OBSERVACIONES Y RESPUESTAS
INVITACION PÚBLICA No 028 DE 2016

ELABORACIÓN DEL ANÁLISIS DEL ESTADO ACTUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA IMPRENTA NACIONAL DE COLOMBIA QUE INCLUYE LA ENTREGA DE LOS DOCUMENTOS TÉCNICOS INDICADOS EN EL ANEXO TÉCNICO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE GESTIÓN COMERCIAL, GESTIÓN DE PRODUCCIÓN, GESTIÓN FINANCIERA Y GESTIÓN INFORMÁTICA

OBSERVACIONES REALIZADAS POR LA FIRMA PRICEWATERHOUSECOOPERS AG LTDA (05/08/2016 a las 11:26 a.m.)

OBSERVACIÓN No 2

El porcentaje de participación solicitado de 6 recursos al 100% y 3 recursos al 50% se encuentra sobredimensionado para las actividades a desarrollar como parte del objeto de contrato para cada uno de estos perfiles. Se recomienda a la entidad revisar detalladamente las asignaciones de cada recurso para ajustar estos porcentajes de manera consistente con las fases del proyecto. Con base en nuestra experiencia en proyectos similares anteriores recomendamos los siguientes porcentajes:

- *1 Gerente 25%*
- *1 Líder de Auditoría 100% solo en las fases de diagnóstico para evitar la pérdida de independencia.*
- *1 Senior de Continuidad 100% solo en la fase de planes de recuperación.*
- *1 Senior de Ethical 100% solo en la fase de pruebas técnicas.*
- *1 Senior de Seguridad 100% en todo el proyecto.*
- *3 Junior de Seguridad 100% en todo el proyecto.*
- *1 Senior de Calidad 30%. Para permitir la revisión documental de los productos finales a entregar a la entidad.*

RESPUESTA

Una vez analizada la solicitud, la entidad aclara que con base en el alcance definido y el tiempo establecido para la ejecución del proyecto, el equipo de trabajo con los requisitos de formación, experiencia mínima y dedicación solicitados, son los que aseguran la ejecución contractual. En consecuencia, se mantienen los requisitos de formación, experiencia mínima, y dedicación establecidos en la Invitación Publica y sus documentos anexos.

OBSERVACIÓN No 3

Las certificaciones incluidas en la modificación 2 del pliego de condiciones no agregan valor al objeto del contrato y si afectan de manera importante la pluralidad de proponentes. A continuación algunas observaciones:

LÍDER DE AUDITORÍA.

- *No es claro porqué para el rol en mención, quien tiene asignadas funciones de diagnóstico dentro del proyecto (No se exigen actividades de auditoría) se le exige contar con experiencia específica desempeñando el rol de Auditor Líder en la norma. Un ingeniero con experiencia en implementación de ISO 27001, experiencia previa en auditoría (no necesariamente 27000) y la certificación requerida AL ISO 27001 también tiene el criterio y la competencia para hacer este tipo de aseguramientos con base en su conocimiento previo para procesos similares y agrega más valor al objeto de contrato. Este perfil afecta de manera importante la pluralidad de proponentes ya que no es común en el mercado que los consultores realicen únicamente actividades de auditoría ISO 27001 desarrollando únicamente y exclusivamente esta función o que sean "Auditores líderes" dentro del equipo. Adicional, para el objeto de este contrato este ajuste no agrega valor a las actividades a desarrollar especificadas dentro de los pliegos técnicos. PwC recomienda el siguiente perfil con base en su experiencia previa:*

** Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a cinco (5) años contados a partir de la fecha de terminación de materias.*

** Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación en los últimos tres (3) años, al menos uno de ellos como líder de equipo.*

** Especialización o maestría en Seguridad de la Información.* ***(Tener en cuenta para puntos adicionales ya que 1 años de estudio no es lo mismo que un curso de 1 semana en AL ISO 27001 y agrega valor al profesional)***

** Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años.*

** Acreditar certificación Auditor Líder ISO 27001 y acreditar al menos una (1) de las siguientes certificaciones: CISSP (Certified Information Systems Security Professional) - ISC2 ó CISA (Certified Information Systems Auditor)- ISACA ó CISM (Certified Information Security Manager) – ISACA.*

RESPUESTA

Una vez analizada la solicitud, la entidad acepta parcialmente la observación y en consecuencia modificará la participación en la implementación de los proyectos relacionados con el objeto de la invitación, de la siguiente manera: "*Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación en los últimos tres (3) años, desempeñando funciones de Auditor Líder (norma ISO 27001) en al menos uno de ellos*".

En consecuencia, los requisitos definitivos de experiencia mínima para el rol "*AUDITOR LIDER*" quedan establecidos de la siguiente manera:

Rol	No. de Personas	Experiencia Mínima.
AUDITOR LIDER Profesional Universitario en Ingeniería (Sistemas, industrial, automatización o electrónico)	1	▪ Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a cinco (5) años contados a partir de la fecha de terminación de materias. ▪ Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación en los últimos tres (3) años, desempeñando funciones de Auditor Líder (norma ISO 27001) en al menos uno de ellos. ▪ Acreditar certificación Auditor Líder ISO 27001:2013. ▪ Acreditar al menos dos (2) de las siguientes certificaciones: CISSP (Certified Information Systems Security Professional) - ISC2, CISA (Certified Information Systems Auditor)- ISACA o CISM (Certified Information Security Manager) – ISACA.

INGENIERO SENIOR (Continuidad):

- *No se tuvo en cuenta la certificación CBCP recomendada por PwC, siendo esta superior a la ABCP requerida. De igual manera no es claro, porqué se solicita ABCP la cual solo exige 1 año en "Continuidad de Negocio) para ser certificada teniendo este ingeniero la responsabilidad expresa de realizar el plan de continuidad tecnológico de toda la organización. Esta cantidad de tiempo (1 año) no es garantía de su competencia para el desarrollo de sus funciones dentro del proyecto, poniendo el riesgo la calidad del producto en esta etapa.*

RESPUESTA

Una vez analizada la solicitud, la entidad acepta la observación e incluirá dentro de la experiencia mínima para el rol "*INGENIERO SENIOR*" las siguientes certificaciones: a) BCLS 2000 (Administración Continuidad de Negocio) – DRI, b) ABCP - Associate Business Continuty Professional – DRI, c) CBCP – Certified Business Continuty Professional, d) APSCP – Associate Public Sector Continuity Professional – DRI, e) MBCP – Master Business Continuity Professional, f) CPSCP – Certified Public Sector Continuity Professional – DRI y, g) Auditor Líder ISO 22301. De la misma manera, las certificaciones mencionadas serán incluidas dentro del numeral "*7.1. CERTIFICACIONES EN SEGURIDAD DE LA INFORMACION*" del "*ANEXO. ESPECIFICACIONES TECNICAS MINIMAS*".

En consecuencia, el requisito relacionado con la certificación en continuidad del negocio para el rol "*INGENIERO SENIOR*" quedará de la siguiente manera: "*Uno (1) de los tres (3) debe*

acreditar la certificación BCLS 2000 (Administración Continuidad de Negocio) – DRI o ABCP - Associate Business Continuty Professional – DRI o CBCP - Certified Business Continuty Professional *o APSCP – Associate Public Sector Continuity Professional – DRI o* MBCP – Master Business Continuity Professional – DRI o *CPSCP – Certified Public Sector Continuity Professional – DRI o Auditor Líder ISO 22301*".

En consecuencia, los requisitos definitivos de experiencia mínima para el rol "*INGENIERO SENIOR*" quedan establecidos de la siguiente manera:

Rol	No. de Personas	Experiencia Mínima.
INGENIERO SENIOR Profesional Universitario en Ingeniería (Sistemas, industrial, automatización o electrónico)	3 (Dedicación 100%)	▪ Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a tres (3) años contados a partir de la fecha de terminación de materias. ▪ Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años. ▪ Acreditar al menos una (1) de las siguientes certificaciones: CISSP (Certified Information Systems Security Professional) - ISC2 o CISA (Certified Information Systems Auditor)- ISACA o CISM (Certified Information Security Manager) – ISACA o Auditor Líder ISO 27001:2013. ▪ Uno (1) de los tres (3) debe acreditar la certificación CEH (Certified Ethical Hacker). ▪ Uno (1) de los tres (3) debe acreditar la certificación BCLS 2000 (Administración Continuidad de Negocio) – DRI o ABCP - Associate Business Continuty Professional – DRI o CBCP – Certified Business Continuty Professional – DRI o APSCP – Associate Public Sector Continuity Professional – DRI o MBCP – Master Business Continuity Professional – DRI o CPSCP – Certified Public Sector Continuity Professional – DRI o Auditor Líder ISO 22301.

INGENIERO SENIOR:

- *Considerar la inclusión de la especialización de seguridad de la información por puntos adicionales en este rol para uno de los ingenieros propuestos ya que no excluye a ningún proponente, pero fortalece el perfil.*

RESPUESTA

Una vez analizada la solicitud, la entidad no acepta la observación y aclara:

1. La obtención de una certificación en un determinado arte o ciencia da a quien la consigue, organización o persona, una ventaja competitiva en aquel mercado en el que participa. Por supuesto, esta certificación debe ser otorgada por un ente reconocido por la comunidad que practica este arte o ciencia o por una organización autorizada por el primero.
2. Las certificaciones CISSP (Certified Information Systems Security Professional) - ISC2, CISA (Certified Information Systems Auditor)- ISACA, CISM (Certified Information Security Manager) – ISACA y Auditor Líder ISO 27001:2013, aseguran que el profesional certificado cuenta con los conocimientos y capacidades requeridas para implementar, mantener y auditar Sistemas de Gestión de la Seguridad de la Información.

INGENIERO JUNIOR:

- No es claro porqué se requiere de la certificación de CDFE ya que el proyecto no considera actividades de "Examen o análisis de fraude" dentro de su alcance o las actividades del mismo.
- No es claro porqué se requiere de la certificación CHFI ya que el proyecto no considera actividades de "Investigación Forense" dentro de su alcance o las actividades del mismo.
- No es claro porqué se requiere de la certificación IPV6 Gold o Silver, la cual se define como una certificación específica en redes para apoyar la implementación y monitoreo hacia redes IPV6, saliéndose drásticamente de la naturaleza del proyecto: "ELABORACIÓN DEL ANÁLISIS DEL ESTADO ACTUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA IMPRENTA NACIONAL DE COLOMBIA QUE INCLUYE LA ENTREGA DE LOS DOCUMENTOS TÉCNICOS INDICADOS EN EL ANEXO TÉCNICO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE GESTIÓN COMERCIAL, GESTIÓN DE PRODUCCIÓN, GESTIÓN FINANCIERA Y GESTIÓN NFORMÁTICA". Como parte de los requerimientos MINTIC se establece la aplicación de mejores prácticas en seguridad para el proceso de transición pero no realizar la transición directamente; esto último, en caso de ser requerido no debería ser revisado detalladamente por la entidad.

Con esto aseveramos que las certificaciones no deben ser excluyentes ni afectar la pluralidad de proponentes para la prestación de este tipo de servicios. Con base en ello recomendamos el siguiente perfil:

** Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a tres (3) años contados a partir de la fecha de terminación de materias.*
** Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años.*
** Acreditar al menos una (1) de las siguientes certificaciones: CompTIA Security+ o Auditor Interno ISO 27001 o Auditor Líder ISO 27001 ó CHFI.*

Considerar la inclusión de puntos adicionales para ingenieros con CEH o CISSP ya que estas acreditaciones, por su nivel de especialidad permiten garantizar a la entidad un excelente recurso para este tipo de proyectos.

RESPUESTA

Una vez analizada la solicitud, la entidad no acepta la observación y aclara:

1. Teniendo en cuenta que las certificaciones "*CDFE - Certified Fraud Examiners*" y "*CHFI – Computer Hacking Forensic Investigator*" solicitadas aseguran que el profesional certificado cuenta con los conocimientos y capacidades requeridas para la prevención, detección e investigación de fraudes y las técnicas y métodos de investigación forense; estos conocimientos y capacidades contribuirán significativamente en la estructuración del "*Proceso de Gestión de Incidentes*" (de Seguridad de la Información) exigido como parte de los resultados o productos esperados.
2. El objetivo de la etapa "*E11 - Transición de IPv4 a IPv6*" no es realizar la transición directamente, se limita a la "Fase I. Planeación del IPv6" de la "*Guía de Transición de IPv4 a IPv6 para Colombia*", documento que hace parte de la estrategia del MinTIC para la adopción del nuevo protocolo en las entidades del país.

INGENIERO DE CALIDAD:

- *No es claro porqué se suprimió la especialización en gestión de calidad por la certificación de AL ISO 9000. Favor tener en cuenta que la especialización considera un año de estudio y la certificación solo 1 semana.*
- *Nosotros recomendamos para este perfil que tuviera la certificación ISO 27001 interno, ya que este, siendo un proyecto de seguridad de la información requiere de personal conocedor de las mejores prácticas relacionadas.*
- *No es claro porque se exige dentro de la experiencia haber asumido el rol de auditor líder o líder, ya que para el objeto de este contrato y las actividades a su cargo, haber formado parte de un equipo como especialista o ingeniero de calidad también lo habilita para el desempeño de sus funciones. Con base en nuestra experiencia previa recomendamos el siguiente perfil.*

** Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a cinco (5) años contados a partir de la fecha de terminación de materias.*

** Acreditar especialización o maestría o posgrado en Gerencia de la Calidad o Gestión de la Calidad o AL ISO 9001.*

** Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación en el rol de calidad, en los últimos tres (3) años.*

** Acreditar certificación Auditor Interno 9001 y auditor interno ISO 27001 ya que como parte del objeto del contrato este profesional debe tener conocimiento del esquema documental de seguridad que se exige por el estándar con base en su experiencia técnica en esta materia. Estas certificaciones junto con los 5 años de experiencia y la especialización en Calidad, garantizan la idoneidad del profesional para el desarrollo de sus funciones dentro del alcance.*

RESPUESTA

Una vez analizada la solicitud, la entidad no acepta la observación y aclara:

1. La obtención de una certificación en un determinado arte o ciencia da a quien la consigue, organización o persona, una ventaja competitiva en aquel mercado en el que participa. Por

supuesto, esta certificación debe ser otorgada por un ente reconocido por la comunidad que practica este arte o ciencia o por una organización autorizada por el primero. La certificación Auditor Líder ISO 9001, asegura que el profesional certificado cuenta con los conocimientos y capacidades requeridas para implementar, mantener y auditar Sistemas de Gestión de la Calidad.

2. La Auditoría Interna puede decirse que es una parte integral de la Auditoría Líder. El auditor interno desarrolla conocimientos y capacidades para planificar y ejecutar auditorías internas y el auditor líder tiene la responsabilidad global de la auditoría y las comunicaciones formales del auditor con el cliente y con el auditado, es decir, el Auditor Líder debe tener conocimientos adicionales y habilidades en cuanto a liderazgo en auditoría, requeridos para asegurar la ejecución contractual en consideración al alcance del proceso de contratación.

BOGOTÁ D.C., 08 DE AGOSTO DE 2016.