**EL INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR "MARIANO OSPINA PEREZ" – ICETEX**

**INVITACIÓN POR LISTA CORTA No. 010-2015**

*"Implementar el Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea así como el Sistema de Gestión de Seguridad de la Información."*

De conformidad con el parágrafo del Artículo 3º del Acuerdo de Junta No. 19 del 19 de junio de 2014, que modificó el parágrafo del Artículo 32 del Acuerdo de Junta No. 30 de septiembre de 2013 que hace referencia a las *"Reglas de Participación"* el cual establece:

***Parágrafo:*** *El ICETEX podrá modificar las reglas de participación mediante adenda. La Entidad podrá expedir adendas hasta el día hábil anterior al vencimiento del plazo para presentar ofertas, salvo en los procesos de Selección Pública cuya publicación debe hacerse con tres (3) días de anticipación al plazo previsto para presentar ofertas.*

*Igualmente podrá modificar mediante adendas el cronograma del proceso después del cierre del mismo y hasta la adjudicación del proceso. La publicación de estas adendas así como de todos los demás documentos que se expidan con ocasión del proceso de selección sólo se podrán realizar en días hábiles y horarios laborales, entre las 7:00 A.M y las 7:00 P.M.*

La Secretaría General, en virtud de lo anterior y con fundamento en las observaciones recibidas al Pliego recibidas mediante correo electrónico contratos@icetex.gov.co, y en las solicitudes realizadas, por los proponentes invitados, dentro del proceso de lista corta No. 10-2015, encuentra necesario modificar mediante la presente adenda No. 1 lo siguiente:

**Modificación No. 1**

Modificación a lo enunciado en el numeral 3.4 del pliego de condiciones del proceso de lista corta No. 10-2015, denominado "**RECURSO HUMANO"**, el cual quedara así:

***"3.4. RECURSO HUMANO***

*Además de indicar el proponente en su propuesta que acepta, conoce y se obliga con su firma a cumplir con las obligaciones descritas, éste debe presentar con su propuesta el siguiente personal mínimo calificado, adjuntando los certificados de formación académica y de experiencia laboral:*

***3.4.1. Gerente de Proyecto***

*Perfil:*

a. *Formación académica*

*Un profesional en Ingeniería relacionadas con Tecnología de la Información o Ingeniería electrónica o Administrador de Empresas o Economista,* con formación académica en:

- Gerencia de Proyectos y

- Estándares de Seguridad de la Información, para lo cual se acepta Certificación en ISO27001.

b. *Experiencia profesional*

*Experiencia acreditada de mínimo cinco (5) años en Gerencia de Proyectos de Implementación de Sistemas de Gestión de Seguridad de la Información o de proyectos de seguridad de la información.*

### *3.4.2 Consultor Senior*

*Perfil:*

a. *Formación académica*

*Un profesional en Ingeniería relacionadas con Tecnologías de la Información con especialización o maestría en seguridad de la información o áreas de ingeniería relacionadas y conocimientos en Estándares de seguridad de la información. Formación académica en estándares de Seguridad de la Información, para lo cual se aceptan cualquiera de las siguientes certificaciones:*

*- Certificación en ISO27001*
*- Certificación CISA*
*- Certificación en CISM*
*- Certificación en COBIT*
*- Otras certificaciones en seguridad de la información*

*b. Experiencia profesional*

*Experiencia acreditada de mínimo cinco (5) años en Gerencia de Proyectos de Implementación de Sistemas de Gestión de Seguridad de la Información o de proyectos de seguridad de la información.*

### *3.4.3 Consultor Junior*

*Perfil:*

a. *Formación académica*

*Un profesional en Ingeniería de Sistemas o áreas de ingeniería relacionadas con temas de tecnología y conocimientos en Estándares de seguridad de la información.*

b. *Experiencia profesional*

- *Experiencia acreditada de mínimo tres (3) años en seguridad de la información.*

*Nota: El proponente deberá presentar certificaciones de estudios del equipo de trabajo así como las certificaciones con las cuales se pretenda acreditar la experiencia de cada una de las personas que conforman el personal mínimo requerido; las certificaciones deberán permitir conocer el nombre de la entidad contratante, fecha de expedición, objeto, valor, plazo, cumplimiento a satisfacción del contrato, teléfono de contacto para confirmar, presentada en papelería de la entidad contratante.*

*Para la presentación de la propuesta el oferente deberá adjuntar las hojas de vida de cada uno de los miembros del equipo de trabajo, con los respectivos soportes y certificados o lo que haga sus veces para acreditar nivel educativo y experiencia laboral.*

*En caso de requerirse validar la experiencia antes señalada el proponente podrá presentar copia de contratos, actas de recibo a satisfacción, cuyo contenido tenga la información requerida que permita efectuar la verificación respectiva.*

*El análisis de los documentos solicitados no da derecho a asignación de puntaje, pero conducirá a determinar si el proponente CUMPLE o NO CUMPLE con las condiciones para participar, lo cual HABILITA o INHABILITARA las propuestas para su evaluación técnica y económica.*

*Cualquier cambio en el personal, fijo o variable, durante la ejecución del contrato, debe ser informado previamente al ICETEX."*

**Modificación No. 2**

Incluir aclaración a lo enunciado en el numeral 4 del pliego de condiciones del proceso de lista corta No. 10-2015, denominado "**ESPECIFICACIONES DEL BIEN OBRA O SERVICIO REQUERIDO"**, el cual quedara así:

***" 4. ESPECIFICACIONES DEL BIEN OBRA O SERVICIO REQUERIDO***

1. *Definición del alcance del Proyecto: Dar continuidad a las actividades de seguridad de la información para que la Entidad tenga implementado un SGSI para todos los*

*procesos con que cuenta, así como, atender las actividades de implementación de GEL programadas por MINTIC para el año 2016.*

2. *Ejecutar las labores diarias de seguridad de la información, velando por el cumplimiento de las políticas y procedimientos que tiene la Entidad, tanto a nivel interno así como con proveedores y aliados estratégicos coordinadas por la Oficina de Riesgos.*

3. *Análisis de cumplimiento de las normas y buenas prácticas acogida y emisión de las recomendaciones aplicables según el caso.*

4. *Implementar actividades tendientes al cumplimiento de las normas relacionadas con seguridad de la información.*

5. *Revisión con periodicidad trimestral del cumplimiento de las normas y buenas prácticas acogidas (ISO 27001, Gobierno en línea, Ley de transparencia, Ley de Tratamiento de Datos Personales, Circular 042 del año 2012 de la Superintendencia Financiera de Colombia, entre otras).*

6. *Desarrollo de los Componentes de Implementación y Evaluación del Desempeño del Modelo de Seguridad y Privacidad de la Información de Gobierno en Línea, las cuales están conformadas por las siguientes actividades:*

   *Componente de Implementación:*

   - *Planificación y control operacional.*
   - *Implementación del plan de tratamiento de riesgo.*
   - *Implementación del plan y estrategia de transición de IPv4 a IPv6.*

   *Componente de Evaluación de desempeño*

   - *Plan de seguimiento, evaluación y análisis del Modelo de Seguridad y Privacidad de la Información (MSPI).*
   - *Evaluación del plan de tratamiento de riesgos.*

   ***Aclaración:** "La Implementación del plan y estrategia de transición de IPv4 a IPv6", va dirigido a realizar seguimiento al plan de estrategia de transición de IPv4 a IPv6, que deberá ser desarrollado por la Dirección de Tecnología del ICETEX.*

7. *Revisión de los documentos actuales que apoyan el SGSI y generar los documentos faltantes requeridos así como la definición del modelo de gobierno del SGSI.*

8. *Revisión de los documentos actuales que apoyan el SGSI y generar los documentos faltantes requeridos.*

9. *Gestión de Riesgos que abarca: Identificación y evaluación de riesgos y controles de 20 procesos y monitoreo de los riesgos ya identificados (otros 20 procesos).*

10. *Generar Tratamientos para aquellos riesgos que resulte con evaluación grave o crítica, actividad conformada por:*

    - *Plan de tratamiento de riesgos.*
    - *Implementación de plan de tratamiento de riesgos.*
    - *Implementación de controles definidos.*

11. *Definición de los indicadores para medir la eficacia de los controles (métricas de seguridad).*

12. *Revisión y actualización de la Declaración de Aplicabilidad de acuerdo con los resultados obtenidos de la evaluación de riesgos y su plan de tratamiento, conformado por:*

    - *Identificación de controles aplicables de acuerdo con el contexto y los procesos dentro del alcance.*
    - *Identificación de exclusiones y controles no aplicables.*
    - *Establecimiento del estado actual de cumplimiento frente a los controles aplicables.*

13. *Definición de respuesta ante incidentes de seguridad de la información, donde se realice la recolección de evidencias y se dé respuesta y atención de incidentes, así como estudio forense de ser necesario.*

14. *Realizar una (1) campaña de capacitación al personal de planta, contratistas y aliados estratégicos.*

15. *Realizar una (1) prueba de Hacking Ético sobre cincuenta (50) IP, de la infraestructura tecnológica de la Entidad (pruebas de vulnerabilidades externas e internas). Adicional, efectuar planes de monitoreo de cierre de vulnerabilidades y realización de pruebas re-test.*

16. *Evaluación del nivel de protección de la red de la Entidad.*

17. *Realizar dos (2) pruebas de ingeniería social bajo 3 escenarios, dirigida a 10 funcionarios cada escenario. Adicional, desarrollar planes para realizar monitoreo de cierre de vulnerabilidades.*

18. *Realizar tres (3) pruebas de revisión de equipos de tesorería (13 equipos) y se desarrollen planes de monitoreo para el cierre de vulnerabilidades.*

19. *Generar las recomendaciones y acciones de remediación sugeridas con base en los hallazgos que se generen producto de las pruebas que se realicen.*

20. *Actualizar el inventario de activos de información con los componentes de seguridad necesarios.*

21. *Implementar los lineamientos de manejo de clasificación de activos de información.*

22. *Generar los conceptos de seguridad de información que requieran las áreas.*

23. *Proyectar el Comité de Seguridad de la Información, con periodicidad trimestral.*

24. *Participar en los Sub-comités de Gobierno de Tecnología.*

25. *Revisión, recomendación y guía de implementación de los perfiles de acceso al sistema de información misional.*

Finalmente y en relación a los demás ítems de los Pliegos de Condiciones del proceso de lista corta No. 010 – 2015, que tiene por objeto contratar "Implementar el Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea así como el Sistema de Gestión de Seguridad de la Información", que no se modificaron en este documento continuarán vigentes.

Dada en Bogotá D.C., a los veintinueve (29) días del mes de diciembre de dos mil quince (2015).

**ORIGINAL FIRMADO**

**CAMPO ELÍAS VACA PERILLA**
Secretario General ICETEX

*Revisó:*

VoB. Técnico **Gerardo Gutierrez Castro Jefe Oficina de Riesgos** (E) ICETEX

Vo.Bo. Claudia Stella Cortes Albornoz - Analista Oficina de Riesgos

Reviso: Jorge Ivan Molina Pardo – Asesor Grupo de Contratación Secretaria General
Proyectó: Angelica P. Chilito Lenis - Contratista Grupo Contratos