**ANEXO No. 10 – REQUERIMIENTO TÉCNICO Y FUNCIONAL PARA SOFTWARE DE RIESGOS Y AUDITORÍA**

Se requiere contar con una solución tecnológica confiable que garantice la integridad, disponibilidad y confidencialidad de la información de los riesgos operacionales a los cuales está expuesto Bancóldex y las auditorías internas realizadas sobre los diferentes entes auditables.

Por favor indique a continuación con claridad, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo.

# REQUERIMIENTOS FUNCIONALES

## Módulo de Riesgo Operacional

### Definiciones

* Riesgo: Es la posibilidad de que la entidad incurra en pérdidas por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano, así como por la ocurrencia de acontecimientos externos asociados a éstos. Incluye el riesgo legal.[[1]](#footnote-1)
* Control: Medida que se aplica para la mitigación del riesgo. Los controles pueden reducir la probabilidad de ocurrencia del riesgo o reducir el impacto de la materialización del mismo.
* Sistema de Administración de Riesgo Operacional - SARO: conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo Operacional, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades identifican, miden, controlan y monitorean el riesgo Operacional.
* Evento SARO: Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado. [[2]](#footnote-2)
* Reporte de Evento SARO: Mecanismo a través del cual se informa a la Oficina de Riesgo Operacional sobre la ocurrencia de un evento.
* Riesgo transversal: riesgos que son aplicables a toda la organización o una parte significativa de esta. Dentro de estos se encuentran los riesgos de desastres naturales, pandemia, asonadas y ataques terroristas, entre otros.
* Tratamiento del riesgo: Decisión que se toma frente a un determinado nivel de riesgo Operacional, los cuales pueden ser: aceptar, eliminar o reducir (remover y transferir)
* Planes de Acción de Riesgos: Hojas de ruta que permiten la implementación de controles para los riesgos.
* Líder de proceso: funcionario encargado de asegurar el cumplimiento de las políticas en la línea de negocio que lidera. Promueve la actualización de los mapas de riesgos y lidera la implementación de los planes de acción para dar tratamiento a los mismos. Aprueba los riesgos que fueron revisados por el Gestor de proceso.
* Gestor de proceso: responsable de apoyar al líder de proceso en la identificación de riesgos y controles. Revisa los riesgos antes de que estos pasen a aprobación por parte del líder.

### Requerimientos funcionales

#### Evaluación de riesgos

* La solución **debe permitir realizar la evaluación de riesgos desde diferentes perspectivas**:
  + Para un proceso.
  + Macroproceso con todos sus procesos.
  + Subprocesos (deseable, no requisito).
  + Producto o servicio del portafolio del Banco. Ejemplo: riesgos del producto “leasing digital”.
  + Canal de distribución de productos o servicios. Ejemplo: evaluación de riesgos del canal “Internet”.
  + Proyecto. Ejemplo: evaluación de riesgos del proyecto interno de automatización de labores operativas con la asistencia de un robot.

En virtud de lo anterior, la solución debe permitir la configuración de las estructuras respectivas que permitan identificar y/o asociar riesgos a estas. Es un plus si el proveedor suministra y hace mantenimiento sobre las bibliotecas de riesgos y controles basados en las mejores prácticas (COSO, Estándar Australiano del Riesgo Operacional, COBIT, ISOs, etc.)

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

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

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

* 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.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución **debe permitir asociar un mismo control a varios riesgos**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución **debe permitir asignar tratamientos a los riesgos** (Aceptar o Reducir). Este tratamiento debe ser parametrizable.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución **debe permitir asociar uno o varios Planes de Acción a cada riesgo**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* **Cada Plan de Acción debe tener información del responsable y fecha de implementación. A los responsables les deberá llegar un correo con la información de su plan de acción. El proponente debe indicar qué se requiere técnicamente para el envío de estas notificaciones (conexiones a correo, plantillas, etc.)**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución tecnológica debe permitir la **asignación de un mismo Plan de Acción a varios Riesgos**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución tecnológica **debe permitir la configuración de una estructura de riesgos y controles que facilite la vinculación entre estos**. Es deseable, no requisito, que se cuente con una biblioteca propia de estos con base en estándares internacionales.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución tecnológica **debe permitir la parametrización y configuración de todos los campos utilizados para la identificación y evaluación de riesgos operacionales**, de acuerdo con lo dispuesto por la Circular Básica Financiera y Contable, considerando además aquellos que fueron incluidos por la metodología específica SARO del Banco:

|  |  |  |  |
| --- | --- | --- | --- |
| **Información Propia de Cada Riesgo** | | | |
| **Campo** | **Variable** | **Tipo** | **Clasificación Interna** |
| ID del Riesgo |  | Calculado por el sistema | Mandatorio |
| Estado | Alfanumérico |  | Mandatorio |
| Descripción del Riesgo | Alfanumérico | Obligatorio | Mandatorio |
| Causa Inmediata | Alfanumérico | Opcional | Auxiliar |
| Causa Mediata | Alfanumérico | Opcional | Auxiliar |
| Tipo de Riesgo (puede ser varios valores para un mismo riesgo) | Alfanumérico | Opcional | Auxiliar |
| Observaciones sobre el riesgo | Alfanumérico | Opcional | Auxiliar |
| Área de Impacto | Alfanumérico | Obligatorio | Mandatorio |
| Factor de Riesgo | Alfanumérico | Obligatorio | Mandatorio |
| Origen del Riesgo (Nivel I) | Alfanumérico | Obligatorio | Mandatorio |
| Origen del Riesgo (Nivel II) | Alfanumérico | Obligatorio | Mandatorio |
| Origen del Riesgo (Nivel III) | Alfanumérico | Obligatorio | Mandatorio |
| Frecuencia | Numérico | Obligatorio | Mandatorio |
| Justificación Frecuencia | Alfanumérico | Opcional | Auxiliar |
| Probabilidad Inherente | Alfanumérico | Calculado por el sistema | Mandatorio |
| Impacto Inherente | Alfanumérico | Obligatorio | Mandatorio |
| Justificación Impacto Inherente | Alfanumérico | Opcional | Auxiliar |
| Zona de Riesgo (Inherente) | Alfanumérico | Calculado por el sistema | Mandatorio |
| Probabilidad Residual | Alfanumérico | Calculado por el sistema | Mandatorio |
| Impacto Residual | Alfanumérico | Calculado por el sistema | Mandatorio |
| Zona de Riesgo Residual | Alfanumérico | Calculado por el sistema | Mandatorio |
| Tratamiento del Riesgo | Alfanumérico | Obligatorio | Mandatorio |
| Vicepresidencia a Cargo del Riesgo (pueden ser varios registros para un mismo riesgo) | Alfanumérico | Opcional | Auxiliar |
|  |  |  |  |
| **Información Propia de Cada Control** | | | |
| **Campo** | **Variable** | **Tipo** | **Clasificación Interna** |
| ID del Control |  | Calculado por el sistema | Mandatorio |
| Descripción del Control | Alfanumérico | Obligatorio | Mandatorio |
| Responsable del Control | Alfanumérico | Opcional | Auxiliar |
| Reducción del Control | Alfanumérico | Obligatorio | Mandatorio |
| Tipo de Control | Alfanumérico | Obligatorio | Mandatorio |
| Naturaleza del Control | Alfanumérico | Obligatorio | Mandatorio |
| Evidencia del Control | Alfanumérico | Obligatorio | Mandatorio |
| Documentación del Control | Alfanumérico | Obligatorio | Mandatorio |
| Frecuencia de Aplicación del Control | Alfanumérico | Obligatorio | Mandatorio |
| Observaciones sobre el Control | Alfanumérico | Opcional | Auxiliar |
|  |  |  |  |
| **Información Propia de Cada Plan de Acción** | | | |
| **Campo** | **Variable** | **Tipo** | **Clasificación Interna** |
| ID del Plan de Acción |  | Calculado por el sistema | Mandatorio |
| Descripción Plan de Acción | Alfanumérico | Obligatorio | Mandatorio |
| Fecha de Implementación del Plan de Acción | Fecha | Obligatorio | Mandatorio |
| Área Responsable del Plan | Alfanumérico | Obligatorio | Mandatorio |
| Nombre del Responsable del Plan | Alfanumérico | Obligatorio | Mandatorio |
| Fecha del Seguimiento (puede haber varios registros para un mismo Plan) | Fecha | Opcional | Auxiliar |
| Descripción de Gestión | Alfanumérico | Opcional | Auxiliar |
| Estado del Plan de Acción | Alfanumérico | Obligatorio | Mandatorio |

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es posible que **en el futuro se deban incluir más campos**, por lo que la solución tecnológica debe ser flexible para tal fin.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* **Algunos de los campos tienen listados de valores que deberán quedar configurados en el sistema y podrán ser actualizados cuando así el Banco lo requiera**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* **La solución tecnológica debe permitir la configuración y parametrización de la metodología de evaluación de riesgo operacional (inherente y residual) del Banco**. Dicha metodología tiene definiciones cuantitativas y cualitativas que deben quedar completamente implementadas en la solución. Más adelante se explica el detalle de la metodología para su respectivo análisis [Metodología de Evaluación de Riesgo Operacional](#_Anexo_1._Metodología). **El** **proveedor debe indicar si para la implementación de la metodología expuesta, requiere realizar desarrollos internos que puedan impactar el tiempo de ejecución del proyecto** o estos pueden ser parametrizados directamente sobre la interfaz de la solución y modificables por el Administrador.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que la solución tecnológica permita **actualizar los cálculos y demás parametrizaciones asociadas a la metodología de evaluación de riesgo operacional, de forma fácil y a través de la interfaz gráfica del usuario**. Esto, considerando que pueden existir cambios normativos o mejoras a la metodología de riesgos que requieran ajustes sobre la solución.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es un deseable, no requisito, que la solución permita configurar diferentes metodologías para la evaluación de riesgos dependiendo el sistema de gestión al cual pertenezcan: SARO, SGSI, SARLAFT, SARE (Riesgo Estratégico), etc. Estas pueden tener cálculos diferentes para la valoración de los riesgos. En caso de que la solución lo permita, y dado que el alcance de este requerimiento es únicamente la implementación de la metodología de SARO, **el proponente debe especificar si la parametrización de las otras metodologías implica la implementación de módulos diferentes a los requeridos para SARO** o si se puede realizar a través del mismo módulo con una ampliación de las horas de implementación y licencias destinadas para tal fin. Asimismo, debe explicar las implicaciones que tendría realizar estas implementaciones adicionales.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que la solución tenga un **tablero de control que permita identificar de forma rápida el estado de los riesgos, indicadores y demás gráficas útiles para la gestión de riesgos del Banco**. De tenerlo, el proponente **debe** enviar el material gráfico de soporte.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que la solución **permita a los usuarios de la Oficina de Riesgo Operativo acceder a los planes de mejoramiento y recomendaciones generados por la auditoría para los procesos**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

##### Mapas de Riesgo

* La solución **debe permitir la generación de como mínimo los siguientes mapas** de riesgos de la metodología SARO:
  + Mapa de Riesgo Inherente para la Entidad - Perfil de Riesgo. (Promedio)
  + Mapa de Riesgo Residual para la Entidad - Perfil de Riesgo. (Promedio)
  + Mapa de Riesgo Inherente por Proceso.
  + Mapa de Riesgo Residual por Proceso.
  + Mapa de Riesgo Inherente por Producto/servicio, canal o proyecto.
  + Mapa de Riesgo Residual por Producto/servicio, canal o proyecto.

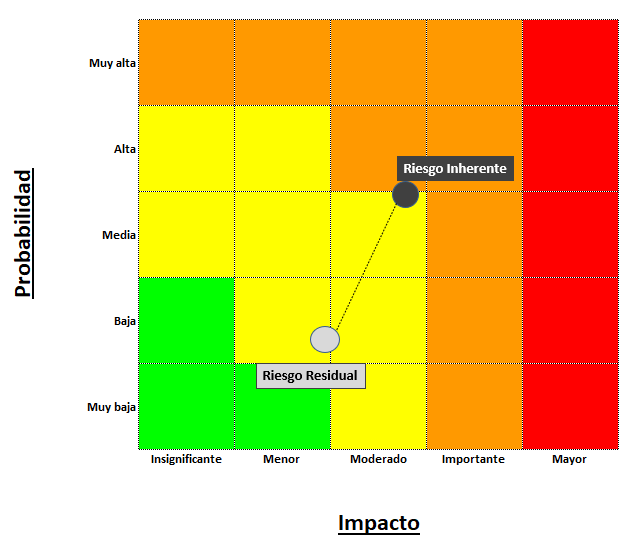
El proponente **debe enviar los mapas de calor tipo** que genera la solución propuesta, indicando con claridad si cumple cada uno de los mapas solicitados en este punto.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

Adicionalmente, si la solución tecnológica permite la parametrización de diferentes metodologías de riesgos (SARLAFT, SGSI, SARE, etc.), es un deseable, no requisito, tener los mismos mapas anteriores tanto por metodología como de forma acumulada (Perfil integral de riesgos). Si aplica este punto, el proponente **debe enviar los mapas tipo** que genera la solución propuesta.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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.** Esto, para ver el movimiento de los riesgos a partir de la aplicación de controles. El mapa ideal sería el siguiente:



El proponente **debe indicar si se cuenta o no con el mapa mencionado** y debe enviar pantalla del mismo.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. **Debe enviar en este campo el mapa tipo** que tiene la herramienta para riesgo inherente y residual. |
|  |

* El proponente deberá enviar **pantallas con las matrices de riesgos** que genera la solución.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

##### Gestión de Eventos de Riesgo Operacional

* **El reporte de los Eventos (riesgos operacionales materializados) debe ser realizado a través de la solución tecnológica** por los funcionarios de la Oficina de Riesgo Operativo (5 funcionarios, máximo 3 concurrentes).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es un deseable, no requisito, que cualquier funcionario del Banco pueda realizar también dicho reporte, en cuyo caso se generaría un **formulario especial con los campos mínimos necesarios.** En caso de que la solución lo permita, debe indicar las implicaciones técnicas de esta actividad, es decir, si se requiere un módulo adicional, si todos los usuarios que deben ser usuarios nombrados/licenciados, etc.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Los eventos de riesgo operacional pueden tener afectación sobre un riesgo existente, bajo la metodología explicada en el [Anexo 1](#_Anexo_1._Metodología). Esta afectación debe verse reflejada sobre la calificación del riesgo residual en la solución tecnológica solicitada. El proponente debe indicar con claridad si la solución ofrecida **permite o no realizar la afectación del riesgo basada en eventos materializados de acuerdo con la metodología expuesta**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* **Los eventos de riesgo operacional pueden tener planes de acción** con sus respectivos responsables y fechas de compromiso, esto debe ser gestionado a través de la solución tecnológica.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución tecnológica **debe permitir asignar un mismo plan de acción a varios eventos** de riesgo operacional.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución tecnológica **debe permitir la parametrización y configuración de todos los campos utilizados para el registro de eventos de riesgo operacional**, de acuerdo con lo dispuesto por la Circular Básica Financiera y Contable, considerando además aquellos que fueron incluidos por la metodología específica SARO del Banco:

|  |  |  |  |
| --- | --- | --- | --- |
| **Campo** | **Variable** | **Tipo** | **Clasificación Interna** |
| ID Evento |  | Calculado por el sistema | Mandatorio |
| Área | Alfanumérico | Obligatorio | Auxiliar |
| Fecha Reporte | Fecha | Obligatorio | Mandatorio |
| Reporte | Alfanumérico | Obligatorio | Mandatorio |
| Evento | Alfanumérico | Obligatorio | Auxiliar |
| Impacto | Alfanumérico | Obligatorio | Auxiliar |
| Factor de Riesgo | Alfanumérico | Opcional | Auxiliar |
| Proceso Originador | Alfanumérico | Obligatorio |  |
| Procesos Impactado (Lista desplegable de la cual pueden seleccionarse varios valores para este campo) | Alfanumérico | Obligatorio | Mandatorio |
| Líneas operativas | Alfanumérico | Obligatorio | Mandatorio |
| Producto o Servicio afectado | Alfanumérico | Opcional | Auxiliar |
| Servicio o Aplicativo Tecnológico | Alfanumérico | Opcional | Auxiliar |
| Clasificación de los riesgos operacionales nivel I | Alfanumérico | Obligatorio | Mandatorio |
| Clasificación de los riesgos operacionales nivel II | Alfanumérico | Obligatorio | Mandatorio |
| Clasificación de los riesgos operacionales nivel III | Alfanumérico | Obligatorio | Mandatorio |
| Caso Linea 800 (Helpdesk) | Alfanumérico | Opcional | Auxiliar |
| Fecha inicio evento | Fecha-Hora | Obligatorio | Mandatorio |
| Fecha finalización evento | Fecha-Hora | Obligatorio | Mandatorio |
| Fecha descubrimiento | Fecha-Hora | Obligatorio | Mandatorio |
| Tipo de evento | Alfanumérico | Obligatorio | Mandatorio |
| Fecha contabilización | Fecha-Hora | Obligatorio | Mandatorio |
| Divisa | Alfanumérico | Obligatorio | Mandatorio |
| Cuantía Bruta | Moneda | Obligatorio | Mandatorio |
| Ctas contables afectadas (Gastos) | Alfanumérico | Obligatorio | Mandatorio |
| Fecha recuperación | Fecha-Hora |  |  |
| Cuantía recuperada por seguros | Moneda | Obligatorio | Mandatorio |
| Cuantía Otras Recuperaciones | Moneda | Obligatorio | Mandatorio |
| Cuantía total recuperada (campo calculado) | Moneda | Obligatorio | Mandatorio |
| Cuantía Neta de Recuperaciones (campo calculado) | Moneda | Obligatorio | Mandatorio |
| Ctas contables afectadas (Ingresos) | Alfanumérico |  |  |
| Comentarios Riesgo Operativo | Alfanumérico | Opcional | Auxiliar |
| Departamento responsable del tratamiento | Alfanumérico | Opcional | Auxiliar |
| Director responsable del tratamiento | Alfanumérico | Opcional | Auxiliar |
| Funcionario responsable del tratamiento | Alfanumérico | Opcional | Auxiliar |
| Definición tipo de tratamiento | Alfanumérico | Opcional | Auxiliar |
| Describir el (los) plan de acción (s) a implementar para minimizar la ocurrencia e impacto del evento | Alfanumérico | Opcional | Auxiliar |
| Tipificación plan de acción | Alfanumérico | Opcional | Auxiliar |
| Estado | Alfanumérico | Obligatorio | Auxiliar |
| Fecha Atención  (dd-mmm-aa) | Fecha | Opcional | Auxiliar |
| Fecha Implementación del Plan o cierre  (dd-mmm-aa) | Fecha | Opcional | Auxiliar |
| Afectación | Alfanumérico | Opcional | Auxiliar |
| Número riesgo afectado | Depende del tipo de ID riesgo de la plataforma | Opcional | Auxiliar |
| Control Afectado | Depende del tipo de ID control de la plataforma | Opcional | Auxiliar |
| Próxima fecha de seguimiento   (dd-mmm-aa) | Fecha | Opcional | Auxiliar |
| Observaciones seguimiento Plan de Acción | Alfanumérico | Opcional | Auxiliar |
| Estado Evento (uso interno) | Alfanumérico | Opcional | Auxiliar |
| Gestor ORO | Alfanumérico | Opcional | Auxiliar |

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es posible que en el futuro **se deban incluir más campos, por lo que la solución tecnológica debe ser flexible para tal fin**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Algunos de los campos tienen **listados de valores que deberán quedar configurados en el sistema y podrán ser actualizados cuando así el Banco lo requiera**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Los eventos de riesgo operacional pueden presentarse por la falla de un control específico en un riesgo, es deseable, no requisito, que la solución tecnológica permita identificar el control que falló.

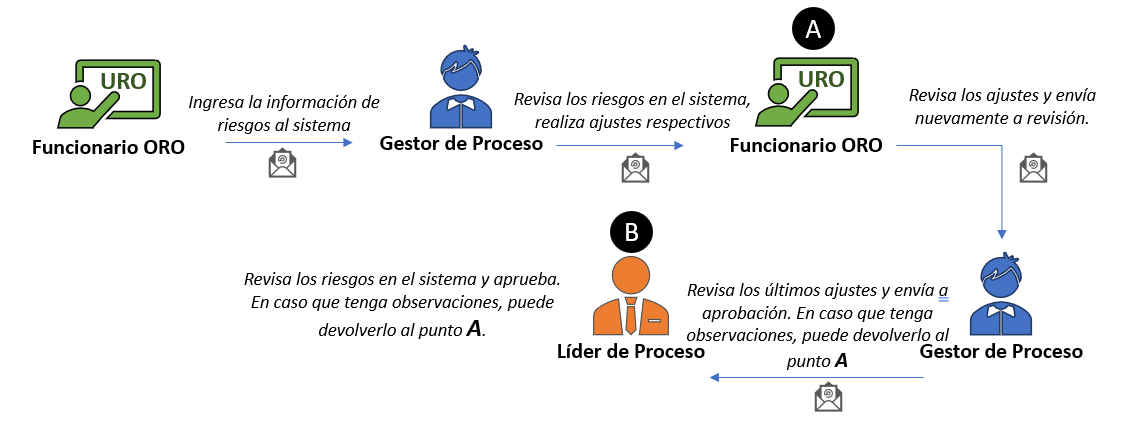
|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Flujos de Información y Aprobación

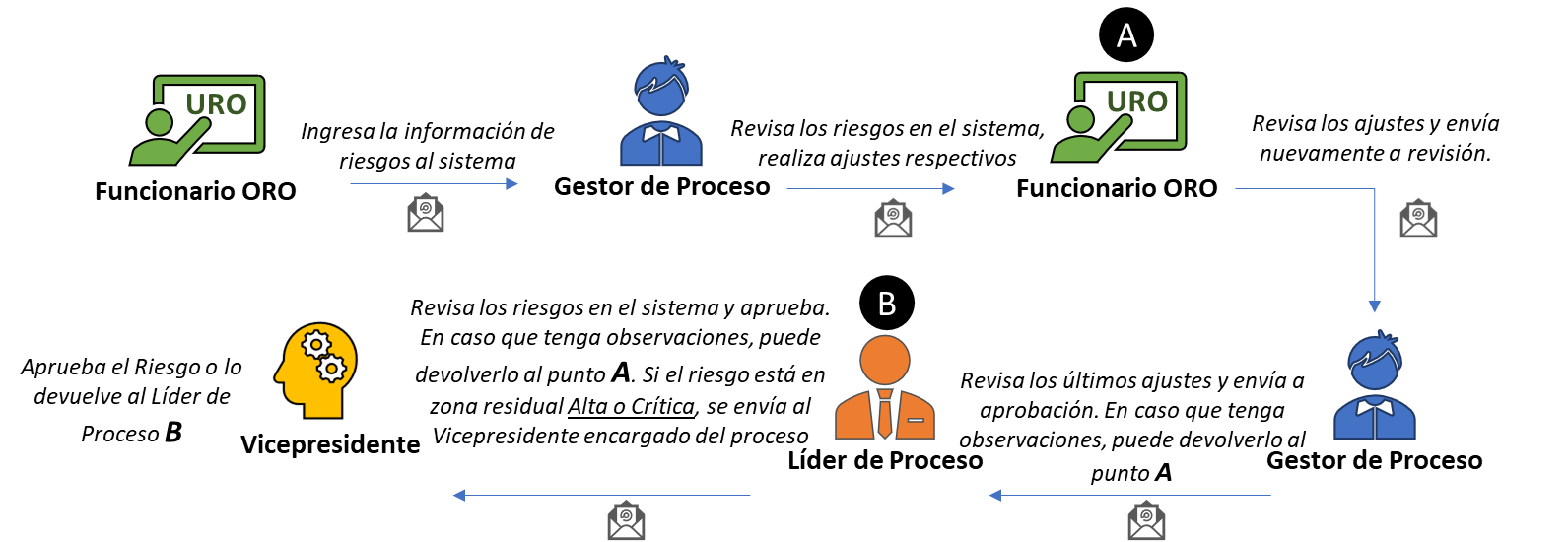
##### Creación/Actualización/Eliminación de Riesgos

* Es deseable, no requisito que la solución tecnológica permita implementar uno o varios de los siguientes flujos para este fin:

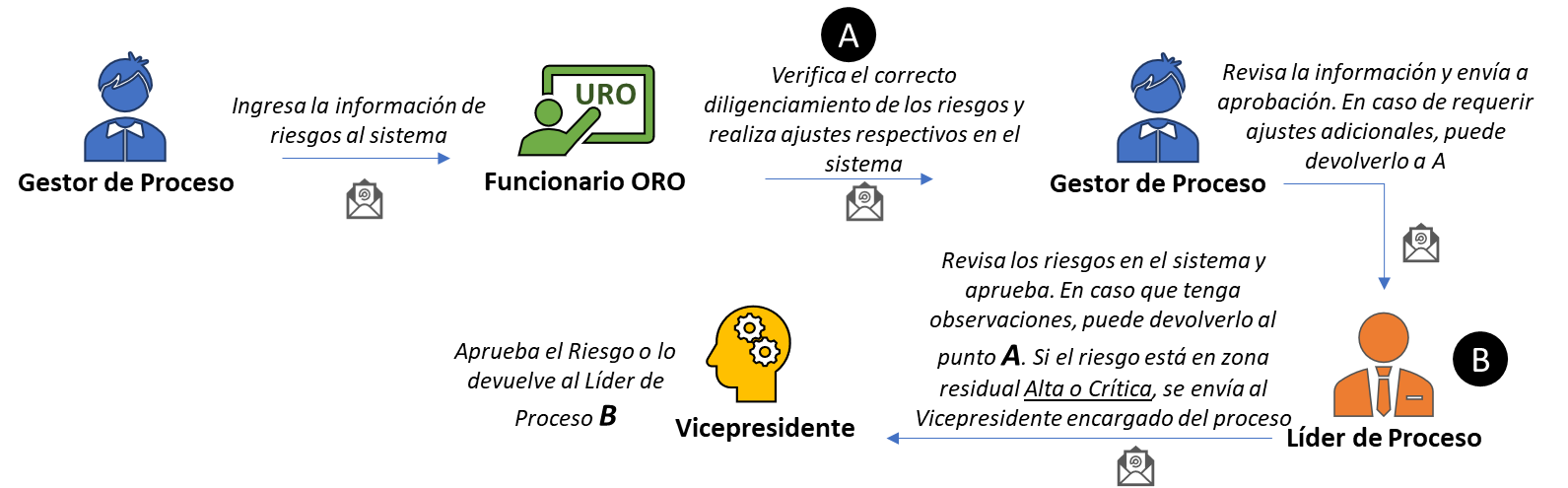
Flujo 1 – Aprobación de Riesgos:



Flujo 2 – Aprobación de Riesgos:



Flujo 3 – Aprobación de Riesgos:



El proponente **debe aclarar cuáles de los flujos expuestos soporta la solución o si cuenta con flujos diferentes propios**, por favor explicarlos.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

##### Asignación de Planes de Acción

* Cuando se asigne un Plan de Acción para el Tratamiento de Riesgos a un funcionario del Banco, es deseable, no requisito, que **la solución tecnológica envíe un correo electrónico con la notificación respectiva al responsable de su ejecución**. Es deseable que se envíen notificaciones N días previos al vencimiento de un Plan de Acción de Tratamiento de Riesgos. **El proponente debe indicar qué se requiere técnicamente para el envío de estas notificaciones (conexiones a correo, plantillas, etc.)**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que cuando se asigne un Plan de Acción para la Gestión de Eventos de Riesgo Operacional a un funcionario del Banco, **la solución tecnológica envíe un correo electrónico con la notificación respectiva al responsable**. Es deseable, que se envíen notificaciones N días previos al vencimiento de un Plan de Acción para la Gestión de Eventos de Riesgo Operacional. **El proponente debe indicar qué se requiere técnicamente para el envío de estas notificaciones (conexiones a correo, plantillas, etc.)**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

##### Notificaciones

* Es un deseable, no requisito, que la solución tecnológica permita parametrizar diferentes tipos de notificaciones orientados a informar responsabilidades (actividades por hacer)

|  |  |  |
| --- | --- | --- |
| ¿Qué? | ¿Cuándo? | ¿A quién? |
| Correo con link vínculo al sitio para revisión. | Se levantan todos los riesgos de un proceso. Se enviaría por demanda a solicitud del funcionario ORO. | Gestor de Proceso |
| Correo con link vínculo al sitio para revisión y aprobación. | Se revisan todos los riesgos de un proceso. Se enviaría por demanda a solicitud del Gestor de Proceso | Líder de Proceso |
| Correo con el detalle del plan de acción y la fecha de compromiso. | Se asigna el Plan de Acción de Tratamiento de un riesgo | Responsable de Plan de Acción |
| Correo con el detalle del plan de acción y la fecha de compromiso. | Se asigna el Plan de Acción de Gestión de un Evento de riesgo operacional | Responsable de Plan de Acción |
| Correo con el detalle del plan de acción y la fecha de compromiso. | Faltan 15 días para el vencimiento del Plan de Acción. | Responsable de Plan de Acción. |

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Reportes

* La solución tecnológica **debe permitir la parametrización de diferentes tipos de reportes a partir de la información que sea cargada en la misma**. En lo posible, que los reportes generados puedan contener tantos campos como sean deseados por el Administrador Funcional de la solución.

El proponente debe indicar con claridad si **puede configurar reportes por demanda del Banco, o si cuenta con un listado específico de reportes predefinidos configurables, caso en el cual, agradecemos enviar el listado**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Entre otros, se espera que la solución tecnológica permita la generación de los siguientes reportes:
  + Total de Riesgos y controles con valoración inherente y residual.
  + Riesgos y controles por proceso con valoración inherente y residual.
  + Riesgos por factor, por origen, etc.
  + Riesgos por metodología de valoración de riesgos (si aplica).
  + Listado total de eventos de riesgo operacional.
  + Reporte de planes de tratamiento con responsables, fechas de vencimiento y avances.
  + Informe de perfil de riesgo del Banco.

El proveedor debe indicar con claridad si **cuenta con estos reportes en su herramienta**. Agradecemos enviar material gráfico como soporte a la respuesta.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Los **reportes deben poder ser exportados fácilmente a Excel**. Deseable, no requisito, que también se envíen directamente a documentos Word para su gestión.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Los **reportes deben permitir filtrado por campos clave**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito que la solución permita la **configuración y visualización de indicadores de riesgos KRI mediante un *dashboard*. El proponente debe enviar pantallas tipo del *dashboard,* si lo tiene.**

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que la solución permita **configurar el diseño de los reportes (logo del Banco, encabezados, etc.),** con el fin de reducir labores operativas y generar valor a la organización.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* El proponente debe enviar **pantallas tipo de los gráficos, indicadores, diseño de reportes e interfaz gráfica de la solución propuesta**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

### Requerimientos no funcionales

* Es deseable, no requisito, que la solución tecnológica **permita ser multiempresa**. Esto, pensando en un futuro, a largo plazo, en el que se integren varias empresas al Grupo Bancóldex o al Grupo Bicentenario. De momento, **solo tendríamos e implementaríamos Bancóldex**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que la solución **permita cargar información de Excel u otras fuentes como los datos de los incidentes reportados a la mesa de servicio para ser utilizada como insumo para poblar los eventos de riesgo operacional**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que la solución tecnológica **permita implementar umbrales asociados al Apetito, Tolerancia y Capacidad de riesgo,** y que en este sentido genere alertamientos cuando las pérdidas económicas de los eventos estén alcanzando este umbral en un periodo de tiempo.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Roles y Perfiles

* Se requiere que los funcionarios de la Oficina de Riesgo Operativo (5) puedan ingresar a realizar la administración funcional de la solución tecnológica. 3 funcionarios lo harían de forma concurrente.
* Es deseable, no requisito, que los gestores de proceso (40 aproximadamente) puedan ingresar a revisar los riesgos de sus procesos.

|  |
| --- |
| Por favor indique a continuación **con claridad**, si existe un rol para esta labor en la solución propuesta. |
|  |

* Es deseable, no requisito, que los líderes o dueños de proceso (25) puedan ingresar a la solución tecnológica para aprobar los riesgos a su cargo.

|  |
| --- |
| Por favor indique a continuación **con claridad**, si existe un rol para esta labor en la solución propuesta. |
|  |

* Se requiere un rol de consultas para que la contraloría o revisoría puedan ingresar sin modificar la información de los riesgos.

|  |
| --- |
| Por favor indique a continuación **con claridad**, si existe un rol para esta labor en la solución propuesta. |
|  |

* Es deseable, no requisito, **que todos los funcionarios (370) puedan informar/reportar la materialización de riesgos en sus procesos (eventos de riesgo operacional) a través de un cuestionario brindado por la solución tecnológica**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, si existe un rol para esta labor en la solución propuesta. |
|  |

* Es deseable, no requisito, que todos los funcionarios puedan ingresar a conocer los riesgos asociados a sus procesos.

|  |
| --- |
| Por favor indique a continuación **con claridad**, si existe un rol para esta labor en la solución propuesta. |
|  |

* 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.).**

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Información Histórica

* **Se espera que la solución tecnológica permita generar una vista (Foto) del perfil de riesgo de la organización con todos sus riesgos, controles, tratamientos y planes de acción.** Es deseable, no requisito, **que esta foto pueda ser conservada intacta para futuras consultas, permitiendo realizar otra evaluación para el año vigente.** Esto, con el fin de tener las versiones anteriores del perfil de riesgo del Banco y así poder ver la evolución del riesgo en el tiempo. **El proponente debe indicar si desde su solución se puede generar esta vista**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución **debe permitir identificar los responsables de la aprobación del riesgo**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe permitir **identificar quién realizó la modificación de algún riesgo**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe permitir **identificar los usuarios que realizan cualquier modificación sobre la plataforma** (adición de procesos, modificación de controles, cambio en metodología, etc.). Logs.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución tecnológica **debe permitir el cargue de los riesgos, controles y eventos actuales en el Banco**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es necesario **mantener la historia de la gestión de riesgos sin que esta se vea afectada por los cambios metodológicos.** Es decir, si los cálculos cambian en el año 2022, la calificación de los riesgos de 2021 no puede verse afectada. **El proponente debe indicar con claridad si la actualización de cálculos en la metodología, realiza una alteración en cascada o solo para la vista del perfil actual**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

## Módulo de Auditoría

### Definiciones

* Plan Anual de Auditoría – PAA: Establece los trabajos de auditoría a realizar para el siguiente año, con los objetivos generales, temas específicos, responsables y tiempos de ejecución. Las actividades que contemplan este plan se encuentran descritas en el Plan Operativo Anual - POA en la estrategia número II - “Prestar servicios de Aseguramiento”.
* Plan Operativo Anual – POA: Herramienta que contiene las estrategias (I-IV), actividades, tareas, capacitaciones y vacaciones que realizará la Contraloría Interna durante el año en curso. A través de esta herramienta se monitorea la gestión del área en el cumplimiento de sus actividades de aseguramiento, consultoría y administrativas.
* Planeación Individual de Trabajos de Auditoría: Etapa de la Auditoría en la que los auditores planean los trabajos de auditoría asignados, para ser desarrollados dentro de cronogramas establecidos, de acuerdo con el Plan Operativo Anual (POA). Para esto deben desarrollarse las etapas de pre - planeación, definición del plan y programa del trabajo, y aprobación.
* Ente Auditable: Cualquier proceso, actividad o riesgo sujeto a ser auditado.
* Plan de mejoramiento: Documento donde se detalla el criterio evaluado, la condición, las causas y respectivas oportunidades de mejora.
* Oportunidad de mejora: Recomendación emitida por la Auditoría del “cómo” pudiera ser solucionada la deficiencia observada.
* Plan de Acción: Plan definido por el dueño de proceso o responsable para subsanar o corregir las observaciones presentadas por la Auditoría. Este plan incluye cada una de las acciones necesarias, incluyendo las fechas de compromiso y responsables para cada una.
* Universo de Auditoría: Es una lista de todas las auditorías posibles que se pueden realizar. Dentro de esta lista se incluye los procesos y subprocesos, planes y proyectos estratégicos, las revisiones normativas, las unidades de negocio y/o dominios que no cuentan con procesos y los riesgos operativos de la organización.

### Requerimientos Funcionales

#### Inventario y cargue de entes auditables

Para la elaboración del Plan Anual de Auditoría, así como para la planeación de cada una de las auditorías, se requiere obtener e integrar diferentes insumos, tales como: Riesgos Operacionales, Riesgos Tecnológicos, Riesgos Estratégicos, Cadena de Valor (Procesos y Subprocesos), normatividad de entes de control externo, marcos de referencia, mejores prácticas y guías.

Con el fin de poder efectuar las auditorías sobre procesos, la solución:

* Debe permitir realizar el cargue y actualizar (manual o automático) dentro del módulo de auditoría el inventario de la cadena de valor del Banco (macroprocesos, procesos y subprocesos).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe permitir el cargue de otros insumos, ejemplo: proyectos, activos de información, resultados de evaluaciones de terceros, resultados de auditorías anteriores, etc.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir, dentro del módulo de auditoría, cargar y actualizar el inventario de riesgos operacionales, tecnológicos, estratégicos, sus controles, sus modificaciones y los eventos de riesgo operacional.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir el cargue e integración de los marcos normativos de entes de control, ejemplo: SARO, SGSI, SARE, SARL, SARC, SARLAFT, SARM, AMV.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir realizar el cargue, actualización e integración de marcos de referencia de control, ejemplo: COSOs, COBITs, ISOs, ITIL, NIAs, SOX.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe integrar visualización e interacción (no modificación) desde módulo de auditoría, con cada riesgo y control del módulo de riesgos operacionales, así como guardar el historial de los riesgos y controles auditados.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Metodología de Planeación Anual

Plan Anual de Auditoría: Se elabora una vez al año, y consiste en la aplicación de una metodología previamente definida, donde se establecieron indicadores cualitativos y cuantitativos, para identificar los entes auditables con mayor riesgo a ser incluidos en el Plan. A cada indicador o ítem se le asigna un porcentaje para obtener la calificación de criticidad y poder realizar la priorización de los entes auditables a asegurar.

Diagram

Description automatically generated

Como resultado de la aplicación de esta distribución, se define el Plan de Auditoría a Corto Plazo (año siguiente) y largo Plazo (2 años siguientes al primero) para dar cubrimiento al 100% del universo, en cada ciclo de 3 años.

En este Plan se establecen/estiman los siguientes aspectos para cada uno de los trabajos a realizar: El trimestre en cual se planea realizar, qué auditores van a participar, el tiempo/duración del trabajo, el objetivo inicial, el alcance y enfoque inicial que se va a dar.

* La solución debe ser parametrizable para **soportar la metodología de Bancoldex**. En caso de que la solución cuente con una metodología propia/diferente, se debe presentar/explicar la misma de manera detallada.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe **ser flexible para soportar ajustes o cambios en la metodología**, definir y asignar parámetros nuevos, cargar valores internos y externos, realizar cálculos, integrar criterios y ponderaciones de priorización, para definir y priorizar las auditorías del Plan.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe permitir parametrizar y **generar diferentes tipos de reportes y gráficos** definidos por Bancoldex, y tener la posibilidad de exportarlos a Office.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* **Generar la propuesta "inicial" del plan anual de auditoría** como resultado de la metodología, y registrar y controlar los posibles cambios que se presenten durante su desarrollo.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Planeación de las Auditorías

Definido el Plan Anual de Auditoría, se inicia con su ejecución, mediante la Planeación de cada una de las auditorías. En esta etapa se analizan de forma individual cada uno de los ítems pre-establecidos con el objetivo de determinar el alcance, enfoque, los procedimientos y pruebas a realizar, los tiempos de duración y el equipo de trabajo.

Diagram

Description automatically generatedDiagram

Description automatically generated

* La solución debe permitir la definición y parametrización del **formato de Pre-planeación de Auditoría**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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; así mismo permitir parametrizar, generar reportes y gráficos y exportar a Office el documento de pre-planeación.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe permitir la definición de Procedimientos y pruebas de auditoría (de acuerdo con el resultado de los elementos analizados en la pre-planeación), y asignarles tiempos y recursos de acuerdo con los perfiles de los auditores (tecnología, financiero, etc.). Así mismo permitir parametrizar, generar reportes y gráficos y exportar a Office el documento de "Plan y Programa".

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Ejecución de las Auditorías

Definido el Plan y Programa de cada Auditoría, se inicia su ejecución, en la cual se documentan el desarrollo y los resultados de las pruebas realizadas, su calificación, y si generan o no Planes de Mejoramiento y recomendaciones.

Diagram

Description automatically generatedDiagram

Description automatically generatedDiagram

Description automatically generated

El trabajo de auditoría tiene un tiempo estimado tanto total, como para cada prueba.

Los auditores proceden a realizar las pruebas, donde una vez concluida cada una de ellas debe ser informada al Contralor para su revisión y aprobación.

El resultado de cada prueba tiene una calificación de acuerdo con su impacto, y genera una acción, con un plazo máximo, de acuerdo con la siguiente tabla:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sin Impacto | Menor | Moderado | Importante | Mayor |
| No genera o genera recomendaciones, cuya implementación será potestad del líder del proceso. | Genera Plan de Mejoramiento. Plazo máximo de implementación de un (1) año. | Genera Plan de Mejoramiento. Plazo máximo de implementación de seis (6) meses. | Genera Plan de Mejoramiento. Plazo máximo de implementación de un (1) año.Implementación de control mitigante de cuatro (4) meses. | Genera Plan de Mejoramiento. Plazo máximo de implementación de un (1) año. Implementación de control mitigante de dos (2) meses. |

En caso de presentarse alguna desviación u observación resultado de la prueba, se procede a elaborar una comunicación intermedia, la cual, de acuerdo con su impacto, tiene diferentes niveles de aprobación, tanto por el área responsable, como dentro de la Contraloría Interna. En este sentido, la solución:

* Debe permitir **parametrizar cada uno de los componentes del proceso de ejecución** (calificación, resultados, criterios, condición causas, efecto, oportunidades de mejora y recomendaciones y plan de acción).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir **llevar trazabilidad de toda la ejecución de los trabajos** (tiempos de ejecución de actividades, alertas e indicadores de operación).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir **parametrizar, generar reportes y gráficos y exportar a Office los informes detallados y reportes de Ejecución de la Auditoría**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir **flujos de actividades entre la auditoría y los auditados** de acuerdo con niveles jerárquicos de aprobación.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir **integrar e indexar los papeles de trabajo respectivos a cada proyecto de auditoría** (integración con Office365 y Onedrive dispuestos por el Banco).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Debe permitir la **formulación de planes de mejoramiento** por parte de la auditoría, así como sus acciones, fechas y responsables por parte de los líderes de los procesos auditados.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Gestión de Planes de Mejoramiento y Seguimiento Plan

Las Acciones de Mejora generadas, deben ser gestionadas por los dueños de las actividades y monitoreadas por el auditor a cargo, hasta que se cierren de manera satisfactoria.

El Plan Anual, tiene seguimiento y monitoreo permanente, para poder identificar su avance y desviaciones y tomar acciones oportunas.

Diagram, schematic

Description automatically generated

* La solución debe permitir **mantener el inventario de planes de mejoramiento integrados por proceso, responsable, fechas de compromiso o vencimientos, riesgos, con registro y soportes de avance o cumplimiento de las acciones definidas por el Auditado**. Así mismo permitir parametrizar, generar reportes y gráficos y exportar a Office.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe **permitir registrar el inventario de recomendaciones y estado (aceptación o no, y gestión).** Así mismo permitir parametrizar, generar reportes y gráficos y exportar a Office.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* **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.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe permitir generar **consultas de los riesgos y controles auditados, y el resultado de estas evaluaciones. Adicionalmente, permitir generar mapas de riesgos de auditoría (mapa sombra: mapa similar al de Riesgo Operacional pero desde la óptica de la Auditoría. No debe afectar la información del módulo de riesgo operacional)**. Así mismo permitir parametrizar, generar reportes y gráficos y exportar a Office.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene (mapa sombra). En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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).**

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Flujos de aprobación

Las actividades y documentos elaborados en las diferentes etapas (comentadas en los numerales anteriores), son remitidos a diferentes participantes del proceso, para su elaboración, revisión y/o aprobación según su nivel jerárquico y definición del área. Estos flujos de actividades deben registrarse y tramitarse a través de la herramienta.

* 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**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución **debe permitir parametrizar el flujo de actividades, registro y soportes de avance (por parte del auditado) así como las revisiones y autorizaciones de ejecución** (cierre acciones de mejoramiento, o reformulaciones, por parte de auditados y auditores según roles).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### 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.**

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

#### Entes de Control y otras actividades

El departamento de Contraloría/Auditoría realiza una serie de actividades/tareas para dar cumplimiento a requerimientos regulatorios, tales como reportes, transmisiones, publicaciones, informes, entre otros. Adicionalmente efectúa coordinación y apoya el flujo de información para apoyar requerimientos de entes externos y mantener actualizada a la Organización y Comité de Auditoría del avance y cumplimiento de estas actividades. **Se busca que la herramienta permita administrar y monitorear el inventario de actividades, el avance de estas y su cumplimiento**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

### Requerimientos no funcionales

* La solución debe garantizar los criterios de confidencialidad, integridad y disponibilidad de los documentos que son utilizados como papeles de trabajos y evidencias. (manejo seguro).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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).** Es posible que se utilicen herramientas como Onedrive que actualmente tiene el Banco como repositorio de información. El proponente debe especificar con claridad en su propuesta, cómo atendería este requerimiento.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe dejar registro (logs) de ejecución de las actividades de planeación, ejecución y seguimiento de la auditoría, así como del flujo de estas.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable, no requisito, que las áreas de riesgo (diferentes a la Auditoría y con un perfil especial) puedan acceder a los resultados de las auditorías y planes de acción sobre los que estén vinculados.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

## Otros requerimientos no funcionales transversales de la solución

* Es importante que la solución sea escalable y que, por tanto, permita **posteriormente implementar otros elementos del enfoque GRC**.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Se espera que la solución tecnológica se presente en **ambiente web,** con un entorno amigable y fácil de usar para los usuarios.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Se requiere que el proveedor entregue todos los manuales técnicos, de administración funcional y de usuario final para el uso de la solución tecnológica.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable que la solución cuente con ayudas interactivas que permitan al usuario identificar las descripciones de los campos, errores en el diligenciamiento, etc.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable que la solución tecnológica permita acceder vía aplicación móvil o que, en su defecto, pueda accederse a través de los navegadores de los móviles, siendo esta de tipo *responsive*.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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.).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe contar con manuales técnicos, manuales de usuario, menús, informes, reportes, módulos, en español.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Los reportes deben ser exportables a Word o Excel para poder realizar su edición en caso tal que se requiera.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* La solución debe permitir generar informes con datos en texto plano o Excel para su fácil manejo por parte de los usuarios, permitiendo filtrar para exportar cualquier elemento de información o campo.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* Es deseable que se pueda realizar consultas en la solución por palabras clave.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

* 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).

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. Puede presentar recursos gráficos si los tiene. En caso de que la solución no cubra este requerimiento, es necesario que lo especifique en este campo. |
|  |

# REQUERIMIENTOS TÉCNICOS Y DE SEGURIDAD

## Observaciones Generales

Los requerimientos técnicos y de seguridad a los que hace referencia este documento se basan sobre el entendimiento de que el servicio a implementar para soportar la gestión de riesgo operacional y de auditoría de Bancóldex utilizará un esquema SaaS. En caso de que la propuesta de implementación sea en nube, el proveedor deberá garantizar el cumplimiento de la Circular Externa 005 de 2019 emitida por la Superintendencia Financiera de Colombia[[3]](#footnote-3) - Reglas relativas al uso de servicios de computación en la nube.

De igual forma, el proveedor del servicio debe garantizar el cumplimiento de lo que le corresponde según Circular Externa 042 de 2012 emitida por la Superintendencia Financiera de Colombia[[4]](#footnote-4).

## Arquitectura software

El proponente deberá describir la arquitectura del software de la solución que está ofreciendo, el proceso de desarrollo asociado y las tecnologías utilizadas.

### Tipo de software

Se deberá describir el esquema bajo el cual se hará la implementación del sistema. El banco desea una solución bajo un esquema SaaS, para esto se deberá documentar si ya se cuenta con una solución base con componentes ya implementados y de acuerdo con los requerimientos específicos del banco es complementar las funcionalidades con desarrollos adicionales o si se va a hacer un desarrollo desde ceros para cumplir con los requerimientos solicitados por el banco.

|  |
| --- |
| Por favor indique a continuación con claridad el tipo de solución propuesta. |
|  |

### Arquitectura

Se deberá describir la arquitectura de la solución ofrecida si está tiene un esquema monolítico o es orientada bajo el concepto de microservicios.

|  |
| --- |
| Por favor indique a continuación cómo es la arquitectura del sistema: |
|  |

### Diagrama de componentes[[5]](#footnote-5)

Se deberá presentar un diagrama de alto nivel donde se describan claramente cada una de las capas, componentes y/o módulos de cómo está construido o cómo se va a construir la solución. Se deben describir las tecnologías y lenguajes de desarrollo utilizados para la construcción de los componentes que conforma el sistema.

|  |
| --- |
| Por favor presente a continuación adjunte un diagrama donde se vean claramente las capas del sistema: |
|  |

### Diagrama de despliegue[[6]](#footnote-6)

Se deberá presentar un diagrama de despliegue donde se explique claramente la arquitectura de despliegue de la solución. El sistema debe tener mínimo 3 capas (Datos, Aplicación, Presentación), este diagrama debe dar una descripción clara de los actores del sistema, componentes de software, la infraestructura y comunicaciones que soportan la solución y donde está desplegada.

|  |
| --- |
| Por favor presente a continuación un diagrama de despliegue donde se vean claramente los servidores que utiliza la aplicación y el software que está desplegado en cada uno de estos. |
|  |

### Licenciamiento

El proponente deberá describir el esquema de licenciamiento de la plataforma, detallando los costos que se aplicará por el uso de esta. Todos los componentes de software requeridos por la plataforma para su funcionamiento deben estar debidamente licenciados o ser de propiedad del proponente.

|  |
| --- |
| Por favor indique a continuación **con claridad** la respuesta a este requerimiento. |
|  |

## Arquitectura infraestructura

### Plataforma tecnológica

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.

La solución propuesta como mínimo debe contar con 3 ambientes el de desarrollo, pruebas y producción. El proponente deberá dar una descripción de como la solución implementa estos ambientes.

|  |
| --- |
| Por favor describa a continuación **con claridad** la plataforma tecnológica que soporta la solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Ambientes

El sistema debe contar con ambientes totalmente independientes para los procesos de desarrollo, pruebas y producción[[7]](#footnote-7). Se deberá presentar una descripción de cómo se tienen implementados estos ambientes para la solución que se está ofreciendo.

Para los ambientes de pruebas y desarrollo solo debe permanecer el software que está siendo probado o desarrollado. Si el Banco no se encuentra en alguna de estas fases, en los servidores no debe permanecer instalación del software ni información del Banco. El proponente debe garantizar la destrucción de estos una vez finalizada la prueba.

Los ambientes mínimos que se esperan sean entregados al Banco son Pruebas y Producción.

|  |
| --- |
| Por favor describa a continuación **con claridad** los ambientes con los que cuenta la solución tecnológica que soporta la solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Ambiente de desarrollo

Es un ambiente que es instalado por los grupos de desarrollo y que tiene como propósito soportar los procesos de codificación de software para el desarrollo de nuevas funcionalidades solicitadas por un usuario.

### Ambiente de pruebas

Es un ambiente donde se instalan las funcionalidades solicitadas por los usuarios con el propósito de que grupos de pruebas o usuarios finales puedan validar y verificar que las funcionalidades implementadas cumplen con los requisitos solicitados.

### Ambiente de producción

Es el ambiente donde los usuarios finales interactúan con el sistema, en este se encuentran todas las funcionalidades que fueron certificadas y que cumplen con las necesidades del usuario.

### Alta disponibilidad

Se deberá explicar a nivel de la infraestructura tecnológica que soportará el sistema, si cuenta con esquemas de alta disponibilidad o con esquemas que permitan extender incorporar esta característica con el fin de garantizar que el sistema seguirá funcionando si alguno de sus componentes presenta una falla.

|  |
| --- |
| Por favor describa a continuación **con claridad** los esquemas de alta disponibilidad que ofrezca la solución propuesta. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Disponibilidad

El proponente deberá especificar en su propuesta el acuerdo de nivel de servicio (SLA[[8]](#footnote-8)) de disponibilidad que se compromete a cumplir sobre la solución que ofrece, el cual debe ser igual o superior al 99.5%. 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. El incumplimiento de este SLA dará lugar a la penalización en los costos que el Banco pague por el servicio contratado. En los casos de indisponibilidad por mantenimientos programados, el proveedor deberá informar a Bancóldex el plan de trabajo establecido con mínimo quince (15) días hábiles de antelación para acordar y aprobar los horarios de los mantenimientos, esto con el fin de no afectar la operación y notificar con tiempo la indisponibilidad de la solución al cliente. El proponente debe describir cómo maneja el procedimiento de los mantenimientos programados sobre el sistema.

|  |
| --- |
| Por favor describa a continuación **con claridad** el porcentaje dedisponibilidadofrecido en la solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Contingencia

Se deberá explicar a nivel de la infraestructura si esta cuenta con esquemas de contingencia donde sus componentes se replican o pueden replicarse a centros de datos secundarios en caso de una falla en el datacenter principal. El proponente debe especificar la ubicación de sus centros de cómputo y de operación alternos.

|  |
| --- |
| Por favor describa a continuación **con claridad** los esquemas de contingencia que ofrezca la solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Escalabilidad

Se deberá explicar si la solución cuenta con la capacidad de escalar vertical u horizontalmente cuando se la demanda de peticiones aumente, detallar si este escalamiento se hace de forma automática o manual y cómo se hace.

|  |
| --- |
| Por favor describa a continuación **con claridad** la escalabilidad de la solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Monitoreo

El proponente deberá contar con monitoreo continuo de su plataforma tecnológica para identificar comportamientos inusuales o ciberataques, dicho monitoreo debe detectar operaciones o cambios no deseados y/o adelantar las acciones preventivas o correctivas cuando se requiera. Este debe informar al banco en su propuesta como hace este monitoreo y establecer las estrategias de notificación y comunicación con el Banco en caso de interrupción.

|  |
| --- |
| Por favor describa a continuación **con claridad** el esquema de monitoreo de la solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Backups

El proponente deberá tomar los backups de la información y del software de acuerdo con la periodicidad que el Banco le señale, para esto se deberá hacer una descripción general del esquema de backup que se tiene implementando. Adicionalmente, deberá entregar de manera periódica, previo acuerdo entre las partes, medios removibles o digitales en el formato que se establezca, la información respaldada para almacenamiento del Banco.

El respaldo de la información debe estar a disposición del Banco cuando la requiera. Las copias de respaldo de la información deben contar con independencia de las de otras entidades que procesan en la nube. La independencia se puede dar a nivel lógico o físico.

|  |
| --- |
| Por favor describa a continuación **con claridad** el esquema de respaldo de la información sobre solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo describir también que mecanismos se utilizarán para entregar la información al banco de acuerdo con la periodicidad que se defina |
|  |

## Arquitectura de seguridad

### Análisis de vulnerabilidades

El proponente deberá ejecutar análisis de vulnerabilidades a todos los elementos de infraestructura que soportan la solución ofrecida, una vez terminada su ejecución se deberá compromete a realizar el plan de remediación en plazo máximo de 30 días para las clasificadas en críticas, 60 días las moderadas y 90 días las bajas. Estos informes con sus respectivos planes de remediación deberán ser entregados al Banco junto con el análisis diferencial comparando con el informe actual y el inmediatamente anterior para su revisión y conservación.

La periodicidad de ejecución de esta actividad deberá ser como mínimo 2 veces al año o cuando haya cambios importantes en la infraestructura y con los lineamientos que establece la Circular 042 de 2012 de la Superintendencia Financiera de Colombia en su numeral 7.

Se deberá dar una descripción si a la infraestructura del sistema ya se le aplica este proceso y con qué periodicidad se realiza, o si se debe implementar esto como un nuevo proceso.

A su vez el proveedor debe compartir los informes test y re-test de los análisis ejecutados con la finalidad de poder garantizar que efectivamente fueron realizados y los hallazgos remediados. Dichos informes serán soporte ante los entes regulatorios.

De preferencia, esta actividad debe ser realizada mediante herramientas homologadas CVE - Common Vunlnerabilities Exposures.

|  |
| --- |
| Por favor describa a continuación **con claridad** el esquema de gestión de vulnerabilidades que se realiza sobre solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Ethical Hacking

El proponente debe ejecutar pruebas de Ethical Hacking y emprender las acciones requeridas para remediar los hallazgos identificados en dichas pruebas, como evidencia de las pruebas es requerido compartir los informes de las pruebas realizadas como soporte de las ejecuciones y remediaciones implementadas.

|  |
| --- |
| Por favor describa a continuación **con claridad** cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Desarrollo seguro

El proponente debe confirmar si cuenta con un proceso de desarrollo seguro y hacer la descripción de cómo hace la implementación de este detallando las herramientas o tareas que realiza para cumplir con este requerimiento. Así mismo, deberá entregar un informe de la ejecución de pruebas de desarrollo seguro donde se evidencie que este no tiene fallas de seguridad, al igual que las pruebas de vulnerabilidad, se requiere que los resultados de los informes sean suministrados para los entes que los soliciten. También es válido presentar un certificado directamente por el fabricante indicando las buenas prácticas de desarrollo con que cuenta y relacionar las certificaciones en cuanto al desarrollo de la solución.

|  |
| --- |
| Por favor describa a continuación **con claridad** la metodología de desarrollo seguro que se emplea sobre la solución propuesta. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Cifrado

El proponente debe garantizar que la información de las operaciones en tránsito o reposo debe estar cifrada, la encripción debe estar basada en estándares y algoritmos reconocidos internacionalmente que brinden al menos la seguridad ofrecida por AES o RSA. Para esto se **deberá hacer una descripción de los diferentes esquemas de cifrado que se utilizan o se pueden implementar en la solución para cifrar la información a nivel de bases de datos, repositorios de archivos, comunicaciones y demás capas del sistema**.

Se debe contar con canales de comunicación cifrados de extremo a extremo y que en lo posible usen rutas diferentes.

|  |
| --- |
| Por favor describa a continuación **con claridad** el tipo y alcance de cifrado sobre la información en reposo y tránsito que se emplea sobre la solución propuesta. Así mismo, explique cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Control de acceso

La solución propuesta debe contar con un módulo de seguridad que permita registrar, parametrizar usuarios, realizar asignación de roles y perfiles y generar reportes de trazabilidad de acciones de usuarios. La solución debe facilitar la aplicación del principio de menor privilegio para los roles y perfiles configurados. Es deseable que la plataforma realice la autenticación a través del directorio activo de Windows del Banco. El proponente debe especificar cómo realizaría esta integración y los requerimientos técnicos que el Banco debe proveer.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

El sistema debe mantener el histórico de usuarios creados por parte del Banco y para efectos de la trazabilidad de las acciones realizadas en este, no se deben permitir la eliminación y/o reutilización de los usuarios. Sin embargo, se debe permitir el bloqueo permanente de los mismos en la aplicación.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

Es un deseable, no requisito, que el sistema tenga habilitado doble factor de autenticación

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

El sistema debe contar con un certificado digital de sitio seguro.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Contraseñas

Cuando la autenticación no está integrada con el directorio activo de Windows, el sistema 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.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Inicio de sesión

El sistema deberá contar con procedimientos de ingreso (log-on) seguro entre ellos:

* Proteger contra intentos de ingreso (*Log-On*) mediante fuerza bruta
* Llevar un registro (Log) con los intentos exitosos y fallidos
* Declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso (Log-On) seguro
* No visualizar una contraseña que se esté ingresando

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a los diferentes puntos de este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Tiempo de sesión

La aplicación debe contar con tiempos de cierre de sesión por inactividad del usuario, el proponente deberá especificar como es el manejo de esta sesión en el sistema, si este es parametrizable o tiene un tiempo fijo, en caso de ser así se debe informar cuanto es este tiempo.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Independencia de la información

El proponente debe garantizar una independencia de la información del Banco y sus backups con respecto a la información de otros clientes que utilicen el software y procesen en la nube, esta independencia se puede hacer a nivel lógico o físico. Se deberá entregar a el Banco la descripción de cómo se está realizando esta independencia. Como también es necesario compartir diagramas de arquitectura que permita soportar la independencia y de esta manera contar con dicha visualización.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Logs

El proponente deberá especificar como el sistema administra los logs de auditoría, los cuales deben permitir la trazabilidad de todas las acciones que realizó un usuario en el sistema. Adicionalmente, deberá garantizar que los logs de todos los componentes de infraestructura que soportan el sistema se encuentran habilitados de manera permanente con el fin de que estos se encuentren disponibles cuando el Banco requiera hacer una investigación. Se debe garantizar la copia de seguridad de estos logs por dos años, en caso de que exista una investigación estos deben ser conservados hasta la finalización de esta, sin modificación de la información grabada inicialmente.

Los logs en la aplicación deben contener como mínimos la siguiente información:

* Usuario que realiza la acción
* Fecha y hora en que se realizó la acción en el sistema
* Identificación de la operación realizada en el sistema y costo de esta para el cliente o usuario (si aplica).
* Dirección IP desde donde el usuario hizo la operación

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Destrucción de la información

El proponente debe contar con mecanismos de borrado seguro de los datos existentes en los medios de almacenamiento, cuando lo solicite el Banco o cuando el proveedor de servicios en la nube elimine y/o reemplace dichos medios y debe certificar la destrucción de esta al Banco. Este debe informar al banco en su propuesta como hace este procedimiento.

|  |
| --- |
| Por favor indique a continuación **con claridad**, los mecanismos de destrucción de la información. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Actualización del software

El proponente deberá garantizar la actualización del producto o de los componentes que integran la solución presentada, detallando la información de los componentes o productos que se van a actualizar. Dentro de la información presentada, se requiere mínimo:

* Versión del producto.
* Fecha de liberación de la versión.
* Mejoras o correcciones implementadas en la versión.
* Prerrequisitos para la actualización.

El proponente deberá contar con herramientas que permitan hacer el control de las versiones que se instalarán en los ambientes de producción, así mismo contar con procedimientos documentados para la instalación del software en producción, debe entregar al Banco cómo se hace este proceso.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

### Estadísticas

El proponente deberá aportar al Banco de manera trimestral las estadísticas de disponibilidad y de uso con respecto a la prestación del servicio. Esta información debe ser conservada por 2 años. El proponente deberá indicar el detalle de la metodología utilizada para el cálculo de la disponibilidad.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Soporte técnico

El proponente deberá describir en la propuesta cómo se va a prestar el soporte técnico para la solución o para los componentes que presente en su propuesta (software base, aplicaciones, servicios, componentes, módulos, etc.). Presentar el esquema de atención, plan de comunicaciones y el equipo de soporte, si es subcontratado, describa el nombre del subcontratista. Los tiempos de atención deben estar basados en Acuerdos de Niveles de servicio los cuales se deben especificar en la propuesta, el incumplimiento de estos dará lugar a la penalización en los costos que el Banco pague por el servicio contratado. Estos tiempos podrán ser sometidos a ajustes por las partes, según la criticidad y urgencia que se presente. Se deberá adjuntar el proceso de gestión de incidentes que se tiene implementado o que se implementará para la operación del sistema describiendo claramente los canales de atención, tiempos de respuesta y las actividades generales del proceso.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Certificaciones

Es deseable que el proponente cuente con certificación vigente ISO 27001 y observar los estándares 27017 y 27018 o puede anexar certificaciones que las reemplacen, las sustituyan o las modifiquen.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Fuga de Información

El proponente debe especificar si la solución cuenta con mecanismos de control para la fuga de información. Se deben especificar cuáles son estos mecanismos.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Sincronización hora legal

El proponente debe comprometerse a que la hora de toda la infraestructura que soporta la solución está sincronizada con la hora legal colombiana. Se debe tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Propiedad, Privacidad y Ubicación de la Información

Toda la información del Banco que se encuentre almacenada en la solución propuesta es de propiedad del Banco y por tanto no podrá ser entregada a terceros. Para efectos de la Ley 1581 el proponente tendrá el rol de encargado de los datos. El proponente debe especificar en su propuesta cómo cumple con este requerimiento.

El proponente deberá garantizar que las jurisdicciones en donde se procesará la información para cualquiera de los ambientes de producción, pruebas o desarrollo cuenten con normas equivalentes o superiores a las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos. Se debe garantizar que esté en alguno de los países autorizados por la Superintendencia de Industria y Comercio.

El proponente deberá indicar la ubicación física o región donde se procesarán y almacenarán los datos.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Incidentes de seguridad de la Información, Ciberseguridad y Protección de datos personales

El proponente debe contar con mecanismos para la gestión de incidentes de ciberseguridad. Este deberá reportar al Banco de forma inmediata cualquier situación que afecte la confidencialidad, integridad o disponibilidad de la información de Bancóldex que se encuentre en la solución propuesta, o cuando se encuentre evidencia de alteración de los dispositivos usados para la solución ofrecida, así como cualquier incidente de seguridad en datos personales por violaciones de seguridad. El proponente deberá especificar en su propuesta cómo implementará este procedimiento en la operación del producto.

En consecuencia, el proponente se debe comprometer a efectuar el manejo del incidente de acuerdo con las instrucciones del Banco bajo previo acuerdo con el proponente, incluyendo la posibilidad de hacer el bloqueo del canal si es requerido. En caso de que el incidente de seguridad diera lugar a una investigación por parte de las autoridades, el proponente deberá facilitar la diligencia y aportar toda la documentación necesaria para la investigación.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Cadena de suministro de tecnología

El proponente deberá comunicar al Banco todos los proveedores que hacen parte de cadena de suministro de la solución propuesta, como mínimo deberá ser una relación que contenga:

* Nombre del proveedor
* Servicio tecnológico que presta
* Año de vinculación con la empresa

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

## Plan de Continuidad

El proponente debe contar con Planes de Continuidad y contingencia para los servicios ofrecidos, los mismos deben cubrir los riesgos a los que se encuentra expuesto el proponente y que pueden afectar la prestación del servicio al Banco.

Ante un evento de falla, se debe cumplir con el Tiempo Objetivo de Recuperación - (RTO) de mínimo 8 horas y el Punto Objetivo de Recuperación - RPO definidos para el proceso de 1 día. Es importante que el proponente indique cómo da cumplimiento a este punto.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

El proponente debe contar con un protocolo de comunicación con el objetivo de informar, en cuanto le sea posible, al Banco sobre cualquier evento o situación de interrupción que pudiera afectar significativamente la prestación del servicio.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

El proponente debe permitir, en la medida de lo posible, vincular al Banco en la ejecución de sus pruebas / ejercicios que resulten necesarias para confirmar la efectividad de los procedimientos de contingencia para asegurar que funcionen en las condiciones requeridas.

El Banco podrá realizar en cualquier momento auditoria al cumplimiento de los requerimientos de continuidad de negocio para la prestación del servicio ofrecido.

El servicio debe contar con un diagrama homologado de la arquitectura de la infraestructura instalada en ambiente contingencia y producción.

|  |
| --- |
| Por favor indique a continuación **con claridad**, cómo la solución da cumplimiento a este requerimiento. En caso de que la solución no cubra este requerimiento en su totalidad o parcialmente, es necesario que lo especifique en este campo. |
|  |

La infraestructura instalada de producción y contingencia debe ser robusta y soportar adecuadamente la comunicación con plataformas transversales y debe tener la capacidad de redirigir automáticamente los servicios que consumen estas plataformas en el caso de que se presenten fallas.

## REFERENCIAS

* Capítulo I del Título II de la Parte I de la Circular Básica Jurídica de la Superintendencia Financiera “CANALES, MEDIOS, SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS”
* Capítulo VI del Título I de la Parte I de la Circular Básica Jurídica de la Superintendencia Financiera “REGLAS RELATIVAS AL USO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE”
* Capítulo V del Título IV de la Parte I de la Circular Básica Jurídica de la Superintendencia Financiera “REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD”
* Ley 1581 de 2012 protección de datos personales

Circular 028 de 2016 Superintendencia Financiera de

A PARTIR DE AQUÍ PONGO TODO - CAROLETAS

# EJECUCIÓN DEL PROYECTO

## Alcance

Dentro del proyecto se espera desarrollar como mínimo las siguientes actividades:

### Fase de Implementación:

#### Etapa 1: Análisis y entendimiento de los requerimientos.

* Identificar y analizar la metodología de gestión de riesgos y eventos de riesgo operacional.
* Identificar y analizar las actividades realizadas en el proceso de auditoría, desde su planeación hasta su seguimiento.

#### Etapa 2: Configuración.

* Configurar la metodología de gestión de riesgo operacional en la solución tecnológica. Incluyendo sus respectivos flujos, visualización de riesgo inherente vs riesgo residual, planes de acción y visualización de mapas de calor.
* Configurar la metodología de gestión de eventos de riesgo en la herramienta (registro, documentación y seguimiento). Incluyendo sus respectivos flujos.
* Cargar la información de los riesgos, controles y eventos que actualmente componen el perfil de riesgo operacional del Banco con fines de pruebas.
* Configurar los reportes e informes definidos para la gestión de riesgos operacionales. Incluyendo las personalizaciones solicitadas.
* Configurar las etapas de la gestión de auditoría en la herramienta (planeación, ejecución y seguimiento). Incluyendo sus respectivos flujos.
* Configurar la gestión de oportunidades de mejora y planes de acción con sus respectivos flujos.
* Configurar los reportes e informes definidos para la gestión de auditoría. Incluyendo las personalizaciones acordadas durante la fase de entendimiento.

#### Etapa 3: Pruebas y Ajustes.

* Realizar pruebas al funcionamiento de los cálculos sobre la metodología de riesgos.
* Realizar pruebas sobre el funcionamiento de los reportes definidos para riesgos operacionales y auditoría.
* Realizar pruebas sobre el flujo completo de la auditoría (Planeación, Ejecución y Seguimiento).
* Realizar pruebas sobre los flujos de trabajo definidos en la herramienta para riesgos operacionales y auditoría.
* Corrección de errores u otros ajustes necesarios detectados por las áreas usuarias durante las pruebas.

#### Etapa 4: Puesta en ambiente Productivo.

* Puesta en producción de las funcionalidades de la solución tecnológica y los respectivos cargues de información iniciales.
* Capacitación en el uso de la herramienta a los diferentes interesados.

### Fase de Operación

* Seguimiento al desempeño de la herramienta implementada (funcionalidades, tiempos de respuesta, interfaz gráfica y posibles ajustes derivados de cambios normativos o metodológicos)
* Soporte a errores reportados, mantenimiento del servicio y actualizaciones.

## Entregables

* PRIMER ENTREGABLE: Documento de entendimiento de los requerimientos. El CONTRATISTA deberá entregar un documento que detalle un informe con la definición de los requerimientos para la gestión de riesgos y de auditoría del Banco, incluyendo al menos: alcance del servicio, los supuestos de la solución, aspectos que no incluye el servicio, restricciones o limitaciones del servicio, riesgos del proyecto, asignación de responsabilidades, definición de los requerimientos funcionales de la solución ofrecida, criterios de aceptación de la solución (resultado esperado), requerimientos no funcionales, ciclo de vida del proyecto y el plan de trabajo detallado.
* SEGUNDO ENTREGABLE: EL CONTRATISTA deberá entregar la configuración del servicio con los criterios de aceptación de la solución definidos en el Documento de entendimiento de los requerimientos del primer entregable. En este entregable se incluye la puesta a disposición de los usuarios de un ambiente de pruebas para validar la ejecución de las funcionalidades solicitadas.
* 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.
* CUARTO ENTREGABLE: EL CONTRATISTA deberá entregar un informe de toda la implementación que contenga como mínimo los manuales de usuario final, de administrador funcional y técnico para el servicio, de forma independiente, según aplique, para la gestión de riesgos y la gestión de auditoría. Así mismo, se debe entregar la documentación completa de los ajustes realizados al proyecto durante la fase de implementación. Se debe contar con una transferencia de conocimiento al equipo técnico y usuario del servicio por parte de El Banco y garantizar la funcionalidad de la aplicación, para lo cual Bancóldex deberá certificar dicha funcionalidad.
* QUINTO ENTREGABLE: El CONTRATISTA deberá entregar un documento que detalle cómo se llevará a cabo el soporte técnico para el servicio implementado. En este se debe documentar como mínimo el alcance, esquema de atención, plan de comunicaciones y el equipo de soporte. Los tiempos de atención deben estar basados en Acuerdos de Niveles de servicio que mínimo deben cumplir con los tiempos RTO (8 horas) y RPO (1 día) establecidos para el proceso de gestión de riesgos y evaluación independiente. También se debe indicar cuál es la cobertura del soporte y qué elementos o actividades no son cubiertas por el mismo e implicarían costos adicionales.

## Metodología del Proyecto

El proponente **deberá especificar a continuación la metodología que utilizará para el desarrollo del proyecto**, considerando el alcance y los entregables mínimos mencionados anteriormente. Esta metodología debe incluir la información referente a gestión de cambios en el proyecto.

|  |
| --- |
| **DESCRIPCIÓN METODOLOGÍA** |
|  |

## Cronograma de Trabajo

El proponente **deberá especificar a continuación el cronograma propuesto para el desarrollo del proyecto**, considerando el alcance y los entregables mínimos mencionados anteriormente.

|  |
| --- |
| **CRONOGRAMA** |
|  |

## Transferencia de Conocimiento

El proponente **deberá especificar a continuación la forma en que realizará la transferencia de conocimiento, documentación funcional y técnica (si aplica),** durante el desarrollo del proyecto.

|  |
| --- |
| **ESTRATEGIA DE TRANSFERENCIA DE CONOCMIENTO** |
|  |

# ANEXOS

## Anexo 1. Metodología de Riesgo Operacional

### Riesgo Inherente SARO

**Tabla de probabilidad inherente**

Actualmente se tiene en cuenta la frecuencia de realización de la actividad que genera el riesgo para poder determinar la escala de probabilidad en la que queda ubicado.

|  |  |  |
| --- | --- | --- |
|  | **Frecuencia** | **Tabla Probabilidad** |
| **Muy Baja** | La actividad se realiza máximo cuatro veces por año. | 20% |
| **Baja** | La actividad se realiza mínimo 5 veces al año y máximo 12   veces al año. | 40% |
| **Media** | La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año. | 60% |
| **Alta** | La actividad se realiza mínimo 366 veces al año y máximo 3.660 veces al año. | 80% |
| **Muy Alta** | La actividad se realiza 3.661 veces o más al año. | 100% |

**Tabla de impacto inherente**

Actualmente se tienen criterios internos cualitativos para determinar la escala de impacto en que queda ubicado un riesgo. Con base en la entrevista que se tenga con el Dueño de Proceso, el impacto

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Impacto Económico** | **Criterio Reputacional** | **Escala progresiva** |
| **Insignificante** | Pérdidas menores a X SMLMV | -Sólo de conocimiento de algunos funcionarios  -No se registró incumplimiento regulatorio | 20% |
| **Menor** | Mayores o iguales a XSMLMV y menores a Y SMLMV | -De conocimiento general de la entidad a nivel interno, de junta directiva y accionistas y/o de proveedores  -Genera recomendación de organismo regulatorio | 40% |
| **Moderado** | Mayores o iguales a Y SMLMV y menores a Z SMLMV | -Afecta imagen con algunos clientes que impacten significativamente los objetivos.  -Requerimiento de organismo regulatorio | 60% |
| **Importante** | Mayores o iguales a Z SMLMV y menores a N SMLMV | -Deterioro de imagen a nivel nacional, con efecto publicitario sostenido a nivel país  -Llamado de atención de organismo regulatorio | 80% |
| **Mayor** | Mayores a N SMLMV | -Deterioro de imagen a nivel internacional, con efecto publicitario sostenido a nivel internacional  -Sanciones de organismo regulatorio | 100% |

**Tabla de severidad inherente (calificación del riesgo sin controles)**

A diferencia de otras metodologías, la severidad inherente no es el resultado de la multiplicación de probabilidad por impacto, sino la combinación de estos dos factores:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Impacto** | | | | |
|  |  | **Insignificante** | **Menor** | **Moderado** | **Importante** | **Mayor** |
| **Probabilidad** | **Muy alta** | Alta | Alta | Alta | Alta | Crítica |
| **Alta** | Media | Media | Alta | Alta | Crítica |
| **Media** | Media | Media | Media | Alta | Crítica |
| **Baja** | Baja | Media | Media | Alta | Crítica |
| **Muy** **Baja** | Baja | Baja | Media | Alta | Crítica |

**Severidad Inherente**

### Riesgo Residual SARO

**Tipos de controles y calificación de efectividad**

|  |  |  |
| --- | --- | --- |
| **Criterios de la efectividad** | | **Puntaje** |
| **Tipo** | Preventivo | 33% |
| Detectivo | 23% |
| Correctivo | 13% |
| **Implementación** | Automatizado | 33% |
| Manual | 20% |
| **Evidencia** | Registro sustancial | 33% |
| Registro material | 20% |
| Registro Informal | 13% |
| Sin registro | 0% |

**Aplicación de Controles y afectación en riesgo**

Con el fin de que los riesgos realicen una transición homogénea por las diferentes escalas de impacto y probabilidad, se determinó una metodología de reducción acumulativa, 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.

Para aplicar el porcentaje de mitigación es necesario identificar si el control reduce la probabilidad o el impacto inherente del riesgo asociado. Un mismo control no puede afectar ambos.

Para los casos en que para un riesgo existe más de un control, el porcentaje de mitigación se aplicará al riesgo residual dejado por el control anterior, este ejercicio para cada una de las variables (Probabilidad o Impacto).

***Ejemplo:*** Se tiene el riesgo 1 cuya calificación inherente es la siguiente:

|  |  |  |
| --- | --- | --- |
| **Probabilidad Inherente** | **Impacto Inherente** | **Severidad Inherente** |
| **Muy Alta** | **Moderado** | **Alta** |
| **100%** | **60%** |
|  |  |  |
| El riesgo 1 tiene varios controles de **probabilidad** y uno de Impacto, con las siguientes características: | | |
| *Control 1* | | |
| **Característica** | **Tipo** | **Puntaje** |
| Reducción | Probabilidad | N/A |
| Tipo Control | Detectivo | 23% |
| Implementación | Manual | 20% |
| Evidencia | Registro Sustancial | 33% |
| **Puntaje Acumulado** | | 76% |
| Tipo control + Implementación + evidencia | |
| **Valor a restar de la probabilidad inherente** | | 38.00% |
| Puntaje Acumulado X 50% | |
|  | | |
| En este caso, se resta de la probabilidad inherente (100%) la mitad del puntaje acumulado del *Control 1*  (76%/2=38%) | | |
|
| **Probabilidad Residual 1** | **Impacto Residual** | **Severidad Residual 1** |
| **Alta↓** | **Moderado =** | **Alta =** |
| **100%-38%=62%** | **60%** |
|  |  |  |
| *Control 2* | | |
| **Característica** | **Tipo** | **Puntaje** |
| Reducción | Probabilidad | N/A |
| Tipo Control | Preventivo | 33% |
| Implementación | Automatizado | 33% |
| Evidencia | Registro Sustancial | 33% |
| **Puntaje Acumulado** | | 99% |
| Tipo control + Implementación + evidencia | |
| **Valor a restar de la probabilidad inherente** | | 49.50% |
| Puntaje Acumulado X 50% | |
|  | | |
| En este caso, se resta de la probabilidad residual 1 (62%) la probabilidad residual 1 (62%) por la mitad del puntaje acumulado del *Control 2* (99%/2=49.5%) | | |
|
| **Probabilidad Residual 2** | **Impacto Residual** | **Severidad Residual 2** |
| **Baja↓** | **Moderado =** | **Media =** |
| 62%-(62%\*49.5%)=**31.31%** | **60%** |
|  |  |  |
| *Control 3* | | |
| **Característica** | **Tipo** | **Puntaje** |
| Reducción | Probabilidad | N/A |
| Tipo Control | Detectivo | 23% |
| Implementación | Manual | 20% |
| Evidencia | Sin Registro | 0% |
| **Puntaje Acumulado** | | 43% |
| Tipo control + Implementación + evidencia | |
| **Valor a restar de la probabilidad inherente** | | 21.50% |
| Puntaje Acumulado X 50% | |
|  |  |  |
| En este caso, se resta de la probabilidad residual 2 (31.31%) la probabilidad residual 1 (31.31%) por la mitad del puntaje acumulado del *Control 3* (43%/2=21.5%) | | |
|
| **Probabilidad Residual 3** | **Impacto Residual** | **Severidad Residual 3** |
| **Muy Baja↓** | **Moderado =** | **Media =** |
| 31.31%-(31.31%\*21.5%)=**24.58%** | **60%** |
|  |  |  |
| *Control 4* | | |
| **Característica** | **Tipo** | **Puntaje** |
| Reducción | Impacto | N/A |
| Tipo Control | Correctivo | 13% |
| Implementación | Automatizado | 33% |
| Evidencia | Registro Material | 23% |
| **Puntaje Acumulado** | | 69% |
| Tipo control + Implementación + evidencia | |
| **Valor a restar de la probabilidad inherente** | | 34.50% |
| Puntaje Acumulado X 50% | |
|  |  |  |
| En este caso, se resta del impacto inherente (100%) la mitad del puntaje acumulado del *Control 4* (69%/2=34.5%) | | |
|
| **Probabilidad Final** | **Impacto Residual Final** | **Severidad Residual Final** |
| **Muy Baja=** | **Menor ↓** | **Baja ↓** |
| **24.58%** | 60%-34.5%=**25.5%** |

#### Afectación – Valoración del Riesgo Residual con base en Eventos

Un evento es un riesgo materializado y este debe afectar la calificación del riesgo en el mapa. Se realizará un ajuste en la calificación de la **probabilidad residual**, cuando se presente un evento de riesgo operacional.

La fórmula para determinar el porcentaje de afectación sobre probabilidad residual está dada por la cantidad de eventos materializados en un periodo sobre la frecuencia de realización de la actividad del riesgo. El resultado se ubica en el rango de criterio de “desempeño del riesgo”, de acuerdo con la frecuencia con que ocurran los eventos y según la siguiente tabla:

|  |  |  |  |
| --- | --- | --- | --- |
| **Desempeño del riesgo** | | | |
| **Rango** | **Desde** | **Hasta** | **% adicional\*** |
| **A** | 0,00% | 0,5% | 0% |
| **B** | 0,5% | 1,0% | 10% |
| **C** | 1,0% | 2,0% | 20% |
| **D** | 2,0% | 25% | 30% |
| **E** | 25% | 100% | 40% |

Por ejemplo: Para el riesgo de sanción por impago de una obligación, se toma en cuenta la cantidad de obligaciones que se tiene en el año (100), y suponiendo que se dejaron de pagar 15 obligaciones, el porcentaje de afectación sería 15/100=15%. Este rango a su vez se encuentra en el rango D de la tabla. Por lo que se sumaría un 30% a la **probabilidad residual después de controles**.

|  |  |  |
| --- | --- | --- |
| ***Evaluación Residual de un Riesgo (sin eventos)*** | | |
| **Probabilidad Residual** | **Impacto Residual** | **Severidad Residual** |
| **Muy Baja=** | **Menor ↓** | **Baja ↓** |
| **24.58%** |
| ***Probabilidad y severidad afectadas por los eventos materializados*** | | |
|
| **Probabilidad Residual** | **Impacto Residual** | **Severidad Residual** |
| **Media↑** | **Menor ↓** | **Media ↑** |
| 24.58% + 30% = **74.58%** |

1. Circular Externa 025 de 2020 Superintendencia Financiera de Colombia [↑](#footnote-ref-1)
2. Circular Externa 025 de 2020 Superintendencia Financiera de Colombia [↑](#footnote-ref-2)
3. https://www.superfinanciera.gov.co/descargas/institucional/pubFile1036287/ance005\_19.zip [↑](#footnote-ref-3)
4. https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile1003495&downloadname=ance042\_12.doc [↑](#footnote-ref-4)
5. <https://en.wikipedia.org/wiki/Component_diagram> [↑](#footnote-ref-5)
6. <https://en.wikipedia.org/wiki/Deployment_diagram> [↑](#footnote-ref-6)
7. <https://en.wikipedia.org/wiki/Deployment_environment> [↑](#footnote-ref-7)
8. <https://en.wikipedia.org/wiki/Service-level_agreement> [↑](#footnote-ref-8)