RESPUESTA A INQUIETUDES
INVITACIÓN N° 00042

TÉRMINOS DE REFERENCIA PARA: Contratar, configurar e implementar una solución tecnológica que soporte la gestión de riesgos y eventos operacionales, así como la gestión de auditoría en todas sus etapas.

Pregunta: 10. Para los resultados finales de impacto y probabilidad residual (basada en controles y basada en eventos) favor indicar la escala de rangos para su ubicación, ejemplo: Muy baja 0-20, baja: 20.1-xxx para tener la escala correcta y generar la ubicación de manera exitosa.
Respuesta: La tabla de probabilidad residual es la misma enviada en el Anexo 10 - D.Anexos, 1.1. Riesgo Inherente SARO.

La tabla de impacto residual sería:

Insignificante: entre 0,000000000% y 20,000%
Menor: entre 20,000000001% y 40,000%
Moderado: entre 40,000000001% y 60,000%
Importante: entre 60,000000001% y 80,000%
Mayor: entre 80,000000001% y 100,00%

Pregunta: 21. De acuerdo al criterio "..la cual consiste en que un control mitigue la probabilidad o el impacto hasta un máximo del 50% del valor inherente, dependiendo de la sumatoria de los criterios de efectividad, lo cual determina el porcentaje de mitigación". En el ejercicio presentado en todos los casos se multiplica por el 50% pero de acuerdo al texto se indica que "hasta un máximo de 50%" es decir que a partir de algún resultado de la sumatoria de criterios de efectividad es que se determina sí es 50, 40, 30 etc ó siempre será 50 de acuerdo al ejemplo descrito?
Respuesta: Confirmamos que en la metodología actual siempre se multiplica por el 50% de esta manera se evita que un control mitigue más del 50% de un riesgo inherente.

Pregunta: 20. Se entiende que con base a la entrevista del dueño de proceso se tiene la ubicación del impacto inherente de acuerdo a la escala descrita que tiene una columna con los descriptores para tipo de impacto económico y reputacional. La inquietud es sí la calificación va sobre la fila teniendo en cuenta ambos descriptores o sí el dueño de proceso puede decir que un riesgo tiene impacto económico en insignificante pero en reputación en mayor, en ese caso cómo se obtendría la impacto teniendo en cuenta el mayor, promedio o promedio ponderado?
Respuesta: En este caso se toma el más ácido. Es decir, si la pérdida reputacional puede ser más grande que la económica, evaluamos el impacto del riesgo considerando la tabla asociada al criterio reputacional.

Pregunta: 19. El documento "Apoyo Evaluación Funcional y Técnico" solicitado en los adjuntos a enviar, equivale al anexo 10?
Respuesta: El Anexo Técnico o Anexo 10 debe estar respondido en su totalidad dentro del documento que detalle la presentación de la propuesta técnica, razón por la cual, se envía el Anexo Técnico en WORD.

El campo "Apoyo Evaluación Funcional y Técnico" puede contener la misma información o dejarse vacío ya que no es obligatorio en el sistema.

Pregunta: 18. En los documentos a adjuntar se solicita un formato de

Experiencia Especifica del Proponente, sin embargo no se evidencia en los anexos enviados. Por favor me indican a cual de ellos equivale?
Respuesta: No se cuenta con un formato definido para la presentación de esta información. El proponente debe unificar todas las certificaciones de experiencia en un único documento que debe ser cargado en el campo "Formato Experiencia Específica del Proponente".

Pregunta: 17. Por favor suministrar detalle o brindar ejemplos de indicadores de riesgos KRI.
Respuesta: Algunos de los KRIs que tenemos en el Banco son:
1. Tecnología: (Eventos relacionados con fallas tecnológicas / Total eventos) *100%. El resultado del indicador para cada mes es el promedio móvil simple de los doce últimos meses.

2. Eventos externos: (Eventos originados por eventos externos/ Total eventos) *100%. El resultado del indicador para cada mes es el promedio móvil simple de los doce últimos meses.

3. Procesos: (Eventos relacionados con fallas en procesos / Total eventos) *100%. El resultado del indicador para cada mes es el promedio móvil simple de los doce últimos meses.

4. Infraestructura: (Eventos originados fallas en infraestructura/ Total eventos) *100%. El resultado del indicador para cada mes es el promedio móvil simple de los doce últimos meses.

5. Recurso Humano: (Eventos originados por recurso humano/ Total eventos) *100%. El resultado del indicador para cada mes es el promedio móvil simple de los doce últimos meses.
6. Desplazamiento de riesgos por la materialización de eventos: Corresponde a los riesgos que presentan un desplazamiento en su probabilidad debido a la materialización de riesgos operacionales.
Su fórmula es: Número de riesgos que presentan desplazamiento en la probabilidad / Total riesgos vigentes.

Pregunta: 16. "Es deseable, no requisito, que la solución cuente con la posibilidad de extraer gráficos basados en los informes que permitan conocer el estado de la gestión de riesgos del Banco. Gráficos de torta, de barras, etc".
A qué se refiere con extraer? Se consulta dado que, el sistema cuenta con un motor de business intelligence que permite generar las gráficas para consulta en línea desde la plataforma.
Respuesta: Este punto está orientado a que el sistema permita exportar esas gráficas que tiene el business intelligence a un excel o un word para poder utilizarlos en reportes o informes internos. No importa que no sean editables estas gráficas.

Pregunta: 15. ¿En cuanto al flujo 1 y 2 de aprobación de Riesgo, detallar que información diligencia el funcionario oro y hasta qué punto llegan para enviar a líder y vicepresidente sería la caracterización, calificación inherente, controles y riesgo residual ó hasta tratamiento?

¿Ambos estarían habilitados para editar todos los campos o uno complementa al otro en ambos escenarios?
Respuesta: El funcionario ORO diligencia toda la información de riesgos y controles. Al Líder y vicepresidente debería llegarles esta información completa.

Lo que hacemos hoy en día solo editan los funcionarios ORO y los otros actores solo envían retroalimentación con observaciones sin modificar directamente Riesgos o Controles. Podría mantenerse de esta forma sin problema. También, si la herramienta lo permite, sería válido que el líder pueda también editar sus riesgos y sus controles, con el fin de evitar reprocesos. Esto se puede acordar durante la fase de entendimiento.

Pregunta: 14. Por favor confirmar que estos campos son alfanúmericos, dado que generalmente se tienen criterios asociados a dichos parámetros del control como por ejm: Naturaleza del control: Manual, automático.
Respuesta: Actualmente estos campos visualmente para los usuarios de la oficina de riesgo operativo son alfanuméricos, no obstante, es importante aclarar que a partir de estos campos hay cálculos que realiza la

metodología de evaluación de riesgos. Es decir, puede que lo que el usuario ve en pantalla sea un "Automático" o "Manual", pero por debajo el sistema esté enviando el valor equivalente al 0.33 o al 0.20.

Pregunta: 13. Por favor ampliar detalle del campo "estado", con un ejemplo de uso, dado que se está mapeando como un campo alfanumérico. Se consulta dado que, en nuestro sistema se maneja un contexto de “estado” alusivo a los estados del flujo de la gestión del riesgo: Identificado, calificado, con controles, etc. Este mismo comentario aplica para los campos de plan de acción dado que registra alfanúmerico. Es importante dado que estos estados son estándar del sistema y no son parametrizables, por tanto de acuerdo a respuesta aplicarán dichas claridades
Respuesta: El campo "Estado" al cual hacemos referencia en este punto es para uso interno y no está relacionado con los flujos propuestos. Esto tiene que ver con que en algún punto se puede tener un riesgo evaluado con todos sus controles pero el dueño de proceso aún no lo ha aprobado y por tanto no podemos asegurar que está "Vigente".

Los valores que tenemos actualmente para este campo son: Vigente, Por Aprobar, Eliminado.

No se pretende cambiar el campo estándar del sistema mencionado por el proveedor. Lo que propondríamos sería tener un campo descriptivo para nuestro "Estado" que sea diferente al del sistema.

Pregunta: 12. Por favor ampliar detalle de este criterio: "La solución tecnológica debe permitir la configuración de una estructura de riesgos y controles que facilite la vinculación entre estos". A qué hace referencia estructura que facilite la vinculación?. Se refiere a que sea identificable en el sistema cuales son los controles que mitigan el riesgo o cual es la relación que se requiere?
Respuesta: Lo ideal es que podamos tener un listado en el cual se puedan ver todos los riesgos y otro listado en el que se tengan todos los controles. El objetivo es que se puedan reutilizar controles para los diferentes riesgos y que no haya que crear el mismo control tantas veces como riesgos lo tengan. Por ejemplo: Existe un control asociado a la mesa de servicio que brinda soporte a los diferentes aplicativos. Si se tienen 100 riesgos asociados a los aplicativos en el Banco, se espera que sobre los 100 riesgos se pueda asociar el mismo control de la mesa de servicio y no que haya que crear un control de mesa de servicio por cada riesgo.

Pregunta: 11. Por favor ampliar detalle sobre el concepto de mapa corporativo dado que cuando se indica varios procesos agrupados se confunde con el siguiente criterio que se puedan asociar diferentes procesos a un riesgo. Por tanto brindar más información para detallar correctamente el alcance de ambos criterios.
Respuesta: Se busca un mapa que permita consolidar el perfil de riesgos (inherente vs residual) del Banco. Esto quiere decir que debe incluir todos los riesgos asociados a todos los procesos. No se trata de una evaluación específica o diferente a la presentada en la metodología sino de una vista de un mapa. Generalmente, al realizar agrupaciones de riesgos o de procesos, se utilizan los promedios de las calificaciones en probabilidad y promedios de calificaciones en impacto para realizar la ubicación sobre el plano cartesiano. Esto aplica también para los mapas de producto, canal, proyecto, etc.
Es importante aclarar que un mismo riesgo puede ser asociado a varios procesos en el Banco. Por ejemplo: El riesgo de indisponibilidad de servicios públicos es un riesgo que afecta todos los procesos del Banco y lo ideal sería crear un solo riesgo de este tipo que se vea en los mapas de los diferentes procesos, en lugar de crear 40 riesgos (uno por proceso) que evidencien la indisponibilidad de servicios públicos.

Pregunta: Agradecemos revisar si este requerimiento se puede modificar para que no aplique de manera tan específica:" Certificado de existencia y representación legal de los proponentes y demás documentos los siguientes aspectos, (i) Que el objeto social principal del proponente se relacione con el diseño, desarrollo y/o implementación de servicios tecnológicos en la gestión de riesgos operacionales, gestión de eventos de riesgo operacional y auditoría;" ya que el objeto social de las empresas suelen registrarse de manera más amplia, incluso con códigos de actividades generales o simplemente puede ser diferente y no tan específico.

Respuesta: También se tienen en cuenta los objetos sociales orientados al soporte, mantenimiento y actualizaciones sobre soluciones tecnológicasen la gestión de riesgos operacionales, gestión de eventos de riesgo operacional y auditoría.

Pregunta: Agradecemos nos puedan confirmar si en caso de que se presente al proceso directamente el fabricante de la solución del software ¿Las certificaciones de experiencia a presentar pueden ser las que los clientes le hayan expedido a sus canales de distribución y en donde aparezca el suministro de la solución del software del fabricante?
Respuesta: Sí. Se acepta la experiencia aportada por los canales de distribución siempre y cuando esta contenga explícito el software sobre el cual se emite certificación.

Pregunta: Agradecemos nos puedan indicar las condiciones, criterios jurídicos, financieros u otros, para poder establecer consorcios o uniones temporales para la presentación al proceso.
Respuesta: Aunque la presente convocatoria no tenía contemplado este tipo de proponentes, se realizará una adenda que permita participar a las figuras de Unión Temporal o Consorcio. En términos generales, las condiciones serán las mismas de los presentes términos de referencia y, en cuanto a la capacidad financiera, por lo menos uno de los miembros del Consorcio o Unión Temporal que conforman el proponente debe tener la capacidad financiera suficiente exigida.

Pregunta: ¿Se requiere la inclusión de los riesgos identificados y metodología para su gestión definida por la entidad o es necesario realizar una revisión para verificar la suficiencia de los riesgos identificados, es decir una consultoría?
Respuesta: Actualmente el Banco cuenta con el inventario de riesgos y controles con sus respectivas calificaciones y estos serán cargados a la solución contratada. No se requiere consultoría.

Pregunta: Términos de referencia: "Tipo de servicio ofrecido (configuración en nube del proveedor o en infraestructura del Banco)."
COMENTARIO: Por favor aclarar esta parte de los términos puesto que de acuerdo con el objetivo el servicio requerido es un Software como Servicio (SaaS) y en el texto se señala que se puede optar por la alternativa de que la infraestructura sea en el Banco.
Respuesta: Se prefiere una implementación en nube, no obstante, el proveedor puede proponer realizar la configuración de su servicio de arrendamiento sobre su infraestructura o nube o puede proponer la implementación en infraestructura del Banco, siempre y cuando se trate de arrendamiento y no compra de software. En caso de proponer hacerlo sobre la infraestructura del Banco, se debe aclarar cuáles son los requisitos de hardware y software para la implementación.

Pregunta:
anexo_no_1_politicas_de_seguridad_de_la_informacion_y_ciberseguridad_para_proponentes_y_proveedores_de_bancoldex_4
2. Cumplir con las políticas de administración de usuarios que se encuentran en el Sistema de Gestión de Seguridad de la Información (SGSI) del Banco.
COMENTARIO: Se puede suministrar por favor las políticas de administración de usuarios que se encuentran en el Sistema de Gestión de Seguridad de la Información (SGSI) del Banco para poder revisar el cumplimiento y aceptación de las mismas.
Respuesta: Gestión de accesos, identidades y contraseñas

1. Bancóldex buscará soluciones de nube integradas con el Directorio Activo de Windows que administra por el Departamento de Tecnología, de ser posible utilizando en toda su extensión definiciones y atributos de unidades organizativas previamente definidas, políticas de grupo y de servicios de red. Cuando la autenticación no esté integrada con el directorio activo de Windows, la solución debe permitir parametrizar las condiciones de las contraseñas tales como: su longitud mínima, el tiempo con el cual los usuarios deben hacer el cambio de contraseña, llevar registro de estas e impedir su reúso.

2. El proceso de autenticación, autorización y gestión periódica de contraseñas para el acceso a servicios ofrecidos por las soluciones de nube cumplirá las políticas definidas por el Banco en esa materia.

3. Bancóldex tendrá bajo su control la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos, así como a las plataformas, aplicaciones y bases de datos que operen en la nube, dependiendo del modelo de servicio contratado.

4. Las conexiones desde y hacia infraestructuras de nube utilizadas por el Banco, deben transitar por el Firewall de la red local.

5. En Bancóldex los accesos a usuarios de los servicios de nube serán habilitados bajo el principio del mínimo privilegio y de acuerdo con los roles y responsabilidades definidos según el cargo desempeñado.

6. El almacenamiento y transporte de contraseña deben ser cifrados.

7. El aplicativo debe permitir al administrador generar contraseña de manera automática y aleatoria.

8. La aplicación debe solicitar cambio de contraseña en el primer ingreso.

9. El campo de contraseña debe ser cifrado para que no pueda ser visualizada en el momento que el usuario la digite.

Pregunta:
anexo_no_1_politicas_de_seguridad_de_la_informacion_y_ciberseguridad_para_proponentes_y_proveedores_de_bancoldex_4
2. Asegurar que, al término del contrato, toda información, software, y demás elementos tecnológicos de propiedad del Banco serán eliminados de manera segura de los equipos del proveedor, cumpliendo con la obligación de confidencialidad y/o atendiendo el acuerdo de confidencialidad que para el efecto se hubiese suscrito.
COMENTARIO: Comedidamente solicitamos a la entidad que tenga en cuenta que por tema de retención documental y por requerimiento de reguladores, no se puede eliminar ni devolver toda la información recibida para el cumplimiento de las obligaciones adquiridas, en la medida de lo posible se devolverá o eliminará la que no sea requerida, por lo que solicitamos que tenga en cuenta que se devolverá toda la información salvo aquellos documentos que respalden informes u opiniones emitidas por el CONTRATISTA, (papeles de trabajo), den soporte ante reclamaciones, quejas o requerimientos judiciales o aquellos que no puedan ser devueltos por temas de retención documental y por requerimiento de reguladores.

Respuesta: El objetivo de este punto es que se garantice que se cuenta con procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio, como lo estipula la normatividad colombiana aplicable.

De acuerdo con la CE005 de 2019 expedida por la SFC, el proveedor debe contemplar el borrado seguro de los datos existentes en los medios de almacenamiento cuando finalice el contrato, cuando lo solicite el Banco o cuando el proveedor de servicios en la nube elimine y/o reemplace dichos medios.

Finalmente, y para mayor claridad, es necesario tener en cuenta que la información a eliminar, una vez el Banco cuente con una copia completa de la misma, es la que se contendrá en la plataforma ofrecida como servicio y NO la asociada a la gestión del contrato como tal. En virtud de lo anterior, se espera que, una vez finalizado el contrato, el proveedor no tenga más acceso a los datos de propiedad exclusiva de Bancóldex como son los concernientes a la gestión de riesgos y auditoría.

Pregunta: Otros requerimientos no funcionales transversales de la solución

Es deseable, no requisito que la solución obtenga la información de arquitectura de procesos y arquitectura de tecnología desde las plataformas que actualmente tiene el Banco para tal fin (Mega).
PREGUNTA: Por favor indicar las capacidades que tiene la solución Mega para exponer la información a ser obtenida por la solución GRC bajo las condiciones requeridas por el Banco. Adicionalmente, por favor indicar la periodicidad con la que se debe realizar la actualización de dicha información
Respuesta: En esta implementación no se contemplan integraciones adicionales salvo que el proponente seleccionado presente Mega como la solución a proveer puesto que nativamente ya traería la información. Por tal razón, se tiene como deseable y no será criterio de evaluación.

Pregunta: Otros requerimientos no funcionales transversales de la solución
La solución debe permitir manejar y conservar la data histórica ante cambios de metodologías o de estructuras de referencia (por modelos, por bases de datos, etc.).
PREGUNTA: Por favor aclarar a qué se refieren con "por modelos, por bases de datos, etc."
Respuesta: Si por alguna razón el proponente debe realizar actualización sobre su modelo de base de datos o su tipo de motor, esto no debe afectar la data histórica de la información de gestión de riesgos. El proveedor debe garantizar que posteriormente se podrá hacer la consulta sobre la misma y para nosotros, el cambio debería ser transparente.

Pregunta: 1.6 Requerimientos no funcionales
La solución debe permitir contar con un repositorio o base de datos de archivos (base documental) y así mismo garantizar el almacenamiento, conservación y custodia de la información de las auditorías y sus papeles de trabajo bajo normatividad colombiana vigente (SFC y Archivo General de la Nación, Normas de Auditoría, entre otras)
PREGUNTA: Por favor indicar el tamaño de almacenamiento estimado que se requiere para el repositorio de archivos, así como la magnitud proyectada de su incremento anual. Adicionalmente, podrían indicarnos por favor el tamaño promedio de los archivos a cargar en el repositorio?
Respuesta: Los archivos a almacenar son documentos de office y los generados por la herramienta (reportes y bases de datos de Planeación Anual), sopores de cada auditoría (documentos de word, PPT), y papeles de trabajo (Office). En promedio se utilizan 15GB almacenamiento anual.

Pregunta: 1.5.4 Ejecución de las auditorías
Debe permitir integrar e indexar los papeles de trabajo respectivos a cada proyecto de auditoría (integración con Office365 y Onedrive dispuestos por el Banco).
PREGUNTA: Por favor aclarar si se requiere adjuntar la documentación dentro de la solución o sólo hacer un link a fuentes externas donde estarán almacenados dichos documentos. Por ampliar como se espera la integración mencionada.
Respuesta: El Banco cuenta con la herramienta OFFICE 365, la cual incluye Onedrive, Sharepoint, Planner, y demás herramientas. El objetivo es no generar duplicidad de documentos en Office 365 y en la herramienta, si esta cuenta con la opción de subir documentos y editarlos en línea sin requerir descargarlos y generar nuevas versiones, puede hacerse desde la herramienta directamente. Se busca la opción mas eficiente posible, en temas de accesibilidad, administración y capacidad.

Pregunta: 1.5.4 Ejecución de las auditorías
Debe permitir llevar trazabilidad de toda la ejecución de los trabajos (tiempos de ejecución de actividades, alertas e indicadores de operación).
PREGUNTA: Para los indicadores de operación, por favor indicar si sólo se refiere a cálculos que se generan con la información del trabajo de auditoría o se requiere generar un formulario con toda la caracterización del indicador (nombre, tipo, frecuencia, umbrales, tendencias, historial, etc.)
Respuesta: Se refiere a indicadores y cumplimiento con base en la información del trabajo, fechas estamadas vs reales, & cumplimiento, etc.

Pregunta: 1.5.3 Planeación de las auditorías

La solución debe integrar (cargar o ingresar) a los campos del formato de pre-planeación, los insumos asociados (normas, procesos, proyectos, metas, controles y riesgos - Planeación anual, GRC, Información y/o protección de activos), para determinar los objetivos y alcance de cada auditoría
PREGUNTA: Por favor aclarar a qué se refieren con los insumos GRC, información y/o protección de activos.
Respuesta: GRC, se refiere al enfoque que se definió dar a la auditoría cuando se defininión en el Plan Anual (Gobierno, Riesgo y/o cumplimiento), y los activos involucrados en la actividad a auditar, que se deben tener en cuenta.

Pregunta: 1.5.3 Planeación de las auditorías
La solución debe permitir la definición y parametrización del formato de Pre-planeación de Auditoría
PREGUNTA: Por favor aclarar si este formato corresponde a la Planeación de cada una de las auditorías, o en caso negativo, qué debe contener este formato?
Respuesta: Sí, es un formato que se diligencia previo al inicio de cada una de las auditorías.

Pregunta: Entregables,
TERCER ENTREGABLE: EL CONTRATISTA deberá acompañar al Banco en el proceso de despliegue en ambiente de producción una vez las pruebas de usuarios sean ejecutadas a satisfacción. Se debe incluir en este aspecto el cargue, configuración y certificación de la información inicial para las funcionalidades de gestión de riesgos y gestión de auditoría.

¿Solicitamos aclarar, Cual es el alcance del acompañamiento que tiene que hacer el proveedor?

Por favor precisar el volumen de información que requieren sea cargado en producción como “Información inicial”. Cantidad de registros, número de archivos, fuentes de información y la antigüedad (¿de este año o años anteriores?).
Respuesta:
En el caso de Riesgo Operacional, se cuenta con un inventario aproximado de 800 riesgos con 2100 controles. Adicionalmente, se espera cargar la Base Histórica de Eventos que cuenta con aproximadamente 9000 registros y cuyo crecimiento estimado anual es de 3000 registros.

En el caso de la Auditoría Interna, la información a cargan serán los Planes de Mejora históricos abiertos y cerrados (aproximadamente 1.400 registros). Adicionalmente los resultados de las auditorías realizadas durante los últimos 5 años

Pregunta: 1.5.1 Inventario y cargue de entes auditables
La solución debe permitir el cargue de otros insumos, ejemplo: proyectos, activos de información, resultados de evaluaciones de terceros, resultados de auditorías anteriores, etc
pregunta: Por favor indicar qué información se carga de evaluaciones de terceros y qué tipo de evaluaciones son
Respuesta: Se cargará el ente que emite la observación, las observaciones (título y detalle), Planes de Acción, responsables, fechas de compromiso y avances.

Pregunta: 1.3.1 Roles y perfiles
Si la solución tecnológica permite administrar diferentes metodologías de riesgos, es deseable, no requisito, que se puedan tener administradores funcionales independientes por cada metodología (SARO, SGSI, SARLAFT, SARE, etc.)
PREGUNTA:Para dimensionamiento de componentes en la propuesta, por favor indicar cuántas metodologías diferentes se llegarían a incluir que requerirían administradores independientes
Respuesta: Solo es parte de esta convocatoria la metodología de evaluación de riesgos del SARO. No se debe generar dimensionamiento para los demás componentes toda vez que no es parte del alcance actual. Lo que se espera es que a futuro se pueda crecer en la plataforma contratada. Posiblemente en próximos años se unan las metoologías SGSI y SARLAFT.

Pregunta: 1.2.1.1 Mapas de riesgo
Es deseable, no requisito, que la información de riesgo inherente y residual por proceso, entidad, metodología, producto, canal o proyecto, etc., puedan verse en un mismo mapa.
PREGUNTA: Por favor aclarar cómo hacen la consolidación del valor de riesgo inherente y residual para cada componente (proceso, entidad, etc.) con base en los riesgos asociados a cada uno
Respuesta: Se busca un mapa que permita consolidar el perfil de riesgos (inherente vs residual) del Banco. Esto quiere decir que debe incluir todos los riesgos asociados a todos los procesos. No se trata de una evaluación específica o diferente a la presentada en la metodología sino de una vista de un mapa. Generalmente, al realizar agrupaciones de riesgos o de procesos, se utilizan los promedios de las calificaciones en probabilidad y promedios de calificaciones en impacto para realizar la ubicación sobre el plano cartesiano. Esto aplica también para los mapas de producto, canal, proyecto, etc.
Es importante aclarar que un mismo riesgo puede ser asociado a varios procesos en el Banco. Por ejemplo: El riesgo de indisponibilidad de servicios públicos es un riesgo que afecta todos los procesos del Banco y lo ideal sería crear un solo riesgo de este tipo que se vea en los mapas de los diferentes procesos, en lugar de crear 40 riesgos (uno por proceso) que evidencien la indisponibilidad de servicios públicos.

Pregunta: 1.2.1 Evaluación de riesgos
La solución debe permitir asignar un mismo riesgo a diferentes procesos, permitiendo así la parametrización de riesgos transversales (aplicables a todos los procesos). Es deseable, no requisito, que estos puedan ser identificados fácilmente a través de alguna marcación para asociarlos a los riesgos.
PREGUNTA:Por favor aclarar si la marcación deseable sería propia de los procesos y cómo esperarían que se hiciera dicha marcación
Respuesta: La marcación es sobre el riesgo ya que este es el que esperamos que sea transversal. Puede realizarse a través de un campo descriptivo del riesgo.

Pregunta: ¿A qué tipos de auditoria realizadas por la contraloría y realizadas por terceros requieren que la solución tecnológica realice seguimiento de hallazgos y recomendaciones?
Respuesta: La Contraloría Interna del banco debe realizar seguimiento a todos los Planes de Mejoramiento generados como resultado de las diferenes auditorías, y poder hacer seguimiento a los Planes de mejoramiento generados por entes externos para el banco.

Pregunta: En anexo 10, numeral 1.5.8 1.5.8. Entes de Control y otras actividades (Se busca que la herramienta permita administrar y monitorear el inventario de actividades, el avance de estas y su cumplimiento.), Agradeceríamos precisar los requerimientos más importantes de este punto para analizar si Podemos satisfacerlos

Respuesta: Son en terminos generales, actividades que se realizadn de manera periódica, como reportes a entes de control, reportes internos, Visitas de entes de control, etc. El objetivo es simplemente tener un control (inventario) de estas actividades, sus fechas compromiso, responsable, detalle de la actividad, alertas, etc.

Pregunta: En anexo 10, numeral 1.5.7 Programa de Aseguramiento y Mejora de la calidad (El departamento de Contraloría/Auditoría desarrolla una serie de actividades, proyectos, indicadores, encuestas, mediciones y calificaciones internas, que permiten el mantenimiento de la mejora continua dentro del equipo. Se busca que la herramienta permita registrar, monitorear y medir, de acuerdo con la capacidad e insumos, estas actividades.), ¿La contraloría del Banco suministraría los formatos de encuestas y formas de evaluación?
Respuesta: Si. El banco suministrará los datos, mediciones, encuestas y planes de acción durante la fase de Análisis detallado de requerimientos.

Pregunta: En anexo 10, numeral 1.5.6 Flujos de aprobación, viñeta dos (La solución debe permitir la parametrización del flujo de actividades y autorizaciones de ejecución de la auditoría (contenido de pruebas,

papeles de trabajo relacionados y acciones de mejoramiento, entre otros)), Agradeceríamos precisar el requerimiento del flujo de actividades y autorizaciones
Respuesta: Los flujos de actividades pueden verse en las imagenes incluidas en el anexo 10.

Pregunta: En anexo 10, numeral 1.5.6. Flujos de aprobación, viñeta uno (La solución debe permitir parametrizar el flujo de actividades, documentación de análisis y autorizaciones del proceso de pre-planeación y de planeación de la auditoría.), Agradeceríamos precisar el requerimiento con respecto al flujo de actividades y los procesos de autorizaciones que se presentan en la pre-planeación y planeación de la auditoria
Respuesta: Los flujos de actividades pueden verse en las imagenes incluidas en el anexo 10.

Pregunta: En anexo 10, numeral 1.5.5. Gestión de Planes de Mejoramiento y Seguimiento Plan, viñeta cinco (Debe permitir consultar el cubrimiento del universo de auditoría (estado de aseguramiento) del Banco, para el año en curso, como para el ciclo de auditoría (actualmente de 3 años)), Agradeceríamos nos indiquen los elementos del universo de auditoria contra el cual se compararía el cubrimiento de la Auditoria durante el año en curso y para el ciclo de tres años.
Respuesta: Los elementos del universo se encuentran en las imagenes incluidas en la sección de Planeación Anual del Anexo 10.

Pregunta: En anexo 10, numeral 1.5.5 ejecución de las Auditorias, viñeta tres (El avance del Plan Anual debe poder consultarse en tiempo real o con cortes especificados por el usuario, detallando el cumplimiento de las Auditorías Individuales, los Planes de mejoramiento del proceso y actividades administrativas detalladas en los numerales 2.2.7. y 2.2.8. Adicionalmente, debe generar versiones adicionales o revisadas del Plan Anual ajustado (registrando historial de cambios en la Planeación y versiones del plan). Así mismo permitir parametrizar, generar reportes y gráficos y exportar a Office) ¿Qué información desean parametrizar con respecto a la Planeación Anual?

Respuesta: El objetivo es poder ver la evolución/cambios realizados en el Plan Anual, con base en el dinamismo del mismo; nuevas auditorías, cambios, inclusion de otros trabajos o proyectos, y en general eventos que hayan afectado el Plan Anual original presentado al comité. poder ver las diferentes "versiones del Plan".

Pregunta: 1.2.1 Evaluación de riesgos
Se requiere que la solución permita realizar la evaluación de riesgos para varios procesos agrupados (mapa corporativo).
Pregunta: Por favor aclarar cómo es la dinámica de este tipo de evaluación, es decir, ampliar cómo se hace la agrupación, cómo se hace la identificación (ej. Un mismo riesgo para varios procesos?), cómo se genera el mapa corporativo, etc.
Respuesta: Se busca un mapa que permita consolidar el perfil de riesgos (inherente vs residual) del Banco. Esto quiere decir que debe incluir todos los riesgos asociados a todos los procesos. No se trata de una evaluación específica o diferente a la presentada en la metodología sino de una vista de un mapa. Generalmente, al realizar agrupaciones de riesgos o de procesos, se utilizan los promedios de las calificaciones en probabilidad y promedios de calificaciones en impacto para realizar la ubicación sobre el plano cartesiano. Esto aplica también para los mapas de producto, canal, proyecto, etc.
Es importante aclarar que un mismo riesgo puede ser asociado a varios procesos en el Banco. Por ejemplo: El riesgo de indisponibilidad de servicios públicos es un riesgo que afecta todos los procesos del Banco y lo ideal sería crear un solo riesgo de este tipo que se vea en los mapas de los diferentes procesos, en lugar de crear 40 riesgos (uno por proceso) que evidencien la indisponibilidad de servicios públicos.

Pregunta: En anexo 10, numeral 1.5.4 ejecución de las Auditorias, viñeta cinco (Debe permitir integrar e indexar los papeles de trabajo respectivos a cada proyecto de auditoría (integración con Office365 y OneDrive

dispuestos por el Banco), ¿Las Herramientas mencionadas están disponibles por el Banco para realizar la Integración?
Respuesta: El Banco cuenta con la herramienta OFFICE 365, la cual incluye Onedrive, Sharepoint, Planner, y demás herramientas.

Pregunta: En anexo 10, numeral 1.5.4 ejecución de las Auditorias, viñeta cuatro (Debe permitir flujos de actividades entre la auditoría y los auditados de acuerdo con niveles jerárquicos de aprobación.), Agradeceríamos precisar los flujos de actividades y niveles de Aprobación mencionadas en el requerimiento.
Respuesta: Los flujos de actividades pueden verse en las imagenes incluidas en el anexo 10.

Pregunta: En anexo 10, numeral 1.5.4 ejecución de las Auditorias, viñeta tres (Debe permitir parametrizar, generar reportes y gráficos y exportar a Office los informes detallados y reportes de Ejecución de la Auditoría), Agradeceríamos precisar a qué tipos de informes y reportes hacen referencia.
Respuesta: Los informes y reportes serán definidos durante el "Análisis y entendimiento de los requerimientos" correspondiente a la fase de implementación mencionada en los Términos de Referencia. Sin embargo, se aclara que se esperan reportes con base en la información cargada en cada una de las etapas, Plan Anual, POA, Formatos de Plan y Programa, Observaciones de Auditoría, Informe final de Auditoría, reportes de avance del Plan y de Auditorías, en cuanto a las gráficas son pie, lineales, columnas, etc.. Por lo anterior, es de gran importancia que el proponente nos envíe en la propuesta técnica los tipos de reportes que provee la solución ofrecida.

Pregunta: 3. Frente a la formalización de la relación contractual:
Solicitud Expresa 1:

Para la formalización de la relación contractual ponemos a su consideración formalizar la misma a través de la propuesta y su respectiva carta de aceptación por parte de ustedes, de acuerdo a lo establecido en el artículo 854 del Código de Comercio Colombiano: “La aceptación tácita, manifestada por un hecho inequívoco de ejecución del contrato propuesto, producirá los mismos efectos que la expresa, siempre que el proponente tenga conocimiento de tal hecho dentro de los términos indicados en los artículos 850 a 853, según el caso.”

Solicitud Expresa 2: En caso de no ser aceptada la opción de formalizar la relación contractual a través de carta de aceptación, ponemos a su consideración nuestra minuta contractual que contiene los lineamientos y clausulas especiales para este tipo de servicios. El sistema no permite adjunta archivos, por favor nos pueden indicar como podemos compartila.

Solicitud Expresa 3:

En caso de no ser aceptada nuestra solicitud anterior y teniendo en cuenta que la entidad tiene establecido para la culminación satisfactoria del proceso de selección, la firma de un contrato con el proponente adjudicatario del presente proceso, solicitamos nos den a conocer la minuta de contrato, con el fin de evidenciar si podemos dar cumplimiento a las cláusulas de dicho documento.

Respuesta: Una vez evaluadas todas las propuestas se adjudicara la convocatoria al mejor proponente. Esta adjudicación se formaliza a través de una carta de aceptación la cual se encuentra condicionada a la firma del contrato.
En este momento no contamos con una minuta que se pueda compartir. Sin embargo les informamos que la misma es elaborada de acuerdo a los terminos de referencia y la propuesta.

Pregunta: En anexo 10, numeral 1.5.4 ejecución de las Auditorias, viñeta dos (Debe permitir llevar trazabilidad de toda la ejecución de los trabajos (tiempos de ejecución de actividades, alertas e indicadores de operación). ¿Agradecemos nos indiquen como definen los Indicadores De operación?

Respuesta: No es clara la pregunta. En términos generales, se tienen muchos indicadores, Fecha planeada vs fecha real, estado (sin iniciar, en curso, terminado), Al dia o vencido, etc., de acuerdo con cada etapa del proceso y cada actividad. Cumplimiento general Plan Anual vs. estado actual, etc.

Pregunta: En anexo 10, numeral 1.5.4 ejecución de las Auditorias

a) ¿Es aceptable que la solución de Auditoria provea el desarrollo de las auditorias de procesos y sistemas con enfoque "basadas en Riesgos críticos"?

b) ¿Todas las auditorias que realiza la contraloría del Banco se ejecutan utilizando solamente los estándares del IIA e ISACA?

c) ¿Es aceptable que las auditorias desarrolladas por la Contraloría del banco incluyan la evaluación del diseño y efectividad de los controles existentes para cada Riesgo, como requisito para diseñar y ejecutar las pruebas de auditoria?

d) ¿Es aceptable que las auditorias que realiza la Contraloría del banco incluyan funcionalidades para diseñar y planear la ejecución de Pruebas de Auditoria?

e) ¿Es aceptable para la Contraloría del banco, que la solución tecnológica propuesta genere de manera automática tres tipos de informes con los resultados de cada auditoria: a) evaluación de control interno; b) pruebas de cumplimiento y c) pruebas Sustantivas?

Respuesta: a) La criticidad de las auditorías se define en el proceso de Planeación Anual presentado en la reunión de aclaración de dudas.

b) SI. El proceso de auditoría del banco se realiza bajo principios del IIA.

c) El diseño y efectividad de los controles pueden ser auditados por la Contraloría, mas el diseño y efectividad reportados por la Oficina de Riesgo Operativo no son considerados como insumo.

d) Las auditorías realizadas por la Contraloría incluyen pruebas de auditoría. Esto es lo que está descrito en el punto 2 Numeral - 1.5.3. Planeación de las Auditorías. Si cuentan con funcionalidades adicionales pueden ser presentadas.

e) Estos pueden ser adicionales a los ya existentes, definidos por la Contraloría del Banco.

Pregunta: 2. Frente a la permisibilidad de una figura asociativa para prestar el servicio.
Solicitud Expresa:
Amablemente solicitamos nos informen si es permitido por ustedes que KPMG presente la propuesta solicitada y ejecute el servicio en conjunto con una tercera parte, es decir una de las siguientes figuras: subcontratista, Unión Temporal, Consorcio, aliado o Reseller
Respuesta: Aunque la presente convocatoria no tenía contemplado este tipo de proponentes, se realizará una adenda que permita participar a las figuras de Unión Temporal o Consorcio.

Pregunta: En anexo 10, numeral 1.5.3 Planeación de las Auditorías, viñeta uno (La solución debe permitir la definición y parametrización del formato de Pre-planeación de Auditoría.), Agradecemos nos indiquen qué datos serán parametrizables en el formato de pre-planeación.
Respuesta: Algunos datos deben ingresarse de manera manual, los datos "parametrizables" (deberían provenir de bases de datos existentes dentro de la herramienta), serían por ejemplo: Los Riesgos Operativos asociados, los Procesos y Subprocesos afectados, los Marcos de referencia asociados, resultado de la auditoría anterior (en caso que se encuentre cargada), datos iniciales de la Planeación Anual, etc.

Pregunta: 1.4 Frente al numeral 8.9 Subcontratistas
8.9. Subcontratos
El adjudicatario de los recursos podrá subcontratar a su propia conveniencia las labores que requiera para la ejecución del contrato, siempre y cuando por este conducto no se deleguen sus propias responsabilidades. En todo caso, ante Bancóldex, el Contratista será el responsable del cumplimiento de todas las obligaciones contractuales.

Solicitud Expresa:

Amablemente solicitamos la siguiente redacción:

"8.9 Subcontratos. El adjudicatario de los recursos podrá subcontratar a su propia conveniencia las labores que requiera para la ejecución del contrato, siempre y cuando por este conducto no se deleguen sus propias responsabilidades. En todo caso, ante Bancóldex, el Contratista será el responsable del cumplimiento de todas las obligaciones contractuales. En cualquier caso, toda responsabilidad aplicará previa verificación de las partes en la que se evidencie que EL CONTRATISTA incurrió en dicha conducta, en todo caso el pago de perjuicios se limitará al valor del contrato a suscribir, excepto en la medida que los daños sean resultado de culpa o negligencia grave o dolo de EL CONTRATISTA según lo determine un fallo ejecutoriado de un juez, tribunal o corte competente, o un laudo arbitral. "

Respuesta: Se revisará su solicitud y en caso de considerarlo pertinente se publicará el ajuste correspondiente en los terminos de referencia.

Pregunta: En anexo 10, numeral 1.5.2 Metodología de Planeación Anual, viñeta tres (La solución debe permitir parametrizar y generar diferentes tipos de reportes y gráficos definidos por Bancoldex, y tener la posibilidad de exportarlos a Office.), Agradeceríamos nos indicaran los tipos de reportes, gráficos y la parametrización deseada
Respuesta: Los reportes y gráficas serán definidos durante el "Análisis y entendimiento de los requerimientos" correspondiente a la fase de implementación mencionada en los Términos de Referencia. Sin embargo, se aclara que se esperan reportes y gráficos con base en la informacioón cargada en cada una de las etapas, con graficas de pie, lineales, etc. Por lo anterior, es de gran importancia que el proponente nos envíe en la propuesta técnica los tipos de gráficos que provee y puede proveer la solución ofrecida.

Pregunta: En anexo 10, numeral 1.5.1 Inventario y cargue de entes auditables, viñeta cinco, (Debe permitir realizar el cargue, actualización e integración de marcos de referencia de control, ejemplo: COSOs, COBITs, ISOs, ITIL, NIAs, SOX.) Solicitamos nos indiquen que información requieren de cada uno de los marcos de referencia y para que fines.
Respuesta: De momento, Bancóldex no tene establecido con exactitud cuales o cuantos se cargarán, ya que actualmente no lo podemos hacer. No obstante, es importante que se tenga la opcion de cargarlos para cuando realicemos este ajuste sobre nuestra metodología. La información a cargar es básicamente la de las listas de chequeo y/o de Controles, para ser seleccionados y utilizados como referentes en las diferentes auditorías.

Pregunta: Frente al numeral iii de la cláusula 8.8 Garantía del contrato.
Pago de salarios, prestaciones sociales, indemnizaciones laborales y demás prestaciones de índole laboral del personal dedicado por el Contratista para la ejecución del Contrato, con una suma asegurada equivalente al treinta por ciento (30%) del precio del Contrato y con una vigencia igual a la del Contrato y tres (3) años y tres (3) meses más.

Solicitud Expresa:

Comedidamente solicitamos a la entidad que revise la posibilidad y la viabilidad de disminuir el porcentaje de la póliza de Pago de salarios, prestaciones sociales, indemnizaciones laborales y demás prestaciones de índole laboral, toda vez que consideramos que las mismas se encuentran un poco elevada, por lo anterior proponemos se reduzca al 20%.

Respuesta: No es posible modificar el texto en mención del Banco.

Pregunta: En anexo 10, numeral 1.5.1 Inventario y cargue de entes auditables, viñeta dos (La solución debe permitir el cargue de otros insumos, ejemplo: proyectos, activos de información, resultados de evaluaciones de terceros, resultados de auditorías anteriores, etc.), solicitamos precisar la información a cargarse por cada Insumo y la forma de ingresar dicha información al sistema
Respuesta: De momento, Bancóldex no tene establecido con exactitud cel detalle exacto de la información a cargar, ya que actualmente no lo podemos hacer. Estos serán definidos durante el "Análisis y entendimiento de los requerimientos" correspondiente a la fase de implementación mencionada en los Términos de Referencia. Es información que se ingresará de manera manual: Proyectos del Banco para el año (nombremi, objetivo, presupuesto, plazo, costo, responsable, entre otros), resultados de auditorias de entes externos (observación, plazo, responsable, fecha de identificación), resultados de auditorías anteriores (calificación, fecha de realización, responsable, alcance, etc). Activos de Información (ID del Activo, el Custodio del Activo, el Contenedor del Activo, Calificación del Activo en términos de Confidencialidad, Integridad y Disponibilidad), entre otros. El algunos casos pordría ser un cargue en batch o de excel o similares.

Pregunta: 1.2. Frente al numeral 15 de la cláusula 8.3 Obligaciones del contratista.

Responder en cualquier proceso administrativo o judicial por cualquier reclamo que reciba EL BANCO, en virtud de una infracción o incumplimiento referente al derecho de propiedad intelectual sobre las aplicaciones por lo que EL CONTRATISTA se hará cargo y asumirá, con sus propios abogados, los gastos de defensa de EL BANCO. De igual forma, EL CONTRATISTA pagará a EL BANCO y/o terceros todos los gastos, daños y/o perjuicios y honorarios profesionales que un tribunal competente en sentencia en firme lo condene a pagar como consecuencia de tal reclamación.

Solicitud Expresa:

KPMG no puede aceptar indemnización y/o responsabilidad ilimitada pues por políticas internas deben estar limitadas en tiempo o cuantía. En virtud de lo anterior, solicitamos se tenga en cuenta la siguiente redacción:

“15. Responder en cualquier proceso administrativo o judicial por cualquier reclamo que reciba EL BANCO, en virtud de una infracción o incumplimiento referente al derecho de propiedad intelectual sobre las aplicaciones por lo que EL CONTRATISTA se hará cargo y asumirá, con sus propios abogados, los gastos de defensa de EL BANCO. De igual forma, EL CONTRATISTA pagará a EL BANCO y/o terceros todos los gastos, daños y/o perjuicios y honorarios profesionales que un tribunal competente en sentencia en firme lo condene a pagar como consecuencia de tal reclamación. En cualquier caso, toda responsabilidad aplicará previa verificación de las partes en la que se evidencie que EL CONTRATISTA incurrió en dicha conducta, en todo caso el pago de perjuicios se limitará al valor del contrato a suscribir, excepto en la medida que los daños sean resultado de culpa o negligencia grave o dolo de EL CONTRATISTA según lo determine un fallo ejecutoriado de un juez, tribunal o corte competente, o un laudo arbitral. “

Respuesta: Se revisará su solicitud y en caso de considerarlo pertinente se publicará el ajuste correspondiente en los terminos de referencia.

Pregunta: Con el fin de estructurar una propuesta competitiva que cumpla con los objetivos esperados por ustedes, y en atención a la importancia del mismo, les solicitamos comedidamente se estudie la viabilidad de

prorrogar el plazo establecido en un período no inferior a diez (10) días hábiles contados a partir de la fecha de cierre la cual está dispuesta actualmente para el próximo 16 de julio de 2021, plazo que igualmente nos permitirá conocer las respuestas a las observaciones como las posibles adendas que sean proferidas por la entidad, las cuales conformaran junto con las demás condiciones de la solicitud, los lineamientos bajo los que estructuraremos la propuesta definitiva a ser presentada.
Respuesta: Se realizará una ampliación del periodo de presentación de la propuesta en 7 días calendario. Esto será oficializado mediante adenda.

Pregunta: En Anexo 1, en la sección de: "Afectación – Valoración del Riesgo Residual con base en Eventos". ¿Es aceptable que el riesgo residual de un evento ocurrido se modifique SOLAMENTE por efecto del incumplimiento (elusión premeditada) de los controles establecidos para gestionar el riesgo o por la inefectividad de los controles establecidos (los controles establecidos no sirven para reducir el riesgo)?
Respuesta: Actualmente la metodología de afectación de eventos sobre riesgos del Banco no considera en específico la falla de los controles como insumo para la evaluación del riesgo residual. Esta afectación se basa en la cantidad de eventos presentados en el último año y, a partir de una tabla de valores, se realiza un cálculo sobre el riesgo residual. Por lo anterior, no sería viable lo propuesto por el proveedor.

Pregunta: En Anexo 10, numeral 6. Arquitectura infraestructura, en la sección 1.18. Disponibilidad, Se solicita precisión sobre lo indicado en el párrafo que dice: "Se debe presentar un reporte mensual a Bancóldex de la disponibilidad de la solución, los motivos o causas de las indisponibilidades que se hayan presentado en el mes y la cantidad de operaciones realizadas por los clientes del Banco", referente a la cantidad de operaciones realizadas por los clientes del banco.
Respuesta: Las "operaciones realizadas por los clientes del Banco" son un ítem específico para plataformas transaccionales contratadas por el Banco y este no es el caso del servicio a contratar a través de esta convocatoria. Por lo anterior, este indicador de disponibilidad es medido en términos de las horas de indisponibilidad de la plataforma al mes (no se tienen en cuenta los mantenimientos programados) sobre el tiempo de disponibilidad acordado con el proveedor.

Pregunta: En Anexo 10, numeral 1.3.1 Roles y Perfiles, viñeta 1. Por favor precisar el significado y alcance de "Realizar la administración funcional de la solución tecnológica".
Respuesta: Hace referencia a que, en caso de que la herramienta permita confiurar diferentes metodologías de riesgos (SARO, SARE, SARLAFT, etc), cada metodología tenga un propio administrador que realice los ajustes sobre los cálculos, listados de valor y demás parametrías que permita el aplicativo.

Pregunta: En Anexo 10, numeral 1.2.3 Reportes, viñeta 4. Se solicita precisar el requerimiento que dice "Los reportes deben permitir filtrado por campos clave"
Respuesta: Se requiere que la herramienta permita realizar búsqueda fácil y rápida de información, y dependiendo del reporte, se deben tener campos clave. Por ejemplo: si estamos en un reporte de controles vs riesgos, es importante poder filtrar por número de control o por el control mismo. Si se trata de un reporte de riesgos por proceso, es importante poder filtrar por riesgos. Etc. Los campos que más usamos para estos filtros son: Proceso, Riesgo, factor de riesgo, probabilidad, impacto, severidad, (inhernetes y residuales) Control, Naturaleza del Control, Tipo de Control, Evidencia, Registro.

Pregunta: En Anexo 10, numeral 1.2.1.2. Gestión de Eventos de Riesgo Operacional, viñeta 6. Bajo el entendido que "En la informática, La parametrización de una base de datos, es la organización y estandarización de la información que se ingresa en un sistema." Agradeceríamos aclarar con el mayor de nivel de detalle posible el alcance de este requerimiento. Dadas la complejidad tecnológica y las implicaciones que tiene este requerimiento, solicitamos especificar el significado y alcance de "debe permitir la parametrización y configuración de todos los campos utilizados para el registro de eventos de riesgo operacional". Observamos que son aproximadamente 40 campos que solicitan parametrizar.
Respuesta: Como parte del cumplimiento normativo colombiano, el Banco debe llevar registro de todos sus eventos de riesgo operacional, apoyándose en lo dispuesto en la Circular 025 expedida por la Superintendencia Financiera de Colombia en 2020, la cual especifica la mayoría de los campos que se detallan

en el requerimiento. Algunos otros campos son de uso interno y nos permite realizar una mejor gestión de los eventos en cuestión, por lo que consideradmos que el Proponente puede diseñar su propio modelo de Base de Datos, siempre y cuando se pueda obtener toda la información que detallamos en el numeral mencionado, con el fin de realizar los reportes normativos.

Pregunta: En Anexo 10, numeral 1.2.1.1 Mapas de Riesgo, viñeta 3. ¿Es aceptable que el mapa de riesgos residuales (severidad riesgo inherente vs efectividad colectiva de los controles establecidos sobre el riesgo) se presente en un gráfico separado del mapa de riesgo inherente, en el que se muestre el efecto de los controles establecidos para reducir la severidad del riesgo inherente?
Respuesta: Sí, es válido. El proponente debe enviar el mapa tipo que tiene la solución ofrecida. En el Anexo 10, numeral 1.2.1.2 viñeta 2, se debe indicar que no se tiene un mapa como el solicitado. En la viñeta 3 se envían todos los mapas tipo que ofrezca la solución

Pregunta: En Anexo 10, numeral 1.2.1 Evaluación de riesgos, viñeta 1. Referente a “La solución debe permitir realizar la evaluación de riesgos desde diferentes perspectivas”. ¿Cuál es la expectativa para la gestión de riesgos por Macroproceso con todos sus procesos y por proyectos?
Respuesta: Se busca un mapa que permita consolidar el perfil de riesgos (inherente vs residual) del Banco. Esto quiere decir que debe incluir todos los riesgos asociados a todos los procesos. No se trata de una evaluación específica o diferente a la presentada en la metodología sino de una vista de un mapa. Generalmente, al realizar agrupaciones de riesgos o de procesos, se utilizan los promedios de las calificaciones en probabilidad y promedios de calificaciones en impacto para realizar la ubicación sobre el plano cartesiano. Esto aplica también para los mapas de producto, canal, proyecto, etc.
Es importante aclarar que un mismo riesgo puede ser asociado a varios procesos en el Banco. Por ejemplo: El riesgo de indisponibilidad de servicios públicos es un riesgo que afecta todos los procesos del Banco y lo ideal sería crear un solo riesgo de este tipo que se vea en los mapas de los diferentes procesos, en lugar de crear 40 riesgos (uno por proceso) que evidencien la indisponibilidad de servicios públicos.

Pregunta: Es aceptable ofertar una solución tecnológica compuesta de tres (3) productos independientes que en conjunto satisfacen los requerimientos técnicos y funcionales solicitados en el anexo 10 ?. Estos productos son: a) CONTROLRISK para Gestión de Riesgos Empresariales ; b) AUDIRISK para Auditoria Interna y de Sistemas basada en Riesgos; y c) AUDIT-IP para Gestión y Seguimiento de hallazgos y recomendaciones de auditorías internas y realizadas por terceros.
Respuesta: Sí, siempre y cuando los 3 sistemas "se hablen" entre sí para poder obtener información para la gestión integral de riesgos.

Pregunta: Términos de referencia, Numeral 5.8 Oferta Económica. ¿ Es aceptable ofertar el tipo de servicio “Configuración e instalación en la Nube, en la infraestructura de BANCOLDEX?.
Respuesta: No es clara la pregunta. Sin embargo, se aclara que se prefiere una implementación en nube, no obstante, el proveedor puede proponer realizar la configuración de su servicio de arrendamiento sobre su infraestructura o nube ó puede proponer la implementación en infraestructura del Banco, siempre y cuando se trate de arrendamiento y no compra de software. En caso de proponer hacerlo sobre la infraestructura del Banco, se debe aclarar cuáles son los requisitos de hardware y software para la implementación.

Pregunta: Requerimientos funcionales
Modulo Riesgo operacional, dentro del punto 1.2 el requerimiento indica:

- Se requiere que la solución permita realizar la evaluación de riesgos para varios procesos agrupados (mapa corporativo).

Solicitamos aclarar un poco más en detalle que significa evaluar los riesgos para procesos agrupados o si es posible tener un ejemplo del mapa corporativo a generar

Respuesta: Se busca un mapa que permita consolidar el perfil de riesgos (inherente vs residual) del Banco. Esto quiere decir que debe incluir todos los riesgos asociados a todos los procesos. No se trata de una

evaluación específica o diferente a la presentada en la metodología sino de una vista de un mapa. Generalmente, al realizar agrupaciones de riesgos o de procesos, se utilizan los promedios de las calificaciones en probabilidad y promedios de calificaciones en impacto para realizar la ubicación sobre el plano cartesiano.

Pregunta: En la descripción de cantidades de licencias (Términos de referencia – Númeral 5.8 Oferta Económica) no se hace referencia al registro y recolección de eventos de pérdida (Cantidades de usuarios y alcance). No son requeridos estos usuarios?
Respuesta: Dentro del anexo técnico, en el punto 1.2.1.2 se especifica que es necesario que los funcionarios de la Oficina de Riesgo Operativo (5) puedan hacer el registro y cargue de eventos de riesgo operacional. Por lo que el licenciamiento de estos usuarios debe contener el registro de eventos en la plataforma y por tanto, estarincluido en la oferta.
De otra parte, se indica que es un deseable, no requisito, que el resto de los funcionarios del Banco puedan realizar el reporte de eventos. Como se trata de un deseable y no un requisito, , en la parte de información complementaria del formato en cuestión, se puede indicar cuál es el valor del licenciamiento respectivo.

Pregunta: En la descripción del contrato en referencia a la vigencia del mismo, (Términos de referencia – Numeral 8.6 Duración del contrato), el proceso de configuración de la plataforma se debe hacer si o si una vez sea activada la misma, de lo contrario no sería viable el acceso a la solución y la personalización requerida para Bancoldex. En consecuencia la duración del contrato debe estar alineada a la vigencia de la suscripción en el esquema SaaS. Este aspecto contractual puede ser revisado?
Respuesta: Se espera que el cobro de las licencias se realice en la fase de operación de la misma y no antes. Si el tiempo de la fase deimplementación es más corto, se reduce el tiempo total del contrato.

Pregunta: La forma de pago propuesta por Bancoldex (Términos de referencia – Numeral 7.3 Forma de pago), no se ajusta a las exigencias y esquema de licenciamiento SaaS del proveedor de nuestra solución, en el cual se hace un solo pago anual por concepto de acceso a la plataforma por 12 meses. Los servicios si pueden ser facturados de forma parcial según entregables. Este punto puede ser revisado?
Respuesta: La forma de pago es la que se encuentra publicada en el numeral 7.3 de los Términos de Referencia. La fase de implementación no puede ser considerada dentro del pago de las licencias toda vez que no se encuentran en completa operación y funcionamiento para el Banco.

Pregunta: Para la validación y evaluación de la experiencia, hay algún formato definido?. No vimos un formato relacionado en la documentación recibida y en la plataforma de presentación si se hace referencia a este formato.
Respuesta: No se cuenta con un formato definido para la presentación de esta información. El proponente debe unificar todas las certificaciones de experiencia en un único documento que debe ser cargado en el campo "Formato Experiencia Específica del Proponente".

Pregunta: En el cronograma general publicado en la plataforma no se hacía referencia a la Sesión virtual de aclaración de dudas sobre los presentes Términos de Referencia y sus anexos para los proponentes, que si esta descrita en el documento términos de referencia. Se va a realizar esta reunión? Considerando que ya pasó la fecha programada será reprogramada?
Respuesta: En los Términos de Referencia se especifica el cronograma de la contratación y se incluye la sesión virtual. Esta reunión tuvo lugar el día 30 de junio y, a medida que los proponentes realizaban la inscripción por la plataforma, se les envió un link para la conexión, tal como se describe en los TDR en el punto 4.6. No se reprograma la actividad.

Pregunta: 10. El punto 6 de la propuesta técnica cual es el alcance de la documentación que se debe entregar a bancoldex?
Respuesta: En cada ítem del punto 6 del anexo técnico se encuentra el detalle de lo que se espera y el alcance de la documentación. Se espera información general asociada a la arquitectura que soporta el servicio a contratar.

Pregunta: 9. El punto 2 de la propuesta técnica a que hace referencia en los input requeridos y las salidas ofrecidas?
Respuesta: No es clara la pregunta.

Pregunta: 8. El punto 1 de la propuesta técnica hace referencia al anexo número 10?
Respuesta: No es clara la pregunta. El Anexo Técnico al que hace referencia es el mismo Anexo 10. Por favor tener en cuenta que en el documento que detalle la presentación de la propuesta técnica se debe dar respuesta a todo el Anexo técnico(Anexo 10), por esta misma razón, se envía el Anexo Técnico en WORD.

Pregunta: 7. 6.3. Documentación de la Propuesta.
En el punto 20 se habla de un campo asociado "Referencias comerciales" donde debe subirse la información solicitada en el numeral 5.5; sin embargo no se evidencia tal campo en los items a adjuntar. Debo encontrarlo con otro nombre? y cual es el mínimo de referencias solicitadas?
Respuesta: El campo "Referencias comerciales" fue reemplazado por "Formato Experiencia Específica del Proponente" y es en este último en el que se debe cargar la información. Se realizará adenda sobre este punto.

No se tiene un número mínimo de referencias solicitadas. El proponente es libre de enviar la cantidad de referencias que considere pertinente.

Pregunta: 6. De acuerdo con el punto 5.4. Capacidad Administrativa."

Debe generarse un archivo con los documentos portafolio de servicios, trayectoria en el mercado y la estructura organizacional para subirse en la plataforma como se indica en "Capacidad administrativa a través de los documentos requeridos al proveedor"?
La plataforma me permitiria subir varios documentos?

Respuesta: No. La plataforma permite enviar un único documento por ítem, por lo que tendrían que unificar el archivo con todos los documentos necearios.

Pregunta: 5. Sobre el punto 6 Arquitectura infraestructura numeral 4.3 plataforma tecnología.

"La propuesta deberá contener la especificación técnica de cada uno de los elementos y componentes que hacen parte de la solución. En esta descripción se deberá mencionar los servidores, sistemas operativos, sistemas manejadores de base de datos y demás componentes que apliquen. El proponente deberá garantizar que, por los próximos 3 años, las herramientas, componentes y demás que integran la solución presentada, estarán vigentes en el mercado con su debido nivel de soporte y de presentarse alguna novedad en este sentido, el proponente deberá comprometerse a realizar la correspondiente gestión para la actualización a la siguiente versión anunciada por el fabricante"

pregunta-¿Para servicio de SaaS requieren específicamente describir los componentes?

Respuesta: Para el Banco es importante conocer las características de la plataforma sobre la cual corren los servicios que tiene contratados, por temas de cumplimiento y seguridad de la información. Por lo anterior, es importante conocer de forma general los componentes que soportan el servicio ofrecido.

Pregunta: 4. En caso afirmativo a la respuesta anterior, ¿pueden los 3 contratos del ejemplo ser ejecutados de manera paralela en el tiempo?

Respuesta: Así es. Para el ejemplo se sumarían los años que se tienen independientemente de si se están realizando de forma paralela.

Pregunta: 3. La acreditación de los años experiencia que se requieren es un factor que se suma entre los años de vigencia de contratos con diferentes clientes?

Ejemplo: si tengo tres (3) contratos cada uno por dos (2) años, con tres (3) clientes diferentes, significa que al enviar las certificaciones de cada cliente estaría acreditando tres (6) años de experiencia?

Respuesta: Así es. Para el ejemplo se sumarían los años que se tienen independientemente de si se están realizando de forma paralela.

Pregunta: 2. Los contratos que han incluido servicios de asesoría para la implementación del software (que tienen una fecha específica para su cumplimiento) y servicios SAAS ó soporte (que son de tracto sucesivo) que se encuentran en ejecución, pueden ser válidos para certificar experiencia, en la porción que han sido cumplidos.

Respuesta: Sí, son válidos. Es importante que en las certificaciones se indique la fecha de inicio y que se encuentran vigentes.

Pregunta: 1. De conformidad con lo establecido en el párrafo primero del numeral 5.5 Experiencia Específica del proponente, de los términos de referencia: "Los Proponentes debera´n acreditar y contar con mi´nimo tres (3) an~os de experiencia en los servicios de disen~o, desarrollo e implementacio´n de soluciones de gestio´n de riesgos y auditori´a" .

Significa esto que la experiencia a acreditar será exclusivamente para los procesos de disen~o, desarrollo e implementacio´n de soluciones de gestio´n de riesgos y auditori´a, y no para los servicios licenciamiento del mismo? ó, por el contrario, es pertinente aclarar que la experiencia a acreditar por parte de los proponenentes inlcuye, no solo disen~o, desarrollo e implementacio´n de soluciones de gestio´n de riesgos y auditori´a, sino tambien, el periodo que los mismo tienen usando las licencias de Binaps.

La inquietud surge, dado que los procesos de disen~o, desarrollo e implementacio´n tienen un periodo corto, único y concreto de ejecución al inicio de la relación contractual, aproximadamente de 3 a 6 meses, de acuerdo al alcance del proyecto. Posterior a esto, se mantiene un servicio de SAAS o de Soporte según el método de adquisición (perpetuo o SAAS), siendo este último el que se prolonga en tiempo.

Respuesta: La experiencia también es aplicable para los servicios de licenciamiento y los periodos en los que se preste el servicio de soporte sobre el mismo.

Bogotá D.C., 15/07/2021