

ANEXO 8 – SOLUCIÓN TÉCNICA Y DE SEGURIDAD

INTRODUCCIÓN:

El proponente deberá describir en su propuesta si proporciona cada funcionalidad solicitada en el presente anexo, para lo cual solicitamos que las respuestas sean diligenciadas como se indica en la tabla detallada al final con el nombre FORMATO PARA CONSOLIDAR RESPUESTAS. Adicionalmente, la herramienta ofrecida debe ser comercial y se debe encontrar en el mercado funcionando de manera exitosa en otros clientes.

1. INFORMACIÓN ESPECÍFICA DE LA SOLUCIÓN TÉCNICA Y DE SEGURIDAD REQUERIDA

1.1 Características generales de la solución. El proponente deberá describir:

- Nombre del producto y Versión del producto (si no es la última versión liberada, explique porque)
- Fecha de liberación de la versión presentada y Fecha de liberación de la próxima versión (si se conoce)
- Idiomas que maneja la solución (se requiere en español)
- Indicar como la solución brinda flexibilidad en la conectividad a la herramienta por parte del usuario final, mostrando la información en línea desde cualquier dispositivo, tales como teléfonos inteligentes, tabletas, equipos de escritorio o portátiles, desde cualquier ubicación.
- Indicar el procedimiento de calidad para garantizar que la solución ofrecida incorporará técnicas avanzadas en cuanto a diseño y herramientas actuales para su construcción que no presentarán errores que impidan su normal funcionamiento.
- Detallar los módulos que contempla la solución propuesta y hacer una descripción de su alcance.
- Detallar por aparte lo relacionado con:
 - ✓ Gestor de Contenido.
 - ✓ Con que herramientas ofimáticas y demás herramientas interactúa.
- Para lo referente a la descripción de los módulos, tener en cuenta:
 - ✓ Nombre completo, especificación de compatibilidad con otros sistemas y plataformas sobre las que puede operar.
 - ✓ Si requiere licenciamiento, propuesta del esquema adecuado de dicho licenciamiento, teniendo en cuenta los ambientes de producción, pruebas y contingencia (si aplica).
- Modo de operación general de la aplicación (localización y distribución de datos, manejo de comunicaciones, modo de procesamiento, etc.) con respecto a lo esperado y descrito en el modelo tecnológico y capacidad actual instalada. NOTA: No se pide la arquitectura, sino el modo de operación a nivel funcional.

- El sitio web tiene un sitemap que sea un sitemap.xml? Lo anterior, por cuanto el Banco requiere contar con un formato amigable al rastreo de los buscadores donde le servimos las urls amigables.
- El sistema permite integrarse con herramientas de geolocalización, como por ejemplo google maps.?
- Si el punto anterior tiene respuesta afirmativa, indicar en donde se implantará.
- El sistema controla el uso de los caracteres especiales que puedan ingresar los usuarios al configurar y crear los nuevos contenidos, garantizando la correcta funcionalidad de la página y del Portal.
- Detallar el cumplimiento que a la fecha tiene implementada la solución para atención de lo pedido por Gobierno en Línea. Especificar como cubre todos sus aspectos y que no está cubierto. entre otros:
 - ✓ Política anti trámites
 - ✓ Servicio al ciudadano
 - ✓ Rendición de cuentas al ciudadano
 - ✓ Política anticorrupción
 - ✓ Política de archivo y gestión documental
- **Licenciamiento y actualizaciones** Detallar el licenciamiento requerido por la solución ofrecida. Se espera que el Proponente ofrezca las licencias en el servicio de hosting.
- El proveedor deberá especificar en su propuesta los tiempos de respuesta o latencia que puede ofrecer para el despliegue de las páginas del portal dependiendo de las características de contenido y el número máximo de usuarios concurrentes.

1.2 Arquitectura Tecnológica. A continuación se pide que el proveedor de respuesta a la Arquitectura tecnológica que dispone la solución ofrecida, teniendo en cuenta que el Banco requiere contratar el servicio de Hosting, por lo que el dimensionamiento se debe dar en términos de licenciamiento y capacidad de TIC. Dar respuesta:

1.3.1 Arquitectura de la solución.

- **Diagrama.** Donde se muestre claramente la arquitectura del sistema de información a implementar en el proyecto. En ésta se deberá hacer una descripción de todos los componentes que se utilizarán en las diferentes capas.
- **Arquitectura.** Detallar el tipo de arquitectura de la solución ofrecida: Monolítica, WEB, Cliente – Servidor, otra.
- **Alta disponibilidad.** Detallar el esquema de alta disponibilidad que se tiene de propuesta para la solución ofrecida.
- El sistema debe tener un código optimizado para alto rendimiento y velocidad

1.3.2 Arquitectura del software: Detallar:

- Sistema Operativo que soporta la solución ofrecida
- Bases de datos: Motor y versiones.
- Software base que soporta la solución ofrecida. VER
- Lenguaje de desarrollo utilizado. VER
- Debe Presentar compatibilidad con los estándares html5 y css3. En caso de presentarse, el proponente deberá detallar con que otros estándares presenta compatibilidad.
- Interfaces de programación.
- Portabilidad.
- Tipos de navegadores que soporta.
- **Presentación de interfaz gráfica.** Detallar para cada uno de los siguientes ítems el alcance
 - ✓ Presentación en diferentes tipos de dispositivos móviles. Especificar los dispositivos y tecnologías compatibles con la solución presentada: dispositivos móviles, equipos de escritorio, portátiles, etc.
 - ✓ Indicar los diferentes tipos de Browser que soporta.
 - ✓ Como es el esquema de adaptación a los diferentes tamaños de salida
 - ✓ La interfaz gráfica debe presentar un diseño intuitivo.
- Detalle el procedimiento para integración con el directorio activo.
- Debe Presentar la facilidad de Streaming Distribución digital de contenido multimedia.
- Especificar como presentará los diferentes componentes que hacen parte de gobierno en línea.
- La arquitectura de software permite Integrar plugins, extensiones, frameworks o componentes de software para ampliar funcionalidades o adicionar nuevas.

1.3.3 Arquitectura del Hardware.

- Detallar en un modelo la arquitectura de hardware que se propone para la solución requerida. Se debe especificar los requerimientos mínimos y óptimos en que trabaja la solución.
- Características de los servidores de aplicaciones y base de datos:
 - ✓ Tipo de servidores
 - ✓ Asignación de servidores
 - ✓ Cantidad de memoria
 - ✓ Características del procesador
 - ✓ Capacidad discos duros
 - ✓ Tarjetas de Red
 - ✓ Enrutadores
 - ✓ Características de disponibilidad y escalabilidad
- Capacidad de almacenamiento (datos, archivos, videos e imágenes)

1.3.4 Arquitectura de comunicaciones.

- Características de disponibilidad y escalabilidad
- Velocidad del canal de comunicaciones
- Medición y registro de parámetros del uso del ancho de banda
- Evaluación y administración del reúso

- Infraestructura física
- Sistema de administración de redes
- Disponibilidad del servicio del canal (Uptime requerido 99.9995%)

2. SOPORTE, MANTENIMIENTO Y CONTINUIDAD.

2.1. Generalidades soporte, mantenimiento correctivo y evolutivo. El proponente debe especificar:

- Indicar el proceso y las metodologías de actualización e instalación de una versión del software del gestor del contenido y demás detalles que se consideren necesarios para que el Banco pueda evaluar los servicios de soporte, actualización y mantenimiento.
- Esquema para garantizar que las herramientas, componentes y demás piezas de software que integran la solución presentada, serán actualizadas con el fin de mantener el soporte por parte del fabricante
- Indicar la política de cantidad de versiones que se liberan por año
- Tipo de soporte y mantenimiento que se ofrecerá en el contrato.
- Tiempos de entrega y los informes que se usarán para el seguimiento.
- El proponente deberá entregar como mínimo la siguiente documentación: Documentación de usuario, operativa, técnica, versión del producto, Fecha de liberación de la versión, mejoras o correcciones implementadas en la versión, prerequisites para la actualización, tiempos estimados para la actualización, otros.
- Detallar porcentaje de la licencia para mantenimiento anual, sobre el costo del licenciamiento de mantenimiento y como se pactaran las prórrogas.
- Esquema para garantizar que las actualizaciones o correcciones de los navegadores actuales del mercado, puedan mantener la funcionalidad en cada uno de ellos.
- Indicar si Los ANS propuestos estiman que el tiempo máximo de atención de un incidente no deberá exceder las dos (2) horas y su solución dependiendo la complejidad o gravedad no deberá exceder de las 72 horas

2.2 Soporte y mantenimiento correctivo.

- Esquema del servicio de soporte y mantenimiento correctivo para la solución o para los componentes que presente en su propuesta (software base, aplicaciones, servicios, componentes, módulos, etc.).
- Niveles de acuerdos de servicio. Servicios, tiempos de respuesta, disponibilidad, prioridades, responsabilidades, documentación, garantías y penalizaciones.
- Esquema de las diferentes líneas de soporte (teléfono, mail, online, presencial, entre otros)
- Esquemas de monitoreo, seguimiento y control.
 - ✓ Incidencias
 - ✓ Problemas
 - ✓ Acuerdos de servicio (SLA). Niveles de acuerdos de servicio.

- ✓ Acuerdos de Operación (OLA)
- ✓ Niveles de atención
- ✓ Controles de cambio
- ✓ Manejo de versiones.
- ✓ Configuraciones (aplicación, base de datos, servidores)
- Soporte sobre la funcionalidad de la solución 7x24x365.

2.3. Mantenimiento evolutivo. Hace referencia a nuevos desarrollos, ya sean solicitados por el Banco o por el Proponente.

- Esquema del servicio de mantenimiento evolutivo
- Niveles de acuerdos de servicio. Servicios, tiempos de respuesta, disponibilidad, prioridades, responsabilidades, documentación, garantías y penalizaciones.
- Esquema definido para nuevos requerimientos.
 - ✓ Capacitación
 - ✓ Consultoría
 - ✓ Desarrollo
 - ✓ Disponibilidad para contar con dichos servicios.
- Lo desarrollos deberán contar con la buena utilización de los estándares de programación y uso

2.4. Continuidad del servicio de TIC.

- Servicio de Contingencia. Describir el servicio de contingencia que tendrá la solución ofrecida a nivel de aplicación y servicio de hosting. Indicar si se cuenta con servicio de datacenter alternativo.
- Disponibilidad del servicio. Indicar los ANS's, los indicadores asociados a continuidad, los cuales se esperan que estén en un porcentaje de disponibilidad del sitio WEB del 99.96%.
- Indicar cuál es el plan de Continuidad del servicio de soporte y mantenimiento para el sitio WEB y el HOSTING.
- Indicar las políticas de respaldo y recuperación del sistema: Datos, aplicación, hosting.
- Indicar el proceso de contingencia para contar con la disponibilidad de los respaldos realizados.
- Indicar los ANS establecidos para contar con procesos de recuperación y disponibilidad de los datos y aplicación.

3. PROCESO DE IMPLANTACIÓN

3.1. Esquema de Implantación y Adecuación.

- Describir la metodología que será utilizada durante la adecuación e implantación de la solución ofrecida.

- ✓ Marco de referencia de la metodología a utilizar. Debe estar alineada a mejores prácticas.
- ✓ Planeación detallada del proceso de instalación y prueba, o del equipo tal como se recibe de fábrica. Incluir una matriz RACI que identifique los roles y sus responsabilidades, tanto de recursos del Proponente como del Banco. Equipo de trabajo: Banco y contratista seleccionado. Detallar para:
 - Pruebas.
 - Producción
- ✓ Indique si la instalación de la solución está a cargo del proveedor en los ambientes de pruebas y producción.
- ✓ Estimar el tiempo que conlleva la instalación de la solución
- ✓ Indicar si hay proceso de capacitación y si es así, que roles por parte del Banco debe participar.
- ✓ Indicar si el proceso de instalación está documentado.
- ✓ Proceso de estimación de tiempo de desarrollo y adecuación para los requerimientos funcionales que se comprometen a realizar.
- ✓ Esquema de funcionamiento.
- Indicar el proceso para ajustar la solución propuesta de acuerdo con las adecuaciones o extensiones necesarias para que la solución ofrecida cumpla totalmente con los requerimientos definidos en estos términos.

3.2. Transición y Conversión de datos/contenidos para la operatividad de la solución. Presentar un plan de cargue inicial y migración de datos para la operatividad de la solución indicando la participación del Banco y del proponente y qué condiciones se requieren para obtener una funcionalidad exitosa. Se espera que el porcentaje de migración del contenido actual frente a la nueva arquitectura esté entre un 30% a 40%.

3.3 Capacitación que brindará a la solución ofrecida. El proponente deberá presentar las condiciones bajo las cuales brindará la capacitación respectiva en todos los componentes que integren la solución:

- Tipo de capacitación: Técnica, operación, administración y usuario.
- Contenido de cada curso, Duración e intensidad horaria.
- Grupo objetivo del curso y requisitos de grupo.
- Recursos necesarios para la capacitación u otras condiciones necesarias.
- En el capítulo de costos, detallar lo pertinente a este ítem

3.4. Pruebas de la solución ofrecida. Indicar si el proceso de pruebas incluye:

- Proceso de pruebas: Describir el proceso que se tiene para gestión de las pruebas del Desarrollador, Técnicas y de usuario.

- Describir el proceso de aseguramiento de la calidad. Detallar un procedimiento para asegurar que las pruebas a realizar por parte del Banco para la aceptación de la solución recibida, contarán con los elementos de calidad necesarios para minimizar el riesgo de ampliar los tiempos estimados para el paso a PRODUCCIÓN.
- Equipo para pruebas. Indicar el equipo que coordinará las pruebas.
- Indicar el equipo por parte del proveedor que atenderá las pruebas los incidentes.
- Indicar el procedimiento para reportar por parte del Banco incidentes o errores que ocurran en las pruebas y el procedimiento de atención. Cuáles son los ANS para su solución.
- Describir cómo serán probadas las funcionalidades actuales y nuevas. Cuál es la propuesta para asegurar que la solución requerida y los nuevos desarrollos cuentan con las debidas pruebas técnicas, la cuales como mínimo deben incluir:
 - ✓ Casos de prueba que contemplen múltiples escenarios de operación. Tener en cuenta escenarios para cargue manual y automática.
 - ✓ Pruebas integrales orientadas a verificar la integridad de operación y de los datos después de la ejecución de diferentes funcionalidades que los comparten.
 - ✓ Pruebas de rendimiento bajo carga
 - ✓ Pruebas de seguridad del software contra ataques
 - ✓ Pruebas de facilidad de uso con usuarios reales.
 - ✓ Pruebas modulares para verificar que la solución ofrecida funciona correctamente.
 - ✓ Pruebas de las interfaces (si se requieren).
 - ✓ Pruebas de funcionamiento del software en el hardware seleccionado
 - ✓ Pruebas para verificar que el servicio ofrecido funciona como se esperaba.
 - ✓ Pruebas de rendimiento (stress) orientada al acceso WEB.
- Indicar el proceso de atención de incidentes y problemas originados por la ejecución de las pruebas.
- El proveedor deberá entregar al Banco los resultados de las pruebas realizadas
- Describir como la solución será probada en ambientes de máxima utilización simulando picos, volúmenes, números de usuarios y en general carga/sobrecarga del sistema.
- Establecer un procesos para hacer más rápidas las pruebas “Celeridad”, con el fin de evitar que se impacten los tiempos estimados para pasó a PRODUCCIÓN.
- El proveedor deberá prever la realización de una prueba de vulnerabilidad antes del paso a PRODUCCIÓN.

3.5. Documentación técnica y de usuario. El proponente seleccionado deberá entregar:

- Documentación técnica y de usuario en español.
- Documentación del proyecto o servicio ofrecido.
- Manual de instalación.
- Manual para el mantenimiento técnico.
- Los manuales deberán cumplir con los estándares especificados en el Manual de Identidad visual y corporativa de Bancóldex
- Deberán entregarse en formato físico y digital
- Debe ser posible descargar del sistema

4 SEGURIDAD DE LA SOLUCIÓN OFRECIDA

El proponente debe describir los aspectos que la solución debe tener para evitar riesgos según el área o campo a la que haga referencia el riesgo. El proponente deberá presentar una matriz de riesgos y sus contingencias, con el fin de disminuir la incertidumbre de prórroga de las actividades detalladas en el cronograma del proyecto.

El proponente debe tener presente al menos los siguientes mecanismos de seguridad a implantar con la herramienta de software que se proponga:

- **Autenticación**

El proponente deberá indicar lo siguiente

:

- ✓ El sistema se adapta para trabajar bajo un esquema Single Sign On.
- ✓ Proceso de confirmación de la identidad del usuario. Antes de que una aplicación pueda autorizar el acceso a un recurso, debe confirmar su identidad. Esta es la primera capa de control de seguridad.
- ✓ Roles de usuarios: La solución debe manejar un control de acceso a las opciones del sistema por roles. Un usuario puede tener asignado uno (1) o más roles.
- ✓ Bloqueo intentos fallidos: Detallar si el sistema ofrecido cuenta con control de acceso al sistema a través de ingreso de usuario y contraseña y si controla los intentos fallidos de registro.
- ✓ Parametrización de la contraseña. Se permite parametrizar la contraseña de acuerdo con políticas internas del Banco referente a número de caracteres, combinación de caracteres.
- ✓ El sistema permite configurar los criterios de creación y cambio de clave del acceso al sistema: tiempo para cambio de clave, caracteres obligatorios, etc.

- **Autorización:**

El proponente deberá indicar el proceso de verificación en caso que un usuario autenticado tenga permiso para obtener acceso a un recurso determinado.

Siguiente capa de seguridad tras la autenticación.

- **Protección de datos:**

El proponente deberá indicar el proceso consistente en proporcionar confidencialidad, integridad y no repudio a los datos.

- **Sistema de control interno (auditorias-logs):**

El proponente deberá indicar el proceso de registro y supervisión de los eventos que se producen en un sistema y que son importantes para la seguridad.

- ✓ Indicar que logs tiene implementados la solución ofrecida.
- ✓ Indicar el proceso de:
 - Registro.

- Consulta. Tiene implementadas consultas que permitan el acceso a estos logs.
 - Permite la consulta de logs a través de opciones de menú u opciones de perfil administrador y se puedan imprimir o exportar a un formato de fácil lectura las consultas.
 - Depuración.
 - Respaldo.
 - ✓ Genera y registra logs sobre las operaciones que un usuario realice en el sistema.
 - ✓ Que información contiene el log. El diseño de los logs debe contener por lo menos la siguiente información: fecha, hora, segundo, comentario.
- **Herramientas de seguridad:** El proponente deberá contar con por los menos las siguientes herramientas de seguridad: Antivirus, antispam, firewall, software para prevenir ataques o intrusiones, entre otros.
 - **Cumplimiento políticas SEGURIDAD DE LA INFORMACIÓN.** El proponente deberá dar respuesta al cumplimiento de las políticas detalladas en el anexo 15: **Políticas del SGSI, Habeas Data, Circular externa 042 de 2012, consideraciones Adicionales.**

5. Servicio de HOSTING.

El proponente deberá proporcionar el servicio de hosting dedicado para alojar la página web. El hosting debe ser dimensionado de tal manera que la página web tenga un óptimo rendimiento y no presente desperdicio de recursos. Igualmente debe contar con los debidos mecanismos de seguridad física y lógica para evitar ataques o intrusiones maliciosas.

A su vez, el proponente detallará el software que se requiere en el hosting para que funcione el CMS:

- El esquema del servicio de hosting dedicado para alojar la página web, teniendo en cuenta los máximos estándares de seguridad que provee el mercado. Debe estar relacionado con la propuesta detallada en el ítem de arquitectura.
- Especificar el esquema de servicio de seguridad que tendrá el servicio de hosting. Accesos no autorizados, ataque de negación de servicio y en general cualquier aspecto relacionado con la estabilidad y seguridad del sitio web en hosting.
- Especificar el esquema de contingencia.
- Se recomienda que el proponente brinde información del tercero que le provee el servicio de hosting (nube).
- El proponente deberá indicar cuáles son los ANS que tiene con el tercero que le provee y deberá presentar los procedimientos de contingencia en caso de caídas o fallas del hosting principal.
- **Se cuenta con WAF.**
- Si se cuenta con un WAF este gestiona ataques de negación de servicio DDoS?
- Se cuenta con servicio de FW

- Análisis de vulnerabilidad al código por lo menos dos veces al año. Hacer directamente al código y otra con las herramientas. Entregar informe de hallazgos
- Tiempo - ANS, para dar respuesta a las vulnerabilidades encontradas.
- Certificados SSL
- Indicar estrategia para hardening “endurecer” el sistema operativo. Se recomienda demostrar que se acogen las buenas prácticas.
- Estrategia para actualizar el hardware y software. Actualización, instalación de parches.

6. Consolidación de respuestas

Se pide a los proponentes consolidar sus respuestas teniendo en cuenta el formato detallado en la tabla adjunta. Cada uno de los ítems, debe tener una respuesta asociada a sus sub-ítem:

| Descripción | CUMPLE | | Detallar la respuesta | Indicar si adjunta documentación adicional e indicar la identificación del documento anexo en la propuesta. |
|---|--------|----|-----------------------|---|
| | SI | NO | | |
| 1- Características generales de la solución | | | | |
| Nombre y versión del producto. Fecha de liberación de la versión presentada. | | | | |
| Idiomas que maneja la solución | | | | |
| Indicar como la solución brinda flexibilidad en la conectividad a la herramienta por parte del usuario final, mostrando la información en línea desde cualquier dispositivo, tales como teléfonos inteligentes, tabletas, equipos de escritorio o portátiles, desde cualquier ubicación. | | | | |
| Indicar el procedimiento de calidad para garantizar que la solución ofrecida incorporará técnicas avanzadas en cuanto a diseño y herramientas actuales para su construcción que no presentarán errores que impidan su normal funcionamiento. | | | | |
| Detallar los módulos que contempla la solución propuesta y hacer una descripción de su alcance. 1- Nombre completo, especificación de compatibilidad con otros sistemas y plataformas sobre las que puede operar. 2- Si requiere licenciamiento, propuesta del esquema adecuado de dicho licenciamiento, teniendo en cuenta los | | | | |

| | | | | |
|---|--|--|--|--|
| ambientes de producción, pruebas y contingencia (si aplica). | | | | |
| Para Gestor de contenido 3- Gestor de Contenido. 4- Con que herramientas ofimáticas y demás herramientas interactúa. | | | | |
| Modo de operación funcional general de la aplicación (localización y distribución de datos, manejo de comunicaciones, modo de procesamiento, etc.) | | | | |
| El sitio web tiene un sitemap que sea un sitemap.xml | | | | |
| Permite integrarse con herramientas de geolocalización, como por ejemplo google maps.? Si el punto anterior tiene respuesta afirmativa, indicar en donde se implantará. | | | | |
| El sistema controla el uso de los caracteres especiales que puedan ingresar los usuarios al configurar y crear los nuevos contenidos, garantizando la correcta funcionalidad de la página y del Portal. | | | | |
| Detallar el cumplimiento que a la fecha tiene implementada la solución para atención de lo pedido por Gobierno en Línea. Especificar como cubre todos sus aspectos y que no está cubierto | | | | |
| Licenciamiento y actualizaciones Detallar el licenciamiento requerido por la solución ofrecida. Se espera que el Proponente ofrezca las licencias en el servicio de hosting. | | | | |
| El proveedor deberá especificar en su propuesta los tiempos de respuesta o latencia que puede ofrecer para el despliegue de las páginas del portal dependiendo de las características de contenido y el número máximo de usuarios concurrentes. | | | | |
| El proveedor deberá especificar en su propuesta otros tiempos. | | | | |
| 5- ARQUITECTURA | | | | |
| Arquitectura de la solución | | | | |
| Diagrama. Donde se muestre claramente la arquitectura del sistema de información a implementar en el proyecto. En ésta se deberá hacer una descripción de todos los componentes que se utilizarán en las diferentes capas. | | | | |
| Arquitectura. Detallar el tipo de arquitectura de la solución ofrecida: Monolítica, WEB, Cliente – Servidor, otra. | | | | |

| | | | | |
|---|--|--|--|--|
| El sistema debe tener un código optimizado para alto rendimiento y velocidad | | | | |
| Alta disponibilidad. Detallar el esquema de alta disponibilidad que se tiene de propuesta para la solución ofrecida. | | | | |
| 3. Arquitectura del software | | | | |
| Sistema Operativo que soporta la solución ofrecida, Bases de Datos: Motor y versiones. | | | | |
| Software base, lenguaje de desarrollo que soporta la solución ofrecida y versión. | | | | |
| Presenta compatibilidad con los estándares html5 y css3. En caso de presentarse, el proponente deberá detallar con que otros estándares presenta compatibilidad. | | | | |
| Interfaces de programación. | | | | |
| Portabilidad. | | | | |
| Tipos de navegadores que soporta. | | | | |
| Presentación de interfaz gráfica: <ul style="list-style-type: none"> • Presentación en diferentes tipos de dispositivos móviles • Indicar los diferentes tipos de Browser que soporta. • Como es el esquema de adaptación a los diferentes tamaños de salida • La interfaz gráfica debe presentar un diseño intuitivo. | | | | |
| Detalle el procedimiento para integración con el directorio activo. | | | | |
| Debe Presentar la facilidad de Streaming Distribución digital de contenido multimedia. | | | | |
| Especificar como presentará los diferentes componentes que hacen parte de gobierno en línea. | | | | |
| La arquitectura de software permite Integrar plugins, extensiones, frameworks o componentes de software para ampliar funcionalidades o adicionar nuevas. | | | | |
| 4. Arquitectura del Hardware. | | | | |
| Detallar en un modelo la arquitectura de hardware que se propone para la solución requerida. Se debe especificar los requerimientos mínimos y óptimos en que trabaja la solución. | | | | |
| Características de los servidores de aplicaciones y base de datos: Tipo de servidores, Asignación de servidores, memoria, Características del procesador, Capacidad discos duros, Tarjetas de Red, Enrutadores, Características de disponibilidad y escalabilidad, | | | | |
| Capacidad de almacenamiento (datos, archivos, videos e imágenes) | | | | |

| | | | | |
|---|--|--|--|--|
| 5. Arquitectura de comunicaciones. | | | | |
| Características de disponibilidad y escalabilidad | | | | |
| Velocidad del canal de comunicaciones | | | | |
| Medición y registro de parámetros del uso del ancho de banda | | | | |
| Evaluación y administración del reúso | | | | |
| Infraestructura física | | | | |
| Sistema de administración de redes | | | | |
| Disponibilidad del servicio del canal (Uptime requerido 99.9995%) | | | | |
| 6. Generalidades soporte, mantenimiento correctivo y evolutivo | | | | |
| Indicar el proceso y que metodologías de actualización e instalación de una versión y demás detalles que se consideren necesarios para que el Banco pueda evaluar los servicios de soporte, actualización y mantenimiento. | | | | |
| Esquema para garantizar que las herramientas, componentes y demás piezas de software que integran la solución presentada, serán actualizadas con el fin de mantener el soporte por parte del fabricante | | | | |
| Indicar la política de cantidad de versiones que se liberan por año | | | | |
| Tipo de soporte y mantenimiento que se ofrecerá en el contrato. | | | | |
| Tiempos de entrega y los informes que se usarán para el seguimiento. | | | | |
| El proponente deberá entregar como mínimo la siguiente documentación: Documentación de usuario, operativa, técnica, versión del producto, Fecha de liberación de la versión, mejoras o correcciones implementadas en la versión, prerequisites para la actualización, tiempos estimados para la actualización, otros. | | | | |
| Detallar porcentaje de la licencia para mantenimiento anual, sobre el costo del licenciamiento de mantenimiento y como se pactaran las prórrogas. | | | | |
| Esquema para garantizar que las actualizaciones o correcciones de los navegadores actuales del mercado, puedan mantener la funcionalidad en cada uno de ellos. | | | | |
| Indicar si Los ANS propuestos estiman que el tiempo máximo de atención de un incidente no deberá exceder las dos (2) horas y su | | | | |

| | | | | |
|---|--|--|--|--|
| solución dependiendo la complejidad o gravedad no deberá exceder de las 72 horas | | | | |
| 7. Soporte y mantenimiento correctivo. | | | | |
| Esquema del servicio de soporte y mantenimiento correctivo para la solución o para los componentes que presente en su propuesta | | | | |
| Niveles de acuerdos de servicio. Servicios, tiempos de respuesta, disponibilidad, prioridades, responsabilidades, documentación, garantías y penalizaciones. | | | | |
| Esquema de las diferentes líneas de soporte (teléfono, mail, online, presencial, entre otros) | | | | |
| Esquemas de monitoreo, seguimiento y control, incidencia, problemas, acuerdos de servicio (SLA), niveles de acuerdos de servicio, acuerdos de operación (OLA), niveles de atención, controles de cambio, manejo de versiones, Configuraciones (aplicación, base de datos, servidores) | | | | |
| 8. Mantenimiento evolutivo. | | | | |
| Esquema del servicio de mantenimiento evolutivo | | | | |
| Niveles de acuerdos de servicio. Servicios, tiempos de respuesta, disponibilidad, prioridades, responsabilidades, documentación, garantías y penalizaciones. | | | | |
| Esquema definido para nuevos requerimientos: Capacitación, consultoría, desarrollo, disponibilidad para contar con dichos servicios. | | | | |
| 9. Continuidad del servicio de TIC. | | | | |
| Servicio de Contingencia. Describir el servicio de contingencia que tendrá la solución ofrecida a nivel de aplicación y servicio de hosting. Cuenta con servicio de datacenter alternativo? | | | | |
| Disponibilidad del servicio. Indicar los ANS's, los indicadores asociados a continuidad, los cuales se esperan que estén en un porcentaje de disponibilidad del sitio WEB del 99.96% | | | | |
| Indicar cuál es el plan de Continuidad del servicio de soporte y mantenimiento para el sitio WEB y el HOSTING. | | | | |

| | | | | |
|--|--|--|--|--|
| Indicar las políticas de respaldo y recuperación del sistema: Datos, aplicación, hosting. | | | | |
| Indicar el proceso de contingencia para contar con la disponibilidad de los respaldos realizados. | | | | |
| Indicar los ANS establecidos para contar con procesos de recuperación y disponibilidad de los datos y aplicación. | | | | |
| 10. Esquema de Implantación y Adecuación. | | | | |
| <p>Describir la metodología que será utilizada durante la adecuación e implantación de la solución ofrecida:</p> <ul style="list-style-type: none"> • Marco de referencia de la metodología a utilizar. Debe estar alineada a mejores prácticas. • Planeación detallada del proceso de instalación y prueba. Incluir una matriz RACI que identifique los roles y sus responsabilidades, tanto de recursos del Proponente como del Banco. • Indique si la instalación de la solución está a cargo del proveedor en los ambientes de pruebas y producción. • Estimar el tiempo que conlleva la instalación de la solución • Indicar si hay proceso de capacitación y si es así, que roles por parte del Banco debe participar. • Indicar si el proceso de instalación está documentado. • Proceso de estimación de tiempo de desarrollo y adecuación para los requerimientos funcionales que se comprometen a realizar. • Esquema de funcionamiento. | | | | |
| Indicar el proceso para ajustar la solución propuesta de acuerdo con las adecuaciones o extensiones necesarias para que la solución ofrecida cumpla totalmente con los requerimientos definidos en estos términos. | | | | |
| 11. Transición y Conversión de datos/contenidos para la operatividad de la solución | | | | |
| Presentar un plan de cargue inicial y migración de datos para la operatividad de la solución indicando la participación del Banco | | | | |

| | | | | |
|---|--|--|--|--|
| y del proponente y qué condiciones se requieren para obtener una funcionalidad exitosa. Se espera que el porcentaje de migración del contenido actual frente a la nueva arquitectura esté entre un 30% a 40%. | | | | |
| 12. Capacitación que brindará a la solución ofrecida. | | | | |
| Tipo de capacitación: Técnica, operación, administración y usuario. | | | | |
| Contenido de cada curso. | | | | |
| Grupo objetivo del curso y requisitos de grupo. | | | | |
| Recursos necesarios para la capacitación u otras condiciones necesarias. | | | | |
| En el capítulo de costos, detallar lo pertinente a este ítem | | | | |
| 13. Pruebas de la solución ofrecida. Indicar si el proceso de pruebas incluye: | | | | |
| Proceso de pruebas: Describir el proceso que se tiene para gestión de las pruebas del Desarrollador, Técnicas y de usuario. | | | | |
| Describir el proceso de aseguramiento de la calidad. Detallar un procedimiento para asegurar que las pruebas a realizar por parte del Banco para la aceptación de la solución recibida, contarán con los elementos de calidad necesarios para minimizar el riesgo de ampliar los tiempos estimados para el paso a PRODUCCIÓN. | | | | |
| Equipo para pruebas. Indicar el equipo que coordinará las pruebas. | | | | |
| Indicar el procedimiento para reportar por parte del Banco incidentes o errores que ocurran en las pruebas y el procedimiento de atención. Cuáles son los ANS para su solución. | | | | |
| Describir cómo serán probadas las funcionalidades actuales y nuevas. Cuál es la propuesta para asegurar que la solución requerida y los nuevos desarrollos cuentan con las debidas pruebas técnicas, la cuales como mínimo deben incluir: <ul style="list-style-type: none"> ✓ Casos de prueba que contemplen múltiples escenarios de operación. Tener en cuenta escenarios para cargue manual y automática. ✓ Pruebas integrales orientadas a verificar la integridad de operación y de los datos después de la ejecución de diferentes funcionalidades que los comparten. ✓ Pruebas de rendimiento bajo carga | | | | |

| | | | | |
|---|--|--|--|--|
| <ul style="list-style-type: none"> ✓ Pruebas de seguridad del software contra ataques ✓ Pruebas de facilidad de uso con usuarios reales. ✓ Pruebas modulares para verificar que la solución ofrecida funciona correctamente. ✓ Pruebas de las interfaces (si se requieren). ✓ Pruebas de funcionamiento del software en el hardware seleccionado ✓ Pruebas para verificar que el servicio ofrecido funciona como se esperaba. ✓ Pruebas de rendimiento (stress) orientada al acceso WEB. | | | | |
| Indicar el proceso de atención de incidentes y problemas originados por la ejecución de las pruebas. | | | | |
| El proveedor deberá entregar al Banco los resultados de las pruebas realizadas | | | | |
| Describir como la solución será probada en ambientes de máxima utilización simulando picos, volúmenes, números de usuarios y en general carga/sobrecarga del sistema. | | | | |
| Establecer un procesos para hacer más rápidas las pruebas "Celeridad", con el fin de evitar que se impacten los tiempos estimados para pasó a PRODUCCIÓN. | | | | |
| El proveedor deberá prever la realización de una prueba de vulnerabilidad antes del paso a PRODUCCIÓN. | | | | |
| 14. Documentación técnica y de usuario | | | | |
| Documentación técnica y de usuario en español. | | | | |
| Documentación del proyecto o servicio ofrecido. | | | | |
| Manual de instalación. | | | | |
| Manual para el mantenimiento técnico. | | | | |
| Los manuales deberán cumplir con los estándares especificados en el Manual de Identidad visual y corporativa de Bancóldex | | | | |
| 14. SEGURIDAD DE LA SOLUCIÓN OFRECIDA | | | | |
| <ul style="list-style-type: none"> • Autenticación • El sistema se adapta para trabajar bajo un esquema Single Sign On. • Proceso de confirmación de la identidad del usuario. Antes de que una aplicación pueda autorizar el acceso a un recurso, debe confirmar su identidad. Esta es la primera capa de control de seguridad. | | | | |

| | | | | |
|--|--|--|--|--|
| <ul style="list-style-type: none"> • Roles de usuarios: La solución debe manejar un control de acceso a las opciones del sistema por roles. Un usuario puede tener asignado uno (1) o más roles. • Bloqueo intentos fallidos: Detallar si el sistema ofrecido cuenta con control de acceso al sistema a través de ingreso de usuario y contraseña y si controla los intentos fallidos de registro. • Parametrización de la contraseña. Se permite parametrizar la contraseña de acuerdo con políticas internas del Banco referente a número de caracteres, combinación de caracteres. • El sistema permite configurar los criterios de creación y cambio de clave del acceso al sistema: tiempo para cambio de clave, caracteres obligatorios, etc. | | | | |
| <ul style="list-style-type: none"> • Autorización: Indicar el proceso de verificación en caso que un usuario autenticado tenga permiso para obtener acceso a un recurso determinado. Siguiendo capa de seguridad tras la autenticación. | | | | |
| <ul style="list-style-type: none"> • Protección de datos: Indicar el proceso consistente en proporcionar confidencialidad, integridad y no repudio a los datos. | | | | |
| <ul style="list-style-type: none"> • Sistema de control interno (auditorías-logs): ✓ Indicar que logs tiene implementados la solución ofrecida. ✓ Indicar el proceso de: <ul style="list-style-type: none"> ▪ Registro. ▪ Consulta. Tiene implementadas consultas que permitan el acceso a estos logs. ▪ Permite la consulta de logs a través de opciones de menú u opciones de perfil administrador y se puedan imprimir o exportar a un formato de fácil lectura las consultas. ▪ Depuración. ▪ Respaldo. ✓ Genera y registra logs sobre las operaciones que un usuario realice en el sistema. ✓ Que información contiene el log. El diseño de los logs debe contener por lo menos la siguiente información: fecha, hora, segundo, comentario. | | | | |
| <p>Herramientas de seguridad: El proponente deberá contar con por los menos las siguientes herramientas de seguridad:</p> | | | | |

| | | | | |
|--|--|--|--|--|
| Antivirus, antispam, firewall, software para prevenir ataques o intrusiones, entre otros. | | | | |
| <ul style="list-style-type: none"> • Cumplimiento. Como cumple con: (Anexo 15 SEGURIDAD DE LA INFORMACIÓN) - CIR 42 - Protección de Datos Personales Ley 1581 de 2012. - Ley 1712 de 2014 de transparencia y del derecho de acceso a la información pública nacional. - Acuerdo Interbancario sobre Requerimientos mínimos de seguridad para los servicios transaccionales ofrecidos a entidades públicas, de noviembre 20 de 2009. - Ley de Habeas Data 1266 de 2008. | | | | |
| 16. Servicio de HOSTING. | | | | |
| El esquema del servicio de hosting dedicado para alojar la página web, teniendo en cuenta los máximos estándares de seguridad que provee el mercado. Debe estar relacionado con la propuesta detallada en el ítem de arquitectura. | | | | |
| Especificar el esquema de servicio de seguridad que tendrá el servicio de hosting. Accesos no autorizados, ataque de negación de servicio y en general cualquier aspecto relacionado con la estabilidad y seguridad del sitio web en hosting. | | | | |
| Especificar el esquema de contingencia. | | | | |
| Si aplica, brindar información del tercero que le provee el servicio de hosting (nube). | | | | |
| Indicar cuáles son los ANS que tiene con el tercero que le provee y deberá presentar los procedimientos de contingencia en caso de caídas o fallas del hosting principal. | | | | |
| Se cuenta con WAF. Si se cuenta con un WAF este gestiona ataques de negación de servicio DDoS? | | | | |
| Se cuenta con servicio de FW | | | | |
| Análisis de vulnerabilidad al código por lo menos dos veces al año. Hacer directamente al código y otra con las herramientas. Entregar informe de hallazgos | | | | |
| Tiempo - ANS, para dar respuesta a las vulnerabilidades encontradas. | | | | |
| Certificados SSL | | | | |
| Indicar estrategia para hardening "endurecer" el sistema operativo. Se | | | | |

| | | | | |
|---|--|--|--|--|
| recomienda demostrar que se acogen las buenas prácticas. | | | | |
| Estrategia para actualizar el hardware y software. Actualización, instalación de parches. | | | | |