INSTITUTO DE PREVISIÓN SOCIAL DE LA FUERZA ARMADA

Manual de Gestión del Riesgo Operacional

Gerencia General

Unidad de Desarrollo Organizacional

Contenido

INTRODUCCIÓN

La Superintendencia del Sistema Financiero de El Salvador, como autoridad supervisora a nivel nacional ha promovido la cultura de la administración de riesgos entre las diferentes entidades sometidas a su inspección y vigilancia, enfatizando en su importancia respecto a los riesgos operativos, lo cual exige una respuesta eficaz, oportuna y coordinada, por parte de las instituciones legalmente vigiladas.

El Riesgo Operativo es definido como la posibilidad de incurrir en pérdidas resultante de las deficiencias, fallas o incongruencias que se pueden presentar por recursos humanos, en los procesos, fallas en la tecnología, en la infraestructura y por eventos externos.

Con el fin de mitigar el riesgo operativo, el Instituto de Previsión Social de la Fuerza Armada (IPSFA), debe contar con elementos de continua ejecución y monitoreo de las diferentes operaciones y procesos, los cuales permiten la reducción de los errores humanos y tecnológicos, de los diferentes tipos de fraude, entre otros.

Por lo cual hace especial énfasis en el Sistema de Administración de Riesgo Operativo. el cual está fundamentado bajo el estándar de la norma técnica NTC ISO 31000:2011.

Es importante tener en cuenta que enfocar al Riesgo Operativo dentro de un sistema de administración, permite optimizar el control de éste tipo riesgo y estimula la identificación de oportunidades de mejora para los procesos de la Institución.

La Gestión de Riesgo Operativo está dirigida a todas las personas que, bajo cualquier modalidad, se encuentran vinculados al IPSFA, y constituye un elemento de apoyo para el cumplimiento de las responsabilidades asignadas, y su contenido debe ser de cumplimiento obligatorio.

I. GENERALIDADES

A. OBJETIVOS

1. Diseñar un manual que sirva de herramienta para la identificación, medición, control y monitoreo, que al mismo tiempo facilite la adecuada administración del riesgo operacional (RO).
2. Establecer la normativa para una adecuada gestión y administración del riesgo operacional.

B. LEGISLACIÓN RELACIONADA

1. NPB4-47 Normas para la Gestión Integral del Riesgo de las Entidades Financieras.
2. NPB4-50 Normas para la Gestión del Riesgo Operacional de las Entidades Financieras.
3. Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las entidades del sector público emitidas por la Corte de Cuentas de la Republica.
4. Disposiciones de Carácter General emitidas por la Superintendencia del Sistema Financiero.
5. Normas Técnicas de Control interno Específicas del IPSFA, Art.38, 39 y 40.
6. Normas Técnicas de Control Interno Especificas del IPSFA.

C. DEFINICIONES

1. **Administración Integral de Riesgo**: Conjunto de objetivos, políticas, procedimientos y acciones que se llevan a cabo para identificar, medir, vigilar y limitar, controlar, informar y revelar, los distintos riesgos a que se encuentra expuesto el IPSFA.
2. **Área originadora de Riesgo:** Son las áreas, unidades, gerencias y unidades de negocio de la Institución donde se originan los riesgos productos de sus propias operaciones o factores externos que los generan.

3. **Comité de Riesgos:** Es la instancia creada con el objetivo de vigilar que las operaciones se realicen ajustándose a los objetivos, políticas y procedimientos para la gestión integral de riesgos.
4. **Factor de Riesgo:** Es la variable económica u operativa cuyos movimientos pueden generar cambios y un impacto financiero en el valor de los activos, pasivos o patrimonio del IPSFA.
5. **Mapa de Riesgos:** Es la representación gráfica de los diferentes riesgos a que están expuestos las distintas unidades y áreas del instituto ,así como la probabilidad de ocurrencia y su impacto en forma clara y objetiva.
6. **Probabilidad de Incumplimiento:** La posibilidad de que un deudor o acreditado no cumpla con sus obligaciones de pago en tiempo y forma de pago.
7. **Proceso:** Conjunto ordenado de etapas y pasos con características de acción interrelacionada, dinámica y progresiva que concluye con la obtención de un resultado.
8. **Riesgo:** Contingencia o probabilidad de sufrir una pérdida material, humana o daño económico, como resultado de la ocurrencia de un evento que altere las condiciones normales. Cualquier situación adversa que derive en repercusiones económicas negativas. Eventos futuros inciertos que causan una pérdida y disminuyen la capacidad de logros de los objetivos.
9. **Riesgo de Crédito:** Es la posibilidad de pérdida, debido al incumplimiento de las obligaciones contractuales asumidas por una contraparte, entendida ésta última como un prestatario o un emisor de deuda.
10. **Riesgos Discrecionales:** Son aquellos resultantes de la toma de una posición de riesgo, tales como el riesgo de crédito.
11. **Riesgos no discrecionales:** Son aquellos resultantes de la operación del negocio pero que no son producto de la toma de una posición de riesgo, tales como el riesgo operacional.
12. **Riesgo Inherente:** Nivel de riesgo propio de la actividad del negocio, sin tener en cuenta el efecto de los controles.

13. **Riesgo Legal:** La pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que el IPSFA lleva a cabo, procesos o actividades como errores en opiniones legales, contratos o fianzas o cualquier documento legal que no permita la exigibilidad de un derecho o la imposibilidad legal de ejecutar un contrato debido en las fallas de la implementación legal.
14. **Riesgo Operacional:** Es aquel que puede provocar pérdidas directas o indirectas como resultado de errores humanos, procesos internos inadecuados o defectuosos, controles internos inadecuados, fallas en los sistemas o a consecuencia de ciertos acontecimientos externos.
15. **El riesgo operacional** es la posibilidad de incurrir en pérdidas debido a fallas en los procesos, las personas, en los sistemas de información y a causa de acontecimientos externos; incluye el riesgo legal que consiste en la posibilidad de ocurrencia de pérdidas debido a fallas en la ejecución de contratos o acuerdos, al incumplimiento de normas, así como a factores externos tales como cambios regulatorios, procesos judiciales, entre otros."
16. **Riesgo Reputacional:** Es la posibilidad de incurrir en pérdidas, producto del deterioro de imagen de la entidad, debido al incumplimiento de leyes, normas o políticas internas, códigos de conducta, lavado de dinero entre otros.
17. **Riesgo Tecnología de información y comunicación:** La pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia del sistema informático y equipo tecnológico, sistemas o aplicaciones, redes y cualquier otro canal de distribución recepción de información para la prestación de servicios a los clientes. Los riesgos del sistema están relacionados a los programas, equipos, infraestructura, sistemas de respaldo, sistemas de seguridad, medios de comunicación, usuarios, capacitación, complejidad, especialistas informáticos, gestión gerencial, capacidad económica del IPSFA y la ocurrencia de eventos externos adversos.

18. **Fraude interno:** Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos o incumplir normas y leyes, en los que está implicado, al menos un empleado de la firma.
19. **Fraude externo:** actos, realizados por una persona externa a la entidad, que buscan defraudar o apropiarse indebidamente de activos o incumplir normas y leyes.
20. **Relaciones laborales:** Actos que son incompatibles con la legislación laboral, con los manuales y acuerdos internos de trabajo, y en general legislación vigente en la materia.
21. **Clientes:** Fallas negligentes o involuntarias de las obligaciones frente a los clientes.
22. **Daños a activos físicos:** pérdidas derivadas de daños o perjuicios a activos físicos de la Institución.
23. **Fallas en los sistemas/** tecnología: pérdidas derivadas de incidentes por fallas tecnológicas.

D. FACTORES DE RIESGO

Se entenderá por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operacional. Los factores de riesgo se clasifican según la NPB4-50 y Reglamento para el uso y control de las tecnologías de información y comunicación en las entidades del sector público en: Procesos, personas, tecnológicos, y acontecimientos externos, los cuales se definen a continuación.

1. **Procesos:** El Instituto deberá gestionar apropiadamente los riesgos asociados a los procesos, con énfasis en las fallas o debilidades que presenten, dado que éstas pueden tener como consecuencia el desarrollo deficiente de las operaciones.

2. **Personas:** Todas aquellas vinculadas al Instituto: Empleados, proveedores, clientes, entre otros. Para la gestión de este factor se establecerán mecanismos preventivos que permitan identificar y gestionar fallas, insuficiencias, negligencia, sabotaje, robo, inadecuada capacitación, apropiación indebida de información, entre otros,

asociadas al personal, vinculado directa o indirectamente a la entidad; de tal modo que se minimice la posibilidad de pérdidas económicas.

Revisar periódicamente la existencia de contratos internos de trabajo, que ampare la vinculación directa, de acuerdo a la legislación laboral respectiva. Por vinculación indirecta entenderemos a aquellas personas que tienen una relación jurídica con la entidad para la prestación de determinados servicios, diferente de aquélla que se origina de un contrato interno de trabajo.

3. **Tecnológicos:** Son aquellos riesgos asociados a la tecnología de información, por ejemplo, los relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, así como la calidad de la información y una adecuada inversión en tecnología. Los riesgos del sistema están relacionados a los programas, equipos, infraestructura, sistemas de respaldo, sistemas de seguridad, medios de comunicación, usuarios, capacitación, complejidad, especialistas informáticos, gestión gerencial, capacidad económica del IPSFA y la ocurrencia de eventos externos adversos.

   La administración del riesgo de sistemas tecnológicos e informático tiene por objetivo evitar o reducir el riesgo, disminuir la probabilidad de ocurrencias y minimizar sus consecuencias. La mayoría de los riesgos pueden ser Mitigados mediante adecuados planes de prevención y contingencia o mantener unos rigurosos sistemas de seguridad.

4. **Acontecimientos Externos:** Este factor incluye los riesgos ocasionados por la alteración, modificación, daño o destrucción de la naturaleza, y/o desastres naturales, así como acontecimientos ajenos al control del Instituto, los relacionados a fallas en servicios críticos suministrados por terceros, atentados delictivos, contingencias legales, entre otros.

E. FUNCIONES Y RESPONSABILIDADES

1. Unidad de Desarrollo Organizacional

La Unidad de Desarrollo Organizacional, es una unidad independiente a todas las unidades del IPSFA, responsable de coordinar con las diferentes unidades el proceso de identificar, Analizar, Evaluar, Tratar, Revisar, y/o Monitorear y Comunicar todos los riesgos que enfrenta el Instituto. Esta Unidad es la generadora de insumos para el Comité de Riesgos y tiene a su cargo implementar las distintas etapas del proceso de gestión de riesgo.

En cumplimiento a las normas NPB4-47 "Normas para la Gestión Integral de Riesgos para las entidades financieras" las funciones de la Unidad de Desarrollo Organizacional son:

a. Coordinar el proceso de Gestión Integral del Riesgo (GIR) en todas sus etapas;
b. Diseñar y proponer a Comité de Riesgos para su aprobación las estrategias, políticas, procedimientos y los manuales respectivos para la gestión integral de riesgos y de cada uno de los riesgos específicos identificados, así como sus modificaciones;
c. Proponer para su aprobación las metodologías, modelos y parámetros para la gestión integral de los distintos tipos de riesgos a que se encuentra expuesto el IPSFA.
d. Informar periódicamente de acuerdo al proceso de (GIR) establecido y autorizado, al Comité de Riesgos sobre la evolución de los distintos tipos de riesgos a que se encuentra expuesta la Institución;
e. Dar seguimiento periódico a las acciones correctivas para la mejora en la gestión de riesgos, los cuales deberá hacer del conocimiento al Comité de Riesgos y Consejo Directivo, según sea el caso;
f. Elaborar y proponer al Comité de Riesgos planes de contingencia para gestionar cada uno de los riesgos en forma particular en situaciones adversas.
g. Reportar oportunamente de forma completa y detallada las fallas en los diferentes procesos operativos que desarrolla la institución, al Consejo Directivo a través del Comité de Riesgos.

2. Comité de Riesgos

En virtud del art. 7 de la norma NPB4-50, el Comité de Riesgos es el encargado de velar por una sana gestión del riesgo de la institución.

Funciones del Comité de Riesgos son:

a. Vigilar que las operaciones se realicen ajustándose a los objetivos, políticas y procedimientos para la administración integral de riesgos.
b. Supervisar que la gestión del riesgo operacional sea efectiva y que los eventos de riesgos sean consistentemente identificados, evaluados, mitigados y monitoreados, y comunicados.
c. Proponer los mecanismos para la implementación de las acciones correctivas requeridas en caso de que existan desviaciones con respecto al nivel de tolerancia al riesgo operacional.
d. Aprobar la normativa de gestión de cada uno de los riesgos.
e. Apoyar la labor de la Unidad de Desarrollo Organizacional (UDO) en la implementación de la gestión de riesgo.
f. Aprobar las actividades a desarrollar por la (UDO).
g. Velar por que la entidad cuente con la adecuada estructura organizacional, estrategias, políticas y recursos para la gestión integral de riesgos.
h. Asegurar e informar al Consejo Directivo la correcta ejecución de las estrategias y políticas aprobadas.
i. Requerir y dar seguimiento a los planes correctivos para normalizar incumplimientos a los límites de exposición o deficiencias reportadas.

3. Unidades y Gerencias del IPSFA

Es responsabilidad de todo el personal del IPSFA:

a. Identificar y evaluar los riesgos en cada una de las áreas y determinar las causas y efectos derivados de los riesgos identificados.
b. Identificar y Reportar a la Unidad de Desarrollo Organizacional los riesgos institucionales a los que se encuentra expuestos con base a los formatos previamente establecidos.

c. Proporcionar información relacionada con eventos de riesgo
d. Gestionar las acciones de monitoreo y control aprobados por el Comité de Riesgos y el Honorable Consejo Directivo, y que son de su responsabilidad.

F. EVENTOS DE RIESGO OPERACIONAL

Los eventos de riesgo operacional son situaciones que ocurren durante un intervalo de tiempo determinado y que afectan el normal desarrollo de las operaciones del instituto, los cuales incluyen los incidentes ocurridos y eventos potenciales que pudieren generar pérdidas económicas que pueden o no afectar el estado de resultados, siendo estos los siguientes:

1. Fraude interno;
2. Fraude externo;
3. Relaciones laborales y seguridad en el puesto de trabajo;
4. Clientes, productos y prácticas de negocio;
5. Daños en activos materiales;
6. Interrupción del negocio y fallas en los sistemas, y
7. Ejecución, entrega y gestión de procesos.

G. ALCANCE

Los principios descritos en este manual son aplicables a todas las áreas y procesos de la Institución.

II. MARCO REGULATORIO

A. NORMAS GENERALES

1. El área encargado de la Gestión de Riesgos, tendrá dentro de sus obligaciones las siguientes:
   a) Proponer ante el Comité de Riesgos para su autorización y posterior aprobación por el Consejo Directivo, las metodologías y políticas para la gestión del riesgo operacional.
   b) Identificar los principales riesgos operacionales, así como proponer al Comité de Riesgos las acciones de control a los mismos.
   c) Asegurar que se establezcan y se revisen los procedimientos y mecanismos mínimos para la gestión del riesgo operacional.
   d) Vigilar el cumplimiento de las políticas, procedimientos y acciones establecidas para la administración del riesgo operacional.
2. El área encargada de la gestión de riesgos institucional, será la responsable de supervisar el cumplimiento de la normativa emitida por la Superintendencia del Sistema Financiero y que sea aplicable a los riesgos operativos de IPSFA.
3. El área encargada de la gestión de riesgos institucional, será la responsable de vigilar que los sistemas informáticos se encuentren adecuados y cumplan con los requerimientos establecidos por la Superintendencia del Sistema Financiero, en relación a la gestión de riesgos operacional.

B. NORMAS ESPECÍFICAS

1.1 **Para la gestión del Riesgo Operacional**

1.2 El área encargada de la Gestión de Riesgos, será la responsable de: Impulsar a nivel institucional la cultura de prevención de riesgo operacional, a través del desarrollo de adiestramientos al personal.

1.3 Realizará el proceso de identificación de los riesgos operacionales por lo menos una vez al año, estableciendo las acciones de control para el tratamiento adecuado de los riesgos asumidos, así mismo, deberá informar los resultados al Comité de Riesgos para su autorización.

1.4 Coordinar el proceso de identificación y medición de los riesgos operacionales; involucrando a todo el personal que considere clave en dicho proceso.

1.5 Presentar al Comité de Riesgos el informe de seguimiento a los riesgos operacionales asumidos por el Instituto, con el fin de identificar las necesidades de mejora en la gestión de riesgo operacional, lo anterior de acuerdo al proceso de Gestión Integral del Riesgo autorizado.

1.6 Ejecutar el seguimiento a los riesgos operacionales, como mínimo dos veces al año, y elaborará un informe sobre la evolución de los mismos, el cual deberá presentar al Comité de Riesgos.

1. Para la elaboración y remisión de la Base de Datos e Informe Anual

2.1 El área encargada de la gestión de riesgos, deberá asegurar la conformación de una base de datos centralizada que permita registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operacional, dicha base deberá contener como mínimo los campos que se detallan en el formulario "Base de Datos" FORM-12-GG-CR-01 (*Formulario No. 1*)

2.2 El área encargada de la gestión de riesgos, será la responsable de clasificar los eventos de riesgo operacional por factores, determinando la frecuencia del evento y el efecto producido, en base a la tabla "Tipos de Eventos por Riesgo Operacional" (Anexo No. 1).

2.3 El área encargada de la gestión de riesgos, será la responsable de remitir a la Superintendencia del Sistema Financiero (SSF) la Base de Datos conteniendo la información sobre los eventos de riesgo operacional, en medios electrónicos, a más tardar el treinta y uno de enero de cada año.

2.4 El área encargada de la gestión de riesgos, deberá remitir a la SSF durante los primeros 30 días calendario siguientes al cierre de cada ejercicio anual, el informe relativo a las acciones realizadas para el control y la evaluación del riesgo operacional, dicho informe deberá contener como mínimo lo siguiente:

a) La definición de la estrategia utilizada para la gestión del riesgo operacional;

b) El detalle de la metodología empleada para la gestión del riesgo operacional;

c) Identificación y evaluación de los riesgos operacionales de eventos críticos ocurridos durante el año, por proceso y/o unidad de negocio y de apoyo; y el detalle de las medidas adoptadas para administrarlos;

d) Detalle de los ejecutivos responsables de las actividades de control de riesgo de los eventos críticos ocurridos durante el año; y

e) Plan de Actividades a desarrollar por la UDO, relacionado con la gestión del riesgo operacional.

2.5 El área encargada de la gestión de riesgos, será la responsable de remitir en forma electrónica a la SSF, el Manual para la Gestión de Riesgo Operacional; así como, las distintas modificaciones que se le realicen a la misma.

III. MODELO DE RIESGO OPERACIONAL

Este modelo permite identificar los riesgos en las áreas organizativas, generar análisis en los que se priorizan los riesgos de acuerdo con su riesgo residual estimado (después de incorporar el efecto de los controles), vincular los riesgos a los procesos y establecer para cada riesgo un nivel objetivo que, por comparación con el riesgo residual, identifica brechas para su gestión.

A. Modelo de 3 Líneas de Defensa

1. **Primera línea:** gestión del (RO) en las Áreas de Negocio y de soporte (en adelante las Áreas), en sus actividades, procesos y sistemas. Las Áreas integran la gestión del (RO) en su día a día, colaboran en la identificación y evaluación de riesgos, establecen el riesgo objetivo, llevan a cabo los controles y ejecutan los planes de mitigación de aquellos riesgos con nivel de riesgo residual superior al aceptable.

En todos los ámbitos de gestión del (RO), son los Gestores de Riesgo Operacional (GRO), quienes aseguran la adecuada gestión del riesgo operacional en sus respectivos ámbitos, impulsando la identificación del riesgo objetivo, el aseguramiento de la implantación de los planes de mitigación y la adecuada ejecución de los controles. La gestión del (RO) en las unidades, se expone, y se sigue en el Comité de Riesgo.

Rol: "Propietarios" de los riesgos y su gestión.

a) Entrega un enfoque coordinado para diseñar, estructurar e implementar la gestión de riesgos en las áreas operativas.
b) Contribuye en la definición de roles y tareas específicas en el proceso y cómo estas podrían ser asignadas y coordinadas en las áreas operativas.
c) Contribuye a la implementación de acciones correctivas del proceso y de los controles.

2. **Segunda línea:** Se ocupan de diseñar y mantener el modelo de RO del IPSFA, y de verificar su correcta aplicación en el ámbito de las distintas Áreas.

Rol: Supervisión o monitoreo de los riesgos.

a) Aporta un enfoque coordinado, así como métodos que ayudan a monitorear el cumplimiento de la gestión de riesgos en la Institución
b) Ayuda a retroalimentar y mejorar la efectividad de los sistemas de gestión de riesgos en la Institución.
c) Contribuye a evitar duplicaciones de trabajo con otras funciones de control.
d) Ayudar a las Áreas a cumplir con su responsabilidad.

3. Tercera línea: Desempeñada por Auditoría Interna:

Proporciona información independiente sobre el ambiente de control al Comité de Riesgo Institucional.

Rol: Aseguramiento Independiente de la Gestión de Riesgos.

a) Informar de su resultado a la Institución y Consejo Directivo.
b) Aporta una serie de métodos de evaluación que pueden ser adoptados (adaptados) en el trabajo de campo de aseguramiento a la gestión de riesgos
c) Contribuye a evitar duplicaciones del trabajo de los auditores internos con las funciones de control y monitoreo.

La gestión del riesgo operacional en el IPSFA debe:

a) Establecer procedimientos que permitan reevaluar periódicamente los riesgos operacionales relevantes a los que el IPSFA, está expuesto para adoptar las medidas de mitigación convenientes en cada caso, una vez considerado el riesgo identificado y el coste de la mitigación (análisis coste/beneficio).

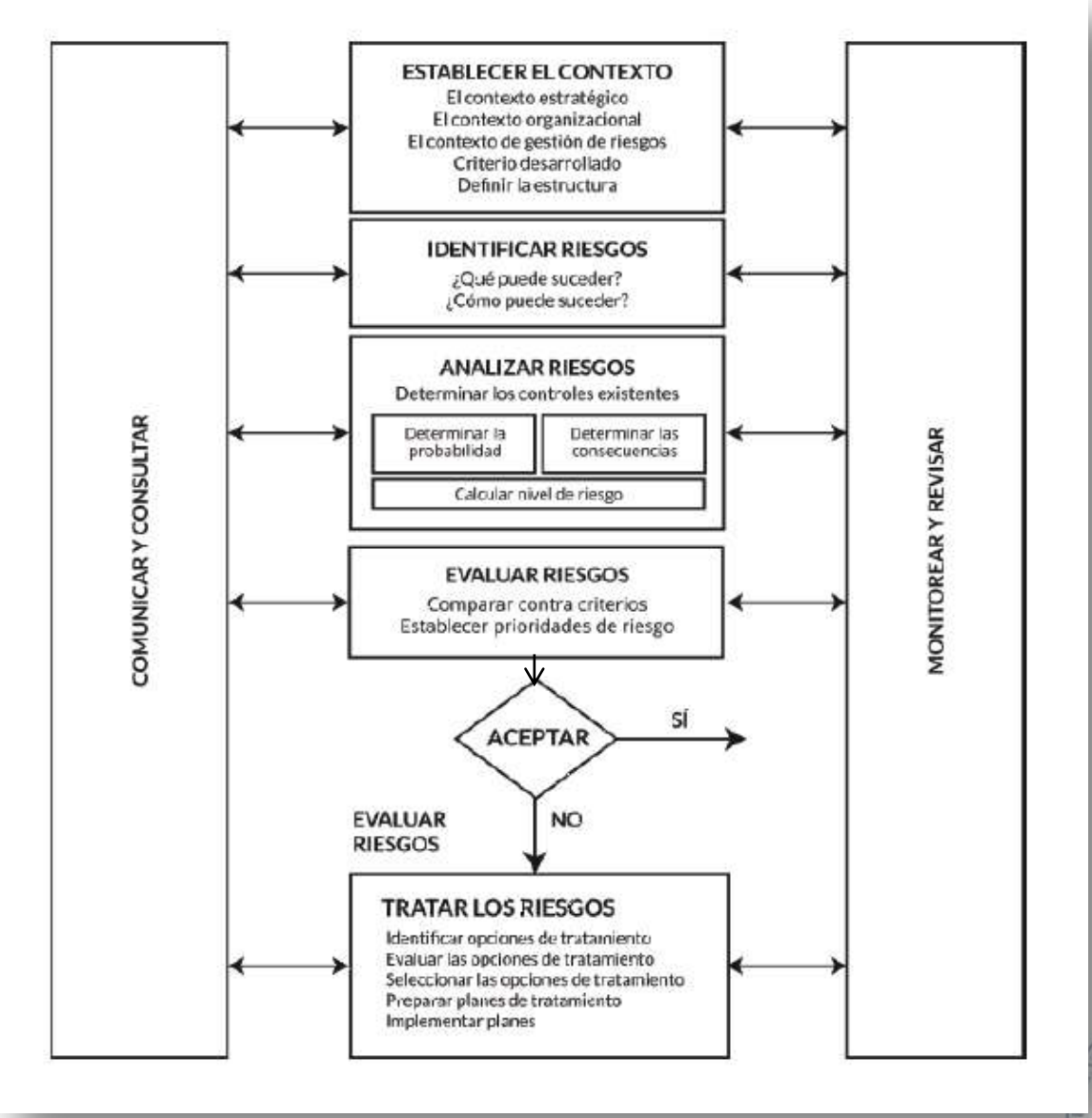
b) Identificar las causas de las pérdidas operacionales que sufra el IPSFA y establecer las medidas que permitan su reducción. Para ello deberán existir procedimientos que permitan la captura y el análisis de los eventos operacionales que ocasionan las citadas pérdidas.

c) Contar con una autoridad para dirigir, informar, supervisar y administrar los recursos con el fin de alcanzar los objetivos de la Institución en forma efectiva, en la que las funciones y responsabilidades de las Áreas que intervienen en la gestión del RO estén claramente definidas.

IV. PROCESO DE LA GESTIÓN DEL RIESGO OPERACIONAL

La administración del riesgo debe ser relevante con el contexto estratégico de la organización, sus metas, objetivos y naturaleza. La alta gerencia deberá asegurar que su política es entendida, implementada y mantenida por todos los niveles de la organización.

El Sistema de Gestión de Riesgos que implemente IPSFA debe comprender las siguientes etapas:



A. ESTABLECER EL CONTEXTO

En esta primera etapa se definen los objetivos del proceso. Es decir, se deja claro qué es lo que se busca con la implementación del Sistema de Gestión de Riesgos y cuál debe ser el alcance del mismo.

El Comité de Riesgos debe ser la instancia con más alto grado de implicación en la difusión de estos objetivos, pues de lo contrario no logrará que el resto de Áreas del IPSFA, se comprometan del modo deseado. Pero no sólo se apoya en una buena difusión. También es preciso definir un presupuesto y destinar los recursos necesarios para la materialización del plan de riesgos.

1. **Contexto Externo**

   Consiste en entender la relación que existe entre la Institución y el entorno externo en el que opera. Este contexto externo incluye factores como políticos, legales, regulatorios, financieros, tecnológicos, culturales y aquellos agentes que tienen fuerte influencia en la opinión y decisión.

2. **Contexto Interno**

   Consiste en entender los factores que influyen al interior de la organización, entre los cuales se resaltan las fortalezas y debilidades, el plan estratégico, la estructura y cultura organizacional, los procesos, la información y tecnología.

B. IDENTIFICAR RIESGOS

Esta fase consiste en reconocer y caracterizar los riesgos tanto internos como externos que pueden generar amenazas de pérdidas e impedir el logro de los objetivos del Instituto y de los procesos durante la ejecución de las actividades operativas, comprendiendo la naturaleza del riesgo a fin de determinar el nivel de riesgo.

El desarrollo de esta etapa es responsabilidad del Enlace de Riesgos de cada Área del IPSFA, en coordinación con la Unidad de Desarrollo Organizacional.

Para dar lugar a la identificación y recolección de los riesgos en cada uno de los procesos de la Institución, la Unidad de Desarrollo Organizacional realiza reuniones de acompañamiento con los Enlace de Riesgos y personal experto de cada una de las áreas.

En estas reuniones se busca por medio de diferentes herramientas (Juicio basado en la experiencia y registros, diagramas de flujos, lluvia de ideas, análisis de escenario y Listas de chequeo), listar y priorizar las debilidades y amenazas para cada una de las fuentes o factores que puedan impactar los objetivos estratégicos, los procesos e iniciativas; realizando un especial énfasis en las causas que lo podrían generar con sus respectivas consecuencias. Adicionalmente el listado de los riesgos deberá considerar las categorías que describen la forma en que se pudiese presentar.

C. ANALIZAR RIESGOS

Es la fase es para comprender la naturaleza del riesgo, para determinar el nivel de dicho riesgo.

1. **Factores de Riesgos:** Los factores de riesgo son las fuentes generadoras de eventos en las que se originan las pérdidas en los procesos y afectan la consecución de los objetivos estratégicos del negocio.
2. **Relaciones Comerciales:** Corresponde a la fuente de riesgo que existe en las relaciones con otras entidades tales como proveedores, arrendatarios, contratistas, afiliados, clientes, etc.
3. **Comportamiento humano:** Corresponde a aspectos tales como error humano, sabotaje, fraude, lavado de activos, extralimitación de atribuciones, negligencia, desconocimiento, etc.
4. **Administración de la Información:** Corresponde a aspectos relacionados con los criterios de Información, confidencialidad, Integridad y disponibilidad.
5. **Eventos Naturales:** Corresponden a sucesos producidos por la fuerza de la naturaleza tales como terremotos, inundaciones, etc.

6. **Circunstancias Externas:** corresponde a cambios ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la Institución, incluyendo legislación u otros factores sociales que pueden generar otras fuentes de riesgo, diferentes a las enumeradas.
7. **Asuntos técnicos y de tecnología:** Fallas tecnológicas que incluyen debilidades que comprometen la seguridad, disponibilidad, calidad, capacidad y desempeño de la infraestructura tecnológica y sistemas informáticos que soportan la institución.
8. **Procesos: Corresponde** a aspectos relacionados con debilidades en los procesos, incluyendo el monitoreo de las actividades y procedimientos de control establecidos.
9. **Infraestructura: Corresponde** al conjunto de elementos de apoyo para el funcionamiento de la Institución, tales como edificios, espacios de trabajo, entre otros, etc.
10. **Categorías de Riesgo:** Hechos o acciones que describen la manera como se materializa el riesgo y afecta negativamente el logro de los objetivos del IPSFA.
    a) **Fraude interno:** Riesgos derivados de algún tipo de actuación encaminada a defraudar, apropiarse de activos indebidamente o a incumplir las regulaciones, leyes o políticas Institucionales en las que se encuentre implicado al menos un colaborador o directivo del IPSFA.
    b) **Fraude externo:** Riesgos derivados de algún tipo de actuación encaminada a defraudar, apropiarse de activos indebidamente o a incumplir la legislación, por parte de un tercero. Esta categoría incluye eventos como: robos, falsificación, ataques informáticos, suplantación, entre otros, etc.
    c) Relaciones laborales: Riesgos derivados de actuaciones incompatibles con la legislación o acuerdos laborales, de higiene o seguridad en el trabajo, por daños a empleados.
    d) **Practicas con clientes,** afiliados, negocios: Riesgos derivados de actuaciones que conllevan al incumplimiento involuntario negligente de una obligación profesional frente a proveedores, clientes o afiliados.

e) **Daños a activos materiales:** Riesgos derivados de actuaciones que conllevan daños o perjuicios a activos materiales; incluyendo desastres naturales, terrorismo, vandalismo, etc.

f) **Interrupción y fallas en los sistemas:** Riesgos derivados de interrupciones de fallas tecnológicas.

g) **Ejecución, entrega y gestión de procesos:** Riesgos derivados de errores en el procesamiento de operaciones o en la gestión de procesos.

D. EVALUAR RIESGOS

Concluida la etapa de identificación, se procede a evaluar los riesgos con el fin de determinar la probabilidad de su ocurrencia frente a cada uno de los factores de riesgo y el impacto que este podría generar en caso de materializarse. La evaluación podrá realizarse en términos cualitativos o cuantitativos según la disponibilidad de información que posea el proceso.

El propósito de la evaluación del riesgo es la comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

Propósito de la evaluación del riesgo:

a) Ayudar en la toma de decisiones, basada en el análisis de riesgos.

b) Toma en cuenta los riesgos que necesitan tratamiento y la prioridad para la aplicación del tratamiento.

La calificación semicuantitativa se realiza con base en la definición de la probabilidad y el impacto que puede llegar a tener o ha tenido el riesgo operativo estudiado, posteriormente se ubica la combinación obtenida (Probabilidad – Ocurrencia) en la Matriz de Riesgos definida para la Institución y de ésta forma se define la calificación para el riesgo respectivo.

1. CRITERIOS DE MEDICIÓN DE RIESGOS

Las probabilidades y los impactos se combinan para determinar el nivel de severidad del riesgo del proceso e iniciativa a evaluar, con el fin de definir los planes de acción que buscarán su mitigación.

Para llevar a cabo la medición de los riesgos, se partirá de un análisis basado en los criterios propuestos por la Unidad de Desarrollo Organizacional y aprobados, Comité de Riesgos y Consejo Directivo respectivamente, con la finalidad de realizar la valoración de la probabilidad de ocurrencia y del impacto de cada riesgo

a) Para la valoración de la (PO) se tendrá en cuenta la observación de los eventos ocurridos y registrados en la base de eventos del año en curso, como también se hará uso de información referente entendida como aquellos eventos de naturaleza similar tanto internos como externos, que se pueden materializar en el proceso y se valoran de acuerdo con el juicio del experto.

b) En los casos que el proceso no posea datos históricos o referentes asociados, la probabilidad de ocurrencia se realizará evaluando criterios asociados a variabilidad, periodicidad de ejecución de la actividad y madurez del proceso.

1.1 **PROBABILIDAD:** Se refiere a la probabilidad de ocurrencia de un evento de riesgo en el desarrollo de sus actividades. Es una función creciente, ya que una probabilidad “Baja” tiene asociada una baja ocurrencia de eventos, mientras que una probabilidad “Alta”, tiene asociada una alta ocurrencia de eventos.

Para determinar el factor de probabilidad de ocurrencia se tendrá en cuenta la siguiente tabla:

Escala de medición para Probabilidad de Ocurrencia

Nivel	Descriptor	Drescripción
1	Remoto	Puede ocurrir sólo en circunstancias excepcionales, y puede presentarse una vez entre 4 y 10 años.
2	Poco probable	Es difícil que ocurra, y puede presentarse una vez entre 2 y 4 años.
3	Posible	Podrá ocurrir algún momento, y puede presentarse una vez entre 1 y 2 años.
4	Probable	Probablemente ocurrirá en la mayoría de las circunstancias, y puede presentarse una vez entre 7 y 12 meses.
5	Casi cierto	Se espera que ocurra en la mayoría de las circunstancias, y puede presentarse una vez entre 1 y 6 meses.

Tabla No. 1

1.2 **IMPACTO:** El impacto es definido para cuantificar las consecuencias resultantes de la ocurrencia de algún evento de riesgo. Es una función continúa, a fin de facilitar el ejercicio de calificación, se clasifica dentro del espacio definido por la Institución, el cual es de cinco (5) categorías.

Escala de medición para Impacto

Nivel	Descriptor	Drescripción
1	No significativo	No genera perjuicios y puede ser asumido por el giro normal de las operaciones ya que no afecta la prestación del servicio, viabilidad institucional o la relación con el cliente. Las pérdidas financieras son pequeñas, menores de $4,999.99 dólares.
2	Menor	Pocos perjuicios que se controlan local e inmediatamente y puede ser asumido por el giro normal de las operaciones ya que no afecta la prestación del servicio, viabilidad institucional o la relación con el cliente. Las pérdidas financieras son medias, entre $5,000.00 y $24,999.99 dólares.
3	Moderado	Se puede ver afectada la eficiencia, disminuyendo la calidad del servicio, generando insatisfacción en el cliente y retrasos en la operación. Las pérdidas financieras son altas, entre $25,000.00 y $49,999.99 dólares.
4	Significativo	Perjuicios extensivos que generan pérdida en la capacidad de producción, generan riesgos asociados importantes y se generan pérdidas financieras importantes, entre $50,000.00 y $99,999.99 dólares.
5	Catastrófico	Se afectan los estándares de los indicadores, se genera incumplimiento regulatorio, se puede poner en riesgo la prestación del servicio, viabilidad del Instituto y se afecta la relación con el cliente. Las pérdidas financieras son enormes, mayores a $100,000.00 dólares.

Tabla No. 2

1.3 **RIESGO INHERENTE:** En esta actividad se califican cada uno de los riesgos operativos identificados, sin tener en cuenta los controles asociados a cada uno de éstos. La medición se realiza de forma semicuantitativa, basándose en el conocimiento que cada uno de los Áreas Organizativas del IPSFA, del cual es responsable.

La multiplicación de la probabilidad por la consecuencia/impacto, da como resultado el riesgo inherente. El resultado de esta primera calificación, sin el efecto de los controles debe quedar reflejado en el mapa colorimétrico de riesgo, el cual se denomina mapa de riesgo, en él se determina cuáles son las zonas de crítico, alto, medio, bajo y muy bajo riesgo, así:

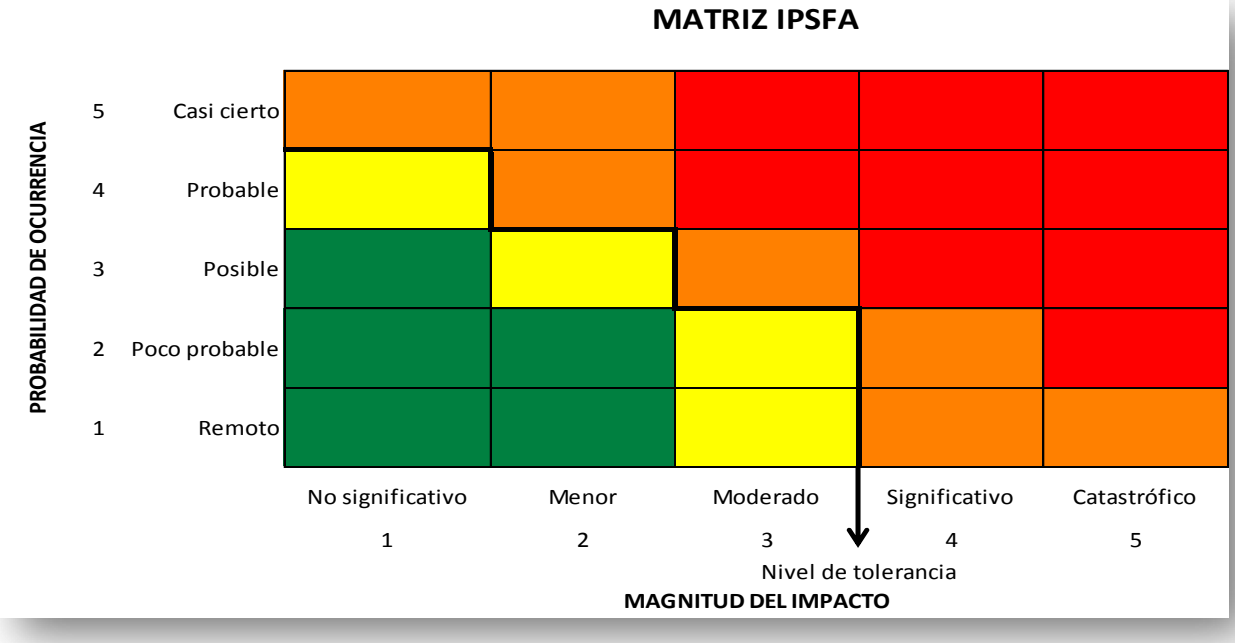


Tabla No. 3

1.4 **NIVEL DE TOLERANCIA:** Es la desviación respecto al nivel de apetito del Riesgo; se relaciona con la cantidad de riesgo institucional, como la volatilidad, o los altibajos que el Instituto puede tolerar.

El Instituto por medio del Comité de Riesgos ha establecido el nivel de tolerancia al riesgo de acuerdo a la Matriz Térmica IPSFA, (Ver Tabla No. 3)

E. TRATAR LOS RIESGOS

Entre las distintas formas de tratar un Riesgo Operativo, el IPSFA. ha, evaluando sus posibilidades por lo cual ha decidido tener en cuenta las siguientes posibilidades:

1. **Evitar el riesgo:** NO proceder con la actividad generadora del riesgo. Este tratamiento se efectuará solo en casos en los que la Institución establezca que el Impacto y Probabilidad sobrepasan los niveles aceptables, y además, en los que ni siquiera la transferencia a un ente externo garantice la seguridad de desarrollar la actividad.
2. **Reducir la Probabilidad de Ocurrencia:** Para actividades en las cuales la Probabilidad sea alta, la Institución establecerá controles inmediatos. Este tratamiento constará de un estudio sobre posibles controles, su aplicabilidad, y además pruebas de su funcionamiento.
3. **Reducir el Impacto:** Este tratamiento, requiere de un estudio exhaustivo del Comité de Riesgo, en el cual se evaluarán las capacidades de la Institución, para disminuir el Impacto que un evento de Riesgo Operativo genere.
4. **Transferir el Riesgo:** Aquellos casos en los que la Institución, después de un estudio minucioso, establezca que el evento no es tratable con medidas internas, por lo cual requerirá de ayuda parcial o total de terceros.
5. **Mitigación del riesgo:** Es una estrategia de gestión de riesgos que consiste en reducir la probabilidad o el impacto de un riesgo sobre la organización. Es decir, que si llega a producirse, sus efectos serán mucho menores que si no se hubiesen adoptado medidas al respecto. Esta opción se usa sobre todo en aquellos casos en que los riesgos son inevitables o no dependen de la organización en sí misma. La clave para una acertada mitigación del riesgo está en las acciones. Algunos ejemplos son:
    a) Adopción de procesos más sencillos en la organización.
    b) Puesta en marcha de ensayos adicionales.
    c) Elección de proveedores o suministrador más fiables.

d) Adición de recursos para la labor preventiva. Para el tratamiento de los Riesgos es necesario tener en cuenta los siguientes aspectos.

6. Responsabilidad y autoridad

Se debe definir y documentar la responsabilidad, autoridad y la interrelación del personal que desempeña y verifica el trabajo de la administración del riesgo operativo, particularmente para las personas que necesitan la autoridad y libertad organizacional para hacer una o más de las siguientes actividades:

a) Iniciar la acción para prevenir o reducir los efectos adversos de los riesgos operativos.
b) Adicionar control al tratamiento de riesgos operativos hasta que el nivel del mismo se vuelva aceptable.
c) Identificar y registrar cualquier problema relacionado con la administración de riesgos operativos.
d) Iniciar, recomendar o proveer soluciones a través de los canales diseñados.
e) Verificar la implementación de soluciones.
f) Divulgar mejoras al interior de la Institución.

7. Recursos

La Institución debe identificar los requerimientos y proveer los recursos adecuados, incluyendo la asignación de personal capacitado para la administración, desarrollo del trabajo y verificación de actividades que incluyan revisiones internas.

8. Revisión del manejo

El Comité de Riesgos de la Institución debe asegurar que se lleve a cabo, una revisión del sistema de administración del riesgo operativo para asegurar su efectividad en cumplir las políticas y objetivos de la administración del riesgo operativo establecidos en el IPSFA. Se deben mantener registros de estas revisiones.

F. COMUNICACIÓN Y CONSULTA

La comunicación y la consulta con las partes involucradas externas e internas deberían tener lugar durante todas las etapas del proceso para la gestión del riesgo. Por lo tanto, se deberían desarrollar tempranamente los planes para la comunicación y la consulta.

Éstos deberían abordar aspectos relacionados con el propio riesgo, sus causas, sus consecuencias (si se conocen), y las medidas que se toman para tratarlo. Es conveniente que tengan lugar la comunicación y las consultas externas e internas eficaces para garantizar que aquellos responsables de la implementación del proceso para la gestión del riesgo y las partes involucradas entiendan las bases sobre las cuales se toman las decisiones, y las razones por las cuales se requieren acciones particulares.

Un enfoque de equipo consultor puede:

a) Ayudar a establecer correctamente el contexto;
b) Garantizar que se entienden y se toman en consideración los intereses de las partes involucradas;
c) Ayudar a garantizar que los riesgos estén correctamente identificados;
d) Reunir diferentes áreas de experticia para analizar los riesgos,
e) Garantizar que los diversos puntos de vista se toman en consideración adecuadamente al definir los criterios del riesgo y al evaluar los riesgos;
f) Asegurar la aprobación y el soporte para el plan de tratamiento;
g) Fomentar la gestión adecuada del cambio durante el proceso para la gestión del riesgo; y
h) Desarrollar un plan adecuado de comunicación y consulta externo e interno

La comunicación y la consulta con las partes involucradas son importantes dado que ellas dan sus opiniones acerca del riesgo con base en sus percepciones de éste. Estas percepciones pueden variar debido a las diferencias en los valores, las necesidades, los conceptos y los intereses de las partes involucradas. Dado que sus puntos de vista pueden tener un impacto significativo en las decisiones que se toman, las percepciones de las partes involucradas se deberían identificar, registrar y tomar en consideración en el proceso de toma de decisiones.

La comunicación y la consulta deberían facilitar los intercambios de información veraz, pertinente, precisa y fácil de entender, teniendo en cuenta los aspectos de la integridad personal y confidencial.

V. REGISTRO DE EVENTOS DE PERDIDA POR RIESGO OPERACIONAL

A. EVENTO DE RIESGO OPERACIONAL:

1. Es un incidente que se presenta en un proceso y cuya consecuencia es que el resultado final del mismo difiere de lo que se había planeado.

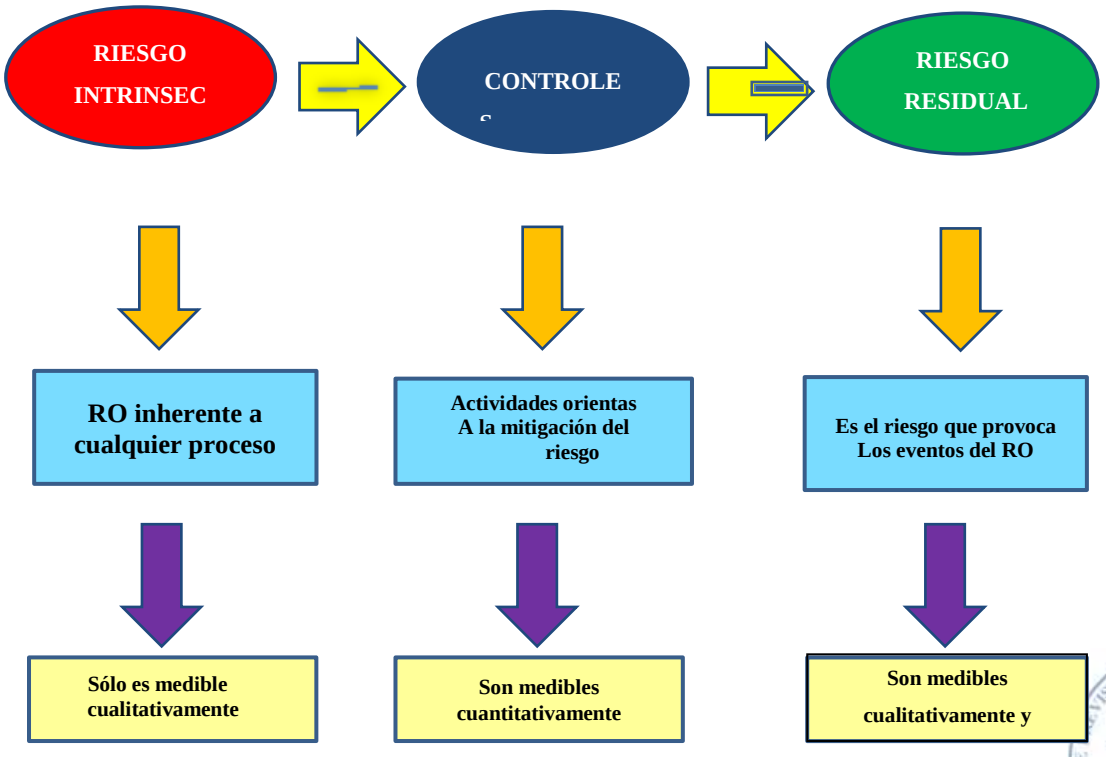
2. Es debido a una falta de adecuación o de un fallo de los procesos, el personal y los sistemas internos o bien por acontecimientos externos.

3. Secuencia de los Acontecimientos

4. Eventos Típicos de Riesgo Operacional

   a) Errores operativos
   b) Fraudes (interno & externo)
   c) Actividad no autorizada
   d) Fugas de talento
   e) Incumplimiento normativo
   f) Caída de sistemas
   g) Fallos de programación
   h) Sobrepasar atribuciones/límites
   i) Accesos indebidos a sistemas
   j) Daños en edificios
   k) Incumplimiento de proveedores
   l) Pérdidas por litigios

5. ¿Qué riesgo provoca eventos de RO?



6. Causas que producen eventos de RO

FACTORES INTERNOS	RRHH	↓ Falta de recursos ↓ Escasa formación ↓ Alta rotación ↓ Outsourcing ↓ Pérdidas de talento	↓ Desastres ↓ Fraudes
	GESTION PROCESOS	↓ Controles deficientes ↓ Defectos en los sistemas ↓ Falta de segregación funcional ↓ Escasa seguridad informática ↓ Falta de planes de contingencia ↓ Exceso de manualidad	

7. No forman parte del Riesgo

Riesgo asociado a la insolvencia de las contrapartidas (clientes) a las que la entidad ha prestado, garantizado. o vendido productos.
Riesgo de pérdidas debido a los movimientos de precios en los mercados (tasas de interés, tipos de cambio, precios de las acciones en bolsa, etc…) en las posiciones que la entidad tiene abiertas
Riesgo asociado a falta de liquidez que impida a la entidad atender sus necesidades de caja para hacer frente a sus obligaciones de pago
Riesgo de inversión o desinversión en negocios o productos, debido al entorno económico, decisiones erróneas o inadaptación a los cambios
Riesgo asociado a la marcha del negocio por caídas en la actividad, en las ventas o estrechamiento de márgenes, sin capacidad de reacción para contrarrestarlo
Riesgo asociado a la implantación de proyectos porque éstos no cumplan con las expectativas o porque se sobrepasen los presupuestos
Es consecuencia de los demás riesgos. Es el riesgo asociado a un cambio en la percepción de los "stakeholders" (grupos de interés) con respecto a la Entidad, perjudicando su imagen y por consiguiente afectando a su capacidad de generar negocio

8. Dependen del número de Impactos

Eventos Simples	Un evento simple es aquél que genera un solo impacto en la contabilidad. Ejemplo: Una multa por incumplimiento normativo
Eventos Múltiples	Un evento múltiple es aquél que genera varios impactos en la contabilidad. Ejemplo: Un fraude de tarjetas de crédito que afecta a muchos clientes
Eventos Monolínea	Un evento monolínea es aquél que afecta a una sola línea de negocio. Ejemplo: Una multa por incumplimiento normativo
Eventos Multilínea	Un evento multilínea es aquél que afecta a varias líneas de negocio. Ejemplo: Un desastre en un edificio en el que están ubicadas dos líneas de negocio.

9. Cuantificación

a) Se realiza consolidando en un solo importe el impacto económico de los diversos tipos de pérdidas, aunque se encuentren registradas en cuentas diferentes.

b) Cada evento informado integra todos los componentes de la pérdida independientemente de la cuenta donde estén registrados La valoración se basa en la información contenida en los registros contables.

c) Incluirá costes de oportunidad (intereses y gastos financieros), pero no el lucro cesante derivado de eventuales pérdidas de negocio.

d) Cuando interviene alguna variable de mercado, (tipo de cambio, de interés, precio de activos financieros, etc.) la pérdida se calcula aplicando los precios existentes en el momento de la identificación del evento (momento en el que la operación deba ser anulada o regularizada).

e) Todos los eventos se reportan en moneda local, independientemente de la divisa en que se haya registrado el evento, al tipo de cambio existente en la fecha de registro contable.

B. METODOLOGÍA PARA EL REGISTRO DE EVENTOS DE RIESGO OPERATIVO

1. Inicio

Jefe / Enlace de Riesgos del Área:

2. Identifica evento de pérdida. al momento de ocurrir un evento,
3. Informa evento de pérdida a la Unidad de Desarrollo Organizacional (UDO).

Técnico de Riesgos:

4. Remite formulario de base de eventos de pérdida por Riesgo Operacional al Enlace de Riesgos del Área. (Formulario No. 1)

Jefe / Enlace de Riesgos del Área:

5. Registran datos en formulario según lo requerido. (Formulario No. 1)
6. Remite vía correo electrónico formulario completado con toda la información de respaldo.

Técnico de Riesgos:

7. Recibe formulario vía correo electrónica con la información requerida. (Formulario No. 1)
8. Ingresa datos en base de eventos de pérdida por Riesgo Operacional Institucional.
9. Informa evento de pérdida a Jefe UDO.
10. Evalúa nivel de riesgo, por tipo de criticidad.
11. ¿Es Riesgo Operativo crítico? Si, ir a paso: 12; No, ir a paso: 14.
12. Informa a Jefe UDO criticidad del Riesgo Operacional

Jefe de la Unidad de Desarrollo Organizacional:

13. Coordina reunión de Comité de Riesgo e informa a dicho Comité.

Técnico de Riesgos:

14. Incluye en informe trimestral.

15. Fin de la Metodología

UNIDAD DE DESARROLLO ORGANIZACIONAL

Formulario No. 1

INSTITUTO DE PREVISION SOCIAL DE LA FUERZA ARMADA	**BASE DE DATOS (Requerimiento SSF)**

ID	Factor de Riesgo	Tipo de evento 1	Tipo de evento 2	Descripción del evento	Fecha inicio	Fecha Fin	Fecha detección	Fecha de registro	Monto	Divisa	Cuenta contable	Proceso	Valor recuperado	Valor recuperado por Seguros	Producto/servicio afectado	Cuantificación de la severidad del daño.

DESCRIPCIÓN DE LLENADO DE BASE DE DATOS DE EVENTOS DE RIESGO OPERATIVO

El objetivo principal de la Matriz de Eventos de Riesgo Operativo es detallar e identificar los eventos pasados que afectaron a la Institución.

1. **Dependencia:** En la parte superior, se señalará el nombre de la Dependencia, responsable de la Base de Datos de Eventos de Riesgo Operativo.
2. **ID:** Código interno que identifique el evento en forma secuencial, inicia con las iniciales ER (Evento de Riesgo), luego con el código del Centro de Costo (Ej. ER51), y al final un numero correlativo (Ej. ER51 001).
3. **Factor de Riesgo:** Es la posibilidad de que ocurran pérdidas como consecuencia de una falla, deficiencia o inadecuación de procesos internos, humanos, tecnológicos o eventos externos.
4. **Tipo de Evento 1:** identificación de la pérdida que origina el evento (interno, externo, relaciones laborales, clientes, productos, activos, interacción del negocio, etc.).
5. **Tipo de Evento 2:** identificación de la pérdida que origina el evento (actividades no autorizadas, robo, fraude, seguridad laboral, etc.).
6. **Descripción del Evento de Riesgo:** Reclamo del Cliente, Debilidad Identificada Internamente, Hallazgos de Auditoria Interna, Externa o Corte de Cuentas.
7. **Fecha de Inicio:** Fecha en que se inicia el evento. día, mes y año.
8. **Fecha de Fin:** Fecha en que finaliza el evento. día, mes y año.
9. **Fecha de Detección:** Fecha en que se descubre el evento. día, mes y año.
10. **Fecha de registro:** Fecha en que se registra contablemente la pérdida económica por el evento. Día, mes, año, hora.
11. **Monto:** El monto a que asciende la pérdida, cuantificación económica de la ocurrencia del evento de riesgo operacional y los gastos derivados de su atención.
12. **Divisa:** Moneda extranjera en la que se materializa el evento.

13. **Cuenta contable:** Identifica las cuentas del Catálogo de Cuentas afectadas.
14. **Proceso**: Identifica el proceso afectado.
15. **Valor recuperado:** El valor total recuperado por la acción directa de la entidad. Incluye los montos recuperados por seguros.
16. **Valor recuperado por Seguros:** Corresponde al valor recuperado por la cobertura a través de un seguro.
17. **Producto o servicio afectado:** Identifica el producto o servicio afectado por el evento de riesgo operacional.
18. **Cuantificación de la severidad del daño:** Monto a que asciende la pérdida (neta de cualquier mitigante o recuperación)