POLÍTICA DE ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES

IBAL SA ESP OFICIAL | SIG SISTEMA INTEGRADO DE GESTIÓN

.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el IBAL S.A. E.S.P OFICIAL, la administración de riesgos es fundamental para asegurar el cumplimiento de su misión institucional y el desarrollo de sus actividades mediante el cumplimiento de los objetivos trazados dentro del Sistema Integrado de Gestión.

Teniendo en cuenta que los riesgos son posibilidades de ocurrencia de toda situación que pueda desviar el normal desarrollo de las actividades de los procesos e impidan el logro de los objetivos institucionales y de procesos para el cumplimiento de la misión de la empresa, el IBAL ha definido criterios orientadores respecto al tratamiento de estos con el fin de mitigar sus efectos en la entidad, siendo éste, el objetivo de la presente política. Con base a esta se pretende en primera instancia, transmitir la posición de la alta dirección sobre la manera de abordar la administración de los riesgos y oportunidades institucionales, socializar con todos los funcionarios un lenguaje común sobre el tema y, por último, difundir los lineamientos que permitan la sostenibilidad de la administración del riesgo.

Las Normas implementadas en la empresa ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018 establecen la importancia de la determinación de riesgos y oportunidades, lo que permite asegurar que el sistema integrado de gestión pueda lograr sus resultados previstos, aumentar los efectos deseables, prevenir o reducir efectos no deseados y lograr la mejora.

2. OBJETIVO GENERAL

Orientar las acciones necesarias para la identificación, valoración y tratamiento a los riesgos (gestión, corrupción, seguridad digital) y oportunidades, con el fin de garantizar el cumplimiento de los objetivos institucionales, alcanzando un nivel aceptable de riesgos residuales en todos los procesos de la empresa IBAL S.A. E.S.P. OFICIAL

3. ALCANCE

Aplica a todos los procesos, proyectos, servicios y planes de la entidad, conforme a la tipología establecida, bajo la responsabilidad de los líderes de proceso y todas las líneas de defensa.

4. CONCEPTOS BÁSICOS RELACIONADOS CON EL RIESGO

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Apetito al riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

CGDI: Comité de Gestión y Desempeño Institucional.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de riesgo: Son las fuentes generadoras de riesgos

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Oportunidad para la seguridad y salud en el trabajo (SST): Circunstancia o conjunto de circunstancias que puedan conducir a la mejora del desempeño de la SST.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Plan de tratamiento de riesgos Digitales: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)

Riesgos para la seguridad y salud en el Trabajo (SST): Combinación de la probabilidad de que ocurra un evento o exposiciones peligrosos relacionados con el trabajo y la severidad de la lesión y deterioro de la salud que pueden causar los eventos o exposiciones.

Riesgos emergentes: Es el riesgo resultante de una incrementada exposición o susceptibilidad frente a un factor desconocido hasta el momento, o bien el asociado a un incremento en la exposición frente a un peligro ya identificado.

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgos y oportunidades: Efectos potenciales adversos (amenazas) y efectos potenciales beneficiosos (oportunidades)

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

TIC: Tecnologías de la Información y las Comunicaciones.

Tolerancia al riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. COMUNICACIÓN Y DIVULGACIÓN

A Nivel Institucional: La divulgación y socialización de la Política de Administración de Riesgos y Oportunidades estará a cargo de los procesos Estratégicos (Planeación estratégica, comunicaciones y relaciones públicas, Sistema Integrado de Gestión). Esta actividad incluye la publicación en la página Web de la entidad.

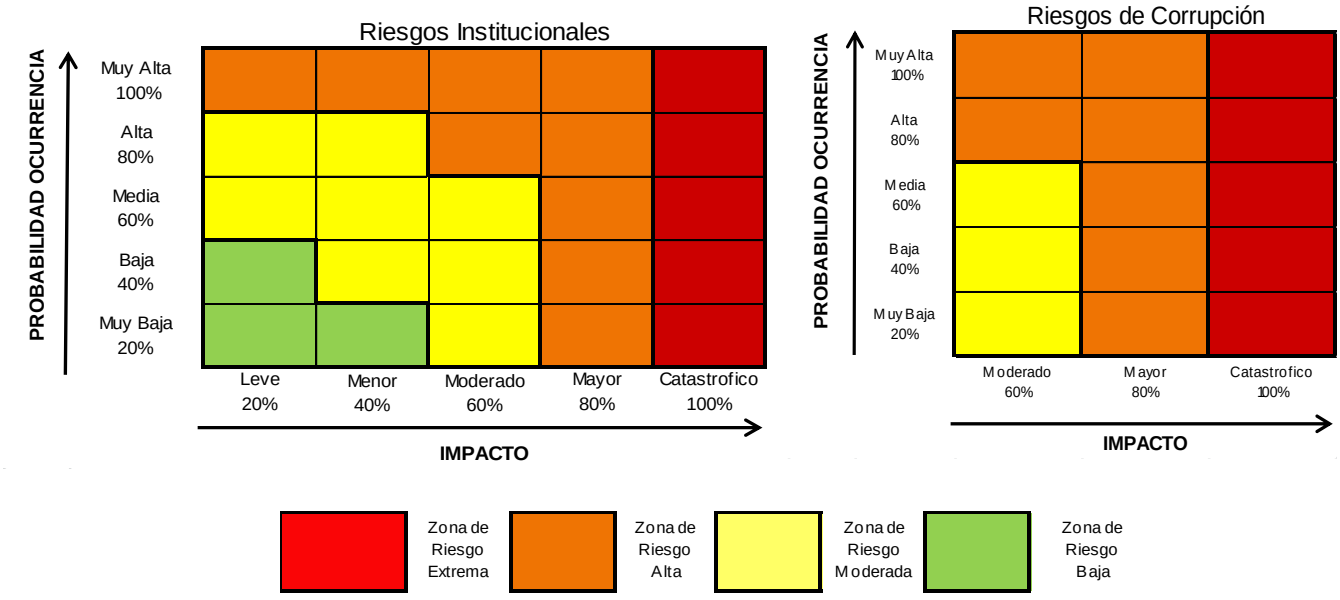
Así mismo, dentro de la estructura organizacional a nivel interno se garantizará un adecuado flujo de la información a todos los niveles de la empresa, esto mediante el uso de herramientas tecnológicas (Intranet, correo institucional, plataforma Spark y demás); esto para el despliegue de información masiva generada por cualquier medio.

A Nivel de Procesos: Estará a cargo de los Líderes de procesos y subprocesos según corresponda, los cuales divulgaran los Mapas de Riesgos por procesos al interior de sus respectivos equipos de trabajo.

6. NIVELES DE ACEPTACIÓN DEL RIESGO

Teniendo en cuenta los riesgos residuales establecidos en cada uno de los procesos y subprocesos según corresponda, el IBAL S.A. E.S.P OFICIAL determina que para los riesgos de gestión y seguridad digital que se encuentren en zona de riesgo baja, se aceptará el riesgo y no requerirá de plan de acción, sin embargo, se continuará monitoreando según la periodicidad definida (*todos los riesgos deben tener acciones de control para evitar la materialización de los mismos*).

En el caso de los riesgos de corrupción no hay aceptación del riesgo, por lo que siempre se debe formular un plan de acción.



La matriz cuenta con cinco (5) filas y cinco (5) columnas, siendo las columnas las alternativas de impacto y las filas son las opciones de probabilidad. Los niveles aceptables de riesgo se establecen de la siguiente manera:

Extremo	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, la Alta Dirección debe establecer el tratamiento e informar al Comité Institucional de Coordinación de Control Interno.
Alto	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe establecer el tratamiento e informar al Comité Institucional de Gestión y Desempeño.
Moderado	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe hacer seguimiento mediante procedimientos existentes.
Bajo	Los riesgos que se ubiquen en esta zona serán aceptados, el líder del proceso debe hacer seguimiento y llevar el registro correspondiente.

- **Niveles de capacidad de riesgo**

En la capacidad del riesgo se determinará el máximo valor del nivel de riesgo que la entidad puede soportar y a partir del cual la alta dirección considera que sería posible el logro de los objetivos de la empresa.

La empresa aplicará los valores de probabilidad e impacto contenidos en la Guía de Administración del riesgo y en el Manual de Metodología de Riesgos SG-M-004, con la participación de la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno, teniendo en cuenta los siguientes valores:

- Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
- Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la empresa, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina "*Capacidad de Riesgo".*

- **Niveles de apetito**

Una vez determinada la capacidad del riesgo se determina el "*apetito del riesgo"* a partir del análisis del nivel del riesgo, el cual se realiza una vez se han identificado los controles para conocer el nivel de riesgo residual, siendo este nivel resultado de la evaluación de la probabilidad con el impacto. Es importante resaltar que el apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la empresa debe o desea gestionar.

- **Niveles de tolerancia**

La tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito del riesgo determinado por la empresa. La determinación de la tolerancia de riesgo es operativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir de riesgos deben ser proporcionadas y

razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia del riesgo.

De acuerdo al apetito, la tolerancia y la capacidad del riesgo, se establece los siguientes niveles de aceptación de los riesgos residual así:

TIPO DE RIESGO	ZONA DE RIESGO MAPA DE CALOR	NIVELES DE ACEPTACIÓN	ACCIONES A TOMAR
GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN	Bajo	Apetito del riesgo y Tolerancia riesgo	Riesgos Aceptados sin plan de acción (Acciones para abordar riesgos)
	Moderado		
	Alto	Capacidad	Riesgos Sopoprtado con acciones correctivas (Acciones para abordar riesgos)
	Extremo	-	Riesgo soportado con acciones correctivas (Acción de contigencia y/o plan de acción)

Nota 1: Para la implementación de los niveles de aceptación se iniciará con lo establecido en el cuadro anterior, pero a medida que se avanza en el proceso se ajustará, según el comportamiento y aceptación por parte de los procesos.

Nota 2: Plan de Acción: El líder del proceso define acciones que permitan mitigar el riesgo residual, este determina fecha de inicio y finalización, el establecimiento de seguimiento que va a realizar durante la ejecución de la acción correspondiente a su avance, este debe de ser reportado junto con el seguimiento al mapa de riesgos y controles establecidos por el mismo.

Es importante resaltar que los anteriores criterios y parámetros fueron tomados con base en lo establecido y recomendado por la Guía de Administración de riesgo del DAFP para la definición de los mismos.

Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

Los valores máximos de escala y los niveles determinados para la capacidad, apetito y tolerancia de los riesgos se establecerán en el *Manual De Metodología De Riesgos SG-M-004.*

CRITERIOS DE CALIFICACIÓN DE PROBABILIDAD E IMPACTO

Los criterios establecidos para la calificación de la probabilidad e Impacto para los riesgos de Gestión y Seguridad Digital se encuentran establecidos en el *Manual De Metodología De Riesgos SG-M-004.*

7. RESPONSABILIDADES Y COMPROMISOS FRENTE AL RIESGO

La responsabilidad está definida mediante las líneas de defensa y en la Entidad se acoge según la siguiente tabla:

LÍNEA DE DEFENSA	RESPONSABLES	ACTIVIDADES
Línea Estratégica	Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno CICCI	✓ Define el marco general para la gestión del riesgo y el control; y supervisa su cumplimiento. ✓ Priorizar y decidir las oportunidades que se implementarán en la empresa. ✓ Asegurar la implementación y desarrollo de las políticas de administración de riesgos ✓ Someter aprobación de la Alta Dirección con el liderazgo del representante legal y la participación del Comité Institucional de Coordinación de Control Interno la Política de Gestión del Riesgo. ✓ Retroalimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. ✓ Revisar la política de administración de riesgos, al menos una vez al año para su actualización y evaluar su eficacia.
Primera Línea	Líderes de proceso	Los líderes de procesos tienen la responsabilidad de gestionar los riesgos y efectúan la gestión a través de su identificación, análisis, valoración, monitoreo, acciones de mejora y mitigación a través del autocontrol ✓ Identificar, valorar, controlar, medir, efectuar seguimiento y actualizar los riesgos que pueden afectar el logro de los objetivos, programas y proyectos de los procesos. ✓ Actualizar los riesgos de gestión del proceso cada vez que se materialicen o se presenten eventos que no han sido contemplados inicialmente y que pueden afectar el cumplimiento de los objetivos del Proceso. ✓ Establecer mecanismos de seguimiento y actualización de los mapa y plan de tratamiento de riesgos (periodicidad, responsables, indicadores, monitoreo).

		✓ Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación ✓ Revisar el adecuado diseño y ejecución de controles establecidos para la mitigación de riesgos e implementarlos en sus procedimientos. ✓ Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio. ✓ Identificar y controlar los riesgos de seguridad digital que puedan afectar al modelo de seguridad y privacidad de información. ✓ Construir los mapas de riesgo, que incluyan los riesgos de gestión, seguridad digital y de corrupción. ✓ Reportar en el SIG los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos por el mismo. ✓ Informar a la oficina de la dirección de planeación (segunda línea) sobre los riesgos materializados que afecten significativamente los objetivos, programas, proyectos y planes de los procesos a cargo. ✓ Socializar al interior de su grupo de trabajo la política y metodología para la administración de riesgos, así mismo comunicar los resultados de la gestión del riesgo. ✓ Delegar, por parte del líder del proceso, el (los) funcionarios que se encargaran de apoyar la identificación, monitoreo, reporte y socialización de los riesgos. ✓ Aplicar los controles identificados y proponer mejoras si hay lugar a ello, para asegurar un efectivo manejo del riesgo. ✓ Desarrollar ejercicios de Autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.

Segunda Línea	Dirección de Planeación	La dirección de planeación tiene como responsabilidad la capacitación, acompañamiento, recomendaciones, monitoreo y evaluación del estado de controles y la Gestión del Riesgo. ✓ Supervisar que la primera línea identifique, analice, valore, evalué y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. ✓ Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. ✓ Promover ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. ✓ Presenta al CICCI el resultado de la medición del nivel de eficiencia de los controles para el tratamiento de los riesgos identificados por los diferentes procesos y subprocesos. ✓ Asegurará que los controles y procesos de gestión del riesgo de la 1º línea de Defensa sean apropiado y funcionen correctamente (supervisión de la implementación de prácticas de gestión de riesgo eficaces) ✓ Verificar que el líder de Seguridad de la Información supervise el desarrollo y mantenimiento de controles de Tecnológicos y de seguridad y privacidad de la información. ✓ Consolidar los Mapas de Riesgos institucionales a partir de la información reportada por cada uno de los procesos (mapa de riesgos del proceso) socializándolo y publicándolo. ✓ Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado e incluido en el mapa de riesgos. ✓ Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
		Esta línea se encuentra bajo la responsabilidad del (la) asesor de la oficina de control interno; el cual efectuará a través del enfoque hacia la prevención la evaluación y seguimiento de la gestión del riesgo institucional. ✓ Asesorar en las metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa. ✓ Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.

Tercera Línea	Oficina asesora de control interno	✓ Identificar y evaluar cambios que podrían tener un impacto significativo en el sistema de control interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. ✓ Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo detectados en las auditorías. ✓ Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad. ✓ Asesorar a la primera línea de defensa de forma coordinada con la dirección de planeación, en la identificación de los riesgos y diseño de controles. ✓ Efectuar recomendaciones sobre la posible incidencia o materialización de riesgos durante las auditorías internas y lo evidenciado en auditorias por entes de control. ✓ Recomendar mejoras a la política de administración del riesgo. ✓ Recomendar al líder del proceso la revisión, análisis y formulación de acciones correctivas, frente a los riesgos de gestión, corrupción y seguridad digital.

8. TIPOLOGÍA DE RIESGOS

RIESGOS DE GESTIÓN	
TIPOLOGÍA	**DEFINICIÓN**
Riesgos Estratégicos	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impacta toda la entidad.
Riesgos Operativos	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Riesgos Ambientales	Posibilidad de ocurrencia de eventos que afecten el desempeño del Sistema de Gestión Ambiental de la entidad.
Riesgos de Seguridad y Salud en el Trabajo	Posibilidad de ocurrencia de eventos que afecten la seguridad y salud de los trabajadores.
Riesgo Financieros	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

Riesgos Tecnológicos	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
Riesgos de Cumplimiento	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
Riesgo de imagen o reputacional	Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
RIESGOS DE SEGURIDAD DIGITAL	
TIPOLOGÍA	**DEFINICIÓN**
Se pueden identificar los siguientes tres (3) riesgos asociados a la seguridad de la información: Pérdida de confidencialidad Pérdida de integridad Pérdida de disponibilidad de los activos de información	Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”. Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales, incluye aspectos relacionados con el ambiente físicos, digital y las personas.
RIESGOS DE CORRUPCIÓN	
DEFINICIÓN	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
RIESGO DE FRAUDE	
DEFINICIÓN	Posibilidad de que la Empresa incurra en una pérdida financiera, cuando una persona (personal vinculado laboralmente a la empresa) que actúa individualmente o en colusión, obtiene una ventaja o beneficio injusto de forma deshonesta o engañosa.

9. IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Para la identificación de los activos de seguridad de la información se tiene establecida la política de Gestión del Riesgo de seguridad digital GT-O-002, en donde se definen los lineamientos y criterios para su implementación, para garantizar tanto su funcionamiento interno como de cara al ciudadano, aumentado así su confianza en el uso del entorno digital.

De igual forma, en donde se analicen los activos de información, mediante la aplicación de la Guía de riesgos del DAFP, para su valoración, clasificación y tratamiento, con el fin de gestionar la confidencialidad, disponibilidad e integridad de la información

10. IDENTIFICACIÓN DE RIESGOS

Para la identificación de los riesgos que pueden afectar los diferentes procesos de la entidad, se debe tener en cuenta el contexto estratégico (Matriz DOFA), la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.
Los objetivos deben incluir el “qué”, “como”, “para qué”, “cuándo”, “cuánto”. Si no están bien definidos los objetivos, no se puede continuar con la metodología de gestión del riesgo.

Es importante también tener en cuenta que cuando se presente una situación que afecta el cumplimiento del objetivo del proceso ***y que no fue contemplada en la identificación de riesgos*** (no conformidades de auditorías del ente certificador, hallazgos de entes de vigilancia y control, entre otros), esta sea incluida, para lo cual se debe actualizar el mapa de riesgos y establecerse los controles para mitigarlo.

- **RIESGOS DIGITALES**

Con relación a los riesgos digitales, estos se podrán identificar en los tres (3) riesgos inherentes de seguridad digital:

Pérdida de la confidencialidad, Pérdida de la integridad, Pérdida de la disponibilidad

Para cada riesgo, se deben relacionar el grupo de activos de cada proceso, y colectivamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización de dicho riesgo estudiado. Para cada clasificación de activo o grupo de activos se pueden tener una serie de riesgos, los cuales la empresa IBAL SA ESP OFICIAL, debe identificar, valorar y posteriormente tratar si el nivel de criticidad del riesgo digital lo amerita.

- **IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO**

Se debe identificar en las actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

- **IDENTIFICACIÓN DE AREAS DE IMPACTO**

Se refiere a la consecuencia económica o reputacional a la que se verá expuesta la empresa, en caso de materializarse el riesgo. ***Ver*** *tabla de impacto del Manual De Metodología De Riesgos SG-M-004.*

11. IDENTIFICACIÓN DE AREAS DE FACTORES DE RIESGO

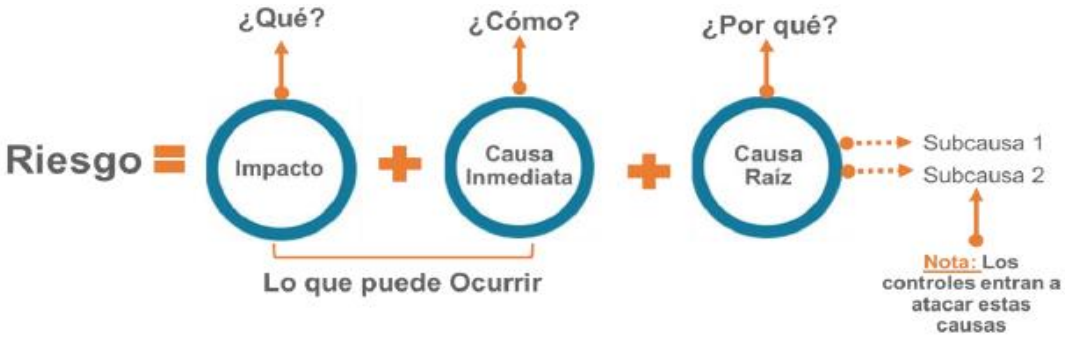
FUENTES QUE GENERAN LOS RIESGOS

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	✓ Falta de procedimientos. ✓ Errores de grabación, autorización. ✓ Errores en cálculos para pagos internos y externos. ✓ Falta de capacitación, temas relacionados con el personal.
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción	✓ Posibles comportamientos no éticos de los empleados. ✓ Fraude interno (corrupción, soborno).
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	✓ Daño de equipos. ✓ Caída de aplicaciones. ✓ Caída de redes. ✓ Errores en programas ✓ Ataques cibernéticos
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	✓ Derrumbes. ✓ Incendios. ✓ Inundaciones.

		✓ Daños a activos fijos
Comunicación Interna	Efectividad en los flujos de información determinados en la interacción de los procesos	✓ Información no oportuna
Evento externo	Situaciones externas que afectan la entidad	✓ Suplantación de identidad ✓ Asalto a la oficina ✓ Atentados, vandalismo, orden público.

12. DESCRIPCIÓN DEL RIESGO

La descripción del riesgo debe ser de fácil entendimiento tanto para el líder como para cualquier persona que lo lea. Debe iniciar siempre con la frase POSIBILIDAD DE y analizar dentro de su estructura lo siguiente:



- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo. Factores de impacto a los que puede estar expuesto el IBAL los cuales son:
  - ✓ Afectación Económica: Afectación presupuestal de la entidad
  - ✓ Afectación Reputacional: Afectación de la imagen de la entidad
- **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo.

Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o sub causa que pueden ser analizadas y tratadas- acciones de control.

Para una adecuada redacción de riesgos se debe tener en cuenta lo siguiente:

- No describir como riesgos omisiones ni desviaciones del control.
- No describir causas como riesgos
- No describir riesgos como la negación de un control
- No existen riesgos transversales, lo que pueden existir son causas transversales

NOTA: Ejemplos de una adecuada redacción de los riesgos, causa y demás (ver manual de metodología de riesgos).

En los **riesgos de corrupción** es necesario que en la descripción del riesgo concurran los componentes de su definición así:

Acción u omisión + **Uso del poder** + **Desviación de la gestión de lo público** + **el beneficio privado** = **Riesgo de Corrupción**

Los riesgos establecidos deben de estar redactados de forma clara y precisa.

De acuerdo a lo establecido en el protocolo para la identificación de Riesgos de Corrupción asociados a la prestación de trámites y servicios del DAFP se determinó lo siguiente:

1. **La corrupción en los trámites administrativos se pueden presentar en dos momentos:**

a) En el momento de efectuar el trámite propiamente dicho, cuando interactúan el ciudadano y el servidor (es decir la ventanilla hacia afuera de la entidad por ejemplo cuando el ciudadano presenta un documento o efectúa un pago).

b) En el momento que se ejecutan los procedimientos al interior de la entidad para dar cumplimiento al trámite (de la ventanilla hacia adentro. La entidad tiene procedimientos internos, como por ejemplo distribuir la documentación recibida entre las áreas internas cambiando el turno).

13. VALORACIÓN DE LOS RIESGOS – NIVELES DE ACEPTACIÓN

Mediante la valoración del riesgo se establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (**Riesgo Inherente**), para ello se deben realizar dos etapas:

ANALISIS DE RIESGOS: Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (**Riesgo Inherente**).

I. **Determinar la Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo, la cual estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

   A continuación, se establecen los criterios para definir el nivel de probabilidad:

TABLA DE PROBABILIDAD

Nivel	Probabilidad	Frecuencia de la Actividad
100%	**Muy Alta**	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.
80%	**Alta**	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.
60%	**Media**	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.
40%	**Baja**	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.
20%	**Muy Baja**	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.

Fuente: Manual metodología de riesgos de la Función Pública v05

II. **Determinar el Impacto:** Para analizar el impacto se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

TABLA DE IMPACTO

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
100%	**Catastrófico**	Pérdida económica superior a 1500 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel Internacional.
80%	**Mayo**	Pérdida económica de 319 hasta 1500 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial.
60%	**Moderado**	Pérdida económica de 21 hasta 318 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos.
40%	**Menor**	Pérdida económica de 11 hasta 20 SMLV.	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	**Leve**	Pérdida económica hasta 10 SMLV.	Solo de conocimiento de algunos funcionarios.

Fuente: Manual metodología de riesgos de la Función Pública v05

Para Los **Riesgos de Corrupción y/o Fraude** se tiene en cuenta solamente los niveles "***moderado, mayor y catastrófico***", dado que estos riesgos siempre serán significativos y se aplicará la tabla de valoración establecida por Secretaría de Transparencia de la Presidencia de la República.

Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del Riesgo.

CALIFICACIÓN DEL IMPACTO PARA LOS RIESGOS DE CORRUPCIÓN

No	Pregunta: Si el riesgo de corrupción se materializa podría…	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		

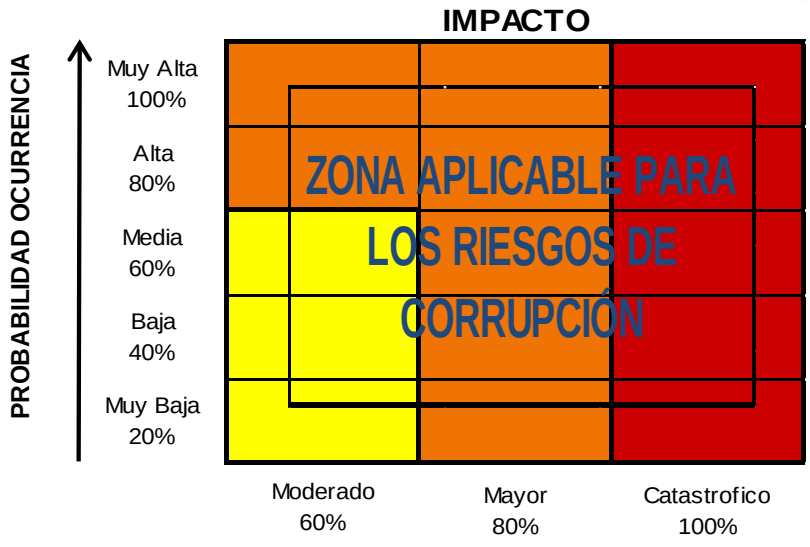
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Nivel	Descriptor	Descripción	Respuestas Afirmativas
1	Moderado	Genera medianas consecuencias para la entidad	1 a 5
2	Mayor	Genera altas consecuencias sobre la entidad	6 a 11
3	Catastrófico	Genera consecuencias desastrosas para la entidad	12 a 19

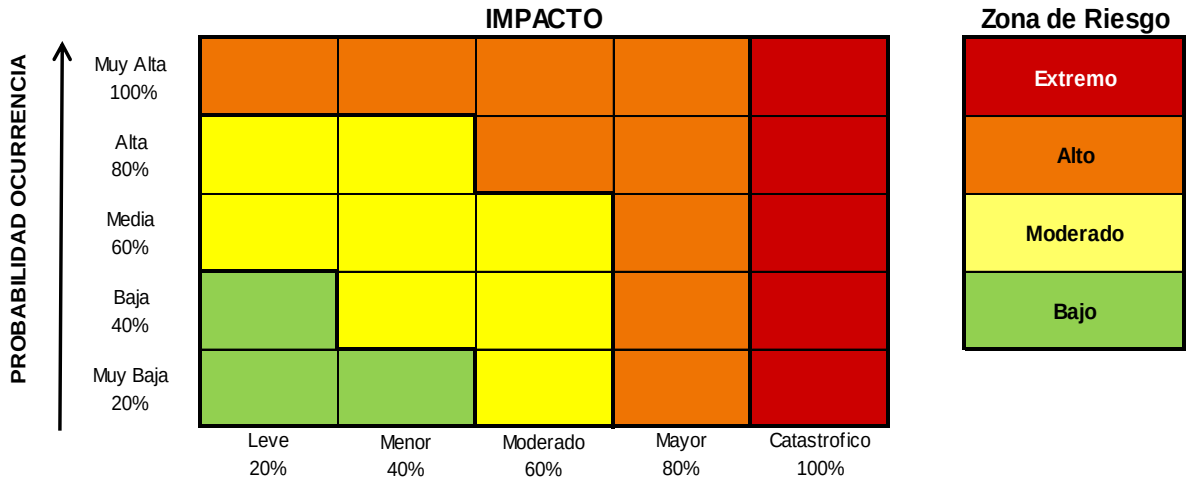
Mapa de calor que aplica a los riesgos de Corrupción y/o fraude de acuerdo a lo niveles mencionados.

Para los niveles de aceptación de los ***riesgos de gestión y seguridad digital***, varían según la celda en que ubican el riesgo residual en la matriz de calor (niveles de severidad), a continuación, se estable los porcentajes establecidos para la determinación de la Probabilidad e Impacto.

- **Mapa de calor para riesgos de Corrupción y Fraude**



- **Mapa de calor para riesgos de Gestión Inherente**



La evaluación de los riesgos inherentes se encuentra de manera detallada en el Manual de metodología de riesgos.

EVALUACIÓN DE RIESGOS: Se busca confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (**Riesgo Residual**). Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo por parte de los líderes de procesos.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.
- Para cada causa debe existir un control.
- Las causas se deben trabajar de manera separada.
- Un control puede ser tan eficiente que ayude a mitigar varias causas, en este caso se debe repetir el control asociado a cada causa.

14. ESTRUCTURA PARA EL DISEÑO Y DESCRIPCIÓN DE UN CONTROL

Para una adecuada redacción del control la Guía para la administración del riesgo propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. El propósito es comparar los resultados del análisis de los riesgos inherentes (sin controles) con los controles establecidos, esto para la determinación de la zona de riesgo final – riesgo residual. A continuación, se lista la siguiente estructura:

- **DISEÑO DE REDACCIÓN DE LOS CONTROLES**

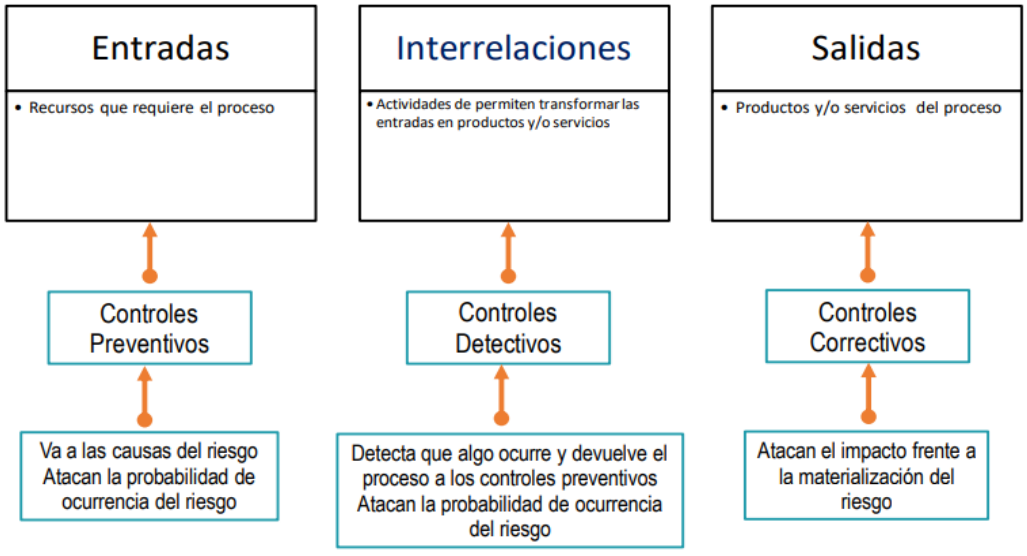
Durante la redacción de los controles es importante considerar que estos se encuentren bien diseñados, es decir, que efectivamente mitiguen las causas que generan la materialización del riesgo, por tanto, como lo establece la metodología de administración del riesgo se debe establecer los siguientes criterios de evaluación:

1. **Responsable**
2. **Periodicidad**
3. **Propósito**
4. **Cómo se realiza la actividad de control**
5. **Qué pasa con las observaciones o desviaciones**
6. **Evidencia**

Ejemplo:

El profesional de Contratación cada vez que se va a realizar un contrato, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor. En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación. Como evidencia deja Lista de Chequeo diligenciada con la información de la carpeta del cliente, y correos solicitando la información faltante en los casos que aplique.

- **TIPOLOGÍA DE CONTROLES**



Así mismo, de acuerdo con la forma como se ejecutan:

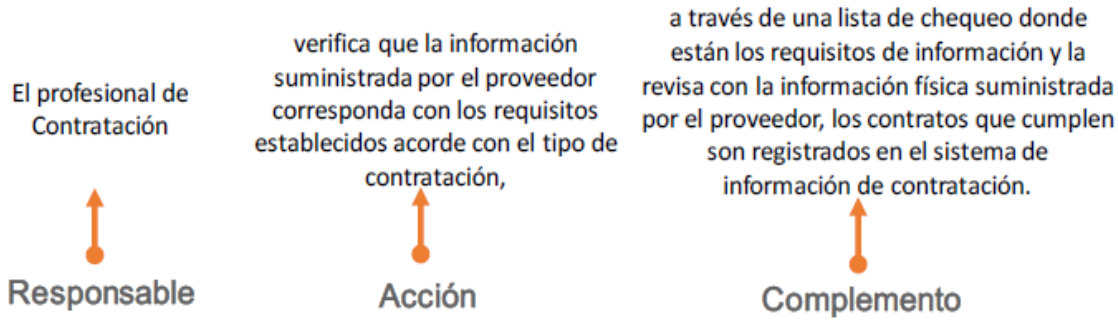
- **Control Manual:** Controles que son ejecutados por personas.
- **Control Automático:** Son ejecutados por un sistema.

Análisis y evaluación de controles – Atributos

De acuerdo a los atributos para el diseño de los controles relacionados con la eficiencia y la formalización se tiene establecida una estructura que facilitará entender su tipología y otros atributos para su valoración. A continuación se describe los componentes:

- ✓ Responsable de ejecutar el control: Identifica el cargo del supervisor que ejecutara el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- ✓ Acción: Se determina mediante verbos que indican la acción que deben realizar como parte del control.
- ✓ Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control

Ejemplo: Aplicado bajo la estructura propuesta para la redacción del control – Criterios de Evaluación



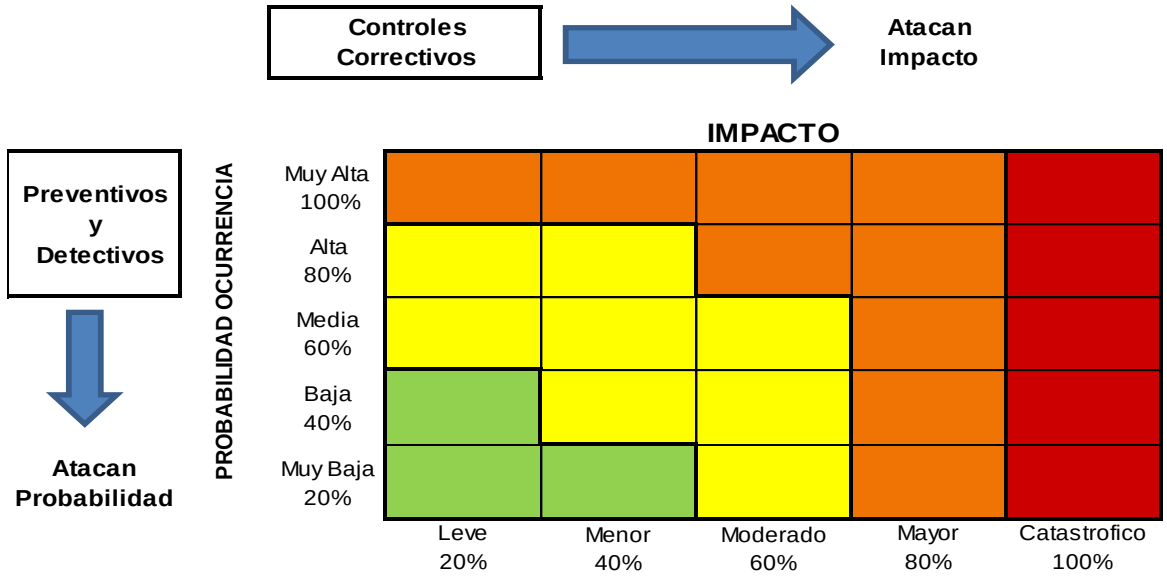
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Los aspectos sin peso son los atributos informativos que no tienen incidencia directa en la efectividad del control, sin embargo, permiten darle formalidad a esté. Los aspectos de tipo e implementación, son atributos que tienen incidencia directa en la efectividad del control, su valoración suma máximo 50% y mínimo 25%. *Ver Manual De Metodología De Riesgos SG-M-004 - Atributos para el diseño del control*

Nota: Siempre que se realicen ajustes a los controles se deben ajustar los documentos, y de igual forma si se hacen ajustes a los documentos del proceso se deben ajustar los controles involucrados y demás.

NIVEL DEL RIESGO RESIDUAL

Este corresponde al resultado de **aplicar la efectividad de los controles** al riesgo inherente. A continuación, se hace ilustración del movimiento en el mapa de calor de probabilidad e Impacto de acuerdo a la tipología de controles de los riesgos **RESIDUALES**



De acuerdo al análisis y evaluación de los controles establecidos por cada uno de los líderes de procesos se valora nuevamente la probabilidad e impacto del riesgo, determinando si los controles disminuyen o no a la probabilidad e impacto del riesgo, bajando así el nivel de exposición de ocurrencia del mismo, procediendo así a ubicar el riesgo en el Mapa de Riesgo Residual.

Es importante resaltar que de acuerdo a la valoración de cada riesgo residual y su ubicación en la zona de riesgo (bajo, moderado, alto y extremo) se estable la opción de manejo (reducir, aceptar y/o evitar). Esto se precisa a partir del nivel de riesgo residual (establecimiento de controles), de la importancia del riesgo, de la probabilidad e impacto de este, de las medidas de tratamiento y el efecto que puede tener sobre los objetivos y políticas de la empresa. ***Ver*** *Manual De Metodología De Riesgos SG-M-004 - Estrategia para combatir el riesgo.*

15. TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

En caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos

para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

OPCIÓN PARA EL MANEJO DEL RIESGO	DESCRIPCIÓN
EVITAR EL RIESGO	Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones Emprendidas.
REDUCIR EL RIESGO	Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la Implementación de controles.
COMPARTIR O TRANSFERIR EL RIESGO	Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, Como en los contratos a riesgo compartido. *Ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de Ubicación segura, en vez de dejarla concentrada en un solo lugar.*
ACEPTAR EL RIESGO	Luego de que el riesgo ha sido reducido o transferido, puede quedar un riesgo residual que se mantiene, en este caso el responsable del proceso simplemente acepta la pérdida residual probable y elabora planes de Contingencia para su manejo.

Los **riesgos de seguridad digital** se podrán mitigar y /o tratar empleando los siguientes controles, tomados del Anexo A del estándar ISO/IEC 27001:2013 y los dominios a los que pertenecen, siempre y cuando se ajusten al análisis de riesgos.

- ✓ A.5 Políticas de seguridad de la información.
- ✓ A.6 Organización de la seguridad de la información
- ✓ A.7 Seguridad de los recursos humanos
- ✓ A.11 Seguridad física y del entorno
- ✓ A.16 Gestión de incidentes de seguridad de la información

De forma similar, el tratamiento de los riesgos digitales es un proceso cíclico, el cual implica la selección de opciones para cambiarlos, por lo tanto, la empresa IBAL SA ESP Oficial, debe tener en cuenta las opciones planteadas en la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” del DAFP: Evitar,

aceptar, compartir o mitigar el riesgo. *Ver Política de Gestión del riesgo de seguridad digital GT-O-002.*

Los **riesgos de Corrupción** de acuerdo a las disposiciones establecidas por la Secretaria de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011 en donde se diseñó una metodología para que todas las entidades determinen su Plan Anticorrupción y de Atención al Ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción. Teniendo en cuenta que los riesgos de corrupción se convierten en una tipología de riesgos que debe de ser controlados por la empresa, éstos deben de ser incorporados en la primera instancia en los mapas de riesgos de los diferentes procesos. A continuación, se relaciona los siguientes lineamientos a tener en cuenta:

- Los riesgos de corrupción deberían tratar de evitarse, estableciendo controles para el hecho de corrupción.

- Los hechos de corrupción son inaceptables e indeseables.

- **Elaboración**: El mapa de riesgos de corrupción lo elabora anualmente cada líder de proceso con su equipo de trabajo, donde se debe establecer revisión constante del mismo.

- **Publicación del mapa de riesgos de corrupción**: Se debe publicar en la página web de la entidad.

- **Ajustes y modificaciones**: Una vez publicado y durante el transcurso de la vigencia, los líderes de proceso podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el Mapa de Riesgos de Corrupción realizando la debida solicitud correspondiente ante la Dirección de Planeación, para este caso concreto, deberán de dejar por escrito los ajustes, modificaciones o inclusiones realizadas.

ZONA DE RIESGO Y TRATAMIENTO

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL	Baja	Se **ACEPTA** el riesgo y se administra por medio de las actividades propias del proceso o procedimiento asociado y se realiza en el reporte bimensual de su desempeño.
RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del Riesgo, se hace monitoreo BIMENSUAL.
	Alta y Extrema	Se adoptan medidas para **REDUCIR O COMPARTIR** la probabilidad o el impacto del riesgo, o ambos; esto conlleva a la implementación de controles. Periodicidad BIMENSUAL.

RIESGOS DE CORRUPCIÓN	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del Riesgo. Periodicidad **BIMENSUAL** de monitoreo para evitar a toda costa su materialización por parte de los procesos.
	Alta y Extrema	**Se adoptan medidas para:** **REDUCIR** la probabilidad o el impacto del riesgo, o ambos; Por lo general conlleva a la implementación de controles. **EVITAR** Se abandonan las actividades que dan lugar al Riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. **TRANSFERIR O COMPARTIR** una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad BIMENSUAL de monitoreo para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.

16. MONITOREO Y SEGUIMIENTO

El monitoreo a los riesgos es de pertinencia de las líneas estratégica, primera, segunda y tercera, los cuales están definidos de la siguiente manera:

- ✓ **Línea Estratégica:** El comité de Coordinación de Control Interno y Comité Institucional de Gestión y Desempeño, realizará monitoreo semestralmente, para verificar el cumplimiento de la política de administración de riesgos y sus respectivos soportes, teniendo en cuenta los criterios de ERCA (Evitar, Reducir, Compartir y Aceptar).
- ✓ **Primera Línea de Defensa:** Los líderes de los procesos en conjunto con sus equipos de trabajo deben monitorear y revisar trimestralmente las acciones tendientes a controlar y gestionar los riesgos.
- ✓ **Segunda Línea de Defensa:** Realizará monitoreo y seguimiento semestralmente de la información contenida en los mapas de riesgos e informes que los líderes de procesos remitan, asegurando que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

Se debe de tener en cuenta los incidentes de **seguridad digital** que hayan afectado al IBAL SA ESP Oficial y también los indicadores definidos para hacer seguimiento a las medidas de seguridad diseñadas. Todo lo anteriormente expuesto contribuye a la toma de decisiones en el proceso de monitoreo del riesgo por parte de la línea estratégica (Alta dirección), Control Interno y las partes interesadas.

SEGUIMIENTO:

- ✓ **Tercera Línea de Defesa:** La oficina de control interno quien provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, este seguimiento se efectuara semestralmente.

Además de la evaluación de riesgos, la Oficina de Control Interno estimará el estado de la implementación, la efectividad de las medidas de administración y el diseño de los controles.

Para el caso concreto de los **Riesgos de Corrupción y Fraude**, la Dirección de Planeación publicará en la página web institucional, de acuerdo a lo establecido en el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. Así como cada cuatrimestre los seguimientos realizados a este.

LÍNEAS DE DEFENSA	PERIODICIDAD DEL MONITOREO Y SEGUIMIENTO	QUIEN REPORTA
Línea Estratégica: Comité de Coordinación de Control Interno y Comité Institucional de Gestión y Desempeño	Semestral	Informe de la oficina Control Interno de Gestión
Primera Línea de Defensa: Líderes de los procesos	Trimestral	Los líderes entregan informe a la Dirección de Planeación- SIG
Segunda Línea de Defensa: Dirección de Planeación	Semestral	Informe consolidado de seguimiento a los procesos
Tercera Línea de Defesa: Oficina de Control Interno de Gestión	Semestral	Realiza seguimiento al monitoreo de la Dirección de Planeación

17. ACCIONES ANTE LA MATERIALIZACIÓN DEL RIESGO

Una vez se materializan los riesgos identificados en el mapa de riesgos institucionales por proceso se deben aplicar las acciones descritas en la siguiente tabla – Acciones de tratamiento a Riesgos.

TIPO DE RIESGO	RESPONSABLE	ACCIONES
		- Informar a la oficina de planeación sobre el hecho encontrado.

RIESGO DE CORRUPCIÓN	**LÍDER DE PROCESO**	- Una vez surtido conducto regular establecido por la empresa (normatividad asociada al hecho de corrupción materializado), se tramitará la denuncia ante la instancia del control correspondiente. - Se identificará las acciones correctivas necesarias y documentales en el Plan de Mejoramiento. - Efectuar el análisis de causas y determinar las acciones preventivas y de mejora. - Actualizar el mapa de riesgos.
	OFICINA DE CONTROL INTERNO	- Informar al líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. - Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados. - Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), informar a las autoridades competentes la ocurrencia del posible hecho de corrupción. - Una vez surtido el conducto regular establecido por la empresa y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. - Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar y actualizar el mapa de riesgos.
RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL (Zona Extrema, Alta y Moderada)	**LÍDER DE PROCESO**	- Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo, documentar en el Plan de Mejoramiento. - Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento, y realizar el análisis y reevaluación de los riesgos del proceso. - Analizar y actualizar el mapa de riesgos. - Informar a la segunda línea de defensa sobre el hallazgo y las acciones efectuadas.
RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL (Zona Baja)	**LÍDER DE PROCESO**	- Establecer las acciones correctivas al interior del proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos. - Para los riesgos de seguridad digital ubicados en esta zona, se deberá llevar un registro de los incidentes que se hayan materializado, con el fin de analizar las causas, las deficiencias de los

		controles implementados y las pérdidas que se puedan generar.
RIESGOS DE GESTIÓN Y SEGURIDAD DIGITAL (Zona Extrema, Alta y Moderada)	**OFICINA DE CONTROL INTERNO**	- Informar al líder del proceso sobre el hecho encontrado. - Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para la revisión respectiva del mapa. - Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. - Verificar y evaluar que se tomaron para las acciones y se actualice el correspondiente riesgo.

18. TRATAMIENTO DE LAS OPORTUNIDADES

Para identificar las oportunidades de mejora se debe tener en cuenta el contexto de la organización, así como las partes interesadas. Otro aspecto a tener en cuenta es que a partir de un riesgo también puede surgir una oportunidad.

Las oportunidades identificadas a través de las herramientas mencionadas, se priorizan por la alta dirección y se llevan al formato **SG-R-033 Acciones para abordar las oportunidades**, donde se establecen los responsables, plazo de ejecución, recursos y evidencias de su implementación.

19. NORMATIVIDAD

- Ley 1474 de 2011: Estatuto anticorrupción. Artículo 73 “Plan Anticorrupción y de atención al ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Departamento administrativo de la función pública -DAFP, Versión 4 de octubre de 2018 y Versión 5 de diciembre de 2020.
- NTC ISO 900: 2015 Norma Técnica Colombiana de Sistemas de Gestión de la Calidad.
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”. Expedida por el Congreso de la República de Colombia.

- Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”. Expedida por el Congreso de la República de Colombia.
- CONPES 3854 del 11 de abril de 2016 “POLÍTICA NACIONAL DE SEGURIDAD DIGITAL”, 3.2. Estrategia de gestión de riesgos de seguridad digital. Expedida por el Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación.
- Decreto 1008 de 2018, “Por el cual se establece los lineamientos digitales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015”. Expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones.

20. CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCION DEL CAMBIO
2019-04-09	01	Se realizan ajustes en el tratamiento del riesgo
2022-05-05	02	Se actualiza teniendo en cuenta la versión 05 del 2020 de la Guía de administración del riesgo del DAFP