Imagen que contiene Logotipo

Descripción generada automáticamente

**Requerimiento Funcional**

**Elaborado por:**

**John Alexander Muñoz**

**Beatriz Gomez**

**Bogotá D.C., 2022**

**Contenido**

[1 TIPOS DE USUARIO 3](#_Toc115219485)

[1.1 Administrador del sistema 3](#_Toc115219486)

[1.2 Responsable entidad 3](#_Toc115219487)

[1.3 Gestor 4](#_Toc115219488)

[2 VIGENCIAS 4](#_Toc115219489)

[3 PARAMETROS 4](#_Toc115219490)

[3.1 Planeación estratégica 4](#_Toc115219491)

[3.2 Mapa de procesos 4](#_Toc115219492)

[3.2.1 Mapa de procesos 5](#_Toc115219493)

[3.2.2 Sedes 6](#_Toc115219494)

[3.3 Procesos e indicadores 6](#_Toc115219495)

[3.3.1 Variables 6](#_Toc115219496)

[4 MODULO GESTIÓN DE RIESGOS 8](#_Toc115219497)

[4.1 Identificar los riesgos para los procesos. 8](#_Toc115219498)

[4.1.1 Variables: 8](#_Toc115219499)

[4.1.2 Información para implementar tooltips en las variables, para mejor entendimiento del usuario. 10](#_Toc115219500)

[4.1.3 Cálculo del Nivel de riesgo inherente 13](#_Toc115219501)

[4.2 Definición de controles para los riesgos 14](#_Toc115219502)

[4.2.1 Variables: 14](#_Toc115219503)

[4.2.2 Información para implementar tooltips en las variables, para mejor entendimiento del usuario. 15](#_Toc115219504)

[4.2.3 Ejemplo 19](#_Toc115219505)

[4.3 Auditoria 20](#_Toc115219506)

[4.4 Salidas y reportes 20](#_Toc115219507)

# TIPOS DE USUARIO

## Administrador del sistema

Crear clientes basado en el proceso de contratación.

Variables:

**Creación del contrato:**

* Id cliente (número contrato)
* Razón social
* Nit
* Representante legal
* Correo
* Dirección
* Departamento
* Ciudad
* Fecha inicio
* Fecha fin
* **Cantidad de sedes**: permite controlar el número de sedes que el cliente podrá gestionar con la herramienta
* **Módulos**: Mostrar los módulos y con checkbox seleccionar los módulos a activar acorde a la gestión contractual.

**Crear usuarios:**

* Crea el usuario responsable de la entidad.

## Responsable entidad

Es creado por el usuario administrador del sistema

1. Es el usuario que se encarga de parametrizar la herramienta, adaptándola a la entidad

**Reglas**:

Debe acceder a todo el aplicativo, esto incluye a la gestión

1. Crear usuarios

* **Gestor**: con acceso a gestión de los procesos asignados.
* **Consulta**: es un super usuario con acceso a modo consulta, tipo auditor.

**Reglas:**

Debe acceder a todo el aplicativo, esto incluye a la gestión

**Reglas:**

* Al momento de crear el usuario gestor deben ser asignado (s) el (los) proceso (s) del cual (es) es responsable.
* Para asignar el subproceso construye la relación:

Sede – macroproceso – proceso – subproceso

* Puede asignar varios procesos

## Gestor

Tipo de usuario creado por el responsable de la entidad

Tiene acceso para la gestión de los procesos asignados, de los cuales es responsable, pueden ser varios procesos.

# VIGENCIAS

* No incluir la vigencia como parte del menú de parámetros
* Las vigencias no van ligadas a la información
* Las vigencias se relacionan con la vigencia del acceso al aplicativo, que alerte al usuario de la necesidad de renovar el contrato
* Se accede a ellas con el calendario ubicado en la barra de menú principal

# PARAMETROS

## Planeación estratégica

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

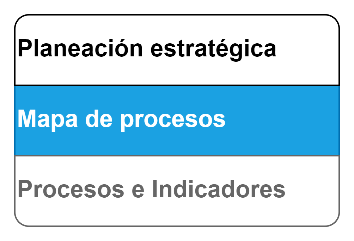
Se registra la misión, visión y objetivos organizacionales de la entidad.

* **Misión**: Se captura en campo de texto
* **Visión**: Se captura en campo de texto
* **Objetivos**: Permitir registro de varios objetivos.

**Reglas**:

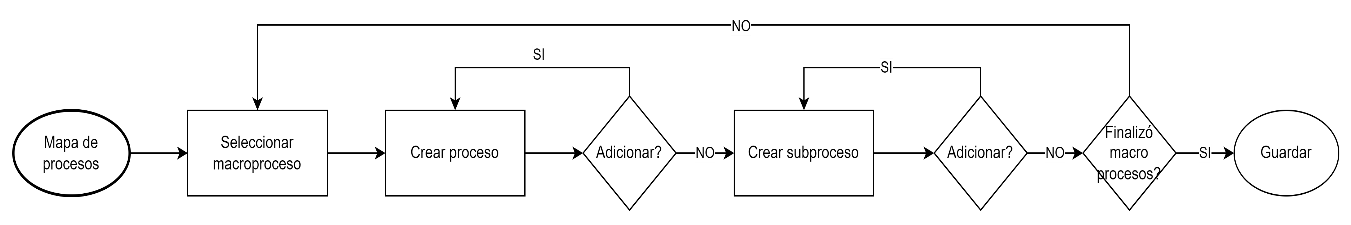
* Permitir editar y actualizar
* No bloquear para establecer como fija. Guardar solamente.

## Mapa de procesos



La estructura se construye creando relaciones entre por Macroproceso – Proceso – Subproceso.

### Mapa de procesos



1. De una lista desplegable selecciona el macroproceso, estos son estándar.

* Estratégicos
* Misionales
* Apoyo
* Evaluación y control

1. Por cada macroproceso debe crear los procesos que lo componen, puede agregar varios procesos por cada macroproceso
2. Por cada proceso el usuario puede permitir crear los subprocesos, puede agregar varios subprocesos por cada proceso.

**Reglas:**

* Al finalizar el proceso de registro y relaciones, se debe obtener lo siguiente:

| **MACROPROCESO** | **PROCESO** | **SUBPROCESO** |
| --- | --- | --- |
| 1. Estratégicos | 1.1 nombre proceso estratégico | 1.1.1 nombre subproceso |
| 1.1.n nombre subproceso |
| 1.n nombre proceso estratégico | 1.n.1 nombre subproceso |
| 1.n.n nombre subproceso |
| 1. Misionales | 2.1 nombre proceso misional | 2.1.1 nombre subproceso |
| 2.1.n nombre subproceso |
| 2.n nombre proceso misional | 2.n.1 nombre subproceso |
| 2.n.n nombre subproceso |
| 1. Apoyo | 3.1 nombre proceso de apoyo | 3.1.1 nombre subproceso |
| 3.1.n nombre subproceso |
| 3.n nombre proceso de apoyo | 3.n.1 nombre subproceso |
| 3.n.n nombre subproceso |
| 1. Evaluación y control | 4.1 nombre proceso de apoyo | 4.1.1 nombre subproceso |
| 4.1.n nombre subproceso |
| 4.n nombre proceso de apoyo | 4.n.1 nombre subproceso |
| 4.n.n nombre subproceso |

* Permitir editar los nombres de los procesos y subprocesos
* Después de guardar, permitir crear registros nuevos para cada macroproceso
* Para eliminar registros contactar el administrador del sistema.
* Graficar el mapa de procesos

### Sedes

El usuario responsable de la entidad debe crear las sedes que componen la entidad.

**Variable**:

* Nombre de la sede
* Asignar los procesos que se definieron en la entidad
* Dibujar el mapa de procesos para cada sede

**Reglas**:

* Opción que se habilita solo si contrata el servicio de sedes.
* Puede agregar tantas sedes tenga habilitadas desde el administrador del sistema.
* En caso de requerir adicionar una sede más debe ser gestionado desde el proceso contractual.

## Procesos e indicadores

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

**Proceso**:

Seleccionar Sede (si aplica) – Macroproceso - Proceso – Subproceso, y por esta selección se crean los indicadores.

### Variables

| Bloque de campos | Campos Sugeridos | Tipo de Campo | Descripción |
| --- | --- | --- | --- |
| **Fecha Creación del Indicador** | Mes | Fecha | **Lista desplegable con los meses**  Mes de creación del indicador (Indica la fecha de inicio de medición del indicador) |
| Año | Fecha | **Lista desplegable con años**  Año de creación del indicador (Indica la fecha de inicio de medición del indicador) |
| **Descripción del Indicador** | Nombre del Indicador | Alfanumérico | Nombre propuesto del indicador (Este nombre podrá ser usado más adelante en los seguimientos o resúmenes) |
| Objetivo del Indicador | Alfanumérico | Descripción del objetivo |
| Categoría | Alfanumérico | **Lista Desplegable**   * Financiero, * Cliente, * Procesos Internos * Aprendizaje y Crecimiento |
| **¿Cómo se mide el indicador?** | Formula | Alfanumérico | Campo que permita registrar la fórmula para el cálculo del indicador definido (posibilidad de editor de fórmulas). |
| Unidad de Medida | Alfanumérico | Unidad de medida del resultado de la medición del indicador  **Lista Desplegable**   * Unidad * Porcentaje |
| Tendencia Esperada | Alfanumérico | **Lista Desplegable**   * Creciente * Estático * Decreciente |
| Periodicidad | Alfanumérico | **Lista Desplegable**   * Diario * Mensual * Bimensual * Trimestral * Semestral * Anual |
| Meta | Numérico | Meta propuesta del indicador (relacionarlo con la unidad de medida seleccionada para el indicador) |
| Rangos de evaluación del % | Alfanumérico | **Lista Desplegable (**Ver Imagen)  Al seleccionar cada opción activar el campo para registrar:   * Adecuado (por defecto meta) * En riesgo (margen a ser definido por el usuario) * Critico (margen a ser definido por el usuario) |
| **Definición de Variables**  Se deben definir como tantas variables existan en el indicador | Tipo | Alfanumérico | **Lista desplegable**   * Medida Base * Medida Derivada   (mensaje para tooltip)  "Las medidas base son obtenidas por medición directa y las medidas derivadas provienen de diferentes datos, por lo general se calculan a partir de la combinación de dos o más medidas base" |
| Nombre de la Variable | Alfanumérico | Campo de texto.  Nombre de la variable utilizada en la fórmula de medición del indicador. |
| Fuente | Alfanumérico | De donde se obtiene la información de la variable.  ej: Reporte… |
| Formula | Alfanumérico | Depende del tipo, aplica si selecciona derivada.  Campo editor de fórmulas (si es posible)  Formula de obtención para las medidas derivadas y N/A para las medidas base |
| **Comunicación del indicador** | A quién se debe comunicar los resultados | Alfanumérico | **Campo de texto**  Debe permitir agregar varias opciones |
| Qué medio será utilizado para la comunicación | Alfanumérico | **Campo de texto**  Debe permitir agregar varias opciones |
| **Revisión** | Nombre | Alfanumérico | **Campo de texto**  Nombre de la persona que revisa la formulación del indicador |
| Cargo | Alfanumérico | **Campo de texto**  Cargo de la persona que revisa la formulación del indicador |
| **Aprobación** | Nombre | Alfanumérico | **Campo de texto**  Nombre de la persona que aprueba el indicador de gestión. |
| Cargo | Alfanumérico | **Campo de texto**  Cargo de la persona que aprueba el indicador de gestión. |

**Imagen (Rangos de evaluación del %)**

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

**Reglas:**

* El indicador se puede modificar.
* Si modifica la meta, implementar validación de la fecha de modificación para la medición y seguimiento.
* Permitir inactivar un indicador y quitarlo de la lista visible.
* En cualquier momento es posible crear uno nuevo indicador para el proceso.
* Si cambia el indicador, debe implementar alerta (“A partir de la fecha de modificación se tendrá en cuenta para seguimiento la nueva información”)
* Implementar alerta al inactivar un indicador.

# MODULO GESTIÓN DE RIESGOS

## Identificar los riesgos para los procesos.

Para cada uno de los procesos se deber realizar la identificación de los riesgos presentes:

### Variables:

| **#** | **Campos** | **Tipo** | **Descripción** |
| --- | --- | --- | --- |
| 1 | Sede | Alfanumérico | Elegir la sede en caso de que tenga habilitado |
| 2 | Proceso | Alfanumérico | Elegir el proceso (De acuerdo con los creados y/o asignados) |
| 3 | Sub-Proceso | Alfanumérico | Elegir el Subproceso (De acuerdo con los creados y/o asignados)  Nota. Debe permitir seleccionar opción "Todos" |
| 4 | Descripción del Riesgo | Alfanumérico | Campo de texto abierto para el registro del usuario |
| 5 | Categoría | Alfanumérico | **Lista Desplegable**   * General * Especifico   (ver tabla descripciones para implementar tooltip por cada opción)  Nota. Debe crear un consecutivo Ej. RG1, RE1, RE2 |
| 6 | Clasificación | Alfanumérico | **Lista desplegable**   * Continuidad de Negocio * Estratégico * Financiero * Información (activa #8) * Legal * Operativo * Reputacional |
| **7** | **Caracterización del Riesgos ¿Cómo Materializa?**  Nota. Pueden ser varias | | |
| 7.1 | Tipo de Riesgo | Alfanumérico | **Lista desplegable**   * Fraude Interno * Fraude Externo * Relaciones Laborales * Clientes * Daños a Activos Físicos * Fallas Tecnológicas * Ejecución y Administración de Procesos |
| 7.2 | Falla | Alfanumérico | **Campo de selección múltiple**   * Actividades no autorizadas * Administración indebida de activos de información * Asonadas * Ausencia de documentación o documentación incompleta de los clientes * Ausencia de documentación o documentación incompleta del proceso * Desastres y otros eventos * Discriminación * Fallas de contrapartes comerciales * Fallas de proveedores o servicios contratados * Fallas en el diseño de los procesos * Fallas en la atención al cliente * Fallas en la definición de los ADS * Fallas en la definición de los servicios * Fallas en la ejecución de los procesos * Fallas en la operatividad de los clientes * Fallas en la segregación de funciones * Fallas en la seguridad del entorno laboral * Fallas en las relaciones laborales * Fallas en los productos * Fallas en los sistemas * Hurto o Fraude * Inoportunidad o inexactitud en la generación de información y/o reportes * Prácticas inapropiadas de negocios o de mercado * Revelación de información del cliente * Vulnerabilidad de los sistemas |
| 7.3 | Factor Riesgo | Alfanumérico | **Lista Desplegable**   * Eventos Externos * Infraestructura * Procesos * Recursos Humanos * Tecnología |
| 7.4 | Descripción de la materialización | Alfanumérico | Campo para registrar por el usuario |
| **8** | **Seguridad de la Información**  Nota. Solo en caso de seleccionar en 6 Información | | |
| 8.1 | Activo de información que se afecta | Alfanumérico | Campo para registrar por el usuario |
| 8.2 | Pilares de seguridad de información | Alfanumérico | CheckBox (selección multiple)   * Confidencialidad * Integridad * Disponibilidad |
| **9** | **Valoración del Riesgo** | | |
| 9.1 | Probabilidad | Alfanumérico | **Lista Desplegable**   * Muy Alta * Alta * Moderada * Baja * Muy Baja |
| 9.2 | Impacto | Alfanumérico | **Lista Desplegable**   * Insignificante * Menor * Moderado * Mayor * Superior |
| 9.3 | Nivel de Riesgo Inherente |  | Calculo (ver mapa de calor) |

### Información para implementar tooltips en las variables, para mejor entendimiento del usuario.

#### Categoría del riesgo

|  |  |
| --- | --- |
| **Categoría del Riesgo** | Descripción |
| General | El Riesgo es inherente a la operación de más de uno de los procesos de la compañía. |
| Específico | El Riesgo se genera únicamente en la ejecución de un proceso particular de la compañía. |

#### Clasificación del riesgo

| **Clasificación del Riesgo** | Descripción |
| --- | --- |
| Continuidad de Negocio | Riesgos de incurrir en pérdidas por eventos de personas, procesos y/o tecnología, que puedan afectar la disponibilidad de los procesos o información. |
| Estratégico | Riesgos de reducción del crecimiento y de incumplimiento de los objetivos empresariales, por la incapacidad de respuesta ante un entorno competitivo dinámico. |
| Financiero | Riesgos derivados de fluctuaciones adversas en las variables financieras que afecten al resultado de la empresa. |
| Información | Riesgos de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el manejo adecuado de la información. |
| Legal | Riesgos de incurrir en pérdidas por sanciones u obligaciones de indemnización por daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. |
| Operativo | Riesgos de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de eventos externos. |
| Reputacional | Riesgos asociados a mala imagen, publicidad negativa, cierta o no, respecto a la compañía y sus prácticas de negocio, que cause pérdida de clientes y/o disminución de ingresos. |

#### Tipo de riesgo

|  |  |
| --- | --- |
| **Tipo de Riesgo** | Descripción |
| Fraude Interno | Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la compañía o incumplir normas o leyes, en los que está implicado al menos un empleado de la organización. |
| Fraude Externo | Actos realizados por una persona externa a la compañía, que buscan defraudar, apropiarse indebidamente de activos o incumplir normas o leyes que perjudiquen la organización. |
| Relaciones Laborales | Actos que incumplen la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia. |
| Clientes | Fallas negligentes o involuntarias en las obligaciones pactadas con los clientes y que puedan impedir el cumplimiento de los servicios contratados. |
| Daños a Activos Físicos | Actos que deriven en daños o perjuicios a los activos físicos de la compañía. |
| Fallas Tecnológicas | Interrupción de los servicios por fallas en la tecnología de información y/o pérdidas derivadas de incidentes por fallas tecnológicas. |
| Ejecución y Administración de Procesos | Deficiencias en la ejecución de procesos, en el procedimiento de operaciones y en las relaciones con proveedores y terceros y/o pérdidas derivadas de errores en la ejecución y administración de los procesos definidos por la organización. |

#### Factor de riesgo

| **Factor de Riesgo** | Descripción |
| --- | --- |
| Eventos Externos | Son eventos asociados a la fuerza de la naturaleza u ocasionado por terceros, que omiten los controles de la entidad en cuento a su causa y origen. Existen factores de riesgo en eventos externos cuando hay fallas relacionadas con: - Fallas en los servicios públicos - Ocurrencia de desastres naturales - Atentados - Otros actos delictivos |
| Infraestructura | Son eventos asociados al funcionamiento de los elementos de apoyo de la organización. Entre otros se incluyen: - Edificios - Espacios de Trabajo - Muebles y accesorios |
| Procesos | Existen factores de riesgo en los procesos cuando hay fallas en: - Definición de políticas y procedimientos. - Estandarización, formalización, actualización y divulgación de procesos. - Definición de objetivos, límite y alcance de los procesos. - Segregación de funciones. - Definición de indicadores de gestión. - Actividades de mejoramiento y su seguimiento. |
| Recursos Humanos | Existen factores de riesgo en el recurso humano cuando hay fallas tales como: - Falta de personal adecuado. - Error Humano. - Inapropiadas relaciones interpersonales y ambiente laboral desfavorable. - Falta de especificación claras en los términos de contratación de personal. |
| Tecnología | Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: Hardware, Software y telecomunicaciones: Existen factores de riesgo en la tecnología cuando hay fallas relacionadas con: - Operaciones de tecnología de información. - Administración de la seguridad de la información. - Continuidad de las operaciones. - Adquisición, desarrollo e implementación de las aplicaciones. - Infraestructura tecnológica. |

#### Probabilidad

|  |  |
| --- | --- |
| **Probabilidad** | **Procesos (tooltip)** |
| Muy Alta | - Puede ocurrir más de una vez al mes - Se espera la ocurrencia del evento en más del 15% de los casos  - ≥ 90% |
| Alta | - Se presenta al menos una vez cada trimestre - Se espera la ocurrencia del evento entre el 10% y 15% de los casos.  - ≥ 75% y < 90% |
| Moderada | - Se presenta al menos una vez cada semestre - Se espera la ocurrencia del evento entre el 5% y 10% de los casos  - ≥ 35% y < 75% |
| Baja | - Se presenta al menos una vez cada año - Se espera la ocurrencia del evento entre en 2% y 5% de los casos  - ≥ 5% y < 35% |
| Muy Baja | - Se ha presentado en alguna ocasión en los últimos 3 años - Se espera la ocurrencia del evento en menos del 2% de los casos  - < %5 |

#### Matriz calificación Impacto

| **Impacto** | **Procesos** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Personas** | **Económico** | **Procesos e Información** | **Riesgo Reputacional / Legal** | **Socio - Ambiental** |
| Insignificante | - Indisponibilidad de menos del 10% de personal no crítico - Lesiones sin incapacidad pero que requieren atención de primeros auxilios o tratamiento médico | - No hay pérdidas económicas - No se generan sobrecostos en la operación | - Afecta el desarrollo de los procesos, sin incumplir ADS internos ni externos -Error u omisión menor - Genera reprocesos insignificantes fácilmente absorbidos por la operación del día a día - No afecta la seguridad de la información - La indisponibilidad o tiempos de inactividad no afectan la operación | - No afecta la imagen de la entidad ante clientes y/o entes de control - Difusión interna sólo a nivel de proceso o equipo de trabajo - Inquietudes por parte de colaboradores que no afectan el clima laboral - No hay incumplimiento contractual o legal | - Ningún impacto social o medioambiental |
| Menor | - Indisponibilidad de entre el 10% y el 20% de personal no crítico - Lesiones con incapacidad parcial temporal (trabajo restringido) | - Las pérdidas económicas no afectan la rentabilidad general del servicio / cliente o la afectan en menos del 10% del EBITDA - Los sobrecostos de la operación son absorbidos con el personal y la infraestructura existente en el proceso | - Afecta ADS internos, pero no externos -Error u omisión moderado - Genera reprocesos menores - Podría causar un impacto menor y fácilmente reparable en la seguridad de la información - La indisponibilidad afecta la operación, pero se continúa el proceso | - Afecta mínimamente la imagen de la entidad ante clientes y/o entes de control - Difusión interna a nivel general en la empresa - Inquietudes por parte de colaboradores o proveedores que afectan el clima laboral de la organización - No hay incumplimiento contractual o legal, pero se generan quejas del cliente | - Contaminación puntual sin consecuencias para el ambiente - Impacto social menor |
| Moderado | - Indisponibilidad de menos del 10% de cargos críticos o entre el 20% y el 40% de personal no crítico - Lesiones con incapacidad total temporal | - Las pérdidas económicas se encuentran dentro de los límites de riesgo materializado para el proceso o afectan el EBITDA entre un 10% a un 20% - Los sobrecostos en la operación requieren de personal o infraestructura existente en otros procesos | - Afecta el ADS del cliente, pero las consecuencias son absorbidas por la operación -Error u omisión sensible - Genera reprocesos moderados - Genera impacto en la seguridad de la información, pero se puede reparar internamente - La indisponibilidad afecta la operación y se requiere el apoyo de otros procesos | - Afecta medianamente la imagen de la entidad ante clientes y/o entes de control - Cobertura adversa puntual en medios a nivel local - Inquietudes por parte de los grupos de interés - Pueden existir no conformidades y/u observaciones contractuales o legales, pero no se generan sanciones o multas | - Daño ambiental leve recuperable en el corto plazo - Impacto social moderado |
| Mayor | - Indisponibilidad entre el 10% y el 20% de cargos críticos o de entre el 40% y 60% de personal no crítico - Lesiones con incapacidad parcial o total permanente | - Las pérdidas económicas se encuentran por fuera de los límites de riesgo materializado o afectan el EBITDA entre un 20% a un 50% - Los sobrecostos en la operación requieren recursos adicionales a los existentes en la compañía | - Afecta el ADS del cliente, con impactos legales -Error u omisión grave - Genera reprocesos mayores - Pérdida de información crítica que no se puede recuperar - Acceso indebido a la información del negocio, incumpliendo acuerdos contractuales -Interrupción del proceso que requiere la ejecución de planes de continuidad | - Afecta altamente la imagen de la entidad ante clientes y/o entes de control - Cobertura adversa de amplia difusión en medios a nivel regional o local en el país y en redes sociales - Pérdida grave o disminución sensible del apoyo o credibilidad de algunos de los grupos de interés - Sanción o Multa incumplimientos contractuales / normativos (confidencialidad, fraudes, calidad). | Daño ambiental significativo recuperable a mediano plazo - Impacto social mayor |
| Superior | - Indisponibilidad de más del 20% de cargos críticos o de más del 60% de personal no crítico - Lesiones fatales | - Las pérdidas económicas por cualquier motivo deben ser cubiertas mediante transferencia a pólizas o afectan el EBITDA en más de un 50% | - Afecta severamente el acceso y la seguridad de la información - Error u omisión severo - Genera alto nivel de reprocesos - Exposición externa o interna de la información del negocio, incumpliendo acuerdos contractuales y normativos - Interrupción del proceso que no puede ser asumida por la operación y debe ser transferida mediante pólizas | - Afecta gravemente la imagen de la entidad ante clientes y/o entes de control - Cobertura adversa de amplia difusión en medios a nivel nacional, internacional y redes sociales  - Pérdida grave del apoyo o credibilidad de todos los grupos de interés - Intervención o cierre parcial o total por parte de entes de control que impida la operación - Incumplimientos contractuales o normativos que lleven a tribunales de arbitramento | Daño ambiental grave no recuperable, o recuperable a largo plazo - Impacto social grave |

### Cálculo del Nivel de riesgo inherente

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Probabilidad / Impacto** | **Insignificante** | **Menor** | **Moderado** | **Mayor** | **Superior** |
| **Muy Alta** | Bajo | Moderado | Alto | Extremo | Extremo |
| **Alta** | Bajo | Moderado | Alto | Alto | Extremo |
| **Moderada** | Bajo | Moderado | Moderado | Alto | Extremo |
| **Baja** | Bajo | Bajo | Moderado | Alto | Extremo |
| **Muy Baja** | Bajo | Bajo | Moderado | Alto | Alto |

## Definición de controles para los riesgos

Para cada uno de los riesgos identificados, se debe realizar la definición de los controles a ser implementados:

### Variables:

| **#** | **Campos** | **Tipo** | **Descripción** |
| --- | --- | --- | --- |
| **1** | **Riesgo mitigado** | Alfanumérico | Campo de selección múltiple  Depende de los riesgos identificados (ID Riesgo)  Debe permitir seleccionar varios riesgos |
| **2. CATEGORIZACIÓN DEL CONTROL** | | | |
| 2.1 | Descripción del Control | Alfanumérico | Campo abierto para libre registro por el usuario |
| 2.2 | Categoría del Control | Alfanumérico | Lista desplegable   * General * Especifico |
| 2.3 | Responsable del Control | Alfanumérico | Campo abierto para libre registro por el usuario |
| 2.4 | Tipo de Control | Alfanumérico | Lista desplegable   * Preventivo * Detectivo * Correctivo * Disuasivo |
| 2.5 | Naturaleza | Alfanumérico | Lista desplegable   * Automático * Semi-automático * Manual |
| 2.6 | Periodicidad | Alfanumérico | Lista desplegable   * AD-HOC * Diario * Semanal * Mensual * Bimestral * Trimestral * Semestral * Anual |
| 2.7 | Referencia del Control | Alfanumérico | Campo abierto para libre registro por el usuario   * Que evidencia queda de la ejecución del control |
| **3** | **Falla que ataca** | Alfanumérico | Depende del riesgo y de las fallas identificadas para el mismo (numeral 4.1 variable 7.2)  Debe traer las fallas y permitir seleccionar de estas.  Pueden ser varias |
| **4** | **Mitiga** | Alfanumérico | Campo de selección múltiple, tipo CheckBox   * Probabilidad * Impacto |
| **5** | **Seguridad y Continuidad** | Alfanumérico | Si uno de los riegos seleccionados es de información, habilitar el checkBox, es decir, Activar si en numeral 4.1, Variable 6=Información   * Confidencialidad * Integridad * Disponibilidad |
| **6** | **Aplicabilidad del control** | Alfanumérico | Campo tipo checkbox   * Requisito de cliente * Requisito normativo   Si se selecciona "Requisito normativo" habilitar un campo abierto "Cual?" |
| **7. VALORACIÓN DEL CONTROL** | | | |
| 7.1 | Diseño | Alfanumérico | Lista desplegable   * Adecuado * Parcialmente Adecuado * Inadecuado |
| 7.2 | Ejecución | Alfanumérico | Lista desplegable   * Adecuado * Parcialmente Adecuado * Inadecuado |
| 7.3 | Efectividad | Alfanumérico | Lista desplegable   * Adecuado * Parcialmente adecuado * Inadecuado |
| 7.4 | Fortaleza del Control | Alfanumérico | Campo que contiene un cálculo, que permite obtener el resultado de:   * Fuerte * Moderado * Débil |

### Información para implementar tooltips en las variables, para mejor entendimiento del usuario.

#### Categoría del control

|  |  |
| --- | --- |
| Categoría del Control | Descripción |
| General | El control permite mitigar riesgos de más de uno de los procesos de la compañía |
| Específico | El control permite mitigar riesgos en la ejecución de un proceso particular de la compañía |

#### Tipo de control

|  |  |
| --- | --- |
| Tipo de Control | Descripción |
| Preventivo | Atacan los factores de riesgo para evitar que la amenaza se materialice, es decir, para evitar que el riesgo se presente |
| Detectivo | Registran la materialización de la amenaza, es decir, la ocurrencia del riesgo, con el fin de tomar acciones frente a ello |
| Correctivo | Actúan directamente en la reducción del impacto y se complementan con los controles detectivos |
| Disuasivo | Inciden en los factores de riesgo para evitar que la amenaza se materialice, pero tienen una menor fortaleza que los preventivos |

#### Naturaleza

|  |  |
| --- | --- |
| Naturaleza del Control | Descripción |
| Automático | El control es ejecutado automáticamente por un sistema automatizado, sin intervención humana |
| Semi-automático | El control es ejecutado por una persona, pero basado en la información generada por un sistema automatizado |
| Manual | El control es ejecutado totalmente por una persona |

#### Periodicidad

|  |  |
| --- | --- |
| Periodicidad del Control | Descripción |
| AD-HOC | El control se ejecuta cuando se requiere |
| Diario | El control se ejecuta diariamente |
| Semanal | El control se ejecuta semanalmente |
| Mensual | El control se ejecuta mensualmente |
| Bimestral | El control se ejecuta cada 2 meses o seis veces al año |
| Trimestral | El control se ejecuta cada 3 meses o cuatro veces al año |
| Semestral | El control se ejecuta cada 6 meses o dos veces al año |
| Anual | El control se ejecuta una vez al año |

#### Diseño del control

| **Diseño del Control** | | | |
| --- | --- | --- | --- |
| Calificación | Pertinencia | Responsable y forma de ejecución | Frecuencia |
| Adecuado | Diseñado para eliminar todas las causas o efectos de la situación de impacto. | Quien ejecuta el control posee las competencias necesarias para hacerlo de manera adecuada. Quien ejecuta el control es la persona adecuada o es el responsable principal de la actividad dentro del proceso El control es automático. El control es semiautomático y durante la ejecución del control se cuenta con la información requerida para realizarlo satisfactoriamente | La frecuencia del control garantiza la mitigación oportuna del riesgo y es razonable teniendo en cuenta la frecuencia de ejecución de la actividad. |
| Parcialmente Adecuado | Diseñado para eliminar algunas causas y/o efectos de la situación de impacto. | Quien ejecuta el control esta medianamente capacitado para hacerlo. Quien ejecuta el control no es el responsable principal de la actividad controlada, pero interviene dentro del proceso e incide en la actividad El control es semiautomático y durante la ejecución del control la información para realizarlo requiere de intervención de otras personas El control es manual y se puede garantizar o verificar su ejecución en el momento oportuno | Poca frecuencia de ejecución del control en relación con la frecuencia de realización de la actividad que supone posible materialización de eventos o detección inoportuna.  Frecuencia de ejecución del control sobredimensionada generando cargas operativas innecesarias. |
| Inadecuado | Mal diseñado, no garantiza la mitigación de la situación aun cuando este bien implementado. | La persona que ejecuta el control no posee las competencias para realizar esta actividad Quien ejecuta el control no es la persona adecuada para ello El control es semiautomático y durante la ejecución del control podría no contarse con la información requerida El control es manual y no se puede garantizar o verificar su ejecución | La frecuencia de ejecución del control no es suficiente para mitigarlo aun cuando sea pertinente y el responsable el adecuado. |

#### Ejecución del control

| **Calificación** | **Resultado del muestreo** |
| --- | --- |
| Adecuado | Más del 80% de las muestras cumplen con los requisitos. |
| Parcialmente Adecuado | Entre el 60% y el 79 % de las muestras cumplen con los requisitos. |
| Inadecuado | Menos del 60% de las muestras cumplen con los requisitos.  El control automático no funciona |

#### Efectividad del control

|  |  |
| --- | --- |
| **Calificación** | **Eventos materializados** |
| Adecuado | No se presentaron eventos relacionados con las fallas que el control mitiga. |
| Parcialmente adecuado | Se presentaron eventos relacionados con alguna de las fallas que el control mitiga |
| Inadecuado | El control presentó eventos por las diferentes fallas que el control mitiga |

#### Fortaleza del control

|  |  |  |
| --- | --- | --- |
| **Fortaleza** | **Descripción** | **Valoración** |
| Fuerte | El control o conjunto de controles mitiga de forma completa las causas para las cuales fue(ron) diseñado(s) | Si el diseño, ejecución y efectividad obtienen calificación de Adecuado, o solo uno de los factores obtiene calificación de Parcialmente Adecuado |
| Moderado | El control o conjunto de controles mitiga parcialmente las causas para las cuales fue(ron) diseñado(s) | Si más de uno de los factores obtiene calificación de Parcialmente Adecuado |
| Débil | El control o conjunto de controles no mitiga el riesgo | Si alguno de los factores obtiene una calificación de Inadecuado |

### Ejemplo

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID Riesgo | Probabilidad | Impacto | Riesgo Inherente | Fortaleza de Control | Que mitiga? | Probabilidad Residual | Impacto Residual | Riesgo Residual |
| RG1 | Moderada | Mayor | Alto |  |  |  |  | Alto |
| RG2 | Muy Alta | Mayor | Extremo | Fuerte | P y I | Moderada | Menor | Moderado |
| RE1 | Moderada | Mayor | Alto | Moderado | P | Baja (2) | Mayor (4) | Alto |
| RE1 | Moderada | Mayor | Alto | Fuerte | P y I | Muy Bajo (1) | Menor (2) | Bajo |
| RE1 | Moderada | Mayor | Alto | Fuerte | I | Moderado (3) | Menor (2) | Moderado |
|  |  |  |  |  | **Total** | **Baja** | **Menor** | **Bajo** |

**Tablas de ponderación**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Probabilidad | Valoración |  | Impacto | Valoración |
| Muy Alta | 5 |  | Insignificante | 1 |
| Alta | 4 |  | Menor | 2 |
| Moderada | 3 |  | Moderado | 3 |
| Baja | 2 |  | Mayor | 4 |
| Muy Baja | 1 |  | Superior | 5 |

**Resultado final**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ejemplo | ID Riesgo | Riesgo Inherente | Controles | Riesgo Residual |
| Ejemplo Riesgo sin controles | RG1 | Alto |  | Alto |
| Ejemplo Riesgo con un control | RG2 | Alto | CG1 | Moderado |
| Ejemplo Riesgo con varios controles | RE1 | Alto | CE1, CE2, CE3 | Bajo |

## Auditoria

## Salidas y reportes