**EL INSTITUTO NACIONAL DE CANCEROLOGÍA, EMPRESA SOCIAL DEL ESTADO - INVITA A PRESENTAR PROPUESTAS PARA CONTRATAR UN SOFTWARE DE CODIGO ABIERTO QUE PERMITA LA ADMINISTRACIÓN DE TODO EL FLUJO EDITORIAL DE LA REVISTA COLOMBIANA DE CANCEROLOGIA, INCLUYENDO LA RECEPCIÓN DE MANUSCRITOS, EL PROCESO DE REVISIÓN POR PARES EVALUADORES Y LA PUBLICACIÓN EN LINEA DE ARTICULOS EN TEXTO COMPLETO, PARA LA VIGENCIA 2019 ACORDE A ESTA INVITACIÓN, SUS ANEXOS Y EL CONTRATO QUE SE CELEBRE PARA EL EFECTO.**

**ANEXO TÉCNICO No.3**

1. **OBJETO**

El Instituto Nacional de Cancerología – Empresa Social del Estado, está interesado en la contratación de un software de código abierto que permite la administración de todo el flujo editorial de la Revista Colombiana de Cancerología, incluyendo la recepción de manuscritos, el proceso de revisión por pares evaluadores y la publicación en línea de artículos en texto completo, para la vigencia 2019.

1. **DESCRIPCIÓN GENERAL DEL BIEN**

El Instituto Nacional de Cancerología – Empresa Social del Estado, está interesado en contratar bajo la modalidad de invitación a cotizar la suscripción de un software de código abierto que permite la administración de todo el flujo editorial de la Revista Colombiana de Cancerología, incluyendo la recepción de manuscritos, el proceso de revisión por pares evaluadores y la publicación en línea de artículos en texto completo.

1. **REQUISITOS HABILITANTES**.

Experiencia específica. El proponente debe contar con una experiencia mínima de cuatro (4) años de asesoramiento en revistas indexadas

1. **CRITERIOS DE CALIFICACIÓN TÉCNICA DE PUNTAJE**.

La calificación de las propuestas se hará sobre la base de 700 puntos que se aplicarán a los siguientes factores así:

|  |  |
| --- | --- |
| CRITERIO | PUNTAJE |
| 1. Experiencia específica y cumplimiento en contratos anteriores
 | 400 |
| 1. Precio
 | 300 |
| TOTAL PUNTAJE | 700 |

La calificación técnica de puntaje total mínima es de 500 puntos.

**a). EXPERIENCIA Y CUMPLIMIENTO EN CONTRATOS ANTERIORES**

Para efectos de la experiencia se revisarán dos subcriterios: monto y tiempo de ejecución.

|  |  |
| --- | --- |
| 1. Monto contratado
 | 200 |
| 1. Tiempo ejecutado
 | 200 |
| TOTAL PUNTAJE | 400 |

* Monto contratado. Se asignará un máximo de doscientos (200) puntos a la propuesta que presente una sumatoria mayor de los montos contratados, sustentada a través de certificaciones de experiencia en el objeto contractual similar al del presente proceso, con revistas indexadas debidamente certificadas por cada contrato. Las certificaciones que cubran más de un año de vigencia, deben tener desagregado el valor de ejecución para cada año. Las certificaciones que no cumplan con dicho requisito no serán tenidas en cuenta. Al mayor monto contratado totalizado se le asignarán doscientos puntos (200), a los demás se les asignará un puntaje inversamente proporcional.
* Tiempo ejecutado. Se asignará un máximo de doscientos (200) puntos a la propuesta que presente una sumatoria mayor de meses completos ejecutados, sustentada a través de certificaciones de experiencia de objeto contractual similar al del presente proceso, con revistas indexadas, debidamente certificadas por cada contrato. Las certificaciones que no cumplan con dicho requisito no serán tenidas en cuenta.

Para que las referencias contractuales sean tenidas en cuenta, deberán anotar adicionalmente el monto o valor total del contrato, término de duración y concepto de cumplido a satisfacción o no del servicio por parte de la entidad contratante.

Las referencias contractuales deben relacionarse directamente con los servicios o bienes a contratar en el presente proceso, deben indicar**:**

* Nombre del contratante, con dirección y teléfono
* Objeto del contrato claramente definido.
* Valor contratado o ejecutado
* Fecha de inicio y terminación del contrato (día, mes, año). Si no indica día específico, se asignará el último día del mes correspondiente referido en la certificación.
* Calidad y cumplimiento.

Estas certificaciones deben ser expedidas por el representante legal de la entidad contratante o por la persona a quien este delegue o esté autorizada para tal fin.

NOTA: Si las referencias presentadas no cumplen con las características enunciadas, o tienen un nivel de calidad y cumplimiento insatisfactorios, no se tendrán en cuenta para su calificación y por lo tanto se les asignará un puntaje de 0.

**b). PRECIO**

Al precio más bajo, se le asignarán trescientos (300) puntos y a los siguientes proponentes se les asignará un puntaje inversamente proporcional.

1. **CARACTERISTICAS ESPECIFICAS DEL SERVICIO**

ED-0101 Soporte técnico y funcional

Suscripción anual a soporte técnico para la plataforma del sistema de gestión de revistas OJS Versión 3.1. Incluye:

* Soporte y acompañamiento durante un año al grupo de editores de la institución para el uso y manejo del sistema de gestión de revistas Open Journal Systems (OJS)
* Actualización permanente
* Copias de seguridad y respaldo
* Asesoría funcional todo el año
* Valores agregados de acuerdo con lo estipulado en la propuesta.

ED-0115 Soporte técnico DOI primer año

* Consultoría + suscripción primer año.
* Servicio anual que incluye la suscripción al sistema
* Crossref y el soporte y acompañamiento durante un año al grupo de editores de la institución para el uso y manejo del DOI para las publicaciones de la entidad.

ED-0117 Paquetes DOI

* Asignación y activación de sufijos DOI.
* Pago a Crossref por concepto de "DOI Deposits".
* Generación y validación de XML de acuerdo con la DTD de CrossRef
* Cargue de metadatos en el sistema de CrossRef

Términos y condiciones

* La única forma de pago es anticipada. La asignación de los números DOI se realizará solamente después de recibir el pago.
* La entrega del paquete DOI se realizará mediante el certificado de garantía de activación DOI que Biteca entregará al cliente una vez recibido el pago correspondiente.
* Los DOI incluidos en el paquete deben utilizarse durante el año de servicio. Si al terminar el año de servicio el cliente no ha activado todos los DOI comprados en el paquete, el cliente puede renovar el servicio de soporte técnico DOI y suscripción a Crossref (ED-0147) para ampliar la vigencia del paquete, en caso de no renovar dicho servicio no se recibirán más solicitudes de activación y se perderán los DOI no activados dentro del paquete.
* El precio del paquete DOI no incluye la suscripción al sistema CrossRef ni soporte técnico frente de DOI o Crossref. Los clientes interesados en la renovación del soporte técnico deberán contratar dicho servicio (ED-0147)
* Para la adquisición de los DOI en instituciones que no estén afiliadas a CrossRef es indispensable contratar el soporte técnico DOI del primer año (ED-0115).
* La activación de los DOI se realizan en un término aproximado de 24 a 48 horas después de recibida la solicitud de activación a través de la mesa de servicios.

ED-0121 Servicio antiplagio

* Servicio de suscripción al sistema antiplagio (iThenticate) para la revisión de artículos de la Revista del Instituto Nacional de Cancerología. Vigencia de un año.

ED-0131 Diagramación artículos en PDF

* Diagramación de artículos en formato PDF
1. **OBLIGACIONES DEL CONTRATISTA PARA LA CORRECTA EJECUCIÓN DEL CONTRATO**

Dentro de la ejecución del documento contractual, el CONTRATISTA se obliga a:

**a).**  **OBLIGACIONES DE CARÁCTER GENERAL**:

1. Cumplir con los ofrecimientos, condiciones y términos de la propuesta que hace parte integral del contrato.
2. Cumplir con las normas ambientales y de seguridad industrial.
3. Dar cumplimiento a sus obligaciones frente al Sistema de Seguridad Social Integral, parafiscales (Caja de Compensación, Sena ICBF), por lo cual el incumplimiento de estas obligaciones será causal para la imposición de multas sucesivas hasta tanto, se dé cumplimiento, previa verificación de la misma mediante liquidación efectuada por la Entidad Administradora.
4. Atender los requerimientos que efectúe el Instituto a través del supervisor del contrato.
5. Actuar con suma diligencia en la ejecución del servicio contratado.
6. Proporcionar todos los materiales y herramientas, así como personal necesario, para el desarrollo del objeto contractual, sin ningún costo adicional para el Instituto.
7. Responder por los daños y perjuicios hasta por culpa leve cuando se cause perjuicio al Instituto o a terceros en la ejecución del objeto contratado, cuando estos sean debidamente comprobados
8. Guardar la confidencialidad de toda la información que le sea entregada y que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o a la que tenga acceso y responderá patrimonialmente por los perjuicios que su divulgación y/o utilización indebida por sí o por un tercero, cause a la administración o a terceros
9. Presentar facturas con los documentos y requisitos exigidos por la DIAN y el INSTITUTO
10. Al terminar el contrato contribuir a la liquidación del mismo
11. Demostrar la implementación de controles de calidad tanto de proceso como de resultado. El proveedor aceptará que la oficina de gestión de la calidad realice en cualquier tiempo el control de calidad y verificación de los estándares de calidad tanto de los servicios ofrecidos.
12. Cumplir con las demás obligaciones, estipulaciones y establecidos en los términos de referencia de la invitación a cotizar, sus anexos y la propuesta presentada, documentos que forman parte integral de ésta contratación.
13. Todas las demás que se deriven del objeto del contrato y permitan llevar a feliz término la contratación que surja de esta convocatoria.

**b). OBLIGACIONES ADICIONALES DE CARÁCTER ESPECÍFICO**

1. Soporte técnico y funcional
2. Soporte técnico DOI primer año (Identificación de única forma del contenido electrónico del artículo)
3. Paquetes DOI
4. Servicio antiplagio
5. Diagramación artículos en PDF
6. Backup de la información de manera trimestral
7. El proveedor debe Contar con sistemas Antivirus, antimalware y Firewall para la protección de servidores, equipos y periféricos, impresoras, redes de datos y voz, y demás sistemas que así lo requieran.
8. El proveedor debe prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de [gusanos informáticos](https://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico).
9. Se debe limitar el uso de la red para aquellos usuarios que realmente lo necesiten, limitar y controlar el acceso de puertos abiertos, e Identificar de forma inequívoca a los usuarios y sistemas que interactúan en la redes.
10. Se deben poder obtener el registro de cada acción o evento que tenga lugar en la red de telecomunicaciones (logs). Estos registros deben servir para contrarrestar el repudio de eventos por parte de los usuarios
11. La información confidencial del instituto se debe transmitir utilizando técnicas de ciframiento, VPN o canal de datos establecido INC de manera segura, fuera del email o sistemas de nube de propiedad y control del PROVEEDOR, ya que no es recomendable que esta se guarde en cuentas de correo que podrían ser atacadas, compartidas con otras campañas o o bien producirse su pérdida ante cualquier error humano o informático.
12. El PROVEEDOR debe evitar la utilización de información de los pacientes y ciudadanos como material de desarrollo, pruebas y/o capacitación durante la ejecución de su servicio. Se deben preparar y contar una data ofuscada o de prueba previamente preparada para realizar estas labores.
13. Se debe separar las incidencias de seguridad internas frente a las externas que corresponden y afectan a los pacientes y ciudadano del INC, con la finalidad de atacarlas a tiempo y tomar las previsiones necesarias. Se debe informar al Supervisor de contrato y Oficial de seguridad de la información en el INC de cualquier incidencia relacionada con seguridad de la información de manera inmediata.
14. El proveedor debe marcar adecuadamente la información o documentos que sean confidenciales del INC, durante todo el ciclo de vida de la data para que sus empleados y administradores de plataformas no tengan la posibilidad de equivocarse en el tratamiento de la información del INC.
15. El PROVEEDOR debe contar con planes de continuidad y de respaldo en caso de ocurrencia de eventos catastróficos. Dichos planes deben ser probados y evidenciados periódicamente mediante informe entregado al INC. El proveedor debe garantizar la continuidad de operación tecnología de la solución, manteniendo documentados y disponibles los procedimientos de contingencia
16. Para asegurar la continuidad del servicio en el sitio o remota EL PROVEEDOR dispondrá de los equipos de recambio necesarios para realizar los cambios en caso de que la reparación de un equipo requiera de soporte especializado o gestión de garantía
17. Los sistemas deben estar protegidos por contraseñas seguras. EL PROVEEDOR debe acogerse al manual de contraseñas seguras del INC, la cual exige que se cumplan las siguientes características:

**Política INC de Contraseñas  para servicios  críticos, usuarios administradores, archivos de configuración de plataformas y/o bases de datos  publicados a internet.**

* Longitud  mínima: 20 caracteres
* Generada por un sistema aleatorio de contraseñas ( Pueden usarla herramienta Password Generation del aplicativo KEEPASS, o usar cualquiera del mercado)
* Alfanumérica (Números y letras)
* Combinación de Mayúsculas y Minúsculas
* Caracteres especiales (mínimo 2)
* Tiempo máximo de vida de la contraseña (TTL): 90 días
* Histórico de contraseñas: No permitir uso de contraseñas utilizadas previamente

**Política Contraseñas  para Usuarios y servicios no críticos**

* Longitud  mínima: 8 caracteres
* Alfanumérica (Números y letras)
* Mínimo 1 mayúscula
* Mínimo 1 carácter especial
* Tiempo máximo de vida de la contraseña (TTL): 45 días
* Histórico de contraseñas: No permitir usar la misma contraseña de los últimos 5 cambios
* Bloqueo de cuenta  por intentos fallidos: Después de 5 intentos
* No debe contener el nombre de usuario, nombre o apellidos del usuario, numero de cedula o documento de identificación.
1. El PROVEEDOR debe contar con políticas de backup o respaldos de información y configuración de los sistemas de red, servidores, máquinas virtuales, sistemas de información, bases de datos y sistemas de almacenamiento. La restauración de dichos backup debe ser probados periódicamente y el PROVEEDOR debe entregar evidencia de la mismas INC.
2. El PROVEEDOR debe gestionar de manera oportuna actualizaciones o parches de sistemas, servidores, telefonía, redes y/o comunicaciones, sin afectación del servicio prestado al INC.
3. El PROVEEDOR debe revisar y registrar de forma periódica los cambios que se pueden producir en las amenazas que existen sobre los sistemas y redes a proteger. Cualquier cambio en los niveles de riesgo o en la aparición de nuevas amenazas deben ser reportados al supervisor de contrato.
4. Cuando ocurran cambios de las configuraciones de seguridad en los sistemas y redes objeto del contrato, es necesario que sean comunicados previamente por escrito al supervisor de contrato y al Oficial de seguridad de la información en el INC, y a ser posible que se realice un backup previamente.
5. El PROVEEDOR debe adaptarse al uso de herramienta de conexión remota o VPN para soporte remoto que recomiende el instituto, y debe adquirir el licenciamiento de la misma si es necesario.
6. El PROVEEDOR debe firmar y cumplir acuerdo de confidencialidad, manejo de datos personales, derechos de autor y deber secreto con el INC.

El PROVEEDOR debe Propender por el buen uso de tipo laboral de recursos de canales, internet, correo y recursos tecnológicos del INC.

1. El PROVEEDOR debe Propender por el buen uso de tipo laboral de recursos de canales, internet, correo y recursos tecnológicos del INC.