La salud es de todos | Minsalud

516337

Instituto Nacional de Cancerología E.S.E
Gestion Documental y Correspondencia
No. Radicacion: SAL-03013-2020
No. Folios: 1
Fecha: 2020-03-13 03:00:17 PM
516337

Bogotá,

Señor
Richard Oliveros
Lider Seguridad
Hack-Inn
liderseguridad@hack-inn.com
Bogotá D.C.

Señor
César Marín
Director Comercial
Locknet
cmarin@locknet.com.co
Bogotá D.C.

Señor
Hugo Campos
Seguridad - Arquitecto de Soluciones de Seguridad
Entelgy Colombia SAS
hugo.campos@entelgy.com
Bogotá D.C.

Señor
Javier Naranjo Buitrago
Account Manager
Lattitude
javier.naranjo@lattitude.la
Bogotá D.C.

Señora
Luz Alejandra Alferez Mendez
Analista de Licitaciones

Calle 1ª Nº 9-85 · PBX: 4320160
NIT: 899.999.092-7
www.cancer.gov.co
Bogotá D.C., Colombia
Incancerologia

Instituto Nacional de Cancerología-ESE
Colombia
Por el control del cáncer

85 Años

La salud es de todos | Minsalud

04IT Colombia SAS

lalferez@o4it.com
Bogotá D.C.

Señora
Maria Fernanda Mosquera C
Senior Advisory Services
EY

fernanda.mosquera@co.ey.com
Bogotá D.C.

Asunto: Respuesta a observaciones Invitación a cotizar No. 087-2020

Respetados señores

La Dirección General del Instituto Nacional de Cancerología ESE remite las respuestas a las observaciones a los términos de condiciones, efectuadas por el Grupo Área Sistemas - Coordinación Grupo Gestión de Soporte Redes y Hardware, equipo técnico para la evaluación dentro del proceso de invitación de la referencia, las cuales, al igual que este oficio, se publicarán en nuestra página de internet www.cancer,gov.co - enlace - contratación, dentro del proceso correspondiente.

Cualquier inquietud adicional puede enviarla al correo invitaciones@cancer.gov.co.

Cordialmente,

CAROLINA WIESNER CEBALLOS
Directora General

Revisó: JUAN CARLOS GUARIN FERRER - Profesional Especializado I
WILSON IBARGUEN LOZANO - Coordinador Grupo Gestión de Compras y Contratación (E.
MARIA YANETH GIL PARRA - Coordinadora Grupo Área Gestión Financiera (E)
JORGE ORLANDO NEIRA ROLDAN - Asesor Dirección General
JUAN JOSE PEREZ ACEVEDO - Subdirector General de la Gestión Administrativa y Financiera

Anexos: RESPUESTA 087-2020.pdf

Anexos: ADENDA No. 3..docx

Anexos: ANEXO TECNICO No. 3 - ADENDA.pdf

DG/CWC/SGGAF/JJPA/GAGF/MYG/GGCC/WIL/Mónica

Calle 1ª Nº 9-85 · PBX: 4320160
NIT: 899.999.092-7
www.cancer.gov.co
Bogotá D.C , Colombia
incancerologia

Instituto Nacional de Cancerología-ESE
Colombia
Por el control del cáncer

85 Años

INVITACIÓN A COTIZAR No. 087 DE 2020

EL INSTITUTO NACIONAL DE CANCEROLOGÍA, EMPRESA SOCIAL DEL ESTADO – INVITA A PRESENTAR PROPUESTAS PARA LOS SERVICIOS PARA EL DESARROLLO PRUEBAS QUE PERMITAN LA IDENTIFICACION DE VULNERABILIDADES, ASÍ COMO PRUEBAS DE HACKING ETICO (PRUEBAS DE PENETRACION) – EXTERNO E INTERNO, SOBRE HARDWARE Y SOFTWARE, SERVIDORES, BASES DE DATOS Y REDES, CORRESPONDIENTES AL SISTEMA DE INFORMACIÓN SAP DEL INSTITUTO NACIONAL DE CANCEROLOGÍA, PARA ESTABLECER EL ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN QUE SE ALMACENA Y PROCESA A TRAVÉS DE LA PLATAFORMA TECNOLOGICA SAP DE LA ENTIDAD, ACORDE A ESTA INVITACIÓN, SUS ANEXOS Y EL CONTRATO QUE SE CELEBRE PARA EL EFECTO.

RESPUESTA A OBSERVACIONES REALIZADAS A
LOS TERMINOS DE CONDICIONES

El Instituto Nacional de Cancerología Empresa Social del Estado, procede a dar respuesta a las observaciones realizadas en tiempo a los términos de condiciones de la presente invitación así:

A) **Observación presentada por la empresa Hack-Inn** Recibidas a través del correo electrónico invitaciones@cancer.gov.co, lunes, 24 de febrero de 2020 10:57 a. m.

PRIMERA PREGUNTA

"... Actualmente nos encontramos en la evaluación, del requerimiento a cotizar, del código 087-2020.

Evaluando los requerimientos, se expone el punto:

comerciante.

- **Presentar el Registro Único de Proponentes (RUP), expedido por la Cámara de Comercio, en la categoría que se encuentre el oferente de acuerdo con el objeto contractual, el cual debe estar vigente, actualizado y renovado, exceptuando los casos normativos.**

Actualmente contamos con experiencia en los servicios solicitados, más no contamos con RUP, esto sería impedimento para poder participar en la invitación

..."

RESPUESTA

El INC se permite manifestar que el artículo 6° de la Ley 1150 de 2007 establece que toda persona natural o jurídica, así como empresas extranjeras con representación en Colombia que deseen participar en procesos de contratación con Entidades del Estado deben estar inscritas en el RUP. Por otro lado el inciso segundo del mismo artículo establece en qué casos no se requiere estar inscrito en el RUP y poder participar en contratación con Entidades del Estado, estas son : a. contratación

directa; b. contratos para la prestación de servicios de salud; c. contratos de mínima cuantía; d. enajenación de bienes del Estado; e. contratos que tengan por objeto la adquisición de productos de origen o destinación agropecuaria que se ofrezcan en bolsas de productos legalmente constituidas; f. los actos y contratos que tengan por objeto directo las actividades comerciales e industriales propias de las empresas industriales y comerciales del Estado y las sociedades de economía mixta y los contratos de concesión de cualquier índole. De acuerdo con lo anterior, y teniendo en cuenta que el objeto del proceso contractual de la Invitación a Cotizar No. 087 de 2020 no se enmarca en ninguna de las excepciones establecidas, se hace necesario que los participantes cumplan con las exigencias del inciso primero del artículo 6° de la Ley 1150 de 2007, esto es, estar inscrito en el RUP, y aportar el mismo vigente al proceso de contratación.

SEGUNDA PREGUNTA

"... Adicional a ello, el requerimiento hace alusión a pruebas sobre 25 IPS, no es claro si dichas ips son públicas o privadas. De estas 25 ips cuantas son públicas? y cuántas son privadas?, Se podría contar con VPN, para la ejecución de las pruebas a las ips privadas?

..."

RESPUESTA

Se aclara que todas las 25 IPs son privadas.

La entidad no autoriza trabajo remoto para el desarrollo de las pruebas y actividades críticas del objeto contractual, debido a la confidencialidad y criticidad de los datos que va a acceder el oferente, ya que se trata del sistema misional donde reposa la historia clínica. Solo se autoriza trabajo remoto a través de VPN de los consultores para realizar una (1) prueba especifica programada y controlada de SAP sobre la VPN, y para temas administrativos, de documentación o de seguimiento.

TERCERA PREGUNTA

"...Por último, es posible saber, cuántas aplicaciones web están expuestas en estas 25 IPS?

..."

RESPUESTA

Ninguna aplicación está expuesta a la web dentro de las 25 Ips.

B) **Observación presentada por la empresa Locknet** Recibidas a través del correo electrónico invitaciones@cancer.gov.co, martes, 25 de febrero de 2020 9:47 a. m.

PRIMERA PREGUNTA

"... Para el Consultor Lider (QA) de seguridad solicitamos que el Certified Ethical Hacking CEH sea solicitado desde la versión 9 o superior ya que la versión 8 no toma en cuenta temas como la computación en la nube y la seguridad móvil. Así mismo la v9 aborda nuevas vulnerabilidades en ciberseguridad como Heartbleed, Shellshock y POODLE, tema que no tiene la v8 y representaría un riesgo para la entidad.

..."

RESPUESTA

Para garantizar la pluralidad de los oferentes del proceso, y ya que la infraestructura de SAP de la entidad es tipo on-premise y tampoco se van a evaluar dispositivos móviles ni computación en la nube, se aceptan las certificaciones CEH v8 y superior como válidas, por lo que no se acepta el requerimiento del proveedor.

SEGUNDA PREGUNTA

"... Solicitamos amablemente que para el Consultor Lider (QA) de seguridad soliciten mínimo 4 de las certificaciones requeridas para garantizar la pluralidad de oferentes, ya que observamos que el perfil solicitado está sesgado a una única persona.
..."

RESPUESTA

La experiencia Exigida por el Instituto para el perfil del Consultor Líder (QA) de Seguridad se complementa con las certificaciones exigidas, que garantizan al instituto la calidad de la consultoría, certifican el conocimiento y competencias del Consultor según el perfil, y garantizan que se apliquen las mejores prácticas y metodologías sobre el objeto contractual, que son los ejercicios de Hacking Ético, Auditoria de Perfiles y Roles sobre SAP, e Ingeniería Social.

Pero en aras de dar pluralidad y garantizar en la participación de más oferentes, se acoge la solicitud realizada por el oferente de solicitar mínimo cuatro (4) de las certificaciones requeridas.

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co - enlace contratación.

TERCERA PREGUNTA

"... Solicitamos amablemente que para el Consultor Senior en Seguridad Informática soliciten mínimo 3 de las certificaciones requeridas para garantizar la pluralidad de oferentes.

..."

RESPUESTA

La experiencia Exigida por el Instituto para el Perfil de Consultor Senior de Seguridad Informática se complementa con las certificaciones exigidas, que garantizan a la entidad la calidad de la consultoría, certifican el conocimiento y competencias del Consultor Senior en seguridad informática, y garantiza que se apliquen las mejores prácticas y metodologías sobre el objeto contractual, que son los ejercicios de Hacking Ético, Auditoria de Perfiles y Roles sobre SAP, e Ingeniería Social

Para garantizar la pluralidad de oferentes sin sacrificar significativamente la calidad exigida para la consultoría, la entidad decide aceptar la sugerencia del oferente, y aprueba un número mínimo de tres (3) certificaciones requeridas para el perfil de Consultor Senior de seguridad informática.

Por lo tanto, y recogiendo todos los cambios sobre certificaciones, se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co – enlace contratación.

C) **Observación presentada por la empresa Entelgy Colombia SAS** Recibidas a través del correo electrónico invitaciones@cancer.gov.co, martes, 25 de febrero de 2020 9:51 a. m.

PRIMERA PREGUNTA

"... Respecto al documento "ANEXO TÉCNICO", en el numeral 2; "REQUISITOS TÉCNICOS", en el párrafo "Experiencia Específica":

Experiencia específica en al menos tres (3) proyectos relacionados con el objeto a contratar, los cuales deben estar relacionados con el sector salud debidamente finalizados y/o en ejecución, a través de un contrato o documento que avale el plan de actividades ejecutados.

Con el objeto de garantizar pluralidad de oferentes, solicitamos a la Entidad modificar el ítem, de manera que la experiencia a certificar sea: "... al menos tres (3) proyectos relacionados con el objeto a contratar, de los cuales al menos uno (1) esté relacionado con el sector salud debidamente finalizados y/o en ejecución...", lo anterior teniendo en cuenta que si bien la razón social de La Entidad, es del sector Salud, la infraestructura a evaluar, tecnológicamente es común e independiente al segmento económico al cual pertenece, máxime que es conocido, que por ámbitos regulatorios locales e internacionales, existen otros segmentos como el Financiero, Petrolero o Energético que lideran los esquemas de aseguramiento de plataformas, con lo que se pueden aprovechar las experiencias certificables en otros segmentos de la industria, en beneficio de la exigencia de La Entidad. Dicha modificación no afecta en nada la calidad del servicio ofertado, por el contrario, si garantiza la pluralidad de oferentes, conforme a lo exigido por el Gobierno Colombiano, en lo que a contratación estatal se refiere.

RESPUESTA

El INC determinó que dentro de la experiencia específica los oferentes debían demostrar la experticia sobre SAP en proyectos ejecutados en el sector salud, ya que en el INC un componente esencial de

la plataforma SAP sobre la cual se va a realizar el ejercicio de Auditoria de roles y perfiles, corresponde al producto de la vertical de salud ISH-MED.

Con el fin de dar pluralidad a los oferentes, y atendiendo el principio de proporcionalidad y razonabilidad en concordancia al objeto de esta invitación, la entidad decide modificar el apartado donde solicita experiencia especifica de tres (3) proyectos relacionados con el objeto a contratar relacionados con el sector salud, y solicitar en cambio la experiencia especifica de los oferentes en al menos dos (2) proyectos relacionados o que contengan actividades de auditoria sobre roles y perfiles de sistema de información SAP, debidamente finalizados, a través de contratos o certificaciones que avalen los planes de actividades ejecutadas.

Al modificar de esta forma la experiencia específica, la entidad ratifica la exigencia para que los oferentes cuenten con experiencia específica en al menos un (1) proyecto relacionado con el análisis de vulnerabilidades (Hacking Ético), donde uno de los activos de información esté relacionado con una aplicación o plataforma relacionada con SAP en la nube o plataforma SAP On Premise el cual debe estar entonces debidamente finalizado, a través de un contrato o certificación que avale el plan de actividades ejecutadas.

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co enlace contratación.

SEGUNDA PREGUNTA

"... Respecto del documento "ANEXO TÉCNICO", en el numeral 2; "REQUISITOS TÉCNICOS", en el párrafo "Perfiles Requeridos: Consultor Líder (QA) de Seguridad:

Consultor Líder (QA) de Seguridad	Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES. Postgrado / Maestría en seguridad de la información o seguridad informática y contar como mínimo con las siguientes certificaciones: • Certified Ethical Hacking CEH v8 o superior vigente • CISSP (Certified Information Systems Security Professional) • CISM (Certified Information Security Manager)

	• IPv6 Forum Certified Security Engineer Silver vigente • RISK MANAGER ISO 31000:2018 • ECIH EC-Council Certified Incident Handler • Manager Cybersecurity ISO 27032 • Lead Auditor ISO 27032 • Implementador Líder ISO 27001:2013

Con el propósito de garantizar pluralidad de oferentes, solicitamos a La Entidad modificar el ítem, de manera que el Perfil Requerido tenga como mínimo dos (2) de las certificaciones listadas, pues considera El Oferente, dentro de su experiencia específica en proyectos de tamaños iguales o superiores al del presente proceso, que un profesional con posgrado en seguridad, experiencia profesional de más de diez (10) años en seguridad y con experiencia en al menos cinco (5) proyectos relacionados con el objeto del contrato, cuenta con la experiencia suficiente para liderar el proyecto. Adicionalmente, se fundamenta el requerimiento teniendo en cuenta que dentro del listado de certificaciones exigido por La Entidad, se encuentran algunas que no se relacionan directamente con el objeto del proceso, por ejemplo, ser la certificación que acredita ser Implementador Líder ISO 27001:2013, pues el objeto del contrato no trata la implementación de un sistema de gestión de seguridad de la información para que se requiera el perfil de Implementador certificado o la certificación "IPv6 Forum Certified Security Engineer Silver" vigente o "RISK MANAGER ISO 31000:2018", etc, que si bien quizá tangencialmente puede aportar dentro del proceso, no debiera ser excluyente dentro del mismo, como se citaba previamente, teniendo en cuenta el objeto contractual.

Ahora bien, genera algo de suspicacia, que se incluyan requerimientos tales como la certificación en "IPv6 Forum Certified Security Engineer Silver", pues como se mencionaba previamente, no tiene una relación, al menos directa, con el Objeto contractual, y es aún menos claro dentro del proceso la exigencia de contar con el nivel "Silver" de la citada certificación.

RESPUESTA

La experiencia Exigida por el Instituto para el Perfil de Consultor Líder (QA) de seguridad se complementa con las certificaciones exigidas, que garantizan a la entidad la calidad de la consultoría, certifican el conocimiento y competencias del consultor líder, y garantiza que se apliquen las mejores prácticas y metodologías sobre el objeto contractual, que son los ejercicios de Hacking Ético, Auditoria de perfiles y Roles de SAP, e Ingeniería Social.

La entidad debido a la observación del oferente revisó las certificaciones y acepta retirar la certificación de implantador líder Iso27001:2013, ya que el alcance no corresponde al ejercicio, y se colocó por error.

En cuanto la certificación Ipv6 Forum Certified Security engineer Silver, la entidad la incluyó debido a que se encuentra ejecutando la transición de direccionamiento IPV4 a IPV6 como una exigencia del Ministerio de Tecnologías de la Información y las Comunicaciones de acuerdo a la resolución 2710 de 2017, para la cual el instituto tenía una fecha límite de 31 de diciembre de 2019 para su adopción.(https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/100569:278-entidades-publicas-tienen-hasta-el-31-de-diciembre-para-adoptar-IPv6-y-evitar-sanciones). Para esto se estipulo utilizar el ejercicio de hacking ético para detectar debilidades de seguridad sobre la nueva implantación ipv6 en la plataforma SAP de acuerdo a la guía de aseguramiento expedida por MINTIC (https://www.mintic.gov.co/portal/604/channels-507_IPv6_2019.pdf), por lo tanto no se trata de un requerimiento tangencial como lo sugiere el oferente. Por tales motivos la certificación Ipv6 Forum Certified Securituy Enginier Silver se consideró como un requisito mínimo para certificar conocimiento sobre seguridad en IPV6 de los oferentes. Pero debido a que los tiempos de cronograma proyecto de Ipv6 en la entidad se han retrasado con su fecha de entrega (agosto de 2020), el ejercicio de hacking ético probablemente se realizará sobre direccionamiento IPV4.

Por lo tanto, la entidad retira la exigencia de esta certificación como una exigencia obligatoria Ipv6 Forum Certified Security engineer Silver.

En cuanto a la certificación Riskmanager ISO 31000:2018, la entidad la solicitó para asegurar que el consultor líder tenga la competencia para auditar eficazmente sobre las mejores prácticas en gestión de riesgo, que por supuesto incluye la identificación de riesgo y controles aplicados sobre el sistema de información y plataforma SAP objeto del contrato.

En atención a la solicitud con el fin de garantizar dar pluralidad a los oferentes, la certificación Riskmanager ISO31000:2018 se retira del listado de certificaciones requeridas como obligatorias.

En atención a la solicitud del oferente y con el fin de garantizar la pluralidad de participantes, pero sin sacrificar las calidad exigida para la consultoría, la entidad decide no aceptar la sugerencia de bajar las certificaciones requeridas para el perfil de consultor líder (QA) de seguridad a dos (2) , y determina que solicitara tan solo un mínimo de cuatro (4) certificaciones para el perfil de consultor líder (QA) de seguridad , de la lista definitiva final de certificaciones admitidas por la entidad.

Para garantizar la pluralidad de oferentes el instituto decide reducir la experiencia profesional mínima del consultor Líder (QA) de Seguridad, de 10 años a 7 años en seguridad informática.

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co enlace contratación.

TERCERA PREGUNTA

"... Respecto del documento "ANEXO TÉCNICO", en el numeral 2; "REQUISITOS TECNICOS", en el párrafo "Perfiles Requeridos: Consultor Senior en Seguridad Informática":

Consultor Senior en Seguridad Informática	Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES. Posgrado en seguridad en redes o seguridad informática o seguridad de la información y mínimo cuatro (4) de las siguientes certificaciones: • CISSP (Certified Information Systems Security Professional) • CISM (Certified Information Security Manager) • CEH -Certified Ethical Hacker - EC-Council. • Auditor Líder ISO 27001:2013 (IRCA). • CHFI - Certified Hacking Forensic Investigator - EC-Council. • CISA - ISACA • Auditor Líder ISO 27032. • ECSA/LPT

Con el objeto de garantizar pluralidad de oferentes, solicitamos a La Entidad modificar el ítem, de manera que el Perfil Requerido tenga como mínimo dos (2) de las certificaciones listadas, pues considera el oferente, dentro de su experiencia específica en proyectos de tamaños iguales o superiores al del presente proceso, que un profesional, con posgrado en seguridad, experiencia profesional de más de cinco (5) años en seguridad y con experiencia en al menos cuatro (4) proyectos relacionados con el objeto del contrato, cuenta con la experiencia suficiente para ejercer como consultor dentro del proyecto. Adicionalmente, se fundamenta el requerimiento teniendo en cuenta que hay certificaciones que exige La Entidad, que no se relacionan directamente con el objeto del proceso, por ejemplo, ser "Auditor Líder ISO 27001:2013", pues el objeto del contrato no contempla el mantenimiento de un sistema de gestión de seguridad de la información para que se requiera un perfil de Auditor Líder en tal sistema de gestión de la seguridad.

Así mismo, genera suspicacia que la certificación que se solicita La Entidad, sea explícita de IRCA, pues al tratarse de una certificación internacional no debiera estar limitado al ente certificador, sino a la certificación en sí. Expuesto lo anterior, se solicita eliminar del listado de certificaciones el Auditor Líder ISO 27001:2013 (IRCA) y en su reemplazo, se sugiere incluir certificaciones que aportan muchísimo más valor al servicio solicitado, las cuales estén directamente relacionadas con el objeto contractual, El Oferente sugiere a la Entidad considerar incluir Certificaciones relacionadas al proceso tales como Offensive Security Certified Profesional - OSCP, Offensive Security Certified Expert - OSCE, EC-Council CHFI o ECSA/LPT.

RESPUESTA

La experiencia Exigida por el Instituto para el Perfil de Consultor Senior de Seguridad Informática se complementa con las certificaciones exigidas, que garantizan a la entidad la calidad de la consultoría, certifican el conocimiento y competencias del Consultor Senior, y garantiza que se apliquen las mejores prácticas y metodologías sobre el objeto contractual, que son los ejercicios de Hacking Ético, Auditoria de Perfiles y Roles sobre SAP, e Ingeniería Social.

La entidad considera que cada una de las certificaciones relacionadas en el listado incluyendo la certificación de Auditor Líder ISO27001:2013 son relevantes para el objeto del proceso. La certificación Auditor Líder ISO27001:2013 en particular permite a la entidad garantizar la idoneidad del perfil y la calidad de la metodología que se aplique en el ejercicio de Auditoria de Roles y Perfiles de SAP, y del ejercicio de Hacking ético en el cual se evaluará la efectividad de los controles del instituto implantados sobre la historia clínica. La entidad dentro de la operación de su SGSI gestiona una política de seguridad de la información y controles de seguridad que se encuentran alineados, y son auditados periódicamente bajo el cumplimiento de la Norma ISO27001:2013 y el MSPI de MINTIC.

En cuanto al Registro Internacional IRCA (T*he International Register of Certificated Auditors (IRCA)* solicitado, la entidad lo uso como referencia del mercado ya que IRCA da certificación de auditores con un reconocimiento mundial y da mayor credibilidad al desempeño del perfil del consultor solicitado.

En aras de dar pluralidad y garantizar la participación de más oferentes se retira la necesidad del reconocimiento IRCA solicitado por el oferente, pero se mantiene dentro del listado de certificaciones la certificación Auditor Líder ISO27001:2013.

En cuanto a las certificaciones sugeridas para inclusión por parte el oferente de acuerdo con el perfil de Consultor Senior de Seguridad Informática, la entidad determina que son suficientes las certificaciones solicitadas inicialmente, por lo tanto, no acepta el requerimiento para agregar las siguientes certificaciones:

- *Offensive Security Certified Profesional*
- *Computer Hacker Forensic Investigator (CHFI) EC-Council*

En cuanto a la adición de la certificación:

- *ECSA/LPT - Certified Security Analyst EC-Council*

Esta certificación ya estaba incluida en el listado como se observa a continuación

Consultor Senior en Seguridad Informática	Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES. Posgrado en seguridad en redes o seguridad informática o seguridad de la información y mínimo cuatro (4) de las siguientes certificaciones: • CISSP (Certified Information Systems Security Professional) • CISM (Certified Information Security Manager) • CEH -Certified Ethical Hacker - EC-Council. • Auditor Líder ISO 27001:2013 (IRCA)
	• CHFI – Certified Hacking Forensic Investigator -EC-Council. • [illegible] • Auditor Líder ISO 27032. • ECSA/LPT

Finalmente, para garantizar la pluralidad de oferentes y a que la entidad requiere mantener la calidad exigida para la consultoría, decide no aceptar la sugerencia del oferente de bajar a dos (2) certificaciones mínimas requeridas, y aprueba un número mínimo de tres (3) certificaciones requeridas para el perfil de Consultor Senior de seguridad informática.

Para garantizar la pluralidad de oferentes el instituto decide reducir la experiencia profesional mínima del Consultor Senior en Seguridad Informática, de 5 años a 3 años en seguridad informática.

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co enlace contratación

CUARTA PREGUNTA

"... Respecto del documento "ANEXO TÉCNICO", en el numeral 2; "REQUISITOS TECNICOS", en el párrafo "Perfiles Requeridos: Consultor Junior en Seguridad Informática":

Consultor junior en Seguridad Informática	Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES. Deseable al menos una (1) de las siguientes certificaciones: • CEH –Certified Ethical Hacker – EC-Council.

	• CISA -Certified Information Systems Auditor - ISACA. • CISSP - Certified Information Systems Security Professional - ISC2. • Auditor Líder ISO 27001:2013.

Con el propósito de contar con un perfil profesional que se ajuste a las expectativas de la Entidad y a los servicios solicitados en el Proceso, solicitamos a La Entidad modificar el ítem, de manera que sea REQUERIDO para el perfil de Consultor Junior en Seguridad Informática el contar con al menos una (1) de las certificaciones listadas, pues considera el oferente, dentro de su experiencia específica en proyectos de tamaños iguales o superiores al del presente proceso, que un profesional en ingeniería, con al menos una (1) de las certificaciones mencionadas, experiencia profesional de más de un (1) año en seguridad y con participación en al menos dos (2) proyectos relacionados con el objeto del contrato, cuenta con la experiencia suficiente para ejercer como Consultor Junior en Seguridad Informática dentro del proyecto.

Nuevamente y por los argumentos expuestos en observaciones previas se solicita eliminar del listado las certificaciones de Auditor Líder ISO 27001:2013 y en su reemplazo, se sugiere incluir certificaciones que aportan muchísimo más valor dentro del proyecto, las cuales sí estarían directamente relacionadas con el objeto contractual; es el caso de certificaciones tales como: Offensive Security Certified Profesional, Offensive Security Certified Expert, EC-Council CHFI o ECSA/LPT.

RESPUESTA

La entidad evaluó como deseable y no como obligatoria la exigencia de una certificación para el perfil de Consultor Junior de Seguridad Informática, y en cambio se realizó exigencia de carrera Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES., Experiencia profesional de mínimo 1 año en seguridad informática, y Experiencia profesional específica en dos (2) proyectos relacionados con el análisis de vulnerabilidades en seguridad informática sobre la infraestructura tecnológica.

En cuanto a la solicitud del oferente de modificar el perfil de Consultor Junior de seguridad informática para que cuente con al menos (1) de las certificaciones, la entidad no acoge la sugerencia del oferente ya que elevaría los requerimientos del perfil en contravía de la trasparencia del proceso y de la pluralidad de oferentes, y por tal motivo mantiene el requerimiento de certificación de este perfil como deseable, es decir, los certificados para este perfil no son obligatorios.

De acuerdo con lo expuesto anteriormente, la solicitud de retirar el requerimiento de auditor líder ISO27001:2013 no tiene incidencia alguna sobre la selección de oferente por no tratarse de un

requisito habilitante obligatorio para el perfil, por lo que la entidad no retira la certificación de auditor líder ISO27001:2013 del listado.

En cuanto a la solicitud de incluir certificaciones como: ECSA/LPT - Certified Security Analyst EC-Council, Offensive security certified profesional, Computer hacker forensic investigator (chfi) ec-council, la entidad considera que son suficientes la certificaciones listadas originalmente, ya que no se constituyen como un requisito habilitante obligatorio. Por lo tanto, no se acepta el requerimiento del oferente.

En consecuencia, se mantiene el perfil de Consultor Junior en seguridad informática sin modificaciones el anexo técnico.

QUINTA PREGUNTA

"... Se solicita de manera atenta a la Entidad indicar si es posible que el personal requerido por La Entidad preste los servicios de manera remota, fuera de las instalaciones de la Entidad, teniendo en cuenta que la dedicación del personal es un factor determinado por el Proponente de acuerdo a la estrategia de prestación del servicio.

RESPUESTA

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co enlace contratación

SEXTA PREGUNTA

"... Respecto del documento "ANEXO TÉCNICO", en el numeral 1.1 "DESCRIPCIÓN DE LAS CARACTERÍSTICAS TÉCNICAS", en la página 4 se menciona:

Para cada tipo de prueba del plan de pruebas se debe especificar:

1. Alcance o cobertura.
2. Objetivo(s).
3. Participantes, y roles de estos.
4. Fecha(s) y hora(s) programadas para la ejecución de la actividad.
5. Paso a paso de la actividad.
6. Indicador propuesto para medir el resultado.
7. Resultado esperado de la actividad

Se solicita a la Entidad considerar que la entrega del cronograma con las Fechas y Horas(s) programadas para la ejecución de las actividades se genere una vez adjudicado el Proceso y firmada el acta de inicio, ya que se pueden presentar variaciones en las fechas estipuladas dentro del cronograma contractual inicial que hagan que sea necesaria la modificación del cronograma con las fecha(s) y hora (s) programadas para la ejecución de las actividades. A cambio de este cronograma, con fechas y horas, se sugiere a la Entidad solicitar a los Oferentes un cronograma del alto nivel que presente hitos relacionados a los servicios requeridos en el proceso.

RESPUESTA

Se aclara al oferente que el cronograma detallado con fechas y horas se entrega a la entidad una vez adjudicado el servicio en la reunión de firma de acta de inicio de contrato.

El plan de pruebas que debe presentar el oferente requiere efectivamente la presentación del cronograma de actividades a un alto nivel, con la duración de actividades y los hitos relacionados los servicios del proceso.

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co enlace contratación.

d) **Observación presentada por la empresa Lattitude** Recibidas a través del correo electrónico invitaciones@cancer.gov.co, miércoles, 26 de febrero de 2020 4:05 p. m.

PRIMERA PREGUNTA

"... Es nuestro interés participar del proceso de la referencia. Entendemos que es viable presentar oferta en forma conjunta en modalidad de Unión Temporal. Sin embargo, solicitamos respetuosamente aclarar si en esta modalidad desde el punto de vista jurídico, es viable que solo uno de los integrantes de la UT aporte el Registro Único de Proponentes?

RESPUESTA

El INC se permite manifestar que el RUP es un documento para verificar la experiencia de los proponentes, en caso de una Unión temporal u otra forma asociativa, si cada integrante aporta experiencia para el cumplimiento de requisitos habilitantes, esa experiencia será revisada en el RUP de cada empresa. Así mismo el INC se permite transcribir lo publicado por la página Colombia Compra Eficiente acerca del RUP en los siguientes términos:

"El Registro único de Proponentes contiene una parte, la lista de bienes, obras y servicios que el proveedor ofrecerá a las Entidades Estatales, identificados con el Clasificador de Bienes y Servicios en el tercer nivel. Esta clasificación del proponente no es un requisito habilitante, sino un mecanismo para establecer un lenguaje común entre los partícipes del Sistema de Compras y Contratación Pública.

De otra parte, el RUP también contiene los contratos inscritos que sirven para acreditar la experiencia de los proponentes en los Procesos de Contratación. La experiencia sí es un requisito habilitante y los proponentes deben inscribirla en el RUP usando los códigos del Clasificador de Bienes y Servicios en el tercer nivel. La experiencia del proponente inscrito en el RUP debe corresponder a la experiencia que la Entidad Estatal solicita en los Documentos del Proceso.

Las Entidades Estatales no pueden excluir a un proponente que ha acreditado los requisitos habilitantes exigidos en un proceso de contratación por no estar inscrito en el aparte de clasificación del RUP con el código de los bienes, obras o servicios del objeto del Proceso de Contratación adelantado, es decir, por la información del clasificación del proponente, pero sí deben verificar que

las condiciones de experiencia correspondan a las exigencias previstas para el Proceso de Contratación.
Ahora bien, la ley 80 de 1993 en el artículo 7°, , reguló formas de asociación de personas naturales y/o privadas denominadas uniones temporales y consorcios, con la finalidad de aunar esfuerzos para presentar conjuntamente una misma propuesta, y consecuentemente alcanzar un fin común que corresponde a la adjudicación, celebración y ejecución de un contrato.

La experiencia del oferente plural (consorcios, uniones temporales o promesas de sociedad futura) corresponde a la suma de la experiencia que acredite cada uno de los integrantes del proponente plural, es decir que, si uno sólo de los integrantes acredita la experiencia requerida por la Entidad Estatal, ésta sirve para acreditar la experiencia exigida en el respectivo Proceso de Contratación."

e) **Observación presentada por la empresa EY** Recibidas a través del correo electrónico invitaciones@cancer.gov.co, miércoles, 26 de febrero de 2020 5:25 p. m.

PRIMERA PREGUNTA

"... Estuvimos realizando la revisión de los pliegos y queremos validar con ustedes la posibilidad de reemplazar las certificaciones que piden para los integrantes del equipo que harán parte de la propuesta por credenciales que acrediten sus años de experiencia, dado que EY cuenta con profesionales que tienen amplia experiencia realizando análisis de vulnerabilidades y pruebas de Ethical Hacking en grandes Compañías del país, sin embargo, los integrantes del equipo tienen postgrado en Seguridad Informática o algunas de las certificaciones mencionadas por ustedes, pero no necesariamente todas las certificaciones que solicitan.

RESPUESTA

La experiencia exigida por la entidad para los perfiles de los consultores se complementa con las certificaciones exigidas, que garantizan al instituto la calidad de la consultoría, certifican el conocimiento y competencias del Consultor según el perfil, y garantizan que se apliquen las mejores prácticas y metodologías sobre el objeto contractual, que son los ejercicios de Hacking Ético, Auditoria de Perfiles y Roles sobre SAP, e Ingeniería Social. Por lo tanto, la entidad no puede retirar completamente la exigencia de certificaciones y reemplazarlos por credenciales que acrediten años de experiencia.

Pero en aras de dar pluralidad y garantizar en la participación de más oferentes, se acoge parcialmente la solicitud realizada, y se modifican las exigencias de certificaciones para los diferentes perfiles y se modifica los años de experiencia para los consultores líder QA de seguridad y consultor senior de seguridad informática.

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co enlace contratación.

f) Observación presentada por la empresa O4IT COLOMBIA SAS

PRIMERA PREGUNTA

"... El objeto de la invitación es: "...PRESENTAR PROPUESTAS PARA LOS SERVICIOS PARA EL DESARROLLO PRUEBAS QUE PERMITAN LA IDENTIFICACIÓN DE VULNERABILIDADES, ASÍ COMO PRUEBAS DE HACKING ETICO (PRUEBAS DE PENETRACIÓN) EXTERNO E INTERNO, SOBRE HARDWARE Y SOFTWARE, SERVIDORES, BASES DE DATOS Y REDES, CORRESPONDIENTES AL SISTEMA DE INFORMACIÓN SAP DEL INSTITUTO NACIONAL DE CANCEROLOGÍA, PARA ESTABLECER EL ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN QUE SE ALMACENA Y PROCESA A TRAVÉS DE LA PLATAFORMA TECNOLÓGICA SAP DE LA ENTIDAD, ACORDE A ESTA INVITACIÓN, SUS ANEXOS Y EL CONTRATO QUE SE CELEBRE PARA EL EFECTO."; dentro de la misma se exige una experiencia especifica en al menos tres (3) proyectos relacionados con el objeto a contratar, las cuales deben estar relacionados con el sector salud debidamente finalizados y/o en ejecución, a través de un contrato o documento que avale el plan de actividades ejecutados.

De acuerdo con lo anterior, y en cumplimiento del principio de proporcionalidad y razonabilidad en concordancia tanto con el objeto y el presupuesto asignado al proceso, solicitamos a la entidad ampliar el requerimiento en cuanto a la exigencia y en su defecto solicitar: "Experiencia especifica en al menos uno (01), máximo tres (03) proyectos relacionados con el objeto a contratar, las cuales deben estar relacionados con el sector salud debidamente finalizados y/o en ejecución, a través de un contrato o documento que avale el plan de actividades ejecutados".

RESPUESTA

El INC determinó que dentro de la experiencia específica los oferentes debían demostrar la experticia sobre SAP en proyectos ejecutados en el sector salud, ya que en el INC un componente esencial de la plataforma SAP sobre la cual se va a realizar el ejercicio de Auditoria de roles y perfiles, corresponde al producto de la vertical de salud ISH-MED.

Con el fin de dar pluralidad a los oferentes, y atendiendo el principio de proporcionalidad y razonabilidad en concordancia al objeto de esta invitación, la entidad decide modificar el apartado donde solicita experiencia especifica de tres (3) proyectos relacionados con el objeto a contratar relacionados con el sector salud, y solicitar en cambio la experiencia especifica de los oferentes en al menos dos (2) proyectos relacionados o que contengan actividades de auditoria sobre roles y perfiles de sistema de información SAP, debidamente finalizados, a través de contratos o certificaciones que avalen los planes de actividades ejecutadas.

Al modificar de esta forma la experiencia específica, la entidad ratifica la exigencia para que los oferentes cuenten con experiencia específica en al menos un (1) proyecto relacionado con el análisis de vulnerabilidades (Hacking Ético), donde uno de los activos de información esté relacionado con una aplicación o plataforma relacionada con SAP en la nube o plataforma SAP On

Premise el cual debe estar entonces debidamente finalizado, a través de un contrato o certificación que avale el plan de actividades ejecutadas.

Se surte adenda No. 2 la cual se encuentra publicada en nuestra página web www.cancer.gov.co enlace contratación.

JENNIFER DAHANA GUTIERREZ LUNA
Coordinadora Soporte redes y Hardware

CARLOS ANDRES GUERRERO GONZALEZ
Oficial de Seguridad de la Información