## ANEXO 11 – REQUERIMIENTO FUNCIONAL 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.

## Módulo de Riesgo Operativo

### Requerimientos funcionales

#### Evaluación de riesgos

* La solución debe permitir realizar la evaluación de riesgos para un proceso (diferentes niveles: macroproceso, subprocesos, etc.), producto, canal, servicio o proyecto, o para varios procesos agrupados (mapa corporativo). En virtud de lo anterior, la solución debe permitir la configuración de las taxonomías 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.)
* La solución debe permitir asignar un mismo riesgo a diferentes procesos (diferentes niveles: macroproceso, subproceso, etc.), productos, canales, proyectos, etc.
* La solución debe permitir parametrizar riesgos transversales los cuales deben poder ser identificados fácilmente a través de alguna marcación y vinculados a los diferentes procesos (diferentes niveles: macroproceso, subproceso, etc.).
* La solución debe permitir parametrizar controles transversales los cuales deben poder ser identificados fácilmente a través de alguna marcación para asociarlos a los riesgos. Así mismo, estos deben poder ser asignados a diferentes riesgos en diferentes procesos, productos, canales, proyectos, etc.
* La solución debe permitir asignar tratamientos a los riesgos (Aceptar o Reducir). Este tratamiento debe ser parametrizable.
* La solución debe permitir asociar uno o varios Planes de Acción a cada riesgo y evento, los cuales deben tener responsable y fecha de implementación. A los responsables les deberá llegar un correo con la información de su plan de acción.
* La solución tecnológica debe permitir la asignación de un mismo Plan de Acción a varios Riesgos y eventos.
* La solución tecnológica debe permitir la configuración de una taxonomía de riesgos y controles y preferiblemente contar con una biblioteca propia de estos con base en estándares internacionales, de forma tal que se facilite y/o estandarice la vinculación entre riesgos y controles.
* 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 |

* Es posible que en el futuro se deban incluir más campos, por lo que la solución tecnológica debe ser flexible para tal fin.
* 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.
* La solución tecnológica debe permitir la configuración y parametrización de la metodología de evaluación de riesgo operativo (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 Operativo](#_Anexo_1._Metodología). El proveedor debe indicar si para la implementación de la metodología expuesta, requiere realizar desarrollos internos o estos pueden ser parametrizados directamente sobre la interfaz de la solución y modificables por el Administrador.
* La solución tecnológica debe permitir actualizar los cálculos y demás parametrizaciones asociadas a la metodología de evaluación de riesgo operativo. Esto, considerando que pueden existir cambios normativos o mejoras a la metodología de riesgos que requieran ajustes sobre la solución.
* Es un deseable 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 destinadas para tal fin. Asimismo, debe explicar las implicaciones que tendría realizar estas implementaciones adicionales.
* Es deseable 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.
* Es deseable que la solución permita a los usuarios de riesgo operativo acceder a los planes de acción y recomendaciones generados por la auditoría para los procesos

##### 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 por Entidad - Perfil de riesgo. (Promedio)
	+ Mapa de Riesgo Residual por Entidad - Perfil de riesgo. (Promedio)
	+ Mapa de Riesgo Inherente por Proceso
	+ Mapa de Riesgo Residual por Proceso
	+ Mapa de Riesgo Inherente por Producto, canal o proyecto
	+ Mapa de Riesgo Residual por Producto, canal o proyecto
* Adicionalmente, si la solución tecnológica permite la parametrización de diferentes metodologías de riesgos (SARLAFT, SGSI, SARE, etc.), se requerirían los mismos mapas anteriores tanto por metodología como de forma acumulada (Perfil integral de riesgos).
* Es deseable 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 deberá enviar pantallas con los tipos de mapas de calor que genera la solución.

##### Gestión de Eventos de Riesgo Operativo

* El reporte de Eventos de Riesgo operativo debe ser realizado a través de la solución tecnológica por los funcionarios de la Oficina de Riesgo Operativo (5 funcionarios, máximo 3 concurrentes). Es un deseable que cualquier funcionario de la Organización 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 y económicas de esta actividad, es decir, si se requiere un módulo adicional, si todos los usuarios que deben ser usuarios nombrados/licenciados y cuál es su costo.
* Los eventos de riesgo operativo 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 metodología expuesta.
* Los eventos de riesgo operativo pueden tener planes de acción con sus respectivos responsables y fechas de compromiso, esto debe ser gestionado a través de la solución tecnológica.
* La solución tecnológica debe permitir asignar un mismo plan de acción a varios riesgos y eventos de riesgo operativo.
* La solución tecnológica debe permitir la parametrización y configuración de todos los campos utilizados para el registro de eventos de riesgo operativo, 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 operativos nivel I | Alfanumérico | Obligatorio | Mandatorio |
| Clasificación de los riesgos operativos nivel II | Alfanumérico | Obligatorio | Mandatorio |
| Clasificación de los riesgos operativos 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 |

* Es posible que en el futuro se deban incluir más campos, por lo que la solución tecnológica debe ser flexible para tal fin.
* 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.
* Los eventos de riesgo operativo pueden presentarse por la falla de un control específico en un riesgo, es deseable que la solución tecnológica permita identificar el control que falló.

#### Flujos de Información y Aprobación

##### Creación/Actualización de Riesgos

* Es deseable 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.

##### Asignación de Planes de Acción

* Cuando se asigne un Plan de Acción para el Tratamiento de Riesgos a un funcionario del Banco, la solución tecnológica debe enviar 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 de Tratamiento de Riesgos.
* Cuando se asigne un Plan de Acción para la Gestión de Eventos de Riesgo Operativo a un funcionario del Banco, la solución tecnológica debe enviar 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 Operativo.

##### Notificaciones

* Se desea que la solución tecnológica permita parametrizar diferentes tipos de notificaciones orientados 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 operativo | 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. |

#### 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. Se contempla en este punto, como deseable una opción de reporteador que permita realizar filtros por diferentes campos (de ser así, por favor especificarlo con claridad).
* Entre otros, se desea 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 operativo
	+ Reporte de planes de tratamiento con responsables, fechas de vencimiento y avances.
	+ Informe de perfil de riesgo del Banco.
* Los reportes deben poder ser exportados fácilmente a Excel. Deseable que también se envíen directamente a documentos Word para su gestión.
* Los reportes deberían permitir filtrado por campos clave.
* Es deseable que la solución cuente con la posibilidad de extraer gráficos basados en los datos del reporteador que permitan conocer el estado de la gestión de riesgos del Banco. Gráficos de torta, de barras.
* Es deseable que la solución permita la configuración y visualización de indicadores de riesgos KRI mediante un *dashboard*.
* Es deseable que la solución permita configurar el diseño de los reportes (logo del Banco, encabezados, fuentes, etc.), con el fin de reducir labores operativas y generar valor a la organización.
* Si la solución cuenta con reportes predefinidos y no son parametrizables, debe enviar el listado de estos.
* El proponente debe enviar pantallas tipo de los gráficos, indicadores, diseño de reportes e interfaz gráfica de la solución propuesta.

### Requerimientos no funcionales

* Es deseable 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.
* Es deseable 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 operativo.
* Es deseable 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.

#### 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.
* Es deseable que los gestores de proceso (50 aproximadamente) puedan ingresar a revisar los riesgos de sus procesos.
* Es deseable que los líderes o dueños de proceso (50 aproximadamente) puedan ingresar a la solución tecnológica para aprobar los riesgos a su cargo.
* Se requiere un rol de consultas para que la contraloría o revisoría puedan ingresar sin modificar la información de los riesgos.
* Es deseable que todos los funcionarios (370) puedan realizar el reporte de eventos de riesgo operativo a través de un cuestionario brindado por la solución tecnológica.
* Es deseable que todos los funcionarios puedan ingresar a conocer los riesgos asociados a sus procesos.
* Si la solución tecnológica permite administrar diferentes metodologías de riesgos, es deseable que se puedan tener administradores funcionales independientes por cada metodología (SARO, SGSI, SARLAFT, SARE, etc.).

#### 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, 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.
* La solución debe permitir identificar los responsables de la aprobación del riesgo.
* La solución debe permitir identificar quién realizó la modificación de algún riesgo (logs de auditoría).
* La solución debe permitir identificar los usuarios que realizan cualquier modificación sobre la plataforma (adición de procesos, modificación de controles, cambio en metodología, etc.)
* La solución tecnológica debe permitir el cargue de los riesgos, controles y eventos actuales en el Banco.
* 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.

## Módulo de Auditoría

### Requerimientos Funcionales

#### Inventario y cargue de entes auditables

* La solución debe permitir realizar el inventario, revisión y evaluación de los diferentes entes auditables (proceso, área, producto, norma, riesgos, etc.), así como sus insumos (proyectos, documentos, etc).
* La solución debe permitir cargar y actualizar periódicamente el inventario de riesgos operativos y sus eventos, así como generar reportes de los mismos.
* La solución debe permitir integrar marcos normativos asociados a los diferentes sistemas de riesgos (SARO, SGSI, SARE, SARL, SARC, SARLAFT, SARM, etc., normas, AMV, entre otras.) y de referencia de control (COSOs, COBITs, ISOs, ITIL, NIAs, etc.). Se debe permitir el cargue del inventario de controles y este debe ser asociable a los entes auditables, para definir y limitar el alcance y enfoque de la auditoría. Es deseable que estos marcos normativos sean cargados y actualizados periódicamente por el proveedor directamente.
* Es deseable que la solución permita integrar otros marcos de control financiero como SOX.

#### Metodología de Planeación Anual

* La solución debe ser flexible para soportar diferentes metodologías de planeación basadas en riesgos. La solución debe ser adaptable y parametrizable.
* La solución debe ser flexible permitiendo integrar criterios y ponderaciones de priorización adicionales a riesgos, para efectos de planeación de anual (metodología de planeación).
* La solución debe permitir definir y asignar parámetros, cargar valores internos y externos, realizar cálculos, para definir y priorizar auditorías.
* La solución debe integrar visualización e interacción (no modificación) desde módulo o menú independiente, con cada riesgo y control (diferenciando la auto-evaluación, las evaluaciones o monitoreos de riesgo de segunda línea de defensa, y evaluaciones independientes de tercera línea de defensa).
* La solución debe permitir parametrizar, generar reportes y gráficos y exportar a Office la propuesta "inicial" del plan anual de auditoría como resultado de la metodología y priorización de los entes auditables, y registrar y controlar los posibles cambios que se presenten durante su desarrollo.

#### Planeación de las Auditorías

* La solución debe integrar (asociar, o ingresar) pruebas de auditoría a funciones, normas, procesos, proyectos, metas, controles y riesgos - Planeación anual, GRC, Información y/o protección de activos.
* La solución debe permitir generar programas de auditoría, y asignarles tiempos y recursos de acuerdo con los perfiles de los auditores.
* La solución debe permitir realizar el control y seguimiento de los planes anuales de auditoría, así como del ciclo de auditoría (varios años). Asimismo, se debe poder generar versiones adicionales o revisiones de la planeación anual ajustada por riesgos emergentes o nuevas necesidades de la Organización (control de cambios y versiones del plan).
* La solución debe permitir parametrizar, generar reportes y gráficos y exportar a Office el documento, registro o salida de pre-planeación.
* La solución debe permitir parametrizar, generar reportes y gráficos y exportar a Office el documento, registro o salida de plan y programa.
* La solución debe permitir, para ejercicio de la auditoría, la inclusión de riesgos identificados por la auditoría, diferentes a los generados desde el ciclo de gestión de riesgos (identificados en el mapa de riesgo).
* La solución debe permitir consultar e integrar información del ciclo de gestión de riesgos incluidos eventos de riesgo y sus planes de acción.
* La solución debe permitir consultar el historial de riesgos y controles auditados con sus resultados.
* Es deseable que la solución pueda integrarse con los sistemas que actualmente tienen la información de procesos/subprocesos, arquitectura tecnológica y activos de información del banco.

#### Ejecución de las Auditorías

* La solución debe soportar la metodología de ejecución de auditoría del Banco con sus diferentes componentes (calificación, resultados, criterios, condición causas, efecto, oportunidades, mejoramiento, acciones de mejoramiento).
* La solución debe permitir llevar trazabilidad de toda la ejecución del plan de auditoría y de los trabajos de auditoría (tiempos de ejecución de actividades, alertas e indicadores de operación).
* La solución debe permitir parametrizar, generar reportes y gráficos y exportar a Office los informes detallados y reportes globales (comunicaciones intermedias, Informes) integrados al flujo de información y trabajo con la organización).
* La solución debe permitir la formulación de planes de mejoramiento y sus acciones, fechas y responsables, por parte de los responsables de los procesos auditados.
* La solución debe permitir integrar e indexar los papeles de trabajo respectivos a cada proyecto de auditoría. Es deseable que se haga uso de las herramientas de Office365 para el versionamiento de los archivos. Adicionalmente, sería deseable que desde la herramienta pueda acceder a los papeles de trabajo que se encuentren en *OneDrive* del Banco para evitar duplicidad de información (integración).
* La solución debe permitir gestionar la relación de la auditoría con las personas o roles de los procesos involucrados (comunicación y alertas), en cada etapa necesaria. En el Banco se cuenta con 40 procesos con sus respectivos líderes. Adicionalmente se requiere acceso para 12 auditores.

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

* La solución debe permitir llevar el inventario de planes de mejoramiento integrados por proceso, responsable y riesgos, con registro o soportes de avance o cumplimiento.
* La solución debe permitir llevar el inventario de recomendaciones y estado (aceptación o no, y gestión).
* La solución debe permitir parametrizar, generar reportes y gráficos y exportar a Office informes y/o reportes detallados y reportes globales (acciones de mejoramiento, abiertas, vencidas aplazadas, indicadores alertas).
* La solución debe permitir parametrizar, generar reportes y gráficos y exportar a Office los informes / reporte periódico (con cortes especificados por el usuario) de la ejecución, avance o cumplimiento del plan. Esto debe poder realizarse por demanda y con filtros de periodos.
* La solución debe permitir parametrizar, generar reportes y gráficos, exportar a Office y mapas de riesgos orientados a informar a la alta gerencia y al Comité de Auditoría respecto al seguimiento regular y periódico de los riesgos (incluyendo los identificados por la Auditoría), especialmente aquellos que están en zonas de severidad no aceptadas por la Organización.
* La solución debe permitir la categorización de los riesgos por características que se puedan asociar por ejemplo a objetivos de negocio, productos, procesos.

#### Flujos de aprobación

* La solución debe permitir parametrizar el flujo de actividades, documentación de análisis y autorizaciones del proceso de preplaneación y de planeación de la auditoría.
* 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).
* 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).

### 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).
* La solución debe 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).
* 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.
* Es deseable que información relevante para la auditoría tal como tableros, acciones básicas y planes de acción puedan ser consultados a través de dispositivos móviles (puede ser a través de *web,* pero de tipo *responsive*).
* Es deseable 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.

## 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.
* Se espera que la solución tecnológica se presente en ambiente web, con un entorno amigable y fácil de usar para los usuarios.
* Se requiere que la solución permita la autenticación con el Directorio Activo de Bancóldex.
* Se requiere que el proveedor entregue todos los manuales técnicos, de administración funcional y de usuario final para el uso de la solución tecnológica.
* Es deseable que la solución cuente con ayudas interactivas que permitan al usuario identificar las descripciones de los campos, errores en el diligenciamiento, etc.
* 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*.
* 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.).
* La solución debe contar con manuales técnicos, manuales de usuario, menús, informes, reportes, módulos, en español.
* Los reportes deben ser exportables a Word o Excel para poder realizar su edición en caso tal que se requiera. Asimismo, se debe permitir la exportación a PDF de estos.
* 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.
* Es deseable que se pueda realizar consultas en la solución por palabras clave.
* Es deseable 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).

## Anexos

### Anexo 1. Metodología de Riesgo Operativo

#### 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 operativo.

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%** |

### Anexo 2. Metodología de Auditoría

Estrategia 1: Aseguramiento o Auditoría

#### Planeación Anual

* 1. Definición Universo de Auditoría (entes auditables): Incluye Riegos, Procesos, subprocesos, Dominios ISO, Cobit, y debe ser flexible para incluir mas en caso de ser necesario.
	2. Priorización: Se establecen pesos para los diferentes aspectos a considerar para la definición de la criticidad y su inclusión en el Plan Anual de Auditoría.



La herramienta debe ser flexible en caso que se desee cambiar los pesos, adicionar o retirar criterios y permitir la inclusión de fórmulas.

* 1. Distribución de Universo de Auditoría: Con base en el apetito de riesgo del Comité de Auditoría (el cual puede cambiar en el tiempo), y el resultado de la priorización, se estratifican los subprocesos y demás entes auditables.



* 1. Definición del Plan Anual: 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,

- Que auditores van a participar,

- El tiempo/duración del trabajo,

- El objetivo inicial

- el alcance y enfoque que se va a dar.

**Estrategia 2: Consultoría o Acompañamiento**

El departamento de Auditoria, puede participar en la participación en diseños, implementaciones o proyectos bajo modalidad de acompañamiento o consulta, lo cual debe ser registrado, y puede afectar el Plan de Auditoría establecido inicialmente. Estos trabajos deben poder ser administrados en la herramienta de manera similar a una auditoría (con sus propios formatos de planeación, informes y flujos de trabajo y aprobaciones específicas).

**Estrategia 3: Programa de Aseguramiento y Mejora de la Calidad**

El departamento de 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 realizar, registrar , monitorear y medir, de acuerdo con la capacidad e insumos, estas actividades.

**Estrategia 4: Entes de Control**

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

#### Planeación Individual de las auditorías:

**Pre-planeación de cada Auditoría**



**Plan y Programa de cada Auditoría**

Una vez aprobada la Preplaneación, se procede a elaborar el documento “Plan y Programa de Auditoría”, teniendo como insumo la Pre-planeación, y deberá ser aprobada por el Contralor.

Una vez aprobado el Plan y programa se procede a citar a reunión de Apertura de la auditoría con los responsables de los procesos a auditar. Durante esta reunión el Plan y Programa puede ser ajustado.

Con resultado final se debe tener el Plan y Programa definitivo, y se da inicio al trabajo de auditoría.

#### Ejecución de los trabajos de Auditoría

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.

En caso de presentarse alguna desviación u observación resultado de la prueba, se procede a elaborar una comunicación intermedia.



La comunicación intermedia, de acuerdo con su impacto, tiene diferentes niveles de aprobación, tanto por el área responsable, como dentro de la Contraloría Interna.

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. |

Se espera que la herramienta administre los Planes de Mejoramiento (responsables, plazos, seguimientos).

Una vez revisadas y aprobadas las pruebas y Planes de Acción (en caso de presentarse) por parte del Contralor, el Auditor Procede a elaborar el Informe de Auditoría.

#### Seguimiento de los resultados de las auditorías

Los Planes de Mejoramiento generados en las auditorías deberán poder ser consultados y gestionados por los responsables (auditados) y monitoreados y revisados para aprobar su cierre una vez se cumplan a satisfacción las actividades acordadas.

La comunicación intermedia, de acuerdo con su impacto, tiene diferentes niveles de aprobación, para su cierre, tanto por el área responsable, como dentro de la Contraloría Interna.