DEPARTAMENTO ADMINISTRATIVO DE CIENCIA, TECNOLOGIA E INNOVACION - COLCIENCIAS -

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

1. PRESENTACIÓN

COLCIENCIAS, como ente rector de la ciencia, la Ciencia, Tecnología e Innovación en el país, en alianza con el Ministerio de Tecnologías de la Información y las Comunicaciones, busca con esta convocatoria el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones en la industria nacional TIC, la administración pública, la academia y la sociedad, con el fin de contribuir con el incremento de la productividad y la competitividad del sector TIC, acercar la actividad investigativa básica al mercado y fortalecer la administración pública.

De acuerdo con lo anterior, la presente convocatoria está orientada a la formulación de políticas, directrices, normas, actos administrativos y otras formas cuyo propósito sea proteger el ciberespacio de amenazas que atenten contra la soberanía nacional y los principios constitucionales.

La ciberseguridad se define como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos y organizaciones tanto públicas como privadas, ante amenazas o incidentes de naturaleza cibernética. Así mismo, dentro de este nodo de innovación se incluye el concepto de ciberdefensa, el cual se define como la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional (Documento CONPES 3701 de 2011).

Para mayor información sobre antecedentes de esta convocatoria y ampliación de la definición del subsistema de innovación revisar el anexo 1.

2. OBJETIVOS

2.1 GENERAL

Cofinanciar proyectos de innovación los cuales estén orientados al fortalecimiento de la ciberseguridad a través de la generación, adaptación, dominio y utilización de nuevas tecnologías que permitan minimizar y contrarrestar apropiadamente los riesgos e incidentes de naturaleza cibernética a los que están expuestas las instituciones del

estado.

2.2 ESPECÍFICOS:

2.2.1 Fortalecer los Nodos de Innovación, impulsados por el Ministerio TIC y COLCIENCIAS, específicamente el nodo de ciberseguridad.

2.2.2 Fortalecer la productividad y la competitividad de la industria TIC nacional, a través del desarrollo de proyectos de innovación que redunden en el uso y apropiación de TIC en las entidades públicas colombianas.

2.2.3 Fortalecer la Cultura de Innovación en el Gobierno, apalancado en un sector TIC altamente innovador.

2.2.4 Fortalecer los vínculos entre sectores productivos, gubernamentales y académicos e investigativos, a nivel nacional, a través del desarrollo de proyectos estratégicos de innovación en ciberseguridad.

2.2.5 Fomentar el flujo de conocimiento y experiencia que las universidades, centros de investigación o centros de desarrollo tecnológico tienen en trabajo en red y prospectiva hacia los Nodos de Innovación.

2.2.6 Apoyar al Gobierno y a través de él a la comunidad en general mediante proyectos innovadores que redunden en una mejor funcionalidad de sus entidades y una mejor atención de éstas al ciudadano.

2.2.7 Apoyar a las instituciones del estado en la incorporación y apropiación de las TIC mediante la ampliación de la oferta de alternativas y soluciones en el mercado.

3. DIRIGIDO A

Alianzas estratégicas entre instituciones ejecutoras y empresas beneficiarias. A continuación se presenta la definición de los participantes.

3.1 Instituciones ejecutoras: se consideran instituciones ejecutoras a las Universidades públicas y privadas, grupos de investigación, desarrollo tecnológico y/o innovación, centros de investigación y centros de desarrollo tecnológico, reconocidos por COLCIENCIAS a la apertura de la presente convocatoria.

Las instituciones ejecutoras serán las responsables de llevar a cabo el aporte científico e investigativo que permita materializar un producto orientado al fortalecimiento de la ciberseguridad en las instituciones del estado y la ejecución de los recursos destinados al proyecto.

3.2 Empresa beneficiaria: se consideran empresas beneficiarias las personas jurídicas, de economía mixta o privadas, con o sin ánimo de lucro del sector productivo y de servicios legalmente constituidas en Colombia. Pueden ser empresas beneficiarias las Microempresas, PyMEs y Grandes Empresas.

De igual forma, las Entidades Públicas entendidas como todos los órganos, organismos y entidades nacionales y territoriales de las ramas del poder público colombiano, con excepción de las Sociedades de Economía Mixta, las Empresas Industriales y Comerciales del Estado y cualquier Sociedad Pública que desarrolle actividades comerciales en competencia con el sector privado que participen en la presente convocatoria, se consideran empresas beneficiarias.

Las empresas beneficiarias aportarán recursos de contrapartida, elaborarán el plan de negocios del producto resultado del proyecto y serán las responsables de la comercialización futura de dicho producto.

Nota:

Una Entidad Pública no puede ser simultáneamente beneficiaria y ejecutora en el mismo proyecto.

4. LINEAS TEMÁTICAS

Las propuestas que se presenten en el marco de la presente convocatoria deberán estar enmarcadas en el Subsistema de Innovación – Sistema de Investigación, Desarrollo e Innovación (I+D+i) de TIC impulsado por el Ministerio de TIC y COLCIENCIAS, en la temática de los Nodos de Innovación en ciberseguridad, específicamente deberán abordar:

- Principios rectores de ciberseguridad
- Educación, formación y divulgación en ciberseguridad;
- Gestión integrada de riesgos e incidentes de naturaleza cibernética
- Identificación, autenticación y autorización
- Aseguramiento de aplicaciones y ambientes móviles en el gobierno
- Tecnologías de la Información y las Comunicaciones para el sector defensa.

Para ampliación sobre las líneas temáticas de esta convocatoria ver el anexo 2.

5. REQUISITOS MÍNIMOS

Los requisitos mínimos para participar en la presente convocatoria, son los siguientes:

5.1 Inscripción del proyecto en el Sistema integrado de Gestión de Proyectos de COLCIENCIAS – SIGP a través del formulario electrónico disponible en el portal de COLCIENCIAS (www.colciencias.gov.co).

5.2 Las alianzas estratégicas deben estar conformadas, como mínimo, por una institución ejecutora y una empresa beneficiaria.

5.3 Los grupos de investigación, desarrollo tecnológico y/o innovación y los centros de desarrollo tecnológico que participen como ejecutores en esta convocatoria, deberán estar reconocidos por COLCIENCIAS a la fecha de apertura de la presente convocatoria.

5.4 Los productos, servicios o procesos de los proyectos de desarrollo tecnológico e innovación resultado de esta convocatoria deben tener como usuario potencial necesariamente a Entidades Públicas, ya sean del orden nacional, departamental y/o municipal o ayudar a que los ciudadanos tengan un mejor acceso a la información o servicios que estas generan.

5.5 Carta de alianza estratégica entre las instituciones ejecutoras y las empresas beneficiarias, firmada por los representantes legales de las entidades, en la cual se designe al ejecutor del proyecto, y la contrapartida de acuerdo con el formato del anexo 3. En caso que el representante legal no cuente con la competencia para asumir los compromisos consignados en la carta de alianza estratégica, deberá presentar documento que lo faculte firmado por el órgano competente.

5.6 Cada una de las empresas beneficiarias deberá acreditar como mínimo veinticuatro (24) meses de constituida a la fecha de apertura de la presente convocatoria.

5.7 Las empresas beneficiarias deberán acreditar experiencia en temas relacionados con ciberseguridad mediante certificaciones de ejecución o actas de finalización de por lo menos tres (3) proyectos terminados en los últimos cinco (5) años hasta la fecha de apertura de esta convocatoria. En el caso de que participe más de una empresa beneficiaria en uno de los proyectos, la experiencia base para la evaluación será la suma de las experiencias individuales de estas.

Se debe presentar un formato por cada una de las empresas beneficiarias que integren la alianza estratégica, ver anexo 4.

5.8 Documento donde conste el acuerdo entre las entidades participantes en el proyecto con respecto a los derechos patrimoniales sobre la propiedad intelectual de los productos resultantes del proyecto. Para estos efectos se recomienda revisar el Reglamento de Propiedad Intelectual del Subsistema de Innovación para el uso y apropiación de TIC en el gobierno que se encuentra en anexo 5 de esta convocatoria.

5.9 Carta de autorización de uso y almacenamiento de datos personales de las personas involucradas en el proyecto, Ver anexo 6.

5.10 Carta de presentación, aval y aceptación de compromisos; relacionando que este proyecto no está siendo presentado por otra convocatoria y no está siendo financiado

con otros recursos del Estado, firmada por el representante legal de la entidad ejecutora, ver anexo 7.

5.11 Las instituciones ejecutoras y/o empresas beneficiarias que hayan contado con participación previa en el Subsistema de Innovación para el uso y apropiación de TIC en el gobierno – Nodos de Innovación, deberán adjuntar certificación expedida por la Secretaría Técnica del mencionado Subsistema en el MINTIC o quien haga sus veces.

Notas:

- Los interesados deberán cumplir con la totalidad de los requisitos mínimos para que su proyecto sea evaluado, en caso contrario no continuarán al proceso de evaluación.
- Las entidades que se presenten en alianzas, uniones temporales o consorcios que tengan contratos o convenios vigentes con COLCIENCIAS deberán estar a paz y salvo con los compromisos adquiridos; de lo contrario no serán considerados para participar en esta convocatoria.
- COLCIENCIAS, podrá solicitar en cualquier momento, información, documentación adicional y aclaraciones.

6. DURACIÓN Y FINANCIACIÓN

El término de duración de los proyectos a financiar será de hasta doce (12) meses.

Se cuenta con OCHOCIENTOS MILLONES DE PESOS M/CTE ($800.000.000) para cofinanciar proyectos en esta convocatoria, los cuales corresponden a recursos de COLCIENCIAS y del Ministerio de Tecnologías de la Información y las Comunicaciones.

La financiación del proyecto se hará bajo el mecanismo de cofinanciación. El monto máximo a financiar por proyecto será de hasta DOSCIENTOS MILLONES DE PESOS M/CTE ($200.000.000).

La contrapartida de la(s) empresa(s) beneficiaria(s), debe ser de la siguiente manera, de acuerdo con lo establecido en la Ley 905 de 2004:

Tamaño de Empresa	Valores de contrapartida Mínimos
Microempresas	25% en especie o en dinero
PYMES	35% en especie o en dinero
Gran empresa	20% en dinero y 40% en especie

Para estructuración del presupuesto ver el anexo 8.

Notas:

- El proyecto presentado no podrá ser financiando simultáneamente por otra convocatoria o con recursos de COLCIENCIAS u otras entidades del Estado.
- En caso de no reintegro de los recursos acordados contractualmente, COLCIENCIAS efectuará el respectivo reporte en el boletín de deudores morosos.

7. CONTENIDO DEL PROYECTO

El proyecto deberá incluir dos componentes: científico-técnico y presupuestal; como se describe a continuación y se detalla en el anexo 8.

7.1 COMPONENTE CIENTÍFICO - TÉCNICO DEL PROYECTO

El proyecto deberá incluir la información que se describe a continuación y que se detalla en el anexo 8.

- Título del proyecto
- Investigador principal y coinvestigadores
- Línea Temática
- Antecedentes
- Resumen ejecutivo.
- Palabras Clave.
- Planteamiento del Problema.
- Justificación.
- Marco conceptual.
- Estado del arte.
- Objetivos: (General, específicos)
- Metodología
- Resultados esperados.
- Productos esperados
- Impactos potenciales.
- Trayectoria del equipo de investigación
- Cronograma
- Bibliografía
- Plan de negocios.

7.2 COMPONENTE PRESUPUESTAL

Este componente deberá presentarse discriminado mensualmente. El valor de la contrapartida deberá estar dado en recursos en efectivo o en especie de acuerdo con lo estipulado en el numeral 6 de esta convocatoria.

El presupuesto deberá presentarse discriminado por rubros, serán financiados con recursos de COLCIENCIAS únicamente los rubros estipulados en el anexo 8.

7.3 Rubros No Financiables

No será financiable con recursos de COLCIENCIAS rubros presupuestales como:

- El personal que sea beneficiario actual de los programas “Jóvenes Investigadores” o “Formación de Doctorados” de COLCIENCIAS, podrá ser vinculado a las actividades investigativas previstas para la ejecución del proyecto, pero en ningún caso, podrá ser financiado al mismo tiempo con los recursos provenientes de COLCIENCIAS asignados a este rubro, en esta convocatoria.
- A través del rubro de personal, no se financiarán los derechos académicos y de matrícula del personal.
- No será financiable con recursos de COLCIENCIAS rubros presupuestales como: construcciones, mantenimiento de equipos e infraestructura, imprevistos, seguros, adquisición de vehículos, mobiliario de oficina, membresías a Sociedades Científicas.
- Comprar de máquinas y equipo de producción corriente.
- Pagos de pasivos, pago de dividendos, aumento de capital de la entidad beneficiaria
- Pagos de dividendos o recuperaciones de capital de la entidad beneficiaria
- Capital de trabajo para la producción corriente
- Inversiones en otras empresas
- Inversiones en planta de producción a escala industrial
- Compra de acciones, derechos de empresas, bonos y otros valores mobiliarios
- Instalaciones llave en mano

8. PROCEDIMIENTO DE INSCRIPCIÓN

8.1 Descargar, descomprimir e instalar la máquina virtual de java de la siguiente dirección: http://www.colciencias.gov.co/sites/default/files/ckeditor_files/files/formularios_sigp/jre-1_5_0_22-windows-i586-p.zip

8.2 Descargar, descomprimir e instalar y diligenciar el formulario electrónico disponible en la sección correspondiente a esta convocatoria del portal institucional de COLCIENCIAS (http://www.colciencias.gov.co). El formulario electrónico es específico para esta convocatoria, asegúrese de diligenciar efectivamente el formulario en cuestión.

8.3 Para enviar el proyecto desde el formulario electrónico, debe *Aceptar los términos y condiciones*, e inmediatamente se activa el botón de *Validar*, si el proyecto es *validado sin errores,* se activa el botón de *Enviar.* Una vez el proyecto sea enviado al Sistema Integrado de Gestión de Proyectos de COLCIENCIAS -SIGP- emitirá una respuesta automática, generando un número de confirmación de recibido en el servidor de COLCIENCIAS, este número garantizará la recepción exitosa del proyecto.

8.4 El número de confirmación de recibido y la contraseña que la entidad asigne al proyecto, le permitirá realizar el envío de los *requisitos mínimos* y hacer el seguimiento del estado del proyecto. Tome nota de este número de confirmación y de la contraseña asignada.

8.5 Para realizar el envío de los *requisitos mínimos* desde el formulario electrónico, debe *dar clic en el botón Adjuntar documentos de requisitos,* inmediatamente el sistema despliega una página del portal de Sistema de Gestión de Proyectos para tal fin. En el campo *proyecto,* digite el número de confirmación de recibido y en el campo correspondiente diligencie la contraseña y proceda a dar clic en el botón *ingresar*. A continuación el sistema despliega la información básica del proyecto y en la parte inferior el detalle de los *requisitos mínimos.*

8.6 Debe adjuntar la totalidad de los documentos que soportan los *requisitos mínimos. S*i requiere anexar documentación adicional del proyecto como: tablas, fórmulas, gráficas, anexos, cartas, etc.), guárdelos en una sola carpeta y adjúntelas como archivo .ZIP o .RAR (archivo comprimido), en el requisito de *Otros adjuntos.* Si requieren cambiar algún archivo de los que previamente adjuntó, puede hacerlo examinando y adjuntando el documento deseado. Recuerde que el formulario solo admite un archivo anexo por cada requisito mínimo, por lo que al cargar un archivo nuevo, éste remplazará el anterior. Usted puede verificar el archivo que adjuntó a través de la página http://201.234.78.164:7777/portal/ del SIGP con el número de confirmación y la contraseña asignada al proyecto.

8.7 Anexando todos los documentos obligatorios se puede *Generar el certificado de requisitos mínimos*, que le sirve de evidencia del envío de los *mismos.* En caso contrario, el sistema enviará el siguiente mensaje de error: *Error - Debe adjuntar los documentos obligatorios para obtener el certificado*, y no permitirá generar dicho certificado.

8.8 Hasta que no estén completos los requisitos mínimos y generado el certificado anteriormente mencionado, no se dará por culminado satisfactoriamente el proceso de inscripción del proyecto.

Notas:

- Se aceptarán únicamente los proyectos que se presenten a través del formulario electrónico con toda la información solicitada en la presente convocatoria.
- No será tenida en cuenta para el proceso de evaluación y selección del Banco de Proyectos Elegibles, la información enviada en medios distintos al SIGP (correo postal, fax, correo electrónico o cualquier otro), ni posterior a la fecha y hora límite establecida. Ver numeral 13 (Cronograma)

9. CRITERIOS DE EVALUACIÓN

Los criterios de evaluación serán los siguientes:

No.	Criterio	Puntaje máximo
1	Calidad y metodología del proyecto.	20

No.	Criterio	Puntaje máximo
2	Equipo de Trabajo	20
3	Resultados e impactos esperados del proyecto en el uso y apropiación de TIC en el gobierno.	20
4	Plan de Negocio	20
5	Participación comprobable de por lo menos una de las entidades ejecutoras en el Subsistema de Innovación para el uso y apropiación de TIC en el gobierno – Nodos de Innovación expedido por la Secretaría Técnica del mencionado Subsistema o quien haga sus veces.	5
6	Participación comprobable de por lo menos una de las empresas beneficiarias en el Subsistema de Innovación para el uso y apropiación de TIC en el gobierno – Nodos de Innovación expedido por la Secretaría Técnica del mencionado Subsistema o quien haga sus veces.	5
7	Interés y/o apoyo comprobable de una o varias entidades estatales en el uso de los resultados del proyecto, a través de la participación en pilotos o prototipos o la participación demostrable en el proyecto. Nota: No se busca que los proyectos generen resultados de uso exclusivo de la(s) entidad(es) estatal(es) participantes.	10
Total		**100**

Para consultar la información detallada de los criterios de evaluación, ver anexo 9.

10. PROCESO DE EVALUACIÓN

Los proyectos inscritos dentro de los plazos establecidos para la presente convocatoria y que cumplan con los requisitos mínimos, serán evaluados por pares y/o panel de expertos seleccionados por COLCIENCIAS, teniendo en cuenta los criterios de evaluación descritos en el numeral 9.

En caso de empate, se tendrá en cuenta aquel proyecto que presente un mayor puntaje en el criterio consensuado 1. Si aún continúa existiendo empate, se tendrá en cuenta aquel proyecto que presente un mayor puntaje en el criterio consensuado 2. De mantenerse el empate se tendrá en cuenta aquel proyecto que presente un mayor puntaje en el criterio consensuado 3. De continuar con el empate, se procederá con aquel proyecto que presente un mayor puntaje en el criterio consensuado 4. Si persistiere el empate se tendrá en cuenta aquel proyecto que presente un mayor puntaje en el criterio

consensuado 5. Si persistiere el empate se tendrá en cuenta aquel proyecto que presente un mayor puntaje en el criterio consensuado 6. Si persistiere el empate se tendrá en cuenta aquel proyecto que presente un mayor puntaje en el criterio consensuado 7. Si por alguna razón, luego de realizado todo el ejercicio descrito anteriormente, continuaran proyectos empatadas, se realizará un sorteo por balotas, del cual se levantará un acta firmada por los que intervienen en el sorteo.

Toda información proporcionada es de carácter confidencial y no será utilizada para ningún fin diferente a la realización de la evaluación. Los expertos evaluadores estarán cobijados por cláusulas de confidencialidad y de no conflicto de interés.

De acuerdo con el CRONOGRAMA de la convocatoria, se concederá un término para solicitar aclaraciones y/o modificaciones a la publicación preliminar del banco de elegibles, una vez éstas sean resueltas, se procederá a la publicación del banco definitivo de proyectos elegibles.

11. BANCO DE ELEGIBLES

Los resultados de la convocatoria se publicarán en la página web de COLCIENCIAS (www.colciencias.gov.co) en las fechas establecidas en el CRONOGRAMA.

Las propuestas que superen setenta (70) puntos ingresarán al banco de elegibles y se asignarán los recursos hasta su agotamiento en estricto orden descendente.

La vigencia del banco de elegibles es de un año a partir de su publicación definitiva. La inclusión de un proyecto en el banco de elegibles, no implica obligatoriedad ni compromiso alguno de COLCIENCIAS o de MINTIC, de asignar recursos, ni genera derecho a recibir apoyos económicos para quienes hayan presentado los proyectos correspondientes.

Notas:

- Surtida la publicación definitiva del banco de elegibles, COLCIENCIAS informará mediante comunicación escrita y/o electrónica a los proyectos que hayan sido seleccionados para ser cofinanciados, indicando las instrucciones y condiciones para suscribir el contrato. A partir de la fecha de comunicación, se contarán quince (15) días calendario como plazo máximo para que los proponentes remitan a COLCIENCIAS la totalidad de la documentación. Vencido el término, en caso que los proponentes no remitan la documentación, se entenderá que desisten de su interés por contratar con COLCIENCIAS y se procederá a co-financiar el siguiente proyecto del banco de elegibles.

- Una vez remitida la minuta del contrato a los proponentes, éstos contarán con un plazo de cinco (5) días hábiles para devolverla firmada a COLCIENCIAS. En caso de correcciones a la minuta, el plazo de devolución se contará a partir del envió de la minuta ajustada, vencido el término anterior, si los proponentes no remiten el contrato firmado, se entenderá que desisten de su interés por contratar y se procederá a seleccionar el siguiente en orden descendente de la lista del banco de elegibles.

12. ACLARACIONES

Una vez publicados los resultados preliminares del banco de elegibles, los interesados podrán presentar solicitudes de aclaraciones y comentarios por un período de tres (3) días hábiles. Por fuera de este término se considera que las reclamaciones son extemporáneas y no serán atendidas.

Las peticiones y reclamaciones se deben presentar ***exclusivamente*** a través del correo electrónico contacto@colciencias.gov.co, con el asunto "Convocatoria Ciberseguridad - 2014".

13. CRONOGRAMA

ACTIVIDAD	FECHA LIMITE
Apertura de la convocatoria	30 de abril de 2014
Cierre de la convocatoria	26 de junio de 2014
Publicación del banco preliminar de proyectos elegibles	29 de julio de 2014
Período de solicitud de aclaraciones del banco preliminar de elegibles	Del 30 de julio de 2014 al 01 de agosto de 2014
Respuesta a solicitud de aclaraciones	6 de agosto de 2014
Publicación del banco definitivo de proyectos elegibles	12 de agosto de 2014

14. PROPIEDAD INTELECTUAL

En desarrollo de lo previsto en el artículo 31 de la Ley 1450 de 2011, en la medida en que los proyectos de ciencia, tecnología e innovación que al amparo de esta convocatoria se declaren elegibles, serían financiados con recursos del presupuesto nacional, el Ministerio de TIC y COLCIENCIAS, salvo motivos de seguridad y defensa nacional, podrán ceder a las entidades, uniones temporales y/o consorcios que desarrollen los proyectos financiados, los derechos de propiedad intelectual que le puedan corresponder, según se establezca en el contrato.

Los participantes del proyecto definirán entre ellos la titularidad de los derechos de propiedad intelectual derivados de los resultados de la ejecución del mismo. De esta definición, resultará un documento donde conste el acuerdo entre las entidades participantes en el proyecto respecto a los derechos patrimoniales sobre la propiedad intelectual de los productos del mismo, requisito necesario para participar de la presente convocatoria. Para estos efectos se recomienda revisar el Reglamento de Propiedad Intelectual del Subsistema de Innovación para el uso y apropiación de TIC en el gobierno que se encuentra en anexo 5 de esta convocatoria.

Nota:

En cualquier evento o medio de divulgación utilizado para difundir los resultados del proyecto se deberá dar el respectivo crédito a COLCIENCIAS y el Ministerio TIC, incluyendo la imagen institucional de las dos instituciones

15. VEEDURIAS CIUDADANAS

Las veedurías ciudadanas establecidas en la ley 850 de 2003, podrán desarrollar su actividad durante la presente convocatoria, conforme a lo estipulado en dicha normativa.

16. ANEXOS

- Anexo 1: Antecedentes y definiciones
- Anexo 2: Temáticas de la convocatoria
- Anexo 3: Carta de conformación de alianza estratégica
- Anexo 4: Carta de acreditación de empresas beneficiarias
- Anexo 5: Reglamento de propiedad intelectual
- Anexo 6: Carta autorización datos personales
- Anexo 7: Carta de presentación y aval
- Anexo 8: Contenidos del proyecto
- Anexo 9: Criterios de evaluación

17. ACEPTACIÓN DE TÉRMINOS Y VERACIDAD

Con la inscripción, los interesados aceptan las características, requisitos y condiciones de la presente convocatoria así como lo dispuesto en los presentes términos de referencia para el desarrollo de la misma y para la entrega del beneficio.

De igual forma declaran que la información suministrada es veraz y corresponde a la realidad. En caso de encontrarse alguna incoherencia e inconsistencia en la información o documentación suministrada, COLCIENCIAS podrá en cualquier momento rechazar la postulación o si es del caso declarar la pérdida del beneficio, sin perjuicio de las acciones legales correspondientes.

Los proponentes aceptan sin condicionamiento alguno la existencia de una obligación solidaria en relación con la presentación de la propuesta, la suscripción y legalización del contrato, así como de su cumplimiento y liquidación (responsabilidad solidaria en las fases pre-contractual, contractual y post-contractual). Los proponentes mantendrán los términos de la propuesta durante el desarrollo y ejecución de la misma y no podrán ser modificados sin el consentimiento previo de COLCIENCIAS y el Ministerio TIC. De igual manera, los miembros de la alianza estratégica que presentan el proyecto, deben designar la persona que, para todos los efectos, hará su representación y señalarán las reglas básicas que regulen las relaciones entre ellos y su responsabilidad. Para la existencia de la obligación solidaria solamente será necesario que la oferta se presente en forma conjunta, en consecuencia no se requiere que se refiera a esta circunstancia de manera expresa.

18. MAYOR INFORMACIÓN

DEPARTAMENTO ADMINISTRATIVO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN - COLCIENCIAS -

Carrera 7 B Bis No. 132-28, Bogotá D.C.
http://www.colciencias.gov.co
Centro de Contacto
Teléfono: (+57 - 1) 6258480 Extensión 2081
Línea gratuita nacional: 018000 914446

En caso de inquietudes o comentarios sobre la presente convocatoria, favor enviar un correo electrónico con el asunto "Convocatoria ciberseguridad – 2014" al correo contacto@colciencias.gov.co

PAULA MARCELA ARIAS PULGARÍN
Directora

Vo.Bo. Director Técnico
Vo.Bo. Secretaría General

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 1 – ANTECEDENTES Y DEFINICIONES

1. Antecedentes Constitucionales y Normativos

La constitución política de Colombia, establece en el artículo 71 que el Estado creará incentivos para personas e instituciones que desarrollen y fomenten la ciencia y la tecnología y las demás manifestaciones culturales y ofrecerá estímulos especiales a personas e instituciones que ejerzan estas actividades; a su vez el Articulo 70 establece que el estado promoverá la investigación, la ciencia, el desarrollo y la difusión de los valores culturales de la Nación.

La ley 29 de 1990, establece en su artículo 1, como una de las obligaciones del estado la de promover y orientar el adelanto científico y tecnológico, e incorporar la ciencia, la tecnología y a su vez en el numeral 5 del artículo 4 faculta a COLCIENCIAS para efectuar convocatorias públicas, basadas en criterios de mérito y calidad.

> *"…Artículo 4 numeral 5. Transparencia. Las instituciones, programas, proyectos y personas objeto de apoyo, se podrán seleccionar mediante* ***convocatorias públicas****, basadas en criterios de mérito y calidad…"* Negrilla fuera de texto.

La ley 1286 de 2009 establece, en su artículo 3. *Bases para la Consolidación de una Política de Estado en Ciencia, Tecnología e Innovación. Además de las acciones previstas en el artículo 2° de la Ley 29 de 1990 y la Ley 115 de 1994, las políticas públicas en materia de estímulo y fomento de la ciencia, la tecnología y la innovación, estarán orientadas por los siguientes propósitos:*

1. Incrementar la capacidad científica, tecnológica, de innovación y de competitividad del país para dar valor agregado a los productos y servicios de origen nacional y elevar el bienestar de la población en todas sus dimensiones.
2. Incorporar la investigación científica, el desarrollo tecnológico y la innovación a los procesos productivos, para incrementar la productividad y la competitividad que requiere el aparato productivo nacional.
3. Establecer los mecanismos para promover la transformación y modernización del aparato productivo nacional, estimulando la reconversión industrial, basada en la creación de empresas con alto contenido tecnológico y dando prioridad a la oferta nacional de innovación.
4. Integrar esfuerzos de los diversos sectores y actores para impulsar áreas de conocimiento estratégicas para el desarrollo del país.
5. Fortalecer la capacidad del país para actuar de manera integral en el ámbito internacional en aspectos relativos a la ciencia, la tecnología y la innovación.
6. Promover la calidad de la educación formal y no formal, particularmente en la educación media, técnica y superior para estimular la participación y desarrollo de las

nuevas generaciones de investigadores, emprendedores, desarrolladores tecnológicos e innovadores.
7. Promover el desarrollo de estrategias regionales para el impulso de la Ciencia, la Tecnología y la Innovación, aprovechando las potencialidades en materia de recursos naturales, lo que reciban por su explotación, el talento humano y la biodiversidad, para alcanzar una mayor equidad entre las regiones del país en competitividad y productividad.

La ley 1286 de 2009, establece en los numerales 1, 4, 5, 6, 9, 8 y 11 del artículo *6. Objetivos generales. Serán objetivos generales del Departamento Administrativo de Ciencia, Tecnología e Innovación - Colciencias:*

1. Crear una cultura basada en la generación, la apropiación y la divulgación del conocimiento, y la investigación científica, la innovación y el aprendizaje permanentes.
4. Articular y enriquecer la investigación, el desarrollo científico, tecnológico y la innovación con el sector privado, en especial el sector productivo.
5. Propiciar el fortalecimiento de la capacidad científica, tecnológica, de innovación, de competitividad y de emprendimiento, y la formación de investigadores en Colombia.
6. Promover el desarrollo y la vinculación de la ciencia con sus componentes básicos y aplicados al desarrollo tecnológico innovador, asociados a la actualización y mejoramiento de la calidad de la educación formal y no formal.
8. Fortalecer el desarrollo regional a través de los Consejos Departamentales de Ciencia, Tecnología e Innovación y políticas integrales, novedosas y de alto impacto positivo para la descentralización de las actividades científicas, tecnológicas y de innovación, integrado a las dinámicas internacionales.
9. Definir y alinear los procesos para el establecimiento de prioridades, asignación, articulación y optimización de recursos de toda clase para la ciencia, la tecnología, la innovación y el resultado de estos, como son el emprendimiento y la competitividad.
11. Promover y fortalecer la investigación intercultural, en concertación con los pueblos indígenas sus autoridades y sabedores, destinado a proteger la diversidad cultural, la biodiversidad, el conocimiento tradicional y los recursos genéticos.

La ley 1286 de 2009, establece en los numerales 5, 6, 7, 9, 11,16 y 22 del artículo 7. *Funciones. El Departamento Administrativo de Ciencia, Tecnología e Innovación - Colciencias, tendrá a su cargo, además de las funciones generales que prevé la Ley 489 de 1998, las siguientes:*

5. Promover el desarrollo científico, tecnológico y la innovación en el país, de acuerdo con los planes de desarrollo y las orientaciones trazadas por el Gobierno Nacional.
6. Propiciar las condiciones necesarias para que los desarrollos científicos, tecnológicos e innovadores, se relacionen con los sectores social y productivo, y favorezcan la productividad, la competitividad, el emprendimiento, el empleo y el mejoramiento de las condiciones de vida de los ciudadanos.
7. Velar por la consolidación, fortalecimiento y articulación del Sistema Nacional de Ciencia, Tecnología e Innovación -SNCTI- con las entidades y actores del sistema, en estrecha coordinación con el Sistema Nacional de Competitividad.
9. Fomentar la creación y el fortalecimiento de instancias e instrumentos financieros y administrativos de gestión para la Ciencia, Tecnología e Innovación.
11. Promover la inversión a corto, mediano y largo plazo, para la investigación, el desarrollo científico, tecnológico y la innovación.

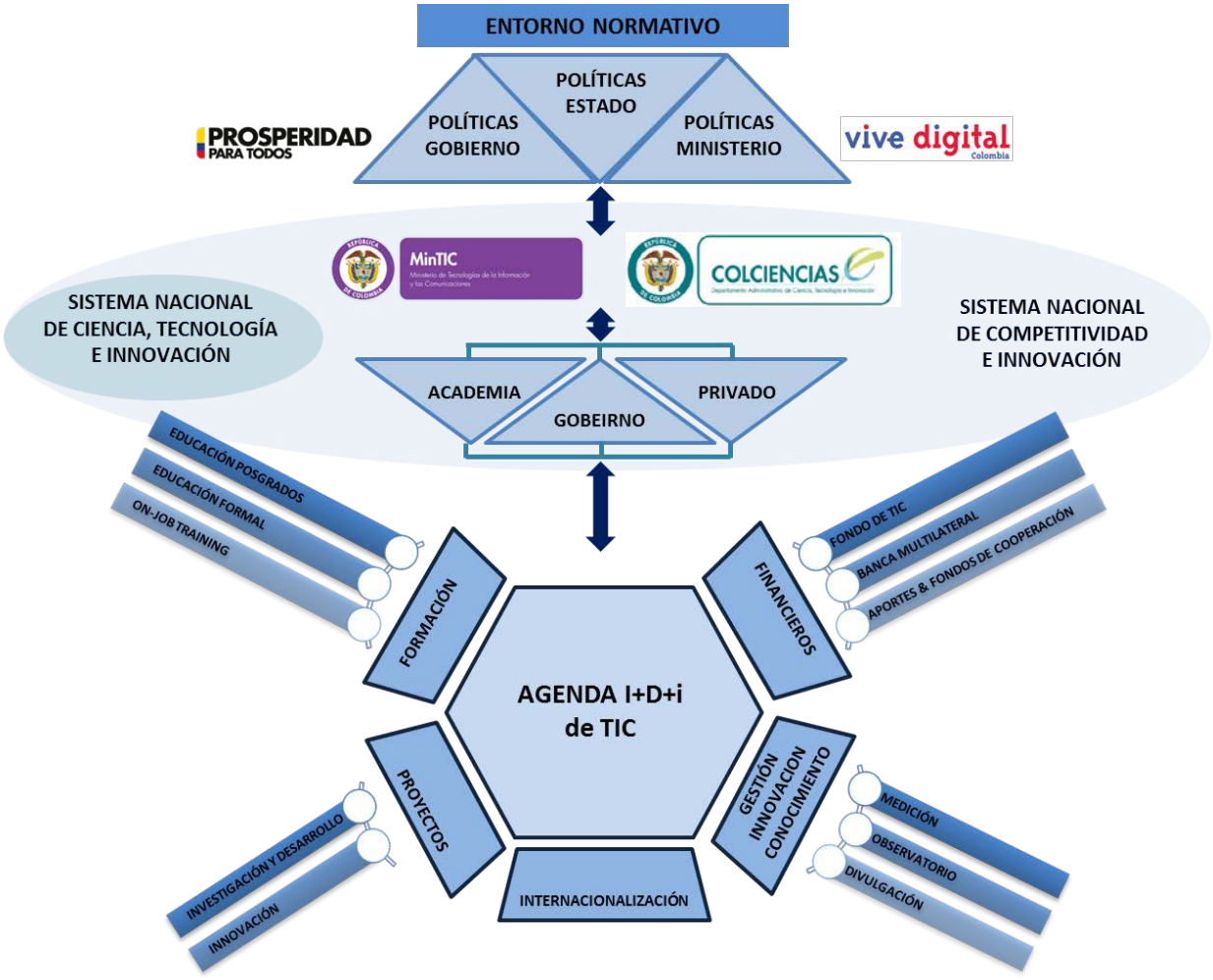
16. Definir prioridades y criterios para la asignación del gasto público en ciencia, tecnología e innovación, los cuales incluirán áreas estratégicas y programas específicos y prioritarios a los que se les deberá otorgar especial atención y apoyo presupuestal.

22. Crear las condiciones para desarrollar y aprovechar el talento nacional, en el país y en el exterior en el campo de ciencia, tecnología e innovación.

2. DEFINICIONES

SUBSISTEMA DE INNOVACIÓN

El Subsistema de Innovación hace parte del Sistema de Investigación, Desarrollo e Innovación (I+D+i) de TIC impulsado por el Ministerio de TIC y COLCIENCIAS, creado para definir una agenda nacional de I+D+i con el fin de fomentar el desarrollo de la Industria TIC y contribuir al desarrollo económico, social y político del país.



Gracias a estas entidades se llevan a cabo los Nodos de Innovación NDI, los cuales buscan congregar colaborativamente a la Industria, la Academia y al Gobierno con el fin de promover soluciones innovadoras que a largo plazo logren convertirse en un referente internacional de innovación, gestión de conocimiento e innovación abierta.

Los nodos de innovación son el elemento fundamental de conformación del sistema de innovación; configuran un punto de encuentro entre la industria, la academia y el gobierno en torno a un tema específico; actúan como puente entre la oferta y la demanda de soluciones de TIC en el ámbito del Gobierno, por medio de la promoción de proyectos innovadores y de alto impacto; crean un modelo de gobernanza replicable que proporciona una estructura de gestión clara.

A través de estos nodos se busca promover el uso y apropiación de TIC, fomentando el oportuno desarrollo de la Industria TI en Colombia y fortaleciendo en gran medida la estrategia Gobierno en línea GEL, lo cual trae consigo grandes beneficios para el desarrollo económico, social y político del país.

Las principales temáticas que abordan estos nodos de innovación son:

- Arquitectura TI para el Gobierno
- Ciberseguridad
- Justicia
- Servicios al Ciudadano
- Salud
- Ciudades Inteligentes
- Big Data Analytics

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 2 - TEMÁTICAS DE LA CONVOCATORIA

AGENDA ESTRATÉGICA DE INNOVACIÓN CIBERSEGURIDAD

1. **CIBERSEGURIDAD**

2. **VECTORES DE DESARROLLO DEL NODO**

   2.1. Principios rectores de ciberseguridad
   2.2. Educación, formación y divulgación en ciberseguridad
   2.3. Gestión integrada de riesgos e incidentes de naturaleza cibernética
   2.4. Identificación, autenticación y autorización
   2.5. Aseguramiento de aplicaciones y ambientes móviles en el gobierno
   2.6. Tecnologías de la Información y las Comunicaciones para el sector defensa

***

1. CIBERSEGURIDAD

Las Tecnologías de la Información y las Comunicaciones, por su característica transversal, se han convertido en el principal vehículo de la sociedad de la información, el soporte fundamental de las estructuras organizacionales y uno de los elementos angulares dentro de las actividades principales de todos los sectores económicos del país. Esta posición ha convertido a las TIC en un activo estratégico dentro de las políticas nacionales e internacionales, y por tal motivo ha hecho visible la necesidad de establecer mecanismos que permitan controlar el uso adecuado de este activo, pues su afectación tendría un serio impacto social, político y económico.

Las Tecnologías de la Información y las Comunicaciones se han involucrado en todos los eslabones de la sociedad moderna, desde las organizaciones públicas y privadas, que cada día se esfuerzan más por incorporar TIC en sus procesos buscando así impulsar la optimización de tiempos y de recursos, la reducción de costos y la agilización en sus procesos; hasta el ciudadano, a través de la computación móvil, los teléfonos inteligentes, las iniciativas nacionales para facilitar el acceso a computadores y conectividad de internet, y la creciente dependencia a la tecnología. Este nuevo esquema ha configurado una sociedad donde la información es el activo principal, donde el concepto de

ciberespacio ha adquirido dimensiones estratégicas, y donde el cuidado de recursos y activos informáticos se ha vuelto un foco fundamental.

La información, apalancada por la velocidad, la capacidad y el acceso que brindan las TIC se ha visto enfrentada a un nuevo panorama de riesgos, donde las amenazas son ahora de naturaleza cibernética, donde los intangibles son críticos para el funcionamiento de las organizaciones y la sociedad en general, y donde los impactos de la materialización de los riesgos siguen siendo reales. Este esquema ha demostrado que los estados requieren plantear estrategias e iniciativas que minimicen la posibilidad de que estos nuevos riesgos se hagan efectivos, que eviten que los ciudadanos, los sectores productivos y el Estado en general se vean afectados, y que con ésto se altere la forma de organización social, económica, política soberana y coercitiva del país.

Para ésto, Colombia ha empezado a plantear una visión rectora consolidada en el documento CONPES 3701, el cual busca generar los lineamientos nacionales de política en ciberseguridad orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. En este marco de referencia se define la ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado y a la ciudadanía en general ante estas nuevas amenazas. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países y Colombia no es la excepción, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado incluyendo a la sociedad civil.

En este contexto, la política criminal, definida por la Corte Constitucional Colombiana en varios pronunciamientos, en especial, aquel contenido en la sentencia C-936-10, la misma es entendida como *"el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción"*. La jurisprudencia constitucional ha reconocido así mismo que la política criminal puede ser articulada por el Legislador a través de la expedición de normas. En este sentido indicó que: *"la legislación penal es manifestación concreta de la política criminal del Estado"*, y que *"la decisión política que determina los objetivos del sistema penal y la adecuada aplicación de los medios legales para luchar contra el crimen y alcanzar los mejores resultados, se plasma en el texto de la ley penal"*.

Así mismo, se precisó que *"la norma penal, una vez promulgada, se independiza de la decisión política que le da origen, conservando la finalidad buscada por su redactor en el elemento teleológico de la norma"*; lo que cobra especial significación, a efectos de alinearse con las políticas públicas de ciberseguridad con miras a reducir, prever y remediar la vulneración a los derechos constitucionales y legales comprometidos por el uso ilegítimo de las Tecnologías de la Información y las Comunicaciones.

Los vectores de desarrollo que aquí se presentan corresponden a directrices marco que se han identificado como prioritarias para Colombia, orientadas a fortalecer la posición del país en términos de ciberseguridad, alineados con las diferentes estrategias y normativas nacionales provenientes desde las entidades del Estado y del sector privado, y que con su fortalecimiento conlleven a mejorar la posición estratégica del país en estos temas. Cada uno de estos vectores está compuesto por líneas temáticas, las que detallan los temas específicos en los cuales se debe enfocar los esfuerzos de innovación en el país.

2. VECTORES DE DESARROLLO

A continuación se presentan los vectores de desarrollo que enmarcan las actividades de innovación alrededor de la temática de ciberseguridad.

2.1 Principios rectores de ciberseguridad

Diferentes países alrededor del mundo han establecido como una de sus estrategias fundamentales el planteamiento de alternativas metodológicas desarrolladas en términos de políticas, normas, procedimientos, estándares y de la definición de niveles específicos de referencia en términos de ciberseguridad que se encuentren alineados con las diferentes estrategias nacionales, con los desarrollos normativos particulares y con las directrices planteadas a través de Ministerios, Unidades Administrativas y Programas nacionales, así como también con legislación internacional, con directrices dadas por los organismos de normalización y estandarización y con políticas establecidas por las diferentes asociaciones internacionales, todo con el fin de fortalecer la posición estratégica del estado en el ciberespacio y enfrentar de manera adecuada los riesgos de naturaleza cibernética a los que se ve expuesto.

El objetivo principal de esta estrategia es orientar todos los esfuerzos nacionales, desde un enfoque estratégico, para fortalecer la posición de estos países en términos de aseguramiento de su infraestructura crítica, de protección de los servicios que proveen a sus ciudadanos y de todos los sistemas y activos sobre los que soportan la operación de las entidades del estado, así como también el establecimiento de una ventaja competitiva en términos de defensa estratégica del ciberespacio y de las Tecnologías de la Información y las Comunicaciones con las que se soportan todas las actividades y procesos del estado. Este planteamiento estratégico se materializa, de manera particular, mediante la creación de guías rectoras, a nivel de regulación y legislación, que especifican de forma puntual y detallada las medidas requeridas para aumentar la seguridad de los sistemas y activos de información que se manejan en los respectivos gobiernos, las cuales deben ser estructuradas de manera conjunta por los diferentes actores de la sociedad para garantizar así su viabilidad y su factibilidad tecnológica, ajustada y alineada con la realidad tecnológica del estado particular de implementación, así como también su pertinencia política y social.

Ante este entorno, se plantea un escenario en el que es posible y necesario complementar y fortalecer el trabajo que se ha empezado a elaborar en Colombia, especialmente el realizado por el Ministerio de Tecnologías de la Información y las

Comunicaciones a través del Programa Gobierno en línea, que ha avanzado enormemente en términos de políticas, procedimientos, controles y recomendaciones técnicas para el fortalecimiento de la ciberseguridad del estado, buscando así cerrar la brecha existente en términos de políticas de prevención, de control y de reacción ante el incremento constante de amenazas informáticas, la ausencia de guías tecnológicas específicas y la heterogeneidad de medidas que se buscan aplicar a las instituciones del Estado colombiano.

De esta forma, es necesario que los diferentes actores de la sociedad, la academia, la empresa y el gobierno, orienten esfuerzos a la generación de proyectos, iniciativas y planteamientos innovadores de política y normatividad pública enfocados en fortalecer la posición del país en términos de gestión de seguridad de la información, definición y aseguramiento de infraestructura crítica, el mantenimiento de ambientes seguros, el aseguramiento de sistemas y la definición de niveles mínimos suficientes para controlar los riesgos y amenazas de naturaleza cibernética, así como las medidas estratégicas para la gestión de la ciberseguridad, y la configuración de un entorno político adecuado para la implementación de medidas para asegurar al Estado en el ciberespacio, pues es necesario apalancar estas nuevas necesidades desde el punto de vista legislativo, donde los mecanismos de control y de vigilancia son fundamentales para garantizar la estabilidad de las instituciones y la consecución de los objetivos estratégicos del estado, potenciando así la transparencia, la oportunidad, y la optimización de recursos.

Las innovaciones en este vector de desarrollo se deben enmarcar en una o varias de las siguientes líneas temáticas:

A. Generación de políticas, directrices, normas, actos administrativos y otras formas jurídicas que dictaminen las formas, tanto tecnológicas como procedimentales, de llevar a cabo el intercambio de información entre las diferentes entidades del estado, entre el gobierno y los diferentes sectores productivos del país y entre la ciudadanía en general, bajo esquemas que garanticen la integridad, la confidencialidad y la disponibilidad de la información.

B. Generación de políticas, normas, actos administrativos, procedimientos legislativos y otras figuras jurídicas orientadas a fortalecer las capacidades y la organización del Estado colombiano para proteger al ciberespacio de amenazas que atenten contra la soberanía nacional y los principios constitucionales.

C. Incorporación de los delitos cibernéticos como elemento fundamental de las políticas, normas, actos administrativos y otras figuras jurídicas, con el fin de fortalecer al Estado en su capacidad para identificar, reconocer y juzgar de manera adecuada estos elementos en los procesos jurídicos, constitucionales, penales, etc., definiendo también los alcances, los niveles de gravedad, las penalidades y los procedimientos necesarios ante la ocurrencia de los mismos.

D. Generación de directrices de protección de la confidencialidad, integridad y disponibilidad de los datos del Estado colombiano durante el ciclo de vida de los mismos, a través de la definición, adopción, ajuste, actualización, incorporación, implementación y valoración de esquemas tecnológicos y procedimentales específicos.

E. Dimensionamiento de políticas de seguridad de la información y ciberseguridad para la incorporación de software en las entidades del Estado, así como para su gestión, dirección, monitoreo, mantenimiento y control, considerando esquemas técnicos, procedimentales, metodológicos y de política nacional.

F. Generación de políticas, normas, actos administrativos, procedimientos legislativos y otras figuras jurídicas orientadas a fortalecer las alianzas y los acuerdos de cooperación y colaboración internacionales de lucha contra amenazas y delitos de naturaleza cibernética, así como aquellos orientados a fortalecer la defensa nacional en el ciberespacio.

G. Estructuración de circulares, políticas, normas, actos administrativos y otras figuras enfocadas a fortalecer las capacidades del estado para garantizar la adecuada identificación/autenticación, autorización de los ciudadanos colombianos, así como protección de la identidad de los mismos.

Es importante resaltar que todos los elementos de innovación deben considerar en su estructuración los resultados que surjan desde las entidades que tienen obligaciones específicas en términos de ciberseguridad según lo definido en el CONPES 3701, tales como los resultados de las iniciativas planteadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, el Ministerio de Relaciones Exteriores, la Fiscalía General de la Nación y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, entre otros.

2.2 Educación, formación y divulgación en ciberseguridad

Uno de los factores fundamentales para garantizar un adecuado conocimiento y desenvolvimiento de los funcionarios públicos, y de la sociedad en general, en temas relacionados con ciberseguridad, radica en la educación y formación de calidad y de alto nivel del recurso humano quien, como ente activo que produce, consume y transforma información, se configura como el eslabón más débil de la cadena de seguridad de la información del Estado. Esta situación se convierte en la razón fundamental para impulsar estrategias orientadas a generar una conciencia de la responsabilidad y una obligación específica de salvaguardar la información como activo fundamental en la sociedad del conocimiento.

Esta nueva responsabilidad recae ante cualquier individuo que forma parte del recurso humano de una institución, que recibe los recursos técnicos y de información, como insumo indispensable para la ejecución de sus funciones laborales, bien sean misionales, de apoyo o estratégicas y que, independiente a la profesión, cargo, funciones o tiempo de servicios prestados a la institución, debe responder con ética y principios sobre la integridad, veracidad, confidencialidad y disponibilidad de la información, así como del uso que se le da a la misma. Es por ésto que se vuelve fundamental poner a disposición de la comunidad en general, las herramientas metodológicas y conceptuales que permitan una preparación cognitiva y psicológica para responder apropiadamente ante un incidente de naturaleza cibernética que ponga en riesgo la información del estado en general, y del ciudadano en particular.

Alrededor del mundo se han generado múltiples iniciativas en este sentido, formalizando los esquemas educativos a través de certificaciones con reconocimiento internacional, programas educativos técnicos y tecnológicos, y programas profesionales de pregrado y posgrado. Esto impulsado por la creciente necesidad de contar con personal altamente capacitado y calificado en temas de ciberseguridad que tengan las capacidades suficientes para afrontar todo el conjunto de nuevos retos que se presentan ante la sociedad de la información, donde el ciberespacio y las tecnologías digitales se convierten en las nuevas herramientas de trabajo, configurando una sociedad totalmente dependiente de las Tecnologías de la Información y las Comunicaciones, situación que cambia radicalmente el panorama habitual de riesgos. Así mismo, este nuevo esquema implica un esfuerzo en realizar actividades de divulgación sobre los avances y oportunidades que se presentan a lo largo de la cadena de valor de la ciberseguridad, el cual debe estar enfocado a todos los sectores de la sociedad.

En este sentido, es necesario establecer estrategias de amplio espectro y profundo impacto con el fin de alinear a los funcionarios públicos y a la sociedad en general ante este nuevo entorno, en el cual la información se convierte en el activo más importante y donde es necesario tomar medidas de protección y de control que no son necesarias en otros ámbitos. Iniciativas que permitan la dinamización de los espacios de estructuración, coordinación y establecimiento de “think tanks”, grupos de discusión y equipos de trabajo orientados a temáticas específicas de seguridad de la información y ciberseguridad..

Teniendo en cuenta esta nueva complejidad, se vuelve imperativo establecer proyectos de innovación en las siguientes líneas temáticas:

A. Establecimiento, estructuración, diseño e implementación de programas de formación técnica, tecnológica y profesional de alto nivel y de calidad internacional, pensum académicos y syllabus curriculares en temas técnicos y legales de seguridad de la información y ciberseguridad.
B. Definición, adopción, estructuración, implementación y prueba de esquemas metodológicos, pedagógicos y educativos de buenas prácticas en seguridad de la información para las entidades del estado y con las que estas interactúen, así como de modelos de enseñanza e incorporación de conocimiento, competencias y habilidades en seguridad de la información y ciberseguridad.
C. Análisis, diseño, estructuración, implementación y evaluación de estrategias de sensibilización y apropiación orientadas a la comunidad en general, por sectores políticos, socioeconómicos, culturales y educativos.

Es importante resaltar que todos los elementos de innovación que se planteen a través de estas líneas temáticas deben considerar los resultados de las estrategias y políticas definidas por el Ministerio de Educación Nacional y del Programa Gobierno en línea.

2.3 Gestión integrada de riesgos e incidentes de naturaleza cibernética

Un elemento fundamental para la adecuada aproximación hacia un Estado con niveles apropiados de ciberseguridad requiere un enfoque estructurado para la gestión y el manejo de los riesgos y amenazas asociadas a los sistemas y activos de información de todas las entidades, por esta razón se ha observado la necesidad de establecer procesos formales que permitan mantener un panorama continuo de la seguridad de la información,

de las amenazas y vulnerabilidades, y de los diferentes elementos de naturaleza cibernética que interactúan dentro de las entidades y entre ellas, con el fin de agilizar el proceso de toma de decisiones para la gestión de los riesgos y de incidentes.

En Colombia se han establecido los lineamientos básicos para el establecimiento organizativo de la respuesta del Estado ante los riesgos e incidentes de naturaleza cibernética, lo que ha puesto a consideración la necesidad de contar con esquemas, modelos, procesos y herramientas que permitan la captura de datos, el análisis, el transporte y la respuesta, de manera integrada, ante este tipo de situaciones. Esto ha impulsado la necesidad de que en el país se realicen procesos de innovación orientados a la generación de soluciones en Tecnologías de la Información y las Comunicaciones que estén en capacidad de buscar, identificar, estructurar, analizar, recuperar, correlacionar y/o integrar datos relacionados con las incidencias de naturaleza cibernética, que se presenten a los largo del país, en las regiones, o en entidades particulares, fomentando la interoperabilidad y el intercambio de datos a través de esquemas desagregados, que le brinden al país en general y a las entidades en particular la capacidad de responder, prevenir y evitar estos eventos y mantener un efecto disuasivo estratégico.

En este orden de ideas, se hace necesario plantear estrategias nacionales concertadas en torno a las dificultades y necesidades expeditas en términos de ciberseguridad, en las cuales se deberán trabajar de manera complementaria la estructuración y puesta en marcha de esquemas tecnológicos de gestión continua que permitan detectar y tratar apropiadamente los riesgos de ciberseguridad, y el establecimiento e implementación de arquitecturas de seguridad que faciliten los procesos de estandarización y medición de los niveles de riesgos y de incidentes, de forma tal que se pueda brindar un cuadro generalizado de indicadores, que sean comparables entre las diferentes entidades, que se puedan estructurar mediante estrategias de federación, y que permitan identificar de manera adecuada la situación nacional en términos de riesgos e incidentes de naturaleza cibernética, brindando un enfoque común entre los diferentes actores nacionales, independientemente de su sector, tamaño o responsabilidades específicas.

Para responder a los retos modernos, teniendo en cuenta la complejidad tecnológica asociada y la gran variedad de entidades que conforman al estado colombiano, se estructuran las siguientes líneas temáticas:

A. Estructuración, diseño, desarrollo e implementación de modelos distribuidos (federados) para la medición (preferiblemente automatizada, continua y en tiempo real) de los mapas de riesgos, amenazas y vulnerabilidades existentes en los sistemas de información del gobierno, para entidades individuales y que permitan la medición comparable por grupos de entidades (por ejemplo, sectores productivos), facilitando la toma de decisiones en cuanto a prevención, protección y detección temprana de incidentes.

B. Estructuración, diseño, desarrollo e implementación de modelos para la gestión federada de incidentes, orientadas al diseño, adaptación, desarrollo, establecimiento y puesta en funcionamiento de sistemas integrados que permitan monitorear, detectar, prevenir, informar, responder, alertar de manera temprana y tratar de forma apropiada incidentes de naturaleza cibernética.

C. Estructuración e implementación de modelos, tecnologías y controles operativos para el uso de activos críticos y de recursos tecnológicos del estado colombiano, así como

para la incorporación de nuevos recursos y la disposición de aquellos que salen de servicio, con el fin de minimizar riesgos asociados al transporte, procesamiento y almacenamiento de información crítica.

D. Estructuración y definición de esquemas tecnológicos y metodológicos de modelado y simulación de riesgos cibernéticos que permitan identificar de manera temprana los riesgos de naturaleza cibernética a las que está expuesto el estado colombiano, y que le brinden al estado la capacidad preventiva y reactiva ante incidentes.

E. Definición, adopción, estructuración, coordinación, formación, entrenamiento, conformación e implementación de centros y equipos de respuesta a incidentes, tanto a nivel nacional como a nivel regional y local, por sectores económicos, que estén en articulación con las iniciativas y esfuerzos planteados desde el ColCERT y el CSIRT de Colombia.

Es importante resaltar que todos los elementos de innovación que surjan en torno a estas líneas temáticas deben considerar en su estructuración los resultados de las estrategias y políticas definidas en términos de gestión de riesgos por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT.

2.4 Identificación, autenticación y autorización

El estado colombiano ha establecido múltiples iniciativas tendientes a unificar los mecanismos de identificación de la ciudadanía colombiana, incorporando así dentro del proceso tecnología de punta para tal fin, sin embargo, todos estos esfuerzos aún no han sido suficientes para garantizar que el estado cuente con mecanismos generalizados, estandarizados, robustos y homogéneos que le permita llevar un registro sobre sus ciudadanos, en aras de proteger sus derechos y libertades constitucionales, de manera transversal a todas las entidades, instituciones y empresas. Esta situación se ve también reflejada en la aparición de esquemas individualizados de identificación en el sector privado, generando así re-procesos y cargas administrativas adicionales, que se podrían minimizar mediante la innovación en modelos, esquemas, mecanismos, herramientas y sistemas que permitan una gestión unificada de la identidad de los ciudadanos colombianos, en términos de autorización y autenticación.

Con el fin de dar respuesta a esta situación, es necesario plantear esquemas innovadores orientados sobre las siguientes líneas temáticas:

A. Definición y estructuración de modelos, esquemas técnicos, procedimentales y metodológicos para la identificación/autenticación ciudadana, los cuales permitan la gestión integrada de identidad para el acceso a servicios, en particular aquellos servicios que se prestan por internet y para la protección de identidad, con base en modelos y experiencias exitosas registradas en otros países.

B. El establecimiento, diseño, estructuración, incorporación, implementación y valoración de esquemas tecnológicos y procedimentales para garantizar la identificación, autenticación y autorización de funcionarios, ciudadanos, activos de información y recursos que acceden a la infraestructura del estado colombiano, mediante la generación de modelos y esquemas de autenticación de múltiple factor.

Así mismo, es necesario que estos esquemas contemplen las iniciativas presentadas por la Registraduría Nacional del Estado Civil, por el Programa Gobierno en línea y aquellas iniciativas puntuales de identificación y registro planteados por los organismos de seguridad del Estado.

2.5 Aseguramiento de aplicaciones y ambientes móviles en el gobierno

Uno de los sectores de mayor dinámica en la economía global es el relacionado con el desarrollo de software y de aplicaciones móviles, el cual, dado el auge de dispositivos electrónicos, la masificación del acceso a internet y la capacidad resultante que brinda el ciberespacio para comunicarse a través de las redes de datos y de compartir información en tiempo real (característica propia de la actual sociedad del conocimiento), se ha convertido en uno de los sectores más críticos y delicados dentro del ecosistema de la ciberseguridad, lo que lo ha llevado a ser un sector pionero, con inversiones considerables, con una proyección acelerada y que genera un mayor interés por parte de la población en general, de los actores políticos y de los organismos de seguridad y defensa del estado.

Este sector, en los últimos años, se ha caracterizado por brindar el soporte fundamental para que las personas interactúen y disfruten de las ventajas presentadas por las Tecnologías de la Información y las Comunicaciones, configurando espacios en los cuales puedan interactuar con sus semejantes o con las entidades del gobierno, permitiéndole hacer uso de los servicios que éstas ponen a disposición de la ciudadanía, y fortaleciendo los resultados de iniciativas como las establecidas por el Programa Gobierno en línea.

Esta situación ha tenido un éxito tal que ha permeado todas las capas de la sociedad, sumergiéndola en toda una plataforma tecnológica con innumerables posibilidades. Esta plataforma, sin embargo, también representa un reto adicional en términos tecnológicos y de gobierno, en la cual se hace necesario establecer y definir un conjunto de responsabilidades adicionales en torno a la necesidad de proteger los datos, la información y los dispositivos que interactúan dentro de este nuevo esquema, para así brindar confianza en el uso de los nuevos servicios, y poder facilitar la interacción entre los ciudadanos y de éstos con el gobierno en general.

De esta forma, para garantizar que todo este conjunto de nuevas interacciones se realicen de manera segura, siguiendo directrices apalancadas en la protección a la ciudadanía y manteniendo el estado dentro de los límites establecidos de ciberseguridad, se hace necesario establecer esquemas innovadores en las siguientes líneas temáticas:

A. Definición, adopción, ajuste, actualización, incorporación, implementación y valoración de modelos de desarrollo de software in-house orientados a suplir las necesidades de seguridad de información en las entidades colombianas, que estén apalancados en estándares internacionales y que se ajusten a las mejores prácticas internacionales en la materia.
B. Definición, adopción, estructuración e implementación de metodologías estándar unificadas, ajustadas al entorno colombiano, para el aseguramiento de la información y del software en los dispositivos móviles que están en uso en las entidades del estado y para aquellos que estén próximos a adquirirse.

C. Definición, adopción, estructuración e implementación de metodologías, procedimientos y estrategias generales para el control de acceso a la información y a contenidos en las entidades del estado y en sectores específicos (p.ej. el sector educativo), los cuales se deben articular desde todas las etapas del ciclo de desarrollo de software y de tecnología específicos.

D. Establecimiento, estructuración, diseño e implementación de modelos, esquemas tecnológicos, procedimentales y metodológicos para el aseguramiento de la información en las diferentes etapas de los ciclos de desarrollo de aplicaciones que son utilizadas en las instalaciones de gobierno, para prestar servicios a la ciudadanía, al gobierno mismo y al sector privado, o que sean de misión crítica.

E. Establecimiento, estructuración, diseño e implementación de modelos, esquemas y soluciones tecnológicos, procedimentales y metodológicos para el aseguramiento de la infraestructura tecnológica que presta servicios a la ciudadanía y utilizada por la población general (cibercafés, cafés internet, telecentros, salas públicas, etc.) que propendan por la oferta de servicios seguros de acceso a Internet.

Es importante resaltar que todos los elementos de innovación que surjan en torno a estas líneas temáticas deben considerar los resultados de las estrategias y políticas definidas en términos de desarrollo de aplicaciones por el Ministerio de Tecnologías de la Información y las Comunicaciones, por el Ministerio de Defensa Nacional, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT y los organismos de normalización y estandarización con reconocimiento en el ámbito colombiano.

2.6 Tecnologías de la Información y las Comunicaciones para el sector defensa

Sin prejuicio de las temáticas anteriormente mencionadas, se hace necesario fortalecer e impulsar programas, políticas, proyectos y desarrollos específicos dentro de las instituciones encargadas de mantener la seguridad y defender la soberanía del estado colombiano en el ciberespacio, con el fin de configurar una ventaja estratégica, operativa y tácticas sobre la inherente asimetría existente en cuanto a ciberseguridad.

Es de especial importancia el planteamiento de esquemas innovadores, tanto a nivel de tecnologías, como de metodologías y procedimientos que le permitan al estado anteponerse a los riesgos que surgen a diario en el ciberespacio, o que son inherentes al uso de Tecnologías de la Información y las Comunicaciones para apalancar las actividades realizadas por los organismos de seguridad del Estado y que, ante la materialización de riesgos, la explotación de vulnerabilidades o el aprovechamiento de debilidades, representan un elemento desestabilizante para la soberanía del estado, la seguridad de los ciudadanos, y los intereses del sector público y privado.

Dentro de este contexto es importante desarrollar iniciativas innovadoras en las siguientes líneas temáticas:

A. Definición y estructuración de esquemas tecnológicos y metodológicos para garantizarle al estado colombiano una ventaja táctica y estratégica en el ciberespacio, a partir de la identificación, perfilación, monitoreo y control de la infraestructura crítica del país, entendida esta como todos los elementos de infraestructura nacional que están expuestos a riesgos de naturaleza cibernética y que, ante la eventualidad de un

incidente pueden generar un impacto catastrófico en la política, economía, sociedad y soberanía del Estado colombiano.

B. La definición, adopción, ajuste, actualización, incorporación, implementación y valoración de tecnologías específicas de defensa y ataque cibernético que debería considerar el estado colombiano para fortalecer su posición en términos de ciberseguridad, para proteger su soberanía y para brindarle herramientas que le permitan cumplir con los deberes definidos constitucionalmente y salvaguardar los derechos de la ciudadanía.

C. Definición, estructuración y diseño de estudios sectoriales que le permitan al estado colombiano identificar de manera temprana las necesidades de innovación en temas de ciberseguridad, y que le permitan anteponerse a los riesgos, tendencias y problemáticas que estén surgiendo en esta materia.

Es claro que muchos de estos esquemas, dada su criticidad y su importancia a nivel estratégico para el estado colombiano, son de carácter confidencial y reservado.

ANEXO 3 - CARTA DE CONFORMACIÓN DE ALIANZA ESTRATÉGICA

A continuación se presentan los contenidos del modelo de carta de conformación de alianza estratégica:

(Ciudad), (Día) de (Mes) de 201_

Señores
COLCIENCIAS
Carrera 7B Bis No. 132 – 28
Bogotá D.C.

Asunto: Conformación de Alianza Estratégica (nombre de la alianza) para la convocatoria (nombre de la convocatoria) de 201_,

Respetados señores,

La presente tiene por objeto presentar la conformación de la Alianza Estratégica (nombre de la alianza), que estará integrada por las siguientes entidades: (nombre de la entidad 1, ejecutora), (nombre de la entidad 2 – empresa beneficiaria),…, etc.; designándose como entidad ejecutora a (nombre de la entidad ejecutora), quien será la encargada de firmar el contrato o convenio resultado de la convocatoria (nombre de la convocatoria) de 201 .

De igual forma, certifico que los grupos de investigación, desarrollo tecnológico y/o innovación que se relacionan a continuación serán los que desarrollarán el proyecto:

Entidad 1 - Ejecutora

Nombre de la entidad 1

Entidad 2 – Empresa beneficiaria

Nombre de la entidad 2

(tantas entidades, grupos de investigación, desarrollo tecnológico y/o innovación, o centros de desarrollo tecnológico y/o innovación como conformen la alianza estratégica……)

Así mismo, los abajo firmantes declaran que:

- Tienen poder y/o representación legal para firmar y presentar el proyecto.
- Este proyecto y el contrato o convenio que llegue a celebrarse en caso de financiación, compromete totalmente a la(s) persona(s) jurídica(s) que legalmente represento.
- La información suministrada es veraz y no fija condiciones artificiales.

- Aceptan y reconocen que cualquier omisión o inconsistencia en la que hayan podido incurrir y que pueda influir en nuestro proyecto, no les eximirá de la obligación de asumir las responsabilidades que les llegue a corresponder como futuros contratistas y renuncian a cualquier reclamación, reembolso o ajuste de cualquier naturaleza, por cualquier situación que surja y no haya sido contemplada en razón de la falta de diligencia en la obtención de la información.
- No se encuentran incursos en ninguna de las causales de inhabilidad y/o incompatibilidad establecidas en el Estatuto General de Contratación y demás normas legales pertinentes.
- Aceptan y autorizan a COLCIENCIAS para que verifique la información aportada en el proyecto.
- Se encuentran al día con las obligaciones y compromisos adquiridos con COLCIENCIAS.
- El proyecto no está siendo financiado por otra convocatoria o con recursos de COLCIENCIAS u otras entidades del Estado

Por otra parte y para el desarrollo de la propuesta las entidades que conforman la Alianza Estratégica aportaran los siguientes recursos de contrapartida, de acuerdo con lo establecido en el numeral 5 de la convocatoria:

Empresa Beneficiaria	Total	Tamaño de Empresa de acuerdo con lo establecido en la Ley 905 de 2004	Monto de contrapartida			
			Especie	% Especie	Efectivo	% Efectivo
Nombre de la empresa	$	XXXX	$	%	$	%
Nombre de la empresa	$	XXXX	$	%	$	%
Total	**$**		**$**	**%**	**$**	**%**

Además, **ACEPTAMOS** expresa e irrevocablemente que conocemos detalladamente las características, requisitos y condiciones de la convocatoria, de manera que nos sometemos a lo establecido en los Términos de Referencia determinados por COLCIENCIAS para el desarrollo de la misma y para la entrega del beneficio.

Con la presente manifestación inequívoca de voluntad, declaramos que en caso de ser beneficiados en la convocatoria, esté será recibido en los términos que COLCIENCIAS establezca; comprendemos y aceptamos que la no aceptación o el incumplimiento de alguna de las condiciones establecidas, dará lugar a la pérdida definitiva del beneficio.

Declaramos que la información suministrada es veraz y corresponde a la realidad. En caso de encontrarse alguna incoherencia o inconsistencia en la información o documentación suministrada, COLCIENCIAS podrá en cualquier momento, rechazar esta postulación o finiquitar el beneficio, sin perjuicio de las acciones legales correspondientes.

Cordialmente,

Firma
Nombre del representante legal entidad Ejecutora

CC_____
Nombre de la entidad Ejecutora
Dirección
Teléfono

Firma
Nombre del representante legal entidad x
CC_____
Nombre de la entidad Ejecutora
Dirección
Teléfono

Firma
Nombre del representante legal entidad x
CC_____
Nombre de la entidad Ejecutora
Dirección
Teléfono
Teléfono

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 4 – CARTA DE ACREDITACIÓN DE EMPRESAS BENEFICIARIAS

A continuación se presentan los contenidos del modelo de carta para certificación de la experiencia aportada por las empresas beneficiarias:

(Ciudad), (Día) de (Mes) de 201_

Señores
COLCIENCIAS
Carrera 7B Bis No. 132 – 28
Bogotá D.C.

Asunto: Certificación de la experiencia de (Nombre de la empresa)

Respetados señores,

Por medio de la presente yo NOMBRE DEL REPRESENTANTE LEGAL, identificado con cédula de ciudadanía número (Número de identificación), como Representante Legal de (Nombre de la empresa), certifico que la entidad mencionada cumple con los requisitos de experiencia mínima exigida en el marco de la convocatoria para conformar un banco de proyectos de desarrollo tecnológico e innovación elegibles en la temática de ciberseguridad para el fomento del uso y apropiación de TIC en el gobierno La experiencia es discriminada de la siguiente manera:

PROYECTO	DURACIÓN	TEMÁTICA	SOCIO-ALIADO-CONTRATISTA
XX	XX	XX	XX
XX	XX	XX	XX
TOTAL	XX		

Cordialmente,

FIRMA
NOMBRE DEL REPRESENTANTE LEGAL O PERSONA NATURAL
CC_____
Dirección – Teléfono

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 5 - REGLAMENTO PROPIEDAD INTELECTUAL

Con miras a contar con un marco de referencia para lograr un acuerdo en esta materia se adjunta una propuesta del Reglamento de Propiedad Intelectual al cual se deberían adherir los participantes de los Nodos Innovación.

INTRODUCCIÓN

En el contexto del Sistema de I+D+i de TIC planteado por el Ministerio de Tecnologías de la Información y las Comunicaciones se hace necesario adoptar una reglamentación clara y precisa que permita determinar los derechos sobre las creaciones intelectuales desarrolladas en su interior.

Al efecto, con base en los principios de la buena fe y la responsabilidad, se ha diseñado el presente reglamento, con el cual se pretende garantizar a los miembros de los Nodos de Innovación los derechos derivados de sus creaciones y aportes intelectuales, crear una cultura de respeto y establecer unos parámetros para el ejercicio de estos derechos que se extenderá a todas las personas que de una u otra manera participen.

A fin de lograr su objetivo primordial de fomento a la innovación, se busca proteger y facilitar la producción intelectual al interior de los nodos de investigación que lo integrarán. No obstante, se deja de presente que los generadores y autores de las creaciones que se generen serán los exclusivos responsables de la veracidad de los contenidos y alcance científico de las mismas, sin perjuicio de la obligación que les compete de respetar toda clase de derechos de terceros, entre ellos los de Propiedad Intelectual.

CAPÍTULO PRIMERO - PRINCIPIOS GENERALES

ARTICULO 1.- SUBORDINACIÓN: El presente reglamento se subordina a la Constitución Política y a las leyes vigentes. En su aplicación e interpretación se tendrán en cuenta las normas y convenios internacionales que regulan la Propiedad Intelectual en Colombia.

ARTÍCULO 2.- PREVALENCIA Y FAVORABILIDAD: En caso de conflicto entre este Reglamento y las normas especiales que regulan la Propiedad Intelectual en Colombia, prevalecerán estas últimas. En todo caso se dará prelación a aquella regulación más favorable para el autor y/o titular de los derechos, según los bienes intelectuales de que se trate, con fundamento en los principios generales previstos en la legislación vigente.

ARTÍCULO 3.- BUENA FE: Basado en el principio de la buena fe se presume que todas las creaciones intelectuales de sus integrantes son de su propia autoría, quienes en el desarrollo de sus actividades respetan los derechos de Propiedad Intelectual.

ARTÍCULO 4.- RESPONSABILIDAD E INDEMNIDAD: Los integrantes de los Nodos de Innovación son responsables de su producción intelectual y que ésta se lleve a cabo sin contravenir o afectar derechos de terceros, por ende, asumen el compromiso de mantener indemne al Sistema I+D+i de TIC de todo tipo de reclamaciones, demandas, denuncias, acciones, pérdidas, contingencias, daños, costos o gastos (incluyendo gastos legales), que se generen por contrariar las disposiciones contenidas en el presente Reglamento, o por actos u omisiones que las pongan en peligro o las afecten y de afrontar las indemnizaciones por daños y perjuicios que surjan de cualquier tipo de acción administrativa, civil o penal.

ARTÍCULO 5.- SANCIONES: El miembro del Nodo de Innovación que llegare a violar algún derecho de Propiedad Intelectual de un tercero será sujeto a las acciones civiles, penales y administrativas a que haya lugar ante la justicia ordinaria, de conformidad con las normas vigentes.

CAPÍTULO SEGUNDO - DE LA PROPIEDAD INTELECTUAL EN GENERAL

ARTÍCULO 6.- La expresión “propiedad intelectual” se utiliza en términos amplios para hacer referencia a todas las creaciones del ingenio humano, y se define como la disciplina jurídica que tiene por objeto la protección de bienes inmateriales, de naturaleza intelectual y de contenido creativo, así como de sus actividades conexas. Esta disciplina comprende básicamente dos áreas o ramas: la Propiedad Industrial y el Derecho de Autor.

La Propiedad Industrial protege principalmente las patentes y nuevas creaciones tales como: Patentes de Invención, Modelos de Utilidad, Diseños Industriales, Esquemas de Circuitos Integrados, y de otro lado, las marcas y otros signos distintivos entre los cuales se encuentran: marcas, lemas, nombres y enseñas comerciales, y denominaciones de origen.

El Derecho de Autor otorga protección a las creaciones expresadas a través de los géneros literario o artístico, tiene por objeto las creaciones o manifestaciones del espíritu expresadas de manera que puedan ser percibidas, y nace con la obra sin que para ello se requiera formalidad alguna.

CAPÍTULO TERCERO - DERECHOS DE AUTOR

ARTÍCULO 7.- Los derechos de autor recaen sobre las obras científicas literarias y artísticas, las cuales comprenden todas las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación.

La protección otorgada al autor tiene como título originario la creación intelectual concreta y materializada, ésto es la forma o medio por el cual las ideas del autor son descritas, explicadas o ilustradas, más no son objeto de protección las ideas, contenidos conceptuales, ideológicos o técnicos como tal.

ARTÍCULO 8.- Se entiende por Autor la persona natural que de manera efectiva realiza, materializa o concreta una creación, hecho que, en consecuencia, lo convierte en el titular originario de los siguientes derechos:

- **DERECHOS MORALES**: que consisten en el reconocimiento que hace la ley al autor sobre la paternidad de la obra realizada y el respeto a la integridad de la misma. Estos derechos tienen el carácter de perpetuos, inalienables, inembargables e irrenunciables y conceden a su titular las siguientes prerrogativas:

  - A reivindicar en todo tiempo la paternidad de su obra y en especial, para que se indique su nombre o seudónimo cuando se realice cualquiera de los actos mencionados en el artículo 12;
  - A oponerse a toda deformación, mutilación u otra modificación de la obra, cuando tales actos puedan causar o acusen perjuicio a su honor o a su reputación, o la obra se demerite y a pedir reparación por esto;
  - A conservar su obra inédita o anónima hasta su fallecimiento, o después de él cuando así lo ordenase por disposición testamentaria;
  - A modificarla, antes o después de su publicación;
  - A retirarla de la circulación o suspender cualquier forma de utilización aunque ella hubiere sido previamente autorizada.

- **DERECHOS PATRIMONIALES:** que consisten en la facultad que tiene el autor o sus derechohabientes de aprovechar y disponer económicamente de una obra publicada, por un tiempo determinado.

  Estos derechos son transferibles a título gratuito u oneroso, o bien por virtud de la ley pueden ser detentados por personas diferentes del autor, como sucede en el caso de obras realizadas en desarrollo de un contrato de trabajo o de un contrato de prestación de servicios.

  El autor de una obra protegida tendrá el derecho exclusivo de realizar o de autorizar uno cualquier de los actos siguientes:

  - La edición, o cualquier otra forma de reproducción;
  - La traducción, arreglo o cualquier otra forma de adaptación;
  - La inclusión en película cinematográfica, videograma, cinta video, fonograma, o cualquier otra forma de fijación, y
  - La comunicación al público, por cualquier procedimiento o medios tales como, la ejecución, representación, recitación o declamación; la radiodifusión sonora o audiovisual; la difusión por parlantes, telefonía con o sin cables, o mediante el uso de fonógrafos, equipos de sonido o grabación y aparatos análogos, y la utilización pública por cualquier otro medio de comunicación o reproducción, conocido o por conocerse.

Las distintas formas de utilización de la obra, son independientes entre ellas; la autorización del autor para una forma de utilización no se extiende a las demás.

ARTÍCULO 9.- Los derechos y prerrogativas de los derechos morales sobre una obra corresponden al autor o coautores de la misma, así:

- **TITULAR EN OBRA INDIVIDUAL**: El titular originario del derecho de autor es el creador de la obra, condición que le permite conservar los derechos morales, aun cuando haya cedido total o parcialmente los derechos patrimoniales sobre la obra.

- **TITULAR EN OBRA EN COLABORACIÓN**: En las creaciones realizadas conjuntamente por dos o más personas naturales cuyos aportes no puedan ser separados o individualizados, la titularidad pertenece en común a todos los coautores.

- **TITULAR EN OBRA COLECTIVA**: En las obras producidas por un grupo de autores, por iniciativa y bajo la orientación de una persona natural o jurídica que la coordine, divulgue y publique bajo su nombre, el titular de los derechos de autor será el editor o persona jurídica o natural por cuya cuenta y riesgo se realizan los aportes de las personas naturales que contribuyen a la obra colectiva.

- **TITULAR EN OBRAS DERIVADAS**: El traductor y el adaptador son dos categorías de titulares originarios.

  La Ley le concede al traductor derechos como titular originario sobre su traducción, por razón de la expresión propia plasmada en la traducción, siempre y cuando para realizar la traducción haya contado con la autorización del autor o titular de los derechos sobre la obra. En todo caso se deberá mencionar al autor y el título de la obra originaria.

  Asimismo, la adaptación de una obra realizada con la autorización previa y expresa del autor o titular de los derechos, concede al adaptador derechos sobre su aporte creativo.

Todo lo anterior se enmarca a lo establecido en el artículo 8 de la ley 23 de 1982, modificada por artículo 2 de la ley 1520 del 2012.

ARTÍCULO 10.- Los derechos y prerrogativas de los derechos patrimoniales sobre una obra pertenecen al autor o a sus cesionarios, así:

1. Al titular de los derechos de autor, acorde con la clasificación prevista en el artículo anterior, que no haya transferido los derechos patrimoniales, en virtud de algún acto de disposición legal o contractual.
2. Al cesionario de los derechos patrimoniales, ésto es, las personas que adquieren la titularidad en virtud de un acto jurídico por el cual el autor o el titular transfiere los derechos patrimoniales sobre la obra, entre otros por:

   - Cesión total o parcial de derechos patrimoniales por acto entre vivos
   - Legados y/o herencias
   - Desarrollo de contratos laborales o de prestación de servicios

ARTÍCULO 11.- A fin de no vulnerar los derechos de autor de una obra o producción protegida, para su utilización deberá contarse con la autorización previa y expresa del titular de los derechos.

Sin perjuicio de lo anterior, se podrá actuar sin autorización del autor en los casos legalmente autorizados, tales como, el Derecho de Cita, la Ilustración para la Enseñanza, etc., siempre y cuando se observen los requisitos que para cada caso de excepción consagra la ley.

CAPÍTULO CUARTO - PROPIEDAD INDUSTRIAL

ARTÍCULO 12-. La Propiedad Industrial protege los derechos derivados de creaciones invenciones que tienen una finalidad industrial o comercial definida, los signos distintivos de productos o servicios, al igual que la represión de la competencia desleal.

ARTÍCULO 13.-. Los derechos de Propiedad Industrial otorgan a sus titulares el derecho exclusivo a la explotación del bien por ella protegido, a través de un registro o un reconocimiento administrativo de la autoridad competente. En algunos casos específicos los derechos se adquieren con el solo uso.

ARTÍCULO 14. La ley define los bienes objeto de protección, y atendiendo al tipo de bien, establece los requisitos y procedimientos para acceder a la misma, a saber:

Las creaciones industriales se protegen a través de patentes de invención, patentes de modelo de utilidad, diseños y secretos industriales.

Por su parte, los signos distintivos de productos y servicios se protegen a través del registro de marcas, lemas, nombres y enseñas comerciales, indicaciones geográficas (denominación de origen, etc.)

CAPÍTULO QUINTO - LA PROPIEDAD INTELECTUAL EN EL ÁMBITO DE LOS NODOS DE INNOVACIÓN PARA EL USO Y APROPIACIÓN DE TIC EN EL GOBIERNO

ARTÍCULO 15 Titulares de Derechos Morales: En dado caso que en desarrollo de un proyecto avocado por los Nodos de Innovación se lleguen a generar resultados protegibles por Propiedad Intelectual, serán titulares de Derechos Morales sobre la obra o creación protegida, de manera general, todos aquellos que hayan participado de manera directa y efectiva en su elaboración.

Sin perjuicio de lo anterior, en todo caso se darán los créditos institucionales que correspondan a todas y cada una de las entidades que intervengan como gestores o entes financiadores del respectivo proyecto.

ARTÍCULO 16 Titulares de Derechos Patrimoniales: En el evento en que en desarrollo de un proyecto avocado por los Nodos de Innovación se lleguen a generar resultados protegibles por Propiedad Intelectual, a prorrata de sus respectivos aportes, serán titulares de los derechos patrimoniales, de manera general, todos aquellos que de alguna manera hayan participado en su creación.

En consecuencia los participantes en el referido proyecto podrán utilizar en su propia actividad la creación intelectual que lleguen a generar. Lo anterior sin perjuicio del cumplimiento de las obligaciones que les corresponda en caso de comercialización de la creación.

En aquellos casos en que el proyecto de innovación haya sido financiado con recursos del presupuesto nacional, la respectiva entidad pública titular de los recursos, salvo motivos de seguridad y defensa nacional, podrá ceder a los demás participantes en el proyecto los derechos de propiedad intelectual que le puedan corresponder. En este evento, los participantes definirán entre ellos la titularidad de los derechos de propiedad intelectual derivados de los resultados de la ejecución de los recursos del presupuesto nacional.

En general, cuando se trate de creaciones y/o desarrollos realizados en virtud de una relación laboral o de un contrato de prestación de servicios civiles, de toda clase de persona que llegue a ser vinculada al proyecto por alguna de las entidades participantes en los Nodos de Innovación, los derechos patrimoniales que se generen con motivo de la ejecución de los trabajos y actividades objeto de la relación laboral o del contrato y que se concreten en éste o en documento adicional; pertenecerán a la entidad participante que hizo tal contratación, a prorrata de su aporte.

Lo anterior sin perjuicio del hecho que la persona que realice de manera efectiva la obra, creación o desarrollo, al amparo del contrato de trabajo o de prestación de servicios, conservará los derechos morales respectivos. Así mismo se le reconocerán y darán los respectivos créditos institucionales que correspondan.

Sin embargo si el trabajo no es resultante de un contrato de obra o de un contrato laboral el autor es quien debe ceder la titularidad de los derechos de los productos y resultados que se obtengan en los proyectos financiados con los recursos del Estado, y es el Estado quien deberá preocuparse para que se realice las debidas licencias a favor del mismo para que sea posible la divulgación de los resultados de los proyectos a los interesados, a través de los canales dispuestos para tal fin, con el objetivo de que éstos sean replicados, apropiados y usados por los distintos actores del Sistema nacional de CTeI y contribuir al desarrollo de procesos de apropiación social de la ciencia, la tecnología e innovación.

Todo lo anterior de acuerdo a lo establecido en el la ley 1450 de 2011.

DEPARTAMENTO ADMINISTRATIVO DE CIENCIA, TECNOLOGIA E INNOVACION - COLCIENCIAS -

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 6 - AUTORIZACIÓN USO Y ALMACENAMIENTO DE DATOS PERSONALES

A continuación se presentan los contenidos del modelo de carta para autorización uso y almacenamiento de datos personales:

(Ciudad), (Día) de (Mes) de 201_

Señores
COLCIENCIAS
Carrera 7B Bis No. 132 – 28
Bogotá D.C.

Asunto: Autorización uso y almacenamiento de datos personales.

En virtud de la Ley Estatutaria 1581 del 2012, mediante la cual se dictan las disposiciones generales para la protección de datos personales, y su Decreto Reglamentario 1377 de 2013, autorizo al Departamento Administrativo de Ciencia, Tecnología e Innovación - Colciencias, considerado como responsable y/o encargado del tratamiento de datos personales, almacenados en bases de datos, las cuales incluyen información que se han reportado en desarrollo de las diferentes actividades y formularios, y en particular los siguientes: nombres, número de documento de identificación, dirección, teléfono fijo y móvil, direcciones, correo electrónico, profesión, hoja de vida académica, certificados de notas, etc.

Los datos serán utilizados para la misión institucional establecida en la ley 1286 de 2009, como ente rector de la Ciencia Tecnología e innovación en Colombia.

Atentamente,

FIRMA
NOMBRES Y APELLIDOS
IDENTIFICACIÓN_____

DEPARTAMENTO ADMINISTRATIVO DE CIENCIA, TECNOLOGIA E INNOVACION - COLCIENCIAS -

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 7 - CARTA DE PRESENTACIÓN Y AVAL

A continuación se presentan los contenidos del modelo de carta de presentación y aval:

(Ciudad), (Día) de (Mes) de 201_

Señores
COLCIENCIAS
Carrera 7B Bis No. 132 – 28
Bogotá D.C.

Asunto: Presentación y aval del proyecto titulado (escriba el nombre del proyecto) a la convocatoria (nombre de la convocatoria)

Respetados señores,

La presente tiene como objeto avalar el proyecto (escriba el nombre del proyecto,) a la convocatoria (nombre de la convocatoria) de 201_, propuesto por la (nombre de la alianzas estratégica…), y manifiesto que el proyecto en comento no está siendo financiado por otra convocatoria o con recursos de COLCIENCIAS u otras entidades del Estado.

Además, **ACEPTO** expresa e irrevocablemente que conozco detalladamente las características, requisitos y condiciones de la convocatoria para conformar un banco de proyectos de desarrollo tecnológico e innovación elegibles en la temática de ciberseguridad para el fomento del uso y apropiación de TIC en el gobierno, de manera que me someto a lo establecido en los Términos de Referencia determinados por COLCIENCIAS para el desarrollo de la misma y para la entrega del beneficio.

Con la presente manifestación inequívoca de voluntad, declaro que en caso de ser beneficiado en la convocatoria para conformar un banco de proyectos de desarrollo tecnológico e innovación elegibles en la temática de ciberseguridad para el fomento del uso y apropiación de TIC en el gobierno, esté será recibido en los términos que COLCIENCIAS establezca; comprendo y acepto que la no aceptación o el incumplimiento de alguna de las condiciones establecidas, dará lugar a la pérdida definitiva del beneficio.

Declaro que la información suministrada es veraz y corresponde a la realidad. En caso de encontrarse alguna incoherencia o inconsistencia en la información o documentación suministrada, COLCIENCIAS podrá en cualquier momento, rechazar mi postulación o finiquitar el beneficio, sin perjuicio de las acciones legales correspondientes.

Cordialmente,

FIRMA
NOMBRE DEL REPRESENTANTE LEGAL DE LA ENTIDAD EJECUTORA DE LA ALIANZA
CC_____
Dirección
Teléfono

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 8 - CONTENIDO DEL PROYECTO

- **Título del proyecto**
- **Investigador principal y coinvestigadores**
- **Línea Temática:** Especificar en cuál de las líneas temáticas definidas por la convocatoria está enmarcado el proyecto.
- **Resumen ejecutivo**: Información mínima necesaria para comunicar de manera precisa los contenidos y alcances del proyecto.
- **Antecedentes:** especificar si el proyecto ha tenido fases anteriores y cuáles han sido los resultados, cuántos recursos se han invertido y cuáles han sido sus fuentes de financiación.
- **Palabras Clave:** Incluir máximo seis (6) palabras clave que describan el objeto del proyecto.
- **Planteamiento del Problema:** Delimitación clara y precisa del objeto de la investigación que se realiza por medio de una pregunta.
- **Justificación:** Factores que hacen necesario y pertinente la realización del proyecto.
- **Marco conceptual:** Aspectos conceptuales y teóricos que contextualicen el problema de investigación en una temática; así como otros aspectos que sean pertinentes a juicio de los proponentes.
- **Estado del arte:** Revisión actual de la temática en el contexto nacional e internacional, avances, desarrollos y tendencias, en cuya elaboración se pueden tener en cuenta estudios de prospectiva y vigilancia tecnológica.

- **Objetivos:**

  - **Objetivo General:** Enunciado que define de manera concreta el planteamiento del problema o necesidad y se inicia con un verbo en modo infinitivo, es

medible, alcanzable y conlleva a una meta.

- **Objetivos Específicos:** Enunciados que dan cuenta de la secuencia lógica para alcanzar el objetivo general del proyecto. No debe confundirse con las actividades propuestas para dar alcance a los objetivos (ej. Tomar muestras en diferentes localidades de estudio); ni con el alcance de los productos esperados (ej. Formar un estudiante de maestría).

- **Metodología:** Exposición en forma organizada y precisa de cómo se desarrollará y alcanzará el objetivo general y cada uno de los objetivos específicos del proyecto, presentando los componentes del mismo y las actividades para el logro de estos.

- **Resultados esperados:** Conocimiento generado en el cumplimiento de cada uno de los objetivos.

- **Productos esperados:** Evidencia del logro en cuanto a generación de nuevo conocimiento, fortalecimiento de capacidades científicas y apropiación social del conocimiento, un prototipo o su equivalente.

- **Impactos potenciales**: Identificar los impactos potenciales de los resultados del proyecto, los productos, servicios o procesos en las necesidades de ciberseguridad en instituciones del estado.

- **Trayectoria del equipo de investigación**: Incluir el estado actual de investigación del equipo que conforma la propuesta. Se debe incluir el tiempo de dedicación y funciones en el marco del proyecto.

- **Cronograma:** Distribución de actividades mensuales de ejecución del proyecto. Asociar a cada actividad el o los objetivos (numerados) relacionados con estos.

- **Presupuesto detallado**: Incluye financiación y contrapartida en especie por rubro en efectivo y en especie.

- **Bibliografía:** Fuentes bibliográficas empleadas en cada uno de los ítems del proyecto. Se hará referencia únicamente a aquellas fuentes empleadas en el suministro de la información del respectivo proyecto. No se incluirán referencias que no se citen. Las citas, en cada uno de los campos del formulario, se utilizarán las normas APA No 6.

Plan de negocios: Documento estratégico que permita determinar las estrategias de mercadeo, tamaño del mercado, usuarios potenciales, proveedores de servicios, capacidad tecnológica requerida, precios, esquemas de comercialización, planes de internacionalización y expansión de mercados y

demás aspectos relacionados con la masificación de los productos, servicios o procesos.

Con el objetivo de generar la posibilidad de negocio consecuente del desarrollo del proyecto, se hace necesario contemplar un plan de negocio que permita la existencia de soluciones a las oportunidades evidenciadas en la Agenda Estratégica de Innovación – anexo 2. Entonces, la propuesta deberá demostrar cómo se ha diseñado la disponibilidad del producto para la solución de las necesidades expuestas.

Como mínimo, el plan de negocio deberá comprender para la comercialización del proyecto los siguientes aspectos: (ampliados si ha lugar)

- Estructura del órgano de administración
- Área jurídico-mercantil
- Área económica
- Área de marketing
- Área de ventas
- Área de producción
- Área de recursos humanos
- Área contable-financiera

Nota: Se deberá aportar toda la información necesaria para la evaluación del proyecto con base en los criterios establecidos en el numeral 9: CRITERIOS DE EVALUACION, de los términos de referencia de la convocatoria.

El componente presupuestal tendrá los siguientes Rubros Financiables:

- Estudios de inteligencia competitiva – incluida vigilancia tecnológica – para los productos relacionados con la (s) innovación (es) propuesta (s).

- Adquisición o arrendamiento de equipo de investigación, simulación, ensayos, pruebas y control de calidad que vayan a ser de propiedad del ejecutor o alquilados temporalmente. Se contempla también el diseño y construcción de equipos, cuando el proyecto que vayan a realizar, lo requiera.

- Materiales utilizados en la fabricación de prototipos y plantas piloto que vayan

a ser propiedad del ejecutor.

- Insumos y reactivos requeridos para el uso de los equipos de laboratorio propios del ejecutor para el desarrollo del proyecto.

- Desarrollo de software.

- Adquisición de software especializado cuya licencia vaya a ser propiedad del ejecutor para investigación, desarrollo y diseño.

- Servicios tecnológicos nacionales o internacionales (Ensayos, pruebas, análisis, simulación y otros).

- Contratación de consultoría científica y tecnológica especializada (igual o menor a 90 días, y de menor valor a 30% del proyecto).

- Viajes nacionales como internacionales relacionados con el desarrollo del proyecto, únicamente para el personal técnico vinculado al proyecto.

- Capacitación y actualización de personal a través de programas de entrenamiento de corta duración únicamente para el personal técnico vinculado al proyecto.

- Asistencia a seminarios y a cursos especializados, con duración menor a 180 días e incluye el valor de la inscripción y los pasajes únicamente para el personal técnico vinculado al proyecto.

- Participación en misiones tecnológicas y pasantías dentro y fuera del país únicamente para el personal vinculado al proyecto.

- Conexión a redes de información para transferencia y apropiación de tecnología.

- Adecuación con destinación específica de laboratorios y planta piloto, por un valor que no supere el 20% del costo solicitado del proyecto.

- Material para la promoción y la difusión de los resultados del proyecto. No se reconoce publicidad, ni actividades de mercadeo como parte de este rubro.

- Gastos de Propiedad intelectual relacionados con los resultados del proyecto o programa.

- Se financiarán imprevistos hasta un 10% de los recursos solicitados a

Colciencias. Por lo tanto, no se aceptarán cambios de rubro durante la ejecución del proyecto.

- **Personal:** Personal con formación científica y técnica, que cuenta con título profesional y/o de posgrado (maestría, doctorado), y vinculación de postdoctorados que estarán a cargo de las actividades investigativas propias de la ejecución del proyecto según el planteamiento científico-técnico.

  Personal con formación en carreras técnicas y tecnológicas con capacidades para apoyar la ejecución de actividades de CTeI.

  Los costos individuales no podrán exceder los topes máximos que COLCIENCIAS defina por resolución.

- **Equipos:** Aquellos necesarios para el desarrollo del proyecto, los cuales pueden ser adquiridos a cualquier título. La financiación para compra de equipos nuevos deberá estar sustentada en la estricta necesidad de los mismos para el desarrollo del proyecto.

- **Materiales e Insumos:** Adquisición de insumos, bienes fungibles y demás elementos necesarios para el desarrollo de algunas actividades previstas. Deben presentarse a manera de listado detallado agrupado por categorías sobre las cuales debe hacerse una justificación de su necesidad y cantidad. (Ej. consumibles, reactivos, herramientas, elementos de protección, controles e instrumentación accesoria, material biológico, audiovisual, de laboratorio y de campo, etc).

- **Bibliografía:** Adquisición de libros, revistas, artículos, suscripciones o acceso a bases de datos especializadas, que sean estrictamente necesarias para una ejecución exitosa del proyecto.

- **Servicios técnicos:** Contrataciones que se hacen para la prestación de servicios especializados y cuya necesidad esté suficientemente justificada, por ejemplo: ensayos, pruebas, análisis de laboratorio y caracterizaciones, etc. Estos no deben incluirse en los gastos de personal.

- **Software:** Adquisición de licencias de software especializado para las actividades de CTeI propias del desarrollo del proyecto. Su necesidad y cantidad debe soportarse en justificaciones técnicas detalladas. No se considerará financiable dentro de este rubro software de uso cotidiano, como por ejemplo procesadores de texto, hojas electrónicas o sistemas operativos.

- **Salidas de campo:** Costos asociados al levantamiento de información en campo, desde fuentes primarias o secundarias, para la consecución de los

objetivos del proyecto.

- **Publicaciones:** Costos asociados a la publicación de artículos, libros, manuales, videos, cartillas, posters, etc. que presenten los resultados del proyecto y sirvan como estrategia de divulgación o apropiación social de los resultados de la investigación.

- **Gastos de administración de proyectos**: Hasta el 10% del valor total del proyecto sin contrapartida en especie, es decir solo por el valor en efectivo, este rubro no podrá ser modificado en la ejecución del proyecto.

Rubros No Financiables

No será financiable con recursos de COLCIENCIAS rubros presupuestales como:

- El personal que sea beneficiario actual de los programas “Jóvenes Investigadores” o “Formación de Doctorados” de COLCIENCIAS, podrá ser vinculado a las actividades investigativas previstas para la ejecución del proyecto, pero en ningún caso, podrá ser financiado al mismo tiempo con los recursos provenientes de COLCIENCIAS asignados a este rubro, en esta convocatoria.
- A través del rubro de personal, no se financiarán los derechos académicos y de matrícula del personal.
- No será financiable con recursos de COLCIENCIAS rubros presupuestales como: construcciones, mantenimiento de equipos e infraestructura, imprevistos, seguros, adquisición de vehículos, mobiliario de oficina, membresías a Sociedades Científicas.
- Comprar de máquinas y equipo de producción corriente.
- Pagos de pasivos, pago de dividendos, aumento de capital de la entidad beneficiaria
- Pagos de dividendos o recuperaciones de capital de la entidad beneficiaria
- Capital de trabajo para la producción corriente
- Inversiones en otras empresas
- Inversiones en planta de producción a escala industrial
- Compra de acciones, derechos de empresas, bonos y otros valores mobiliarios
- Instalaciones llave en mano

CONVOCATORIA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN INSTITUCIONES DEL ESTADO - 2014

ANEXO 9 - CRITERIOS DE EVALUACIÓN

A continuación se describen los criterios de selección de los proyectos:

1. Calidad y metodología del Proyecto

Coherencia de la metodología con los resultados e impactos esperados. El proyecto deberá describir claramente el conjunto de procedimientos, actividades, y/o tareas a ser utilizados para alcanzar los objetivos, resultados, e impactos esperados del proyecto.

a. Coherencia interna y tratamiento particular de antecedentes, objetivos, metodología, actividades, presupuesto, cronograma y duración.
b. Adecuación del grupo ejecutor del proyecto a los objetivos planeados.
c. Conocimiento de los antecedentes científicos y tecnológicos en la temática del proyecto
d. Revisión de productos de Propiedad Intelectual para la conformación del estado del arte (patentes, modelos de utilidad, registro del diseño, registro de marca, etc.)

2. Equipo de Trabajo

La documentación del proyecto deberá presentar el grupo de personas que conforman el equipo que llevará a cabo el proyecto; incluyendo las hojas de vida de cada uno de los integrantes, su dedicación al proyecto, las labores/tareas que cumplirán así como el costo de su participación.

3. Resultados e impactos esperados del proyecto en el uso y apropiación de TIC en el gobierno.

El proyecto deberá describir breve y claramente sus resultados e impactos esperados relacionando cómo cada uno de ellos afecta a:

a. El objetivo y los objetivos específicos de la convocatoria.
b. Los vectores y las líneas temáticas descritas en la Agenda Estratégica de Innovación – Anexo 4.
c. Las entidades públicas que puedan ser usuarias de los resultados del proyecto o a los ciudadanos para que tengan un mejor acceso a la información o servicios que las entidades públicas generan o prestan.

4. Plan de Negocio

Documento estratégico que permita determinar las estrategias de mercadeo, tamaño del mercado, usuarios potenciales, proveedores de servicios, capacidad tecnológica

requerida, precios, esquemas de comercialización, planes de internacionalización y expansión de mercados y demás aspectos relacionados con la masificación de los productos, servicios o procesos.

Con el objetivo de generar la posibilidad de negocio consecuente del desarrollo del proyecto, se hace necesario contemplar un plan de negocio que permita la existencia de soluciones a las oportunidades evidenciadas en la Agenda Estratégica de Innovación – anexo 2. Entonces, la propuesta deberá demostrar cómo se ha diseñado la disponibilidad del producto para la solución de las necesidades expuestas.

Como mínimo, el plan de negocio deberá comprender para la comercialización del proyecto los siguientes aspectos: (ampliados si ha lugar)

- Estructura del órgano de administración
- Área jurídico-mercantil
- Área económica
- Área de marketing
- Área de ventas
- Área de producción
- Área de recursos humanos
- Área contable-financiera

5. **Participación comprobable de por lo menos una de las entidades ejecutoras en el Subsistema de Innovación para el uso y apropiación de TIC en el gobierno expedido por la Secretaría Técnica del mencionado Subsistema.**

   La certificación de participación en el Subsistema de innovación y sus actividades se podrá solicitar a través del correo subsistemadeinnovacion@mintic.gov.co con asunto: certificación de participación. En el cuerpo del correo se debe incluir la siguiente información:

   a. Nombre completo de la entidad ejecutora solicitante
   b. NIT de la entidad solicitante
   c. Dirección de correo electrónico al que debe ser enviado el certificado

6. **Participación comprobable de por lo menos una de las entidades beneficiarias en el Subsistema de Innovación para el uso y apropiación de TIC en el gobierno expedido por la Secretaría Técnica del mencionado Subsistema.**

   La certificación de participación en el Subsistema de innovación y sus actividades se podrá solicitar a través del correo subsistemadeinnovacion@mintic.gov.co con asunto: certificación de participación. En el cuerpo del correo se debe incluir la siguiente información:

   a. Nombre completo de la entidad beneficiaria solicitante

b. NIT de la entidad solicitante
c. Dirección de correo electrónico al que debe ser enviado el certificado

7. Interés y/o apoyo comprobable de una o varias entidades estatales en el uso de los resultados del proyecto, a través de la participación en pilotos o prototipos o la participación demostrable en el proyecto.

El interés o apoyo de una o varias entidades estatales deberá ser fácilmente comprobable, por lo cual la documentación del proyecto debe claramente identificar cuáles son estas entidades estatales interesadas o que apoyan el proyecto, cuál es la naturaleza de este interés y apoyo y cómo este afecta el proyecto.