes de pruebas y resultado del estudio de vulnerabilidades de lo solicitado, deberá efectuarse en un plazo no mayor a **22 (veintidós) días hábiles** a partir de la entrega de la orden de compra.

6.6 Forma de pago

La OPC CCSS cancelará contra factura, de conformidad con el producto entregado y el visto bueno del responsable técnico de la compra.

Se deberá gestionar el pago mediante el Sistema de Compras Públicas SICOP a nombre de la Operadora de Pensiones Complementarias y de Capitalización laboral de la CCSS, S.A, cédula jurídica 3-101-271020.

6.7 Supervisión de la ejecución del contrato

El ingeniero Luis Fernando Vargas Díaz, jefe del área de Tecnologías de Información, será el administrador de la contratación por parte de la OPC CCSS, así como de verificar la correcta ejecución de esta contratación, por lo cual dará su aprobación de que el servicio se ha recibido a total satisfacción, previo al pago correspondiente.

El ingeniero Daniel Eduardo Lobo Mora, especialista de la Infraestructura de Tecnologías de Información, será el supervisor técnico de la contratación por parte de la OPC CCSS, mismo que será el encargado de responder todas las consultas técnicas que surjan como parte de este concurso.

6.8 Plazo de adjudicación

La OPC CCSS contará con un plazo máximo para adjudicar de 6 días hábiles.

6.9 Formalización de la contratación

Una vez perfeccionada la relación contractual con el adjudicatario, se procederá con la confección de la orden de compra mediante SICOP, donde se solicitará la cancelación de las especies fiscales respectivas; una vez recibida la cancelación de especies, se procederá con la aprobación de la orden de compra, la cual funge como orden de inicio para la ejecución contractual y corre o inicia el plazo de entrega correspondiente.

6.10 Multas

Si existiera atraso en la fecha de entrega, según el plazo definido, el contratista deberá cubrir por concepto de cláusula penal, por cada día hábil de atraso, la suma equivalente al 3% (tres por ciento) del monto total adjudicado.

6.11 Garantía de cumplimiento

El adjudicatario, dentro de los cinco días hábiles posteriores a la fecha en que quede firme el acto de adjudicación, debe depositar una garantía de cumplimiento por el 5% (cinco por ciento) sobre el total del monto adjudicado, y por cualquiera de los medios que se indican expresamente el artículo 42 del R.L.C.A.

En caso de entregarse títulos valores de inversión deberán ser endosados a nombre de la OPC CCSS. La vigencia de la garantía debe ser por el plazo ofertado más un mes adicional.

En caso de realizarla por medio de transferencia o depósito bancario, debe hacerlo mediante las cuentas siguientes:

- Cuenta corriente en colones número 100-01-095-000678-9 del Banco Nacional de Costa Rica.
- Cuenta cliente en colones número 15109510010006785 del Banco Nacional de Costa Rica.

Se debe indicar en el detalle del depósito "*Garantía de Cumplimiento y el número de la contratación.* Además, debe ser otorgada en la misma moneda en la cual se cotizó la oferta. Si la moneda adjudicada es el dólar de los Estados Unidos de América (E.E.U.U.), y la garantía se entrega en efectivo, se deberá depositar el monto equivalente en colones, considerando el tipo de cambio superior a la de la fecha del depósito, para prever eventuales variaciones.

6.12 Recepción provisional y definitiva del servicio

Una vez definida la fase de planificación, el adjudicatario en conjunto con la OPC CCSS iniciará la ejecución y documentación del estudio requerido por lo que el adjudicatario deberá brindar estrecha colaboración a los personeros que la OPC CCSS designe y que formen parte del proyecto.

El proyecto se recibirá en forma definitiva a entera conformidad de la OPC CCSS, solamente cuando en la revisión técnica se pueda verificar el cumplimiento de todos los requisitos y obligaciones de la contratación en forma correcta por parte del adjudicatario y cuando, además, se haya finalizado con la fase de implementación, así como con la entrega de la documentación que resulte necesaria para acreditar tal cumplimiento, todo a criterio del responsable técnico de la contratación.

Se deberá formalizar una fase de cierre del proyecto, en la cual se entregue la documentación requerida, su alcance, recomendaciones, capacitación y cualquier otro elemento necesario solicitado en el pliego de condiciones.

7. METODOLOGÍA DE CALIFICACIÓN DE OFERTAS

Para efectos de la calificación de ofertas se utilizarán los siguientes criterios:

Cuadro N°1. Metodología de calificación

Criterio	Aspecto Evaluado	Puntaje
Precio	Precio	**70%**
Experiencia del Personal	Años de experiencia adicionales a los solicitados en el cartel	**15%**
Certificaciones del Personal	Cantidad de certificaciones adicionales	**15%**

Precio (70 puntos – Cuadro N°1)

A la oferta con el menor precio se le asignarán 70 puntos. A las demás ofertas se les aplicará la siguiente fórmula:

$$\frac{Oferta\ de\ menor\ costo}{Oferta\ a\ valorar} * 70$$

Experiencia del Personal (15 puntos – Cuadro N°1)

Se asignará puntaje (hasta un máximo de 15 puntos) sobre los años adicionales de experiencia a los exigidos en el apartado Condiciones de Admisibilidad según la siguiente tabla de años de experiencia adicionales que tenga el personal que ejecutará el proyecto. La cuantificación de la experiencia se realizará de la siguiente forma:

$$Experiencia\ del\ personal = \frac{\sum Experiencia\ individual}{\text{Cantidad de personal propuesto}}$$

De 1 años a 2 años de experiencia adicionales del equipo de trabajo	5%
De 3 años a 4 años de experiencia adicionales del equipo de trabajo	10%
De 5 años de experiencia o más adicionales del equipo de trabajo	15%

Certificaciones del Personal (15 puntos – Cuadro N°1)

Se asignarán 3 puntos (hasta un máximo de 15 puntos) por cada certificación adicional a las exigidas en el apartado Condiciones de Admisibilidad que posea el personal propuesto para desarrollar el proyecto (NO se tomará en consideración para esta ponderación, personal del oferente que NO participe en forma directa en el proyecto y NO sea parte del equipo de trabajo propuesto para atender la implementación requerida en el presente cartel).

Las certificaciones y/o competencias sobre las cuales aplicará el puntaje mencionado será solamente sobre las siguientes:

- EC-Council Certified Security Analyst (ECSA)
- Certified EC-Council Instructor (CEI)
- Offensive Security Certified Professional (OSCP)
- Certified in Risk and Information Systems Control (CRISC)
- Senior Security Tester (SST)
- GIAC Certified Penetration Tester (GPEN)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- Certified Information Systems Auditor (CISA)

8. ESPECIFICACIONES TÉCNICAS DE LA CONTRATACIÓN

Las especificaciones técnicas del objeto del contrato se detallan en el anexo 1.

9. OBSERVACIONES FINALES

En todo lo no previsto en estas especificaciones se aplicará la Ley de Contratación Administrativa, su Reglamento y el Reglamento Interno de Compras de la OPC CCSS publicada en La Gaceta alcance N° 134 del 20 de julio 2018.

MARIA ALEJANDRA ZUÑIGA ANGULO (FIRMA)

Firmado digitalmente por MARIA ALEJANDRA ZUÑIGA ANGULO (FIRMA)
Fecha: 2018.11.01 09:36:14 -06'00'

ANEXO No. 1

ESPECIFICACIONES TÉCNICAS

10. CONSIDERACIONES TÉCNICAS GENERALES

10.1 La entrega del servicio requerido se llevará a cabo en las instalaciones de la OPC CCSS en San Pedro Barrio Dent de la Esquina Noreste del Mall San Pedro 200 metros oeste y 200 metros norte, sobre el Boulevard Dent.

10.2 El adjudicatario NO podrá conectar equipo alguno a la red de la OPC CCSS sin la autorización respectiva del Área de Tecnologías de Información, para lo cual el oferente debe aceptar, cumplir y respetar los lineamientos al respecto de la OPC CCSS.

10.3 El adjudicatario deberá proveer todo lo referente a equipos y software utilizado por sus técnicos o funcionarios, requeridos para la correcta ejecución y pruebas del servicio a realizar, por ejemplo: sistema operativo de las máquinas del equipo de trabajo, antivirus, aplicaciones generales, ofimática, herramientas de configuración y cualquier otro software complementario. Todos los costos asociados correrán por cuenta del oferente que resulte adjudicado.

10.4 El oferente que resulte adjudicado deberá aceptar las condiciones sobre políticas y reglamentos internos de la OPC CCSS que le apliquen durante la ejecución de sus labores, para lo cual deberá expresamente en la oferta dejar constancia sobre su aceptación.

10.5 El oferente que resulte adjudicado no deberá almacenar información de la OPC CCSS sin previa autorización. No se permitirá el uso de discos flexibles, cintas, unidades de almacenamiento externo, “quemado” de discos compactos, ni cualquier otro dispositivo similar; ni envío de papelería con información crítica o altamente sensible ya sea por fax, carta u otros.

10.6 El servicio que se brinde, una vez firmado el contrato, deberá ser idéntico en todo detalle al indicado previo a la firma de este, no aceptándose la entrega de un tipo diferente de producto y/o servicio.

11. PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

11.1 El adjudicatario y su personal deberán comprometerse a utilizar y procesar todos los datos institucionales dentro de un ámbito de discreción, privacidad e integridad, de acuerdo con las políticas de control y seguridad institucionales. En ninguna circunstancia el adjudicatario podrá utilizar información de la OPC CCSS para propósitos no contemplados en los procedimientos normales de desarrollo del servicio solicitado. La utilización indebida o negligente de los recursos institucionales, por prácticas imputables al adjudicatario, serán consideradas factores de incumplimiento a la contratación y objeto de las sanciones administrativas y penales correspondientes.

11.2 Es obligación del adjudicatario presentar firmado, ante la proveeduría institucional, dentro de los tres días hábiles siguientes al comunicado de orden de compra, un documento como compromiso de confidencialidad de cualquier información que, debido a su trabajo, la empresa o el personal de esta conociere. De requerirse la salida de información de los sistemas de la OPC CCSS, se hará bajo permiso expreso del responsable técnico de la contratación; el adjudicatario deberá efectuar la solicitud por escrito con la respectiva justificación. La OPC CCSS no está obligada a permitir la salida de dicha información si contraviene sus intereses.

11.3 Para la atención del punto anterior, el oferente que resultase adjudicado con la contratación para la elaboración de cualquier producto descrito en el presente cartel se compromete a cumplir a cabalidad lo indicado en la siguiente cláusula de acuerdo de confidencialidad:

ACUERDO DE CONFIDENCIALIDAD: El adjudicatario reconoce que en el desempeño de las labores que llevará a cabo en virtud de este contrato, podrá tener acceso a información estrictamente confidencial de la OPC CCSS. Que en virtud de la negociación que iniciarán las partes, la OPC CCSS ha revelado, o podrá revelar al adjudicatario, y ambas partes pueden haber tenido acceso o conocimiento o podrán tenerlo a cierta información confidencial, ya sea en forma oral o escrita, posteriormente confirmada en documentos impresos o electrónicos, y; que es esencial para las partes que durante el curso de la negociación y en todo otro momento posterior, las partes, su personal o cualquier tercero que tuviere acceso a ella, no divulgue, revele o comunique de forma alguna, sea directa o indirectamente, a ninguna persona (física o jurídica), excepto cuando ello redunde en beneficio de las partes, cualquier información confidencial que una parte pudiese haber adquirido en el curso de su relación contractual con la otra parte. La expresión “Información Confidencial” comprenderá toda información que haya sido proporcionada por la OPC CCSS al adjudicatario de manera escrita, ya sea por medio electrónico y/o impreso, o aquella información que haya sido proporcionada de forma oral y que haya sido confirmada posteriormente por escrito en forma electrónica y/o impresa, la cual podría referirse a secretos, know-how, registros, informes, especificaciones, información técnica, análisis, estudios, mapas, modelos, propuestas e interpretaciones; e información comercial, contractual, legal y financiera, incluyendo, sin limitarse a evaluaciones de mercado, identificación e información sobre clientes o clientes potenciales, inversiones y acuerdos sobre desarrollo de proyectos, cartas de intención, acuerdos preliminares de entendimiento, desarrollo de planes de presupuesto, contratos de proyecto, los borradores respectivos y los cronogramas; contratos financieros, modelos y propuestas; y toda comunicación, nota, evaluación, recomendación o proposición y similares relacionadas con lo antedicho; planes, estrategias, costos, usos, aplicaciones de productos y servicios, resultado de investigaciones o experimentos, y todo aparato, producto, proceso, composición, muestra, fórmula, programa de computación, política de precios, información financiera, método de hacer negocios, manuales de procedimiento, procedimientos para capacitación y reclutamiento, procedimientos contables, estado y contenido de los contratos de la OPC CCSS con sus clientes y/o proveedores y consultores, la filosofía de negocios de la OPC CCSS, los métodos y técnicas de fabricación y servicios

utilizados, desarrollados, investigados, creados o vendidos por la OPC CCSS, antes o durante el período de relación profesional y que no están disponibles al público en general, o que a OPC CCSS mantiene en confidencialidad (para efectos de este documento la “Información Confidencial”). Las partes convienen, salvo lo dispuesto en este acuerdo, en no revelar, usar, copiar o permitir que se copie en ningún momento, ya sea durante o luego de terminada la relación contractual entre las partes, ninguna información confidencial sin el consentimiento previo de la OPC CCSS. El adjudicatario manifiesta que durante y con posterioridad a la vigencia de este contrato, no utilizará la información para fines distintos de los estrictamente requeridos para el desarrollo de las labores descritas en este cartel. La OPC CCSS autoriza desde ya a usar y revelar la Información Confidencial sólo dentro de la respectiva organización del adjudicatario y solo con sus empleados, asesores, directores, gerentes o socios, u otras entidades financieras quienes necesitan conocer esa información para el desarrollo de los negocios conjuntos entre las partes, bajo el entendido que dichos empleados, asesores, directores, gerentes o socios, u otras entidades financieras preservarán y protegerán la confidencialidad de la información con todos los alcances expresados en este acuerdo. El adjudicatario conviene en adoptar todas las medidas necesarias a fin de proteger la información confidencial del uso no autorizado, la reproducción, copia y/o divulgación, y proteger la información confidencial por lo menos con el mismo empeño como si protegiera su propia y más valiosa información confidencial. En el caso en que el adjudicatario se vea obligado a revelar la información confidencial total o parcialmente en virtud de orden judicial, o de cualquier otra autoridad competente, deberá informar inmediatamente a la OPC CCSS de tal situación y el adjudicatario desde ya acepta que ante este hecho entregue a las autoridades respectivas la información solicitada, quedando exonerada de toda responsabilidad derivada de dicho acto, lo cual es aceptado por la OPC CCSS. El adjudicatario se compromete a tomar todas las medidas necesarias para evitar que sus empleados, funcionarios y apoderados hagan uso indebido de la información, en caso de que sucediera lo antes descrito, el adjudicatario será responsable por los daños y perjuicios ocasionados. El adjudicatario entiende que la protección de la información confidencial es crítica a los intereses de la OPC CCSS y que su uso no autorizado, copia o revelación causaría un daño irreparable a la OPC CCSS y/o a sus actividades. En consecuencia, el adjudicatario será responsable y acuerda en indemnizar y mantener indemne a la OPC CCSS por los daños y perjuicios, por haber revelado de cualquier forma la información confidencial de la OPC CCSS. Asimismo, el adjudicatario manifiesta que no revelará dicha información confidencial a terceros, sin la previa autorización por escrito de la OPC CCSS. Esta obligación de respetar la confidencialidad aquí asumida subsistirá después de finalizada por la causa que fuere la contratación detallada en el presente cartel. Este acuerdo de confidencialidad no surtirá efectos sobre aquella información, que de conformidad con la legislación costarricense ha de considerarse de interés público.

11.4 De comprobarse divulgación, parcial o total, de la entidad por parte del adjudicatario, la OPC CCSS procederá a realizar las acciones necesarias para que se apliquen las sanciones correspondientes según la Ley.

11.5 La OPC CCSS no está en la obligación de acceder a la solicitud de salida de información ya sea de sus sistemas informáticos o alguna otra información de cualquier índole solicitada por la empresa adjudicada.

11.6 Si el adjudicatario incumple con lo estipulado en la Ley N° 8968 Protección de la Persona frente al Tratamiento de sus Datos Personales y su Reglamento, la OPC CCSS S.A, tendrá derecho a ser indemnizada en su totalidad por cualquier daño en sus bienes y sus derechos.

12. ASPECTOS TÉCNICOS GENERALES

12.1 La OPC CCSS se reserva el derecho de solicitar al oferente el detalle de información técnica de los dispositivos, metodología y herramientas de análisis, para validar que cumplan con los requerimientos definidos en el cartel.

12.2 El servicio adjudicado deberá ser ejecutado a entera satisfacción por parte de la administración de la OPC CCSS conforme las condiciones indicadas en el cartel.

12.3 Si durante la ejecución del servicio, el adjudicatario dañara o afectará cualquiera de los activos de la OPC CCSS por razones de omisión, negligencia, ejecución técnica indebida o ejecución técnica no autorizada por la OPC CCSS, el adjudicatario se hará responsable de reparar o sustituir los componentes dañados o afectados sin costo alguno para la OPC en un plazo razonable previamente aprobado por la OPC CCSS. Si por el daño o afectación causada, se viera interrumpida la continuidad en la prestación de los servicios de la entidad, el adjudicatario deberá cubrir todos los costos necesarios o adicionales que fueran requeridos para restablecer la prestación de los servicios de la OPC CCSS que quedaron fuera de operación, producto de los daños o afectación presentada. La OPC CCSS se reserva el derecho de entablar los procesos legales correspondientes, a fin de que le sean resarcidos los montos estimados, por los daños y perjuicios ocasionados durante el tiempo en que sus servicios estuvieron fuera de operación.

12.4 El adjudicatario deberá considerar la **ejecución de un segundo proceso** como el solicitado en un periodo de seis meses después de aprobado y entregado el primero servicio para lo cual, deberá considerar en su oferta económica la realización de este. El mismo deberá elaborarse con base en los hallazgos identificados y soluciones propuestos en el primer análisis a efecto de verificar las correcciones realizadas por parte del área técnica para mitigar la vulnerabilidad expuesta.

13. GARANTÍA DEL OBJETO

13.1 El adjudicatario debe brindar garantía sobre el servicio de (1) mes, posterior a la recepción definitiva de la solución por parte de la OPC CCSS. Esta garantía debe cubrir lo estipulado en este cartel.

13.2 La garantía aplicará sobre fallas en el producto entregado, entendiendo por falla todas aquellas condiciones que no estén de acuerdo con las especificaciones solicitadas por la OPC CCSS en la contratación.

13.3 Durante el periodo de vigencia de la garantía todos los gastos (incluido la mano de obra) incurridos correrán por cuenta del oferente.

13.4 El contratista deberá brindar una garantía adicional de al menos dos (2) meses posteriores a la recepción definitiva de la solución en la cual se compromete a corregir cualquier inconveniente que surja por defectos de ejecución conforme lo solicitado en la contratación y quedará a disposición de atender cualquier incidencia o falla relacionada con el servicio entregado durante el periodo de vigencia de la garantía. Se exonera de dicha garantía al contratista en caso de determinarse una modificación que atente contra la integridad del servicio ejecutado y que la misma haya sido realizada por parte del personal de la OPC CCSS o un tercero.

13.5 La garantía solicitada en el punto anterior deberá venir por escrito y firmada por el representante legal de la empresa o en su defecto, quien esté facultado para tal acto

14. DOCUMENTACIÓN

14.1 Toda la documentación generada y entregada en cualquier etapa del proceso, una vez adjudicada la contratación al proveedor respectivo, debe ser debidamente validada y aprobada por el personal del área de Tecnologías de Información de la OPC CCSS autorizado y asignado para tal fin.

14.2 Durante la implementación del(os) servicio(s), se requiere la entrega de los siguientes documentos en formato digital editable (formato Word):

- Documentación de la reunión de inicio de proyecto y su respectiva acta de inicio de proyecto con las revisiones que se estimen y sus ajustes aprobados por la OPC.
- Cronograma inicial del proyecto con la totalidad de actividades a ejecutar, así como sus respectivas revisiones (versiones) y ajustes aprobados (cambios al cronograma).
- Lista de chequeo o similar detallada de la totalidad de la implementación a realizar (con explicación de las acciones ejecutadas) en donde la versión final de dicho documento corresponda exactamente con lo realizado al momento de avalarse la entrega del servicio.
- Documentación de la reunión de cierre de proyecto y su respectiva acta de cierre de proyecto.

14.3 Para la generación de la documentación antes señalada, el oferente debe considerar al menos como parte de la estructura de los documentos que así lo permitan, una portada,

un índice o tabla de contenido, una descripción general del documento, un segmento para revisión (versiones) y un segmento de aprobación que considere al menos fecha, ejecutores y revisores, apéndices o anexos y glosario cuando aplique. Adicionalmente, el documento deberá tener fuentes de apoyo para la revisión de la información contenida tales como capturas de pantalla, esquemas, secuencias y cualquier otro elemento que le permita al lector comprender fácilmente el documento y los procedimientos incluidos (cuando aplique), mismo que deberá conservar un orden lógico de ideas, temas y subtemas incluidos en este.

14.4 El adjudicatario debe suministrar suficiente documentación técnica (catálogos, manuales técnicos, pruebas) que especifique las características del servicio, entre estas: metodología, tipo de prueba, modelo, herramientas utilizadas para el escaneo, informe de resultados. Esta deberá presentarse en forma escrita o digital en idioma español o inglés para la verificación por parte del personal técnico de la OPC CCSS.

14.5 La presentación del informe ejecutivo o gerencial deberá ser realizado de forma presencial con apoyo visual, en la misma se deberán explicar los hallazgos detectados, sus soluciones y se deberán atender las consultas del personal presente.

14.6 Tanto el informe ejecutivo como los informes técnicos deberán ser redactados en idioma español.

14.7 Para la presentación de los informes finales (a nivel técnico y gerencial) se debe incluir los siguientes puntos generales.

14.8 La portada deberá considerar al menos:

- Título del informe
- Fecha final de entrega del informe
- Nombre completo de los autores del informe y sus respectivos roles durante la ejecución del proyecto
- Nombre de la empresa adjudicataria del servicio
- Nombre de la empresa receptora del servicio

14.9 La sección de control del documento debe contener al menos:

- Historial de versiones (manejo de versiones, fecha de cambios, responsable(s) de ejecutar el(os) cambio(s), descripción del(os) cambio(s))
- Firma y nombre completo del personal responsable de ejecutar las pruebas y del personal encargado de aprobar el informe final.

14.10 La tabla de contenido deberá indexar cada una de las secciones del informe mediante la definición de índices numerales de página.

14.11 La tabla de ilustraciones deberá indexar cada una de las imágenes, cuadros, diagramas, tablas, reportes, gráficos, anexos al informe mediante la definición de índices numerales de página.

14.12 Se deberá incluir el alcance a través del cual se debe identificar el marco de acción en el cual se basará la formulación del informe.

14.13 Se deberán incluir los objetivos a cumplir mediante el desarrollo del informe, los cuales deben ser coherentes con la definición de objetivos del presente cartel.

14.14 Se debe incluir un apartado de Anexos conformado por todos aquellos documentos, evidencias, imágenes y otros elementos que resulten del desarrollo del estudio, que permita referenciar los hallazgos y conclusiones del informe.

14.15 Se debe incluir un apartado de Glosario conformado por un listado de conceptos con sus correspondientes definiciones y explicaciones, a modo de enciclopedia o diccionario.

14.16 Se debe incluir un apartado de Bibliografía conformado por los recursos usados como referencia para el desarrollo del presente informe, dicha bibliografía debe seguir los lineamientos según las normas de la American Psychological Association (APA).

14.17 Deberá desarrollarse como parte de los informes finales un resumen ejecutivo mediante un breve análisis de los aspectos más relevantes que resultaron durante el desarrollo del proyecto con base al contexto de cada uno de los informes. El mismo debe dar a conocer de forma resumida la metodología implementada, hallazgos, resultados y recomendaciones de alto nivel. El límite máximo del resumen ejecutivo corresponde a una página.

14.18 El informe a nivel gerencial debe ser de fácil asimilación, la presentación de los resultados en forma práctica, orientado a su exposición de manera ejecutiva; el adjudicatario debe contemplar realizar la exposición ante la administración, con la visita de al menos un representante en la oficina de la OPC CCSS de forma presencial, el expositor podrá apoyar en caso de requerirse su presentación con el uso de videoconferencia incluyendo al personal técnico que ejecutó el estudio.

14.19 El informe gerencial solicitado además de los puntos generales por informe debe tomar en consideración los siguientes puntos:

- Incluir un resumen de hallazgos con la enumeración de todas las vulnerabilidades detectadas, ordenadas y priorizadas según el nivel de riesgo que representa, utilizando para ello al menos reportes gráficos (matrices de riesgo basadas en mapas de calor) para la representación cualitativa de los niveles de riesgo, de acuerdo con el conjunto de vulnerabilidades detectadas durante la ejecución del proyecto.

- Incluir un resumen de conclusiones sobre los riesgos identificados y las consecuencias asociadas a estos ante la materialización de dichos riesgos.

- Incluir un resumen de recomendaciones y contramedidas con la enumeración y descripción de cada una de las acciones pertinentes y priorizadas para lograr corregir o mitigar las vulnerabilidades encontradas en orden de prioridad, tomando en consideración para ello la valoración de riesgos.

14.20 Se deben entregar un informe detallado de lo siguiente, como producto del desarrollo del estudio:

- Direcciones IP revisadas y su estado durante la revisión (activa - no activa).
- Equipos de red detectados dentro del perímetro de red expuesto a Internet.
- Puertos y protocolos según el estado (abierto, cerrado y filtrado).
- Vulnerabilidades validadas y ordenadas según nivel de riesgo por cada uno de los puertos y protocolos de red detectados.
- Vulnerabilidades detectadas, ordenadas y priorizadas según nivel de riesgo por cada uno de los equipos de la red interna y direcciones IP detectadas.
- Servicios de red expuestos a Internet.
- Vulnerabilidades validadas y ordenadas según nivel de riesgo por cada uno de los servicios de aplicaciones web detectados.
- Gráficos que permitan una representación cuantitativa de las vulnerabilidades encontradas, mediante la formulación de los siguientes reportes:

  - Gráfico según cantidad de vulnerabilidades por direcciones IP.
  - Gráfico según cantidad de vulnerabilidades por equipos de red.
  - Gráfico según cantidad de vulnerabilidades por servicios de red.
  - Gráfico del top N de equipos con más vulnerabilidades detectadas.

14.21 Informe a nivel técnico que comprenda un detalle de los procedimientos utilizados y tareas realizadas para ejecutar las pruebas, métodos para validar los hallazgos encontrados, clasificación y priorización de las vulnerabilidades según nivel de riesgo, descripción de amenazas expuestas, así como las acciones necesarias y/o recomendaciones para mitigar o corregir cada una de las vulnerabilidades detectadas

14.22 El informe técnico solicitado además de los puntos generales por informe debe tomar en consideración los siguientes puntos:

- Escenario de red identificado con al menos el siguiente apartado:

  - Diagrama lógico, que represente las configuraciones actuales de los equipos de red con base en direcciones IP, puertos y protocolos, permitiendo definir las políticas de filtrado.

- Descripción detallada de cada una de las pruebas ejecutadas con al menos:

    - Fecha y hora de ejecución.
    - Responsable técnico que realizó la prueba y el(los) responsable(s) de validar la ejecución.
    - Definición de herramientas y métodos utilizados para llevar a cabo la prueba.
    - Ámbito de ejecución, donde se detalle la serie de elementos de red (puertos, protocolos, servicios, equipos, direcciones IP) que se vieron inmersos durante la ejecución de la prueba.
    - Objetivo principal de cada prueba.
    - Descripción del procedimiento de realización de la prueba, donde se definan la serie de pasos necesarios para su ejecución.
    - Conclusiones y enumeración de vulnerabilidades, mediante el análisis y validación de los resultados de la prueba.
    - Referencias a los anexos que evidencien objetivamente la ejecución de la prueba y sus resultados.

- Análisis de cada una de las vulnerabilidades encontradas con al menos:

    - Clasificación de la vulnerabilidad según nivel de riesgo e impacto.
    - Descripción técnica y específica (concisa) de la vulnerabilidad.
    - Descripción de la serie de métodos de cómo se aprovecharía la vulnerabilidad por parte de agentes externos malintencionados.
    - Definición de la serie de amenazas priorizadas, a las que se está expuesto dado la vulnerabilidad encontrada.
    - Definición de los elementos de red y servicios que se ven afectados directa o indirectamente ante las amenazas producto de la vulnerabilidad.
    - Referencias a los anexos y bibliografía que permitan ahondar en información acerca de la vulnerabilidad encontrada.

- Plan de acciones para corregir o mitigar cada una de las vulnerabilidades con al menos:

    - Responsable técnico que definió las acciones recomendadas.
    - Clasificación de las recomendaciones según niveles de criticidad o riesgos.
    - Correlación de acciones con respecto a cada vulnerabilidad por corregir o mitigar.
    - Definición de cada una de las acciones de forma detallada, cada recomendación deberá ser descrita con base al criterio del propio responsable de la definición de las acciones, tomando en cuenta que la recomendación sea fehaciente, evitando que las mismas sean planteadas de manera general y poco práctica.
    - Priorizar y ordenar cada una de las acciones necesarias según un orden lógico para corregir o mitigar cada vulnerabilidad.
    - Definición de los recursos, conocimientos técnicos, prácticas de monitoreo, configuraciones, entre otros elementos que se consideren necesarios, para poder llevar a cabo las acciones recomendadas por vulnerabilidad identificada.

15. CONSIDERACIONES DE LA CONTRATACIÓN

CARACTERISTICAS GENERALES

15.1 Analizar la situación actual de la seguridad de telecomunicaciones mediante un estudio de vulnerabilidades de los elementos de red expuestos a internet.

15.2 Implementar pruebas de reconocimiento, escaneo y verificación que permitan enumerar cada una de las vulnerabilidades.

15.3 Alinear las pruebas, informes y conclusiones con base en las mejores prácticas de estándares y metodologías aceptadas en términos de procesos de elaboración de análisis de vulnerabilidades mediante estudios de penetración.

15.4 Clasificar y priorizar las vulnerabilidades encontradas de acuerdo con niveles de riesgo e impacto para la organización.

15.5 Formular una serie de soluciones o acciones que permitan corregir o mitigar los riesgos ante cualquier elemento externo malintencionado, validando la efectividad de las medidas aplicadas para minimizar las vulnerabilidades encontradas.

CONDICIONES DEL ANÁLISIS

15.6 Las pruebas de penetración serán únicamente de forma externa, por lo cual el adjudicatario no tendrá ni necesitará acceso lógico, físico o información alguna de la arquitectura tecnológica de la OPC CCSS.

15.7 Se deberán documentar previamente las IP públicas que utilizará el adjudicatario para ejecutar las pruebas de penetración, esto con el fin de separar el estudio de penetración de posibles ataques reales, las mismas deberán ser notificadas a la OPC CCSS antes de iniciar las pruebas de penetración.

15.8 La evaluación técnica de las vulnerabilidades debe imitar las prácticas de un ataque con “cero-conocimiento” ejecutado desde Internet hacia la plataforma de servicios de conexión externa de la OPC CCSS (“caja negra”).

15.9 Las pruebas podrán realizarse a cualquier hora del día y/o noche, siempre y cuando se garantice que la ejecución de estas no afecte el rendimiento ni la continuidad de las operaciones y servicios de la OPC CCSS.

15.10 Los mecanismos y métodos que se utilicen deben basarse en “ethical hacking” y tienen que ser capaces de ejecutar las pruebas de forma controlada, quedando totalmente prohibido todo tipo de pruebas de denegación de servicios.

15.11 No se permite el uso de técnicas de ingeniería social (envió de correos electrónicos fraudulentos, phishing, llamadas telefónicas, uso de software malicioso, manipulación) para la obtención de información sensible.

15.12 Se debe contar con mecanismos que permitan monitorear continuamente el ancho de banda, con el objetivo de determinar si las pruebas ameritan pausarse por posibles saturaciones de red, procurando siempre no afectar la calidad ni disponibilidad de los servicios brindados por la OPC CCSS.

15.13 Las pruebas deben realizarse individualmente al menos para cada una de las IP públicas y equipos expuestos en el perímetro de red accesible desde Internet.

15.14 Las pruebas deberán ser capaces de permitir realizar un sondeo o detección de la red expuesta a Internet con el objetivo de obtener información expuesta de los servicios y de los equipos de telecomunicaciones, terminales de conexión y servicios habilitados, permitiendo describir amenazas potenciales de seguridad de los recursos, según sus características y configuración inferida, a fin de determinar con exactitud potenciales amenazas y vulnerabilidades a que están expuestos los elementos antes mencionados.

15.15 Se deberá presentar el análisis de la arquitectura de red y su topología, donde se identifique los componentes tecnológicos que son críticos para la OPC CCSS.

15.16 Las pruebas deben ser exhaustivas, efectivas y comprobables, que permitan determinar cada una de las vulnerabilidades y discernir los falsos positivos que se puedan generar.

15.17 Los mecanismos y herramientas utilizadas en cada una de las pruebas deben brindar una serie de evidencias objetivas y debidamente documentadas que demuestren claramente cada una de las vulnerabilidades que se encontraron producto del estudio, el oferente podrá utilizar como metodología de referencia la “OSSTMM – Open Source Security Testing Methodology Manual” o la “EC-Council Ethical Hacking Methodology” así como alguna otra metodología estándar similar reconocida y aceptada por la OPC CCSS de previo a la ejecución del servicio.

15.18 La metodología técnica por seguir debe tomar en cuenta al menos las fases de reconocimiento, escaneo, análisis de vulnerabilidades, evaluación de riesgos e informes.

15.19 Se debe aplicar una variedad de técnicas suficientes para la fase de reconocimiento (“information” “gathering”, “footprinting”, “system hacking”) que permita obtener al menos la ubicación, rangos de direcciones IP, proveedores de conectividad, resolución de nombres de dominio y servicios habilitados.

15.20 El oferente debe efectuar al menos las siguientes revisiones de seguridad: escaneo de puertos de todas las direcciones del segmento, pruebas de penetración a los servicios publicados y análisis de vulnerabilidad a aplicaciones Web, análisis de vulnerabilidades de los elementos de infraestructura del segmento público.

15.21 El oferente a través del uso de herramientas especializadas deberá ser capaz de detectar las principales vulnerabilidades a nivel de aplicación tales como “Code Revelation”, “Cross-site Scripting”, “SQL-injection”.

15.22 Se deben aplicar una variedad de técnicas suficientes para la fase de escaneo y enumeración (dialers, port scanners, networks mappers, sniffers, vulnerability scanners, banner grabbing, sweepers, OS fingerprint, firewalk, SNMP enumeration, Nessus, Nexpose, GFI Languard, Foundstones o cualquier herramienta compatible) que permita enumerar áreas a proteger, despliegue de información de servicios de red disponibles (usuarios, grupos, tablas de ruteo), equipos de red, filtros de seguridad, puertos activos, protocolos y vulnerabilidades.

15.23 En la fase de análisis y validación de vulnerabilidades se deben utilizar bases de datos y herramientas automatizadas que permitan comparar los hallazgos encontrados con base en amenazas conocidas, para lo cual se pueden consultar los siguientes repositorios: Common Vulnerabilities and Exploits – CVE, Open Source Vulnerability DataBase – OSVDB, Bugtraq, GDB, Mitre, Security Focus, FrSIRT BugTraq, NTBugTraq, Packetstorm, Metasploit, Vendors-Information, Exploit-DB, Security-News, US-CERTS Alerts, SysAdmin Audit Network Security – SANS, CISSP-Discussion sin limitarse a los repositorios mencionados.

15.24 Las pruebas deben identificar la trayectoria del tráfico TCP/UDP desde internet hacia los servicios de la organización, con ello también deducir las políticas de filtrado, la sensibilidad y vulnerabilidad de dichos filtros.

15.25 El conjunto de herramientas utilizadas para realizar las pruebas debe documentarse y clasificarse según corresponda (Information Gathering Tools, Network traffic analysis, Vulnerability Identification Tools, Penetration Tools, Source code auditing), dichas herramientas deberán generar según sea el caso, reportes detallados según la metodología que se hace referencia en el punto 15.17.

15.26 Cada una de las vulnerabilidades debe referenciarse mediante información bibliográfica que apoye y permita generar criterio de esta (manejo de literatura o enlaces a sitios de Internet referente a todas las vulnerabilidades identificadas).

15.27 El estudio debe clasificar y priorizar las vulnerabilidades basadas en niveles de riesgo para ello se debe hacer uso de mejores prácticas aceptadas por la industria que utilizan métricas específicas para valorar el impacto y probabilidad de amenaza, se deben tomar en cuenta para dicho propósito al menos los indicadores de medición del Common Vulnerability Scoring System – CVSS sin limitarse solamente a dichos indicadores de medición.

TRANSFERENCIA DE CONOCIMIENTO

15.28 Las pruebas deben tratar de vulnerar la seguridad y permitir conocer hasta dónde un atacante externo podría penetrar la red, o que elementos podrían facilitar un eventual ataque, tratando de lograr acceso a las mismas conociendo únicamente el segmento de direcciones IP públicas utilizado por la OPC CCSS.

15.29 Culminado la entrega del estudio, se debe incluir como una actividad, al menos una capacitación sobre concienciación de seguridad de la información, con una duración de al menos una hora, considerando un aproximado de 90 colaboradores; se deben programar como mínimo cuatro grupos o sesiones de capacitación, el horario y fechas para cada sesión de capacitación será establecido por la OPC CCSS.

15.30 Para reforzar el punto anterior, debe incluirse como mecanismo de verificación y análisis, en un plazo no mayor a cinco días después de realizada la capacitación, la ejecución de una prueba de ingeniería social o suplantación de identidad, seleccionando como muestra al menos la mitad del personal de la Operadora. Se deberá entregar un informe de resultados de vulnerabilidades encontradas en ese momento, con las recomendaciones para mitigar el riesgo que podrían generar las mismas.

15.31 Para el punto anterior, la prueba deberá ser realizada en un horario previamente autorizado por el personal técnico responsable de seguridad de la información de la OPC CCSS; se pueden utilizar herramientas automáticas de envío masivo de correos (phishing), llamadas telefónicas suplantando a personas clave de la organización (internas o externas), soporte, help desk, solicitud de instalación de software, malware controlado, entre otros; la OPC CCSS proporcionará direcciones de correo y teléfonos en caso de requerirse.

15.32 Los resultados obtenidos en el estudio deberán permitir la implementación por parte de la OPC CCSS de un proceso de administración de vulnerabilidades (Vulnerability Management Process) para lo cual, el oferente deberá facilitar a la organización los insumos necesarios (planificación, plantillas, roles, actividades) que le permitan desarrollar tal proceso. Dicho proceso deberá atender las mejores prácticas al menos de NIST-National Institute of Standards and Technology Vulnerability Management Program o del SANS-SysAdmin Audit Network Security Vulnerability Management.

15.33 Los resultados obtenidos durante la explotación de vulnerabilidades deberán ser validados de forma manual a fin de eliminar resultados falsos positivos.

RESULTADOS ESPERADOS

15.34 La OPC CCSS se reserva el derecho de comprobar la realización de las pruebas mediante la indagación de sistemas de bitácoras de equipos de red y monitoreo propios de la organización. Para ello se utilizará fecha y hora de ejecución de las pruebas declaradas en el informe técnico solicitado en el cartel.

15.35 El adjudicatario deberá elaborar informes que incluyan recomendaciones oportunas y priorizadas de las acciones necesarias para corregir o mitigar cada una de las vulnerabilidades detectadas, por cada hallazgo debe detallarse su criticidad, facilidad de explotación e indicaciones para su resolución. Las mismas no se permite que sean genéricas, estas deben ser redactadas de forma práctica y detallada, permitiendo así definir claramente la acción a ejecutar.

15.36 Los informes deberán presentarse en un periodo máximo de **cinco días naturales** contados a partir de la ejecución de la totalidad de las pruebas realizadas y dentro del plazo estipulado en la contratación.

15.37 Los informes deberán comprender los resultados de cada ejecución de monitoreo de vulnerabilidades y totalidad de las pruebas efectuadas con el fin de determinar puntos vulnerables por cada dirección IP pública analizada, así como los dispositivos expuestos a Internet.

15.38 Los informes entregados por el adjudicatario, deberán ser entregados en un medio digital de forma encriptada, serán revisados como una versión borrador conforme los criterios definidos en el cartel; en caso de ser rechazados por el encargado técnico de la contratación, el oferente deberá remitir los mismos nuevamente ajustados acorde con los hallazgos identificados en un plazo no mayor a **tres días naturales** aplicando el enunciado definido las veces necesarias hasta corregir la situación y dentro de los plazos estipulados en la contratación.

15.39 Una vez aprobados, los informes deberán ser presentados en formato electrónico (al menos en .docx y .pdf) contenidos en un medio óptico (DVD o CD), o Pen Drive USB, con seguridad (al menos acceso a través de contraseña).

15.40 El adjudicatario debe mantener completa la documentación de todo el trabajo realizado a lo largo del proceso con respecto a los hallazgos, análisis, pruebas ejecutadas, recomendaciones, elementos de referencia, que soporten el trabajo ejecutado al momento de presentar los informes requeridos y sustentar las recomendaciones. Dicha información deberá entregarse al encargado técnico de la contratación de la forma estipulada en el presente cartel.

15.41 La estructura y contenido de estos informes deben ser alineados a las mejores prácticas según corresponda, las metodologías ofrecidas deben cumplir los estándares nacionales e internacionales de competencia en materia de seguridad de la información, y que se encuentren en vigencia tales como ISC2, ISECOM, EC/COUNCIL, OWASP, ISO 27001 y ISO 27002.

15.42 El oferente deberá presentar las conclusiones y resultados obtenidos a la **Comisión de Tecnologías de Información de la OPC CCSS** para lo cual, deberá coordinar con al menos **cinco días naturales de antelación**, la ejecución de la reunión.