(Este Reglamento y Guía no han sido publicados en el diario oficial "El Peruano", se descargaron de la página web de la Superintendencia Nacional de Aseguramiento en Salud, con fecha 07 de febrero de 2014.)

REGLAMENTO PARA LA GESTIÓN DEL RIESGO OPERACIONAL EN LAS INSTITUCIONES ADMINISTRADORAS DE FONDOS DE ASEGURAMIENTO EN SALUD

CAPITULO I
DISPOSICIONES GENERALES

Artículo 1°.- Del Objeto

La presente norma tiene por objeto establecer el procedimiento para la gestión del riesgo operacional en las Instituciones Administradoras de Fondos de Aseguramiento en Salud, en cumplimiento de las competencias conferidas por la Ley N° 29344, Ley Marco de Aseguramiento Universal en Salud, el Decreto Supremo N° 008-2010-SA, Reglamento de la Ley Marco de Aseguramiento Universal en Salud, el Decreto Legislativo N° 1158, Decreto Legislativo que dispone medidas destinadas al fortalecimiento y cambio de denominación de la Superintendencia Nacional de Aseguramiento en Salud y demás normas complementarias y conexas.

Artículo 2°.- Ámbito de Aplicación

Las disposiciones del presente Reglamento son de aplicación sobre las Instituciones Administradoras de Aseguramiento en Salud que comprenden aquellas entidades o empresas públicas, privadas o mixtas, creadas o por crearse, que reciban, capten y/o gestionen fondos para la cobertura de las atenciones de salud o que oferten cobertura de riesgos de salud, bajo cualquier modalidad, siendo el registro en la Superintendencia Nacional de Salud requisito indispensable para la oferta de las coberturas antes señaladas.

Las IAFAS que se encuentran bajo el ámbito de la Superintendencia de Banca y Seguros y Administradoras Privadas de Fondos de Pensiones reguladas por la Ley N° 26702 y el Decreto Legislativo N° 1051, se encuentran exceptuadas del cumplimiento de la presente norma.

Artículo 3°.- Definiciones y Acrónimos

Para efectos de la presente norma son de aplicación las definiciones del artículo 3° del Decreto Supremo N° 008-2010-SA, Reglamento de la Ley Marco del Aseguramiento Universal en Salud, así como los contenidos en el presente artículo.

a. **Apetito por el riesgo**: El nivel de riesgo que la Instituciones Administradoras de Fondos de Aseguramiento en Salud está dispuesta a asumir en su búsqueda de retorno económico o retorno social o valor.

b. **Evento**: Un suceso o serie de sucesos que pueden ser internos o externos a las Instituciones Administradoras de Fondos de Aseguramiento en Salud, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

c. **Evento de pérdida por riesgo operacional**: El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional.

d. **Información**: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje, por ejemplo: cualquier forma de registro físico, electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

e. **Proceso**: Conjunto de actividades, tareas y procedimientos organizados y repetibles, debidamente interrelacionados, que toman insumos y producen resultados.

f. **Proceso Crítico**: Son aquellos que son considerados indispensables para la continuidad de las operaciones y servicios, y que son identificados en el análisis de impacto en el negocio.

g. **Proveedor Crítico**: Modalidad de gestión mediante la cual una empresa contrata a un tercero que brinda soporte a un proceso crítico, cuya falla o suspensión del servicio puede paralizar sus operaciones. Están incluidos los que participan directamente en el proceso (ejecución) o indirectamente.

h. Plan de Gestión de Riesgo Operacional: Consiste en el documento que contiene la identificación de los riesgos operacionales del proceso y su tratamiento.

i. **Riesgo**: La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la Instituciones Administradoras de Fondos de Aseguramiento en Salud.

j. **Riesgo Legal**: Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.

k. **Riesgo estratégico:** La posibilidad de pérdidas por decisiones del Directorio asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

l. **Subcontratación**: Modalidad de gestión mediante la cual una Institución Administradora de Fondos de Aseguramiento en Salud contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por ella misma y que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a las Instituciones Administradoras de Fondos de Aseguramiento en Salud al afectar sus ingresos, solvencia, continuidad operativa o reputación.

m. **Riesgo de Reputación**: La posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

n. **Tiempo objetivo de recuperación**: Es el tiempo establecido por la Institución Administradoras de Fondos de Aseguramiento en Salud para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.

o. **Tolerancia al riesgo**: El nivel de variación que la Institución Administradora de Fondos de Aseguramiento en Salud está dispuesta a asumir en caso de desviación de los objetivos Institucionales trazados.

SUNASA I.R.A.R.

Artículo 4°.- Riesgo operacional

Entiéndase por riesgo operacional a la posibilidad de ocurrencia de pérdidas financieras originadas por factores como procesos inadecuados, deficiencias o fallas en las personas, en la tecnología de información, o por eventos externos. El Riesgo Operacional incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

Las IAFAS deben realizar una gestión adecuada del riesgo operacional que enfrentan, para lo cual observarán los criterios mínimos indicados en el presente Reglamento.

Artículo 5°.- Factores que originan el riesgo operacional

Son factores que originan el riesgo operacional los siguientes:

a. **Procesos internos:** Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios. Estos riesgos están relacionados al diseño inapropiado de los procesos, políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

b. **Personal:** Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben gestionar los riesgos asociados a su personal como: la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, alta rotación, pérdida de talento, concentración de funciones, entre otros.

c. **Tecnología de información:** Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben gestionar los riesgos asociados a la tecnología de información, relacionados a: fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas, la compatibilidad e integración de los mismos, problemas de calidad de data e información, la inadecuada inversión en tecnología, utilización de estándares de información, entre otros.

d. **Eventos externos:** Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben gestionar los riesgos asociados a eventos externos ajenos a su control, como por ejemplo fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados, actos delictivos, pandemia y epidemias, entre otros factores.

Artículo 6°.- Eventos de pérdida por riesgo operacional

Los eventos de pérdida por riesgo operacional podrían ser los siguientes:

a. **Fraude interno**: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas Organizacionales en las que se encuentra implicado, al menos, un miembro de la Organización y que tiene como fin obtener un beneficio ilícito.

b. **Fraude externo**: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c. **Relaciones laborales y seguridad en el puesto de trabajo**: Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d. **Asegurados y prácticas Organizacionales**: Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación organizacional frente a los asegurados.

e. **Daños a activos materiales**: Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

f. **Interrupción del negocio y fallos en los sistemas**: Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

g. **Ejecución y gestión de procesos**: Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

Artículo 7°.- Base de Datos de Eventos de Pérdida

Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deberán contar con una base de datos de los eventos de pérdida por riesgo operacional. Debe tenerse en cuenta que un evento puede tener como efecto una o más pérdidas, por lo cual las empresas deberán estar en capacidad de agrupar las pérdidas ocurridas por evento.

La base de datos deberá cumplir con los siguientes criterios:

a. Deben registrarse los eventos de pérdida originados en toda la empresa, para lo cual se diseñarán políticas, procedimientos de captura, y entrenamiento al personal que interviene en el proceso.

b. Debe registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas:

- Código de identificación del evento.
- Tipo de evento de pérdida.
- Descripción del evento.
- Fecha de ocurrencia o de inicio del evento.
- Fecha de descubrimiento del evento.
- Fecha de registro contable del evento.
- Monto(s) bruto(s) de la(s) pérdida(s), moneda y tipo de cambio.
- Monto(s) recuperado(s) mediante coberturas existentes de forma previa al evento, moneda, tipo de cambio y tipo de cobertura aplicada.
- Monto total recuperado, moneda y tipo de cambio.
- Cuenta(s) contable(s) asociadas.

En el caso de eventos con pérdidas múltiples, las Instituciones Administradoras de Fondos de Aseguramiento en Salud podrán registrar la información mínima requerida por cada pérdida, y establecer una forma de agrupar dicha información por el evento que las originó.

De otro lado, podrá registrarse información parcial de un evento, en tanto se obtengan los demás datos requeridos.

c. Debe definirse un monto mínimo de pérdida a partir del cual se registrará un evento en la base de datos.

d. Debe definirse un monto mínimo de pérdida a partir del cual deberá contarse con un expediente físico o electrónico que contenga información adicional a la solicitada en el literal b. y que permita conocer el modo en que se produjo el evento, características especiales y otra información relevante, así como las acciones que hubiera tomado la Institución Administradoras de Fondos de Aseguramiento en Salud, incluyendo entre otras las mejoras o cambios requeridos en sus políticas o procedimientos. Dicho monto mínimo deberá ser aprobado por el Comité de Riesgos.

SUNASA IR.A.R.

CAPITULO II
GESTION DE RIESGO OPERACIONAL

Artículo 8°.- Proceso de la Gestión de Riesgo Operacional

Consiste en la evaluación y calificación del riesgo operacional por parte de las Instituciones Administradoras de Fondos de Aseguramiento en Salud incluyendo:

a. Autoevaluación de Riesgos de Operación a los Procesos definidos como claves o críticos de la Institución.
b. Evaluación de Nuevos Productos y Servicios.
c. Gestión de Planes de Continuidad Operativa del Negocio y Servicios que prestan.
d. Evaluación de Subcontratación con Proveedores de Servicios Críticos.
e. Evaluación de una Base de Datos de Eventos de Pérdida por Riesgo Operacional
f. Evaluación de Cambios Significativos en productos, servicios, procesos y sistemas.

Artículo 9 °.- Políticas de Gestión de Riesgo Operacional

Consiste en la administración de riesgo operacional por el Directorio o máxima autoridad ejecutiva, la Gerencia General o su equivalente, así como por delegación el Comité de Riesgo; basándose en lo siguiente:

a. Estrategias claras, definidas y supervisadas.
b. Responsabilidades establecidas para la ejecución e implementación del proceso de administración de riesgos de operación en la Institución Administradora de Fondos de Aseguramiento en Salud.
c. Sólida cultura de controles internos en todos los niveles de la Institución Administradora de Fondos de Aseguramiento en Salud, incluyendo una clara definición de responsabilidades y una correcta segregación de funciones.
d. Integración en la administración de riesgos desde la planificación, desarrollo y monitoreo.
e. Sistemas de reporte para la comunicación de riesgos.
f. Planes de Contingencia y de Continuidad Operativa de la Institución Administradora de Fondos de Aseguramiento en Salud, adecuados a las necesidades, probados y actualizados en forma periódica.

Artículo 10°.- Responsabilidades del Directorio o Máxima Autoridad Ejecutiva.

Tienen las siguientes responsabilidades específicas respecto a la gestión del riesgo operacional:

a. Definir la política general para la gestión del riesgo operacional de la Institución Administradora de Fondos de Aseguramiento en Salud.
b. Gestionar los recursos necesarios para la adecuada gestión del riesgo operacional, incluyendo la continuidad del negocio y servicios, a fin de contar con la infraestructura, metodología y personal apropiado.
c. Establecer un sistema de incentivos que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.
d. Aprobar el manual de gestión del riesgo operacional.
e. Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.
f. Establecer un sistema adecuado de segregación de funciones y delegación de facultades.
g. Asegurarse que la Institución Administradora de Fondos de Aseguramiento en Salud cuenta con una efectiva gestión del riesgo operacional y continuidad del negocio o servicios que prestan, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

SUNASA I.R.A.R.

h. Aprobar una política general que defina el alcance, principios y guías que orienten la gestión de la continuidad del negocio o servicios que prestan.

Artículo 11°.- Responsabilidades de la Gerencia General o equivalente

La Gerencia General u órgano equivalente inmediato inferior al Directorio o máxima autoridad ejecutiva de la Institución Administradora de Fondos de Aseguramiento en Salud tiene las siguientes funciones:

a. Implementar la política de gestión del riesgo operacional conforme a las disposiciones establecidas por el Directorio o equivalente.
b. Al 28 de febrero de cada año deberá informar a la Superintendencia Nacional de Salud presentando un Plan de Gestión de Riesgo Operacional que deberá contener como mínimo:
   - La Identificación de los riesgos operacionales por proceso;
   - La evaluación de los riesgos identificados;
   - Las medidas para administrar el riesgo, dentro de las cuales se encuentran las medidas para mejorar la gestión de riesgos y las acciones tomadas en relación a los informes de los diversos grupos involucrados en la evaluación de los riesgos;
   - La relación de funcionarios responsables en las actividades de control; y
   - El Plan de mitigación y control de riesgos.

Artículo 12°.- Comité de Gestión de Riesgo

El Comité de Gestión de Riesgo será designado por el Directorio o máxima autoridad ejecutiva, contará con un libro de actas y deberá estar conformado como mínimo por los siguientes miembros:

a. Un miembro del Directorio o máxima autoridad ejecutiva
b. Un miembro de la Gerencia General o equivalente
c. Un miembro del Área de Riesgo

Artículo 13°.- Funciones de Comité de Gestión de Riesgo

El Comité de Gestión podrá asumir las funciones que a continuación se establecen:

a. Aprobar por delegación del Directorio o máxima autoridad ejecutiva lo siguiente:
   - Los objetivos, lineamientos y políticas para la gestión de riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud, así como las eventuales modificaciones que se realicen a éstos.
   - Los límites de exposición o niveles de tolerancia a riesgos que la Institución Administradora de Fondos de Aseguramiento en Salud puede asumir durante sus actividades, así como, los casos especiales de excesos a estos límites o niveles.
   - Las estrategias a ser implementadas para corregir las desviaciones significativas que se experimenten, sobre los límites de exposición o niveles de tolerancia a riesgos aprobados.
   - La delegación de autoridad y el establecimiento de autonomías para la toma de riesgos.
   - La metodología, parámetros, modelos, escenarios y procedimientos que se tendrán en cuenta para identificar, medir, monitorear, tratar y comunicar los distintos tipos de riesgo a los que se encuentra expuesta la Institución Administradoras de Fondos de Aseguramiento en Salud, tanto a nivel individual como a nivel integral.
b. Aprobar y poner en conocimiento, la normativa interna sobre la gestión de riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud, en función de los lineamientos previamente aprobados por el Directorio o máxima autoridad ejecutiva según sea el caso.

SUNASA R.A.R.

c. Evaluar las propuestas o proyectos que se presenten e impliquen la toma de exposición al riesgo o estrategias que pudieran alterar, de manera significativa, el perfil de riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud.
d. Monitorear la exposición al riesgo de la Institución Administradora de Fondos de Aseguramiento en Salud.
e. Supervisar que la Institución Administradora de Fondos de Aseguramiento en Salud cumpla con la regulación vigente en materia de riesgos, subsanen las observaciones y recomendaciones que formulen la Superintendencia Nacional de Salud.
f. Elaborar Informes Anuales de Riesgos de acuerdo con lo establecido por el Directorio o máxima autoridad ejecutiva.
g. Elaborar informes periódicos para el Directorio o máxima autoridad ejecutiva, de ser el caso, para informar de manera oportuna el manejo de riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud y ejercicio de las funciones del Comité.
h. Proponer la estructura organizacional, la delegación de autoridades y el establecimiento de autonomías para el manejo de riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud.
i. Proponer la implementación de recursos para el adecuado desarrollo de la gestión de riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud.
j. Proponer mejoras en la Gestión de Riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud.
k. Otras que apruebe el Directorio o máxima autoridad ejecutiva.

Artículo 14°.- Área de Riesgos

El Área de Riesgos es aquella asignada como área especializada en la gestión de riesgos de la Institución Administradora de Fondos de Aseguramiento en Salud y cumple con las siguientes funciones:

a. Proponer políticas, procedimientos, roles, responsabilidades y metodología para la gestión del riesgo operacional y gestión de la continuidad del negocio en la Institución Administradora de Fondos de Aseguramiento en Salud.
b. Participar en el diseño y actualización del manual de gestión del riesgo operacional.
c. Desarrollar la metodología para la gestión del riesgo operacional.
d. Apoyar y asistir a las demás áreas de la Institución Administradora de Fondos de Aseguramiento en Salud, para la aplicación de la metodología de gestión del riesgo operacional.
e. Evaluar el riesgo operacional, en forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo, tecnológico o informático.
f. Consolidar y desarrollar reportes e informes sobre la gestión del riesgo operacional por proceso o unidades de negocio y apoyo.
g. Identificar las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.
h. Velar por una gestión competente de riesgos y continuidad del negocio.
i. Informar a la máxima autoridad ejecutiva y al Comité de Riesgos los aspectos relevantes de la gestión de riesgos y gestión de la continuidad del negocio.
j. Asegurar que la gestión de la continuidad del negocio y servicios que prestan, sea consistente con las políticas y procedimientos aplicados para la gestión de riesgos.
k. Aplicar una metodología de autoevaluación del Riesgo Operacional en la Institución Administradora de Fondos de Aseguramiento en Salud.

SUNASA R.A.R.

CAPITULO III
AUTOEVALUACION DE RIESGO OPERACIONAL

Artículo 15°.- Autoevaluación de Riesgo Operacional

La Institución Administradora de Fondos de Aseguramiento en Salud efectuará una autoevaluación de riesgo operacional conforme a lo siguiente:

a. Identificación y priorización de procesos claves o críticos.
b. Determinación del alcance del proceso y designación de expertos.
c. Inducción general de Gestión de Riesgos Operacionales a los Expertos del proceso y riesgos relacionados, de las Instituciones Administradoras de Fondos de Aseguramiento en Salud;
d. Identificación, análisis y documentación de los riesgos y controles.
e. Presentación final a los Gerentes de área de las Instituciones Administradoras de Fondos de Aseguramiento en Salud.
f. Comunicación y Monitoreo.

Artículo 16°.- Fases para la Gestión de Riesgo Operacional

La gestión de los riesgos operacionales deben considerar, sin ser limitativo, las siguientes fases:

a. **Identificación de riesgos operacionales**: Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben contar con un mecanismo de identificación de riesgos y desarrollar una lista de riesgos claves y emergentes que puedan afectar significativamente el rendimiento y propuesta de valor.

b. **Evaluación de riesgos operacionales**: Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben contar con un mecanismo de análisis de riesgos y aplicar los criterios de riesgo estandarizados para determinar el origen, causa, probabilidad de ocurrencia, y de potencial consecuencia de cada uno de los riesgos identificados. Dependiendo de las circunstancias, el análisis puede ser cuantitativo, cualitativo, o ambos.

c. **Tratamiento de riesgos operacionales**: Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben contar con un mecanismo de tratamiento de riesgos que implique determinar si el riesgo residual es tolerable para la Institución Administradora de Fondos de Aseguramiento en Salud para la toma de decisión.

d. **Monitoreo de riesgos operacionales**: Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben contar con un mecanismo de monitoreo y realizar revisiones periódicas para mantener actualizada la matriz de riesgos, observar las tendencias e identificar los cambios en los entornos internos/externos, así como nuevos riesgos claves y emergentes que puedan afectar significativamente el rendimiento y propuesta de valor.

e. **Reporte de riesgos operacionales**: Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deben contar con un mecanismo de comunicación y reporte de riesgos operacionales y remitir la información tanto a las líneas de autoridad alta como a las líneas medias dentro de la Institución Administradora de Fondos de Aseguramiento en Salud. La información debe llegar oportunamente y debe estar en una forma y formato claro. Los reportes de riesgo se deben centrar en el cumplimiento de los objetivos de la gestión de riesgos de operación de la Institución Administradora de Fondos de Aseguramiento en Salud y en el cumplimiento de requerimientos regulatorios. Asimismo deberán contemplar la identificación de los riesgos que están aumentando o disminuyendo y aquellos riesgos que puedan afectar significativamente el rendimiento o propuesta de valor y necesiten atención inmediata.

Artículo 17°.- Manual de Gestión del Riesgo Operacional

La Institución Administradora de Fondos de Aseguramiento en Salud previamente a la autoevaluación de riesgo operacional deberá elaborar un manual de gestión de riesgo operacional que contendrá por lo menos los siguientes aspectos:

a. Políticas para la gestión del riesgo operacional.
b. Funciones y responsabilidades asociadas con la gestión del riesgo operacional del Directorio, la Gerencia General, el Comité de Riesgos, la Unidad de Riesgos (o la unidad especializada, si corresponde) y las unidades de negocio y de apoyo.
c. Descripción de la metodología aplicada para la gestión del riesgo operacional.
d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición al riesgo operacional de la empresa y de cada unidad de negocio.
e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

Artículo 18°.- Metodología para la Autoevaluación de Riesgo Operacional

La metodología para la autoevaluación de riesgo operacional se desarrolla tomando en cuenta los siguientes componentes:

a. **Ambiente interno**: Que comprende, entre otros, los valores éticos, la idoneidad técnica y moral de sus funcionarios y colaboradores; la estructura organizacional y las condiciones para la asignación de autoridad y responsabilidades.

b. **Establecimiento de objetivos**: Proceso por el que se determinan los objetivos organizacionales y estratégicos de la Institución, los cuales, deben encontrarse alineados a la visión y misión de la Institución Administradora de Fondos de Aseguramiento en Salud, ser compatibles con la tolerancia al riesgo y el grado de exposición al riesgo aceptado.

c. **Identificación de riesgos**: Proceso por el que se identifican los riesgos internos y externos que pueden tener un impacto negativo sobre los objetivos de la Institución Administradora de Fondos de Aseguramiento en Salud. Entre otros aspectos, considera la posible interdependencia entre eventos, así como los factores influyentes que los determinan.

d. **Evaluación de riesgos**: Proceso por el que se evalúa el riesgo de una Institución Administradora de Fondos de Aseguramiento en Salud, actividad, conjunto de actividades, área, portafolio, producto o servicio; mediante técnicas cualitativas, cuantitativas o una combinación de ambas.

e. **Tratamiento**: Proceso por el que se opta por aceptar el riesgo, disminuir la probabilidad de ocurrencia, disminuir el impacto, transferirlo total o parcialmente, evitarlo, o una combinación de las medidas anteriores, de acuerdo al nivel de tolerancia al riesgo definido.

f. **Actividades de control**: Proceso que busca asegurar que las políticas, estándares, límites y procedimientos para el tratamiento de riesgos son apropiadamente tomados y/o ejecutados. Las actividades de control están incorporadas en los procesos de negocio y las actividades de apoyo; incluye los controles generales, los de aplicación a los sistemas y tecnologías de información relacionada. Buscan la eficacia y efectividad de las operaciones de la Institución Administradora de Fondos de Aseguramiento en Salud, la confiabilidad de la información financiera u operativa, interna y externa, así como el cumplimiento de las disposiciones legales y cumplimiento regulatorio que le sean aplicables.

SUNAS I.R.A.R.

g. **Información y comunicación**: Proceso por el que se genera y transmite información apropiada y oportuna a la dirección, la gerencia, el personal, así como a interesados externos tales como asegurados, ciudadanos, proveedores, accionistas, trabajadores, supervisores y reguladores. Esta información es interna y externa, y puede incluir información de gestión financiera y operativa.

h. **Monitoreo**: Proceso que consiste en la evaluación del adecuado funcionamiento de la Gestión de Riesgos y la implementación de las modificaciones que sean requeridas. El monitoreo debe realizarse en el curso normal de las actividades de la Institución Administradora de Fondos de Aseguramiento en Salud y complementarse por evaluaciones independientes o una combinación de ambas. Incluye el reporte de las deficiencias encontradas y su corrección.

CAPITULO IV
REQUERIMIENTOS DE INFORMACION

Artículo 19°.- Informe a la Superintendencia

Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deberán presentar a la Superintendencia Nacional de Salud informes anuales referidos a la gestión del riesgo operacional. Dichos informes deberán ser remitidos a más tardar el 28 de febrero del año siguiente al año de reporte.

La Superintendencia Nacional de Salud podrá requerir la actualización periódica de los informes.

Artículo 20°.- Información adicional

La Superintendencia Nacional de Salud podrá requerir a la Institución Administradora de Fondos de Aseguramiento en Salud cualquier otra información que considere necesaria para una adecuada supervisión de la gestión del riesgo operacional.

DISPOSICIÓN COMPLEMENTARIA TRANSITORIA

ÚNICA.- Las Instituciones Administradoras de Fondos de Aseguramiento en Salud deberán implementar el presente reglamento en un plazo que no podrá exceder de los ciento ochenta (180) días hábiles, contados desde su entrada en vigencia.

SUNASA R.A.R.

SUNASA
SUPERINTENDENCIA NACIONAL DE ASEGURAMIENTO EN SALUD

Guía para autoevaluación de Riesgo Operacional en las Instituciones Administradoras de Fondos de Aseguramiento en Salud

1. INTRODUCCION

Con el proceso de Gestión de Riesgo Operacional (GRO), las Instituciones Administradoras de Fondos de Aseguramiento en Salud (IAFAS) tienen la oportunidad para evaluar sus procesos internos, desde la perspectiva de análisis de riesgos. Por tanto, podrán realizar una gestión más eficaz mediante un enfoque preventivo, sugiriendo estrategias adecuadas para el tratamiento de los riesgos detectados.

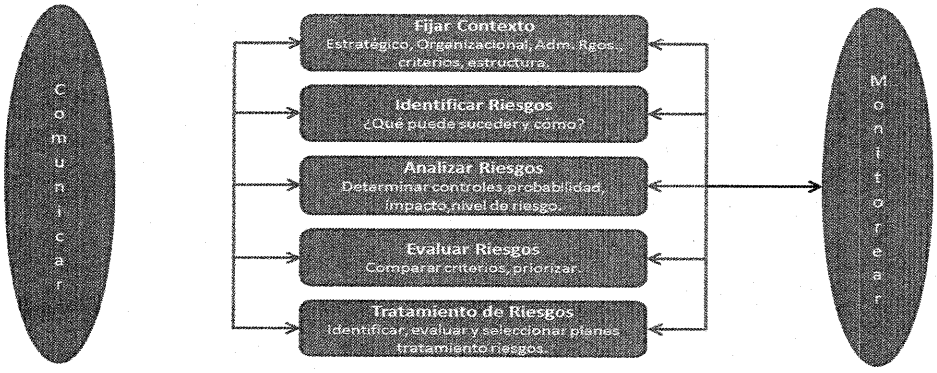
La presente Guía de Autoevaluación del Riesgo Operacional está alineada a estándares internacionales como la ley americana Sarbanes-Oxley Act "SOX", COSO, Solvencia II, entre otros; destinadas a asegurar un mayor nivel de transparencia y confiabilidad en la información que las IAFAS e IPRESS presentan. Estándares nacionales implementados por otras entidades supervisoras como la Contraloría General de la República y la Superintendencia de Banca, Seguros y AFP. Debido a las coincidencias importantes entre estos métodos de análisis para fines de GRO, hemos integrado estas visiones de manera que se aproveche al máximo, las sinergias entre ambos.

Esta metodología está basada en políticas y procedimientos diseñados para una apropiada documentación de los procesos, la identificación de los riesgos y su adecuada medición.

Las IAFAS podrán aplicar esta guía como una forma de autoevaluación o como modelo de gestión del riesgo operacional a implementar en su organización.

2. PROCESO DE GESTION DEL RIESGO OPERACIONAL (GRO)

El estándar australiano AS/NZS 4360-1999 ha sido identificado y adoptado como base metodológica para el proceso de autoevaluación con el enfoque de la gestión del riesgo operacional. Este estándar define el proceso como un ciclo continuo, tal como se aprecia en el siguiente gráfico:



El objetivo a mediano y largo plazo es implantar un esquema avanzado y automatizado de GRO que permita correlacionar la información obtenida de los procesos de autoevaluación de las organizaciones supervisadas, con información completa y sistemática obtenida de la base de datos de eventos de pérdida y posteriormente, se pueda monitorear satisfactoriamente.

Este esquema avanzado debería incluir:

- Proceso automatizado de autoevaluación.
- Base de datos de eventos de pérdida.
- Gestión de la continuidad del negocio y servicios que prestan.
- Base de datos de indicadores claves de riesgo.
- Elaborar y formalizar los contratos y acuerdos con proveedores críticos de bienes y servicios, así como, los procesos subcontratados; y la
- Evaluación de riesgos de las operaciones de introducción o cambios significativos de nuevos productos y servicios.

3. METODOLOGIA DE SUPERVISION DE RIESGO OPERACIONAL

3.1 Inducción y /o capacitación

El Gerente General de la IAFAS es el responsable de la inducción y capacitación permanente de este modelo, al Área de Riesgos de la organización o quien haga las veces.

El Área de Riesgos de la IAFAS o quien haga sus veces deben tener auto evaluadores que serán quienes apliquen la presente guía.

3.2 Notificación y requerimiento de información

Una vez definida el Área de Riesgos de la IAFAS cuáles serán las unidades a las que se realizara el proceso de autoevaluación, el jefe del área deberá notificar y solicitar a la unidad la información pertinente de acuerdo a los criterios definidos en el ANEXO A.

3.3 Identificación y priorización de procesos

Identificar y priorizar los procesos significativos de la IAFAS, según los lineamientos definidos en el documento "Criterios de Evaluación" (Ver ANEXO A). La IAFAS evaluara la pertinencia de este Anexo o elaborará otro documento de acuerdo a su perfil.

3.4 Determinación del alcance del proceso y designación de expertos

Antes de iniciar el relevamiento es importante definir el alcance del proceso crítico, es decir mapear los subprocesos y actividades que forman parte del proceso cuya evaluación será motivo de la autoevaluación.

También se identifican las áreas que participan y se obtiene la relación de expertos del proceso y riesgos relacionados.

En la definición del alcance participan la Gerencia General y el Área de Riesgos de la IAFAS.

3.5 Inducción General de GRO a los expertos de la IAFAS

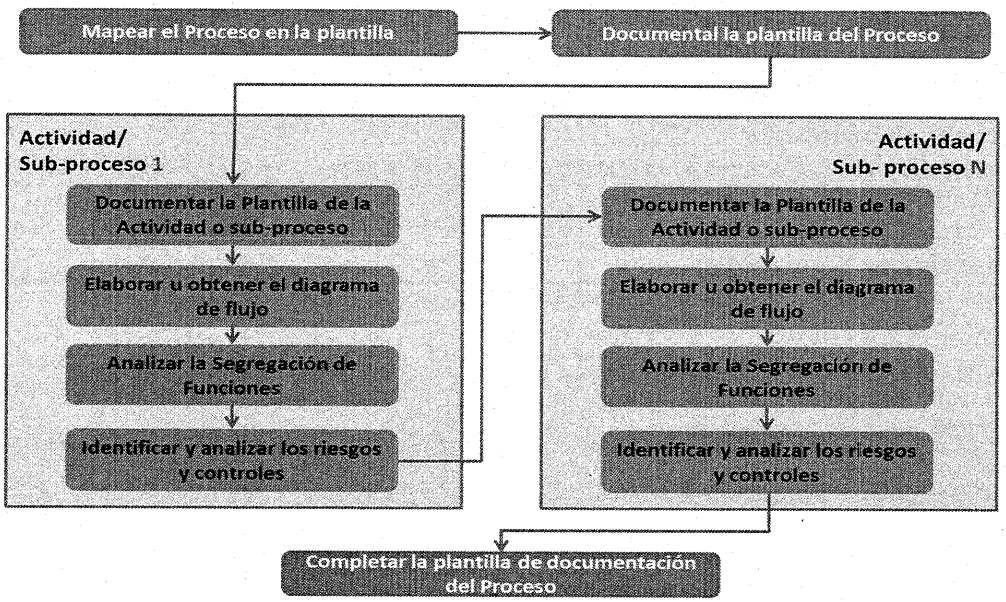
Al iniciar la autoevaluación, se realiza una presentación a los expertos del proceso-riesgos relacionados de la IAFAS, introduciendo los conceptos generales y la metodología de autoevaluación de GRO.

Se identifican las actividades relevantes y se define el cronograma de trabajo para el relevamiento y validación de la documentación.

3.6 Identificación, análisis y documentación de los riesgos y controles

Iniciada la autoevaluación, en esta fase, se obtiene un conocimiento general y detallado de los procesos significativos y sus actividades. Permite analizar la segregación de funciones, identificar y analizar los riesgos y controles y en los casos relevantes, plantear medidas para la mejor gestión de los riesgos identificados, definiéndose los plazos para su aplicación y los responsables de los mismos.

En el gráfico siguiente, se muestra el flujo del análisis y documentación de los riesgos y controles por procesos y actividades, que deben analizarse mediante sesiones de trabajo con los expertos del proceso de la IAFAS:



Como parte del **proceso de documentación**, es necesario distribuir el tiempo de las reuniones con los expertos de los procesos-riesgos en reuniones de relevamiento y de validación de la documentación, empezando con un fuerte énfasis en el relevamiento y evolucionando a una validación conforme avanza el proceso.

Como parte del **relevamiento general de los procesos** significativos se elabora e identifica lo siguiente:

- Diagrama de bloques de las actividades/sub-proceso,
- El objetivo, antecedentes y descripción,
- Los productos y servicios involucrados,
- Las cuentas contables y aseveraciones relacionadas,
- Las aplicaciones de informática que se utilizan.

Del mismo modo, como parte del **relevamiento general** de cada una **de las actividades** que forman parte de los procesos significativos, se elabora e identifica lo siguiente:

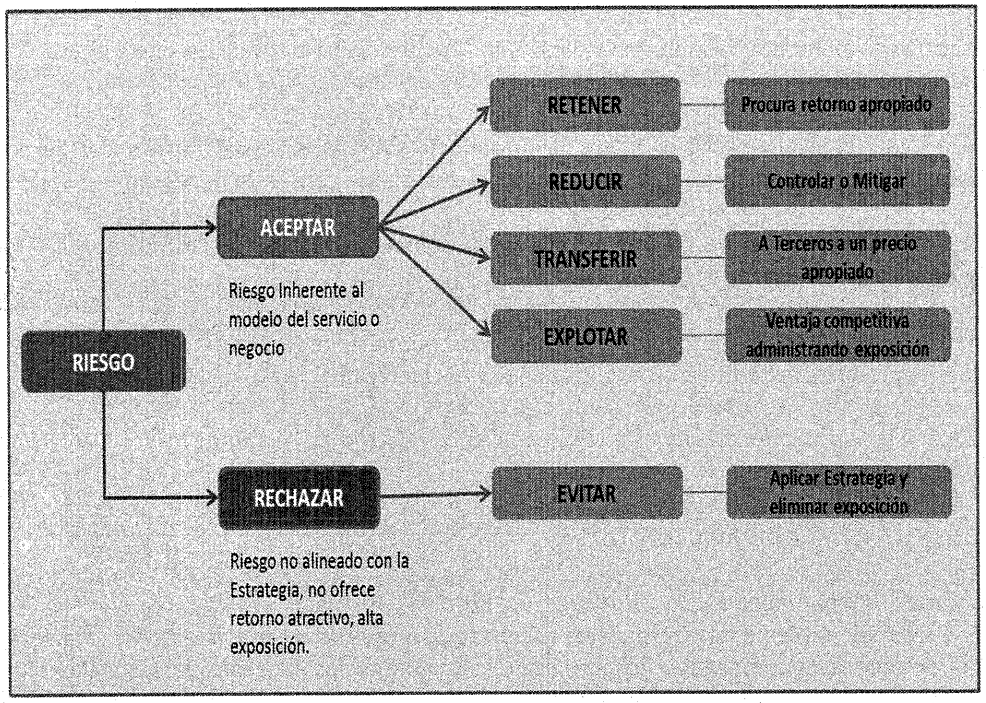
- Datos generales de la actividad/sub-proceso,
- Análisis de la actividad/sub-proceso,
- Consideraciones adicionales para actividades no rutinarias,
- Generar un diagrama de flujo o descripción de las actividades que incluye base de datos, documentos, unidades que intervienen, riesgos y controles identificados.

En el **análisis de la segregación de funciones** se identifican a las personas que desempeñan las actividades relacionadas a los procesos y se determina la existencia de una adecuada segregación de funciones en el "proceso critico".

La **identificación de los riesgos** consiste en un ejercicio consciente de búsqueda de riesgos, incluso de aquellos que pudieran no estar bajo el control de la IAFAS. Para esto, se generan listas amplias de posibles eventos de riesgo por cada una de las actividades involucradas y una vez identificados los posibles eventos de riesgo, se consideran sus causas y escenarios posibles.

Las técnicas utilizadas para la identificación de los eventos de riesgo incluyen juicios basados en la experiencia y en los registros, diagrama de flujos y entrevistas con los expertos de los procesos-riesgos.

Se analizan y miden los riesgos combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes, y se les otorga una criticidad de riesgo en acuerdo con los expertos de cada proceso.
Las estrategias para gestionar los riesgos materiales incluyen identificar los rangos de opciones para mitigar los riesgos, evaluar estas opciones y preparar planes de acción y su implementación, tal como se puede observar en el siguiente gráfico:



El resultado del análisis de riesgos, se valida con cada uno de los expertos de los procesos-riesgos de las entidades supervisadas, para su debida presentación a los gerentes de área del proceso evaluado.

3.7 Presentación final a los jefes de las unidades evaluadas

El jefe del equipo de autoevaluación, informa a los gerentes de área y/o responsables/dueños del proceso, el resultado del análisis de riesgos y los planes de acción propuestos para la mitigación.
Los gerentes de área y/o responsables/dueños del proceso aprueban los planes de acción para mitigar los riesgos. Posteriormente, se entregan los documentos finales para su administración.

3.8 Comunicación y Monitoreo

El Comité de Riesgos y el Directorio de la IAFAS, periódicamente, realiza el seguimiento de la implementación de los planes de acción sugeridos (propuestos por los supervisados) para la mitigación de los riesgos.

Esta fase de la metodología es un ciclo continuo, por tanto, es necesario diseñar un mecanismo de monitoreo y actualización permanente, dado que diversos factores podrían cambiar los procesos, las probabilidades y las consecuencias de un resultado, así como podrían afectar los costos y la conveniencia de las distintas estrategias de tratamiento.

3.9 Plantillas, Formatos y Guías GRO

Las plantillas, formatos y guías de GRO facilitan el registro y documentación de la metodología cada vez que es aplicada:

- Ver el detalle de las plantillas y formatos en el ANEXO B de este Manual.
- Ver el detalle de las guías de GRO en el ANEXO C de este Manual.

4. EVALUACIÓN DE NUEVOS PRODUCTOS Y SERVICIOS

La evaluación de riesgos en nuevos productos o servicios de la IAFAS, antes de su lanzamiento al mercado, busca asegurar que los riesgos de operación asociados al lanzamiento de un nuevo producto, canal o servicio, sean identificados, analizados y gestionados oportunamente.

En tal sentido al momento de la autoevaluación, la Gerencia General evaluará que se hayan realizado las siguientes actividades:

a) Determinar el nivel de criticidad del nuevo producto sobre la evaluación preliminar del concepto, en base a la información disponible y la documentación que se considere necesaria.

b) Realizar el análisis del riesgo operacional y presentar los resultados del mismo, de acuerdo a los lineamientos definidos por la SUNASA.

c) Validar que el Área de Riesgos haya presentado al Comité de Riesgos y al Directorio los principales nuevos productos que tuvieron análisis del Riesgo Operacional.

d) Revisar que en el informe anual a la , reporten la relación de cada nuevo producto evaluado y los principales riesgos operacionales identificados.

5. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio es un proceso efectuado por el Directorio, la Gerencia y el personal, quienes implementan respuestas efectivas para que la operatividad del negocio de la IAFAS continúe de una manera razonable, con el fin de salvaguardar los intereses de sus stakeholders, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la organización.

La Gerencia General de la IAFAS deberá supervisar la elaboración y ejecución de los diferentes planes de continuidad del negocio y el plan de recuperación de tecnología de información, para lo cual, tendrá que verificar que exista lo siguiente:

a) Capacitación al personal de la IAFAS, sobre los procedimientos de declaración de contingencia, para que esté familiarizado con el proceso de recuperación.
b) Coordinación y programación para realizar las diferentes pruebas anuales.
c) Identificación de los usuarios claves responsables de esta actividad.
d) Diseño de un proceso de cascada de llamadas o comunicación del incidente.
e) Revisión y aprobación de los resultados obtenidos en las pruebas, así como de las actualizaciones del plan.
f) Reporte anual a la sobre los principales aspectos de la gestión de la continuidad del negocio, incluyendo el programa de pruebas de los planes de continuidad.

6. CONTRATACIÓN Y SUBCONTRATACIÓN CON PROVEEDORES DE BIENES Y SERVICIOS CRÍTICOS

Con el fin de gestionar los riesgos operacionales asociados a la contratación y subcontratación con proveedores críticos, la IAFAS deberá establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos contratados y subcontratados.

Durante la autoevaluación, el evaluador deberá evaluar los siguientes aspectos:

a) Que los acuerdos de contratación y subcontratación estén formalizados mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, responsabilidades del proveedor y de la IAFAS, entre otras cláusulas.

b) Que el Área de Riesgo haya participado en el proceso de formalización del contrato con los proveedores, definidos como críticos o claves para la IAFAS, identificando los riesgos operativos relacionados a la negociación y prestación del servicio.

c) Que los contratos de tercerización o de provisión de servicios críticos, cuenten con cláusulas que establezcan de manera explícita, entre otros aspectos: 1) niveles de servicio esperado, 2) las desviaciones máximas toleradas, 3) los requerimientos de confidencialidad de la información, 4) los mecanismos de control que faciliten la revisión por las instituciones financieras, auditoría interna, auditoría externa y la .

d) Que se cumplan criterios de selección y contratación correspondientes a la entidad que se supervise (pública o privada).

7. EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Los eventos de pérdida por riesgo operacional deben ser agrupados de la manera descrita a continuación:

a) **Fraude interno:** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, normas o políticas organizacionales en las que se encuentra implicado, al menos, un miembro de la organización y que tiene como fin obtener un beneficio ilícito.

b) **Fraude externo**: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c) **Relaciones laborales y seguridad en el puesto de trabajo**: Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d) **Asegurados y prácticas organizacionales**: Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación organizacional frente a clientes concretos o del diseño de un producto o servicio.

e) **Daños a activos materiales**: Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

f) **Interrupción del negocio y fallos en los sistemas**: Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

g) **Ejecución y gestión de procesos**: Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

Base de datos de eventos de pérdida

Registros que detallan eventos de pérdida sobre aquellas pérdidas ya materializadas y las que se esperan materializar (posibles pérdidas), provisionadas o no, asociadas a eventos ocurridos como resultado de riesgos operacionales de las diferentes áreas o unidades de una organización.
La base de datos de eventos de pérdida retroalimenta a la gestión del riesgo operacional y, en un futuro, el cálculo de requerimiento de capital por riesgo operativo.

La autoevaluación del Área de Riesgos de la IAFAS se efectuará de acuerdo a lo dispuesto por el Directorio o máxima autoridad ejecutiva de la IAFAS.

8. EVALUACIÓN DE CAMBIOS SIGNIFICATIVOS EN SERVICIOS, PROCESOS Y SISTEMAS

Los cambios significativos podrán considerar, sin ser limitativos, los siguientes aspectos: cambios de la infraestructura tecnológica que soporta los principales productos y/o servicios, fusión con otra organización, cambios significativos en los procesos de negocio de la IAFAS, entre otros.

Se deberá verificar que:

a) El Área de Riesgo haya participado selectivamente en algunos proyectos de cambio, principalmente en aquellos cuyo impacto es significativo tanto en inversión como en el mismo servicio, proceso o sistema.

b) El Área de Riesgo haya realizado el análisis de riesgo operacional revisando la documentación que acompaña al proyecto.

c) Que la IAFAS haya reportado a la , en el informe anual, los cambios significativos en los procesos y su impacto sobre la continuidad del negocio.

9. FORMATOS DE LA METODOLOGIA DE GESTION DEL RIESGO OPERACIONAL (GRO)

En estos formatos se registra la información de la evaluación de riesgos que sirve para:
1) El análisis, tratamiento y monitoreo de los riesgos de la IAFAS.
2) El monitoreo de la implementación de los hallazgos y acciones de mejora de la IAFAS.
3) La documentación de riesgos y controles de las entidades supervisadas.

Los formatos a utilizar son:

- Formato GRO-01 Plantilla resumen de procesos
- Formato GRO-02 Plantilla de documentación de procesos
- Formato GRO-03 Plantilla de documentación de segregación de funciones
- Formato GRO-04 Plantilla de identificación y medición de riesgos, controles y tratamiento por actividad o sub-proceso
- Formato GRO-05 Plantilla diagrama de flujo de actividades o sub-procesos
- Formato GRO-06 Plantilla de documentación de dinámicas contables
- Formato GRO-07 Plantilla de tratamiento y monitoreo por actividad o sub-proceso
- Formato GRO-08 Plantilla resumen de los activos de información

9.1 Encabezado de Formatos y Campos a rellenar

Los siguientes son los campos comunes a llenar en todas las plantillas:

- **Fecha de elaboración:** Indicar mes y año en que se termina la documentación del proceso.
- **Institución:** Nombre o razón social de la entidad.

- **Tipo de Institución:** El tipo de IAFAS (SIS, EsSalud, Fuerzas armadas, EPS, autoseguros, prepaga, etc.).
- **Código SUNASA:** Identificación de la entidad según el tipo de Institución.
- **Nombre del Proceso:** Corresponde al nombre del proceso materia de evaluación, definido como el conjunto de actividades repetitivas para obtener un producto o servicio para un cliente interno o externo.
- **Responsable del Proceso:** Nombre del funcionario, gerente o jefe encargado de la actividad o sub-proceso.
- **Evaluador:** Funcionario encargado del relevamiento de información.

9.2 Formato GRO- 01 Plantilla Resumen de Procesos

Resume los datos de la actividad y contacto del sub-proceso materia de evaluación.

- **Nombre de la Actividad o Sub-proceso:** Dentro de un proceso determinado, corresponde al nombre de la actividad materia de evaluación, conceptuada como el conjunto de pasos que tienen un objetivo y un entregable definido.
- **Código:** Formado por el código del proceso seguido del número correlativo correspondiente a la actividad en evaluación. Puede ser el código que la IAFAS usa o, en contrario, determinar un código interno.
- **Gerencia Responsable:** Consignar el nombre de la gerencia o departamento que es responsable del proceso y/o actividad en evaluación.
- **Gerente Responsable:** Consignar el nombre del gerente que es responsable del proceso y/o actividad en evaluación.
- **Jefatura Responsable:** Consignar el nombre del área a la que pertenece el proceso y/o actividad en evaluación.
- **Jefe o Experto Responsable:** Consignar el nombre del Jefe del área a la que pertenece el proceso y/o actividad en evaluación.
- **Norma(s) Interna(s) de la Actividad o Sub-proceso:** Consignar el número y nombre de la(s) norma(s) que están relacionadas con la actividad en evaluación.

9.3 Formato GRO- 02 Plantilla de Documentación de Procesos

En este formato se registran todos los datos solicitados a fin de documentar los procesos, sus riesgos y controles asociados.

- **Diagrama de Bloques o Descripción del Proceso:** Colocar en bloques las actividades o sub-procesos involucrados en el proceso, haciendo una pequeña descripción del inicio y fin de cada una de ellas.
- **Productos / servicios involucrados:** Indicar los productos y/o servicios involucrados en el proceso.
- **Cuentas contables o Partida Presupuestal:** Indicar las cuentas contables relacionadas al proceso o para el caso de entidades públicas, la partida presupuestal asignada.
- **Aplicaciones TIC utilizadas:** Indicar las aplicaciones utilizadas de tecnología de información y comunicación con sus respectivos códigos, si los tuvieran.
- **Información adicional:** Colocar la información adicional que el evaluador considere necesaria anotar.

9.4 Formato GRO- 03 Plantilla de Documentación de Segregación de Funciones

En este formato se reportan las actividades más significativas del proceso indicando al responsable de efectuar las funciones operativas, de autorización, custodia, registro y control para cada actividad. Permite identificar si un mismo empleado es responsable simultáneamente de las funciones de autorización y control.

9.5 Formato GRO- 04 Plantilla de Identificación y Medición de Riesgos, Controles y Tratamiento por Actividad o Sub-proceso

9.5.1 Identificación de los Riesgos de cada Actividad o Sub-proceso

En este bloque se registran los posibles eventos de riesgos operacionales a los que puede estar sujeta la actividad. La lista deberá ser lo más amplia posible.

- **Cuentas asociadas o Partida Presupuestal:** Colocar las cuentas contables únicamente en caso que la materialización de un evento afecte directa o indirectamente la exactitud y fidelidad de los registros contables de la entidad. En su defecto la partida presupuestal asignada que se afecte.

- **Aseveración Contable:** Aplicable únicamente en caso que la materialización de un evento afecte directa o indirectamente la exactitud y fidelidad de los registros contables de la entidad, indicar en este campo la forma o formas en que sería afectada, utilizando las aseveraciones correspondientes que se indican en la guía GRO- 11 *"Aseveraciones Contables sobre los Estados Financieros"*.

- **Número de Riesgo:** Indicar un código correlativo para cada riesgo, en forma ascendente desde R1 hasta Rn.

- **Descripción del Riesgo:** Describir, en sus propias palabras, el riesgo identificado y sus posibles causas y eventos. (Ejemplo: *"Que se presenten suplantaciones en la atención médica")*.

- **Código del Evento:** Consignar el código correspondiente a la clasificación de eventos según la Guía GRO- 12 *"Categorización de Eventos de Riesgo Operacional"*. Consignar el que mejor se ajuste al riesgo identificado descrito.

- **Evento:** Colocar el nombre del riesgo que corresponde a la *"Categorización de Eventos de Riesgo Operacional"* de la Guía GRO- 12.

- **Código de Origen:** Consignar el código que corresponde al riesgo operacional origen, según la Guía GRO- G13 *"Categorías de Riesgo Operacional- Origen"*. Consignar el que mejor se ajuste al riesgo identificado descrito.

- **Origen:** Categoría/sub-categoría que corresponda al riesgo identificado, según la Guía GRO- 13 " *Categorías de Riesgo Operacional- Origen"*.

9.5.2 Controles Existentes

En este bloque se pretende registrar los controles existentes en la actualidad, respecto a los riesgos identificados.

- **Número de Control:** Se indica un código correlativo para cada control, en forma ascendente desde C1 hasta Cn, considerando asignar el mismo código a un mismo control, si se repitiera.

- **Descripción del control existente:** Describa, con sus propias palabras, los controles que se aplican actualmente a cada riesgo de la actividad materia de evaluación.

- **Cargo Responsable:** Consignar el cargo de la persona designada como responsable del control.

- **Código de control:** Precisar el código correspondiente a tipo de control, según corresponda a la clasificación de controles precisados en la Guía GRO- 14 *"Categoría de Controles Estándares"*. Consignar el que mejor se ajuste al control descrito.

- **Tipo de Control:** Considere las siguientes definiciones según clasificación: Preventivo, Detectivo, de Aplicación, Generales TI y Manual; según lo definido en la Guía GRO- 15 *"Clasificación de los Controles"*.

- **Nivel de Control Existente:** Registrar los niveles de Estricto, Alto, Regular, Bajo, o Inexistente según corresponda de acuerdo con la Guía GRO- 16 *"Niveles de Control de Riesgo Operacional"*. Consignar el que mejor se ajuste a los controles descritos.

9.5.3 Características del Control

Aquí se detalla características complementarias del control existente.

- **Frecuencia del Control:** Se refiere a la periodicidad con que ejecuta el control. Ej.: diario o por transacción, semanal, quincenal, mensual, trimestral, semestral, anual, etc.

- **Documentos revisados como parte del control**: Indicar el nombre de los formatos, reportes, archivos o pantallas que se utilizan al ejecutar el control.

- **Evidencias del control:** Se refiere a la "prueba" de que el control fue ejecutado, describiendo, por ejemplo:
  - Formatos, archivos, reportes o pantallas utilizados, que hayan sido impresos, revisados y visados por los responsables.
  - Si existe alguna conciliación impresa y firmada como producto de la revisión.
  - Si se imprimen pantallas de la aplicación y son firmadas por los responsables, luego de revisar las operaciones.
  - Si se imprimen asientos contables y son firmados por el responsable de registrarlos y el responsable de revisarlos.
  - Si es que existen aprobaciones o autorizaciones automáticas en los aplicativos que puedan ser fácilmente identificadas.

- **Disposición de diferencias y excepciones:** Describir las acciones tomadas al identificar errores o excepciones como resultado de la ejecución del control, respondiendo a las preguntas: ¿Qué se hace?, ¿Quién lo hace?, ¿Cuándo?, ¿Qué documentos se utilizarían como parte de la regularización?, ¿Cuál es la evidencia de la regularización?, entre otras.

9.5.4 Medición de los Riesgos Existentes

En este bloque se registra información necesaria para determinar el nivel del riesgo, en función al impacto y su probabilidad de ocurrencia. Esta estimación se basa en el Nivel de Riesgo Controlado, es decir, aquel que toma en consideración los controles actualmente establecidos.

- **Impacto:** Consignar los valores correspondientes a la calificación del impacto por tipo de Entidad a Supervisar, según lo precisa la Guía GRO- G17A, G17B, y G17C *"Impacto Cualitativo si se materializa un riesgo"*. Consignar el que mejor se ajuste a su percepción del riesgo.

- **Probabilidad:** Consignar los valores correspondientes a la calificación de probabilidad según lo precisa la Guía GRO- G18 *"Probabilidad Cualitativa de Ocurrencia de un determinado riesgo"*. Consignar el que mejor se ajuste a su percepción del riesgo.

- **Nivel de Riesgo:** Corresponde al valor resultante de multiplicar el valor del impacto por el valor de probabilidad del propio cuadro.

- **Criticidad:** Corresponde registrar en este casillero el grado de criticidad correspondiente al nivel de riesgo controlado, obtenido de aplicar la Matriz de clasificación de criticidad de Riesgo Operacional, precisados en la Guía GRO- G19 *"Matriz de Criticidad de Riesgos Operativos"*, que clasifica los riesgos en No Aceptables, Extremos, Altos, Moderados y Bajos.

9.5.5 Tratamiento del Riesgo Actual

En este bloque se registran las decisiones con relación al tratamiento del riesgo, de acuerdo a los objetivos de la unidad y su apetito de riesgo.

- **Tratamiento Adicional:** Corresponde a las acciones de Evitar, Transferir, Reducir, Retener, Aprovechar, según corresponda a las decisiones adoptadas por el dueño del proceso o servicio conforme a las descripciones precisadas en la Guía GRO- G20 *"Tratamiento de Riesgo Operacional"*. Debe ser consistente con el nivel de control existente y el nivel de control objetivo.

9.5.6 Localización del Impacto del Riesgo

En este bloque se identifican los rubros u objetivos claves definidas por la IAFAS, en los que impacta el riesgo identificado. Se marcará con una "X" aquellas áreas de impacto que sean relevantes a cada riesgo identificado.

- La Guía GRO- G21 *"Áreas de Impacto cuando se materializan los riesgos operativos"* proporciona información de cada uno de los Objetivos Clave.

9.5.7 Plan de Adecuación

En este bloque se identifican las recomendaciones a implementar, en coordinación con Experto, Jefe o Gerente del proceso.

- **Plan de Acción:** Precisar con sus propias palabras el o los planes de acción que piensa ejecutar con relación al tratamiento del riesgo.

- **Responsable:** El nombre y cargo de la persona responsable en implementar el plan de acción; de preferencia, el Gerente o Jefe del proceso.

- **Observaciones:** Campo reservado a las anotaciones que el evaluador considere importante realizar.

9.6 Formato GRO- 05 Plantilla Diagrama de Flujo de actividades o sub-procesos

En este formato se elabora el flujograma de los procesos analizados, el cual debe incluir los riesgos y controles identificados.

9.7 Formato GRO- 06 Plantilla de Documentación de Dinámicas Contables

En este formato se identifican las cuentas contables, su dinámica y comentarios u observaciones adicionales de importancia.

9.8 Formato GRO- 07 Plantilla de Tratamiento y Monitoreo por Actividad o sub -proceso

En este formato se detallan los planes de acción a implementar para mitigar los riesgos significativos de cada actividad. Incluye:

- Número del Riesgo
- Descripción del Riesgo
- Área o Unidad Responsable
- Nombre del Gerente Responsable
- Descripción del Plan de Adecuación
- Fecha de Inicio
- Fecha de Término
- Fecha de Seguimiento
- Observaciones

9.9 Formato GRO- 08 Plantilla Resumen de los Activos de Información

En este formato se detallan todos los activos de información más importantes de cada proceso crítico del negocio, a fin de identificar y evaluar sus riesgos, controles y tratamientos.

- La Guía GRO- 22 *"Guía para la Identificación de Activos de Información críticos del Proceso"* proporciona una orientación en base a preguntas, para determinar la información crítica y registrarla en el formato GRO-08.

- **¿Qué es un Activo de Información?**
  Es una información importante para el negocio, que se encuentra almacenada en algún lugar intangible o tangible y debe estar protegida adecuadamente ya que tiene un valor significativo para la organización.

  De manera general un Activo de Información debe tener las siguientes características:
  - Valor para la organización en términos de servicio al cliente, salud del asegurado o paciente, vida humana, privacidad, impacto financiero para la entidad, impacto financiero para el asegurado o paciente, requerimientos legales-regulatorios, ventaja competitiva y/o imagen pública.
  - No es fácil de reemplazarlo sin tener involucrado un costo, conocimiento, tiempo y/o recursos.
  - Algunos ejemplos de Activos de Información (ISO 17799): archivos físicos y electrónicos, bases de datos, documentación del sistema, manuales de los usuarios, material de formación, procedimientos operativos, de soporte, planes de continuidad, configuración del soporte de recuperación, reportes financieros o gerenciales, historias clínicas, entre otros.

- El formato incluye los siguientes campos:
  - **Número del Activo de Información:** Asignación de una codificación interna para un mejor control; por ejemplo: AFI-001.
  - **Nombre del Activo de información**: Consignar en forma breve, el nombre conocido del documento, archivo, reporte, etc.
  - **Descripción del Activo de información**: Describir las características más importantes del activo: si son manuales, electrónicos, seguridad, información que contiene, etc.
  - **Responsable del Activo de información**: Cargo del responsable de custodiar y actualizar los activos de información.
  - **Ubicación del Activo de información**: Dirección o ruta de carpeta guardada, archivo físico del área, etc.
  - **Usuarios del Activo de información**: Áreas que tienen acceso a esta información o documentación.
  - **Observaciones:** Información adicional de importancia, así como, algunas acciones de mejora que se puedan detectar y que sirven para incluirlas como riesgo en la matriz GRO-04.

SUNASA
SUPERINTENDENCIA NACIONAL DE ASEGURAMIENTO EN SALUD

FORMATOS o PLANTILLAS
Gestión de Riesgos Operativos

- **Formato GRO- 01 Plantilla Resumen de Procesos**
- **Formato GRO- 02 Plantilla de Documentación de Procesos**
- **Formato GRO- 03 Plantilla de Documentación de Segregación de Funciones**
- **Formato GRO- 04 Plantilla de Identificación y Medición de Riesgos, Controles y Tratamiento por Actividad o Sub-proceso**
- **Formato GRO- 05 Plantilla Diagrama de Flujo de actividades o sub-procesos**
- **Formato GRO- 06 Plantilla de Documentación de Dinámicas Contables**
- **Formato GRO- 07 Plantilla de Tratamiento y Monitoreo por Actividad o sub-proceso**
- **Formato GRO- 08 Plantilla Resumen de los Activos de Información**

SUNASA
I.R.A.R.

SUNASA
SUPERINTENDENCIA NACIONAL DE ASEGURAMIENTO EN SALUD

PLANTILLA RESUMEN DE PROCESOS

Gestión de Riesgos Operativos

Código del Formato: GRO-01

Fecha de Elaboración	
Institución	
Tipo de Institución	
Codigo SUNASA	
Nombre del Proceso	
Responsable del Proceso	
Evaluador	

Nombre de la Actividad o Sub-Proceso	Código Actividad	Gerencia / Departamento Responsable	Nombre Gerente Responsable	Jefatura Responsable	Nombre Jefe o Experto Responsable	Norma (s) Interna (s) de la Actividad o Sub-proceso

SUNASA
I.R.A.R.

SUNASA

PLANTILLA DE DOCUMENTACION DE PROCESOS

Gestión de Riesgos Operativos **Código del Formato: GRO-02**

Fecha de Elaboración	
Institución	
Tipo de Institución	
Codigo SUNASA	
Nombre del Proceso	
Responsable del Proceso	
Evaluador	

Diagrama de Bloques o Descripción del Proceso

Productos o Servicios Involucrados	

Cuentas Contables Involcuradas o Partida Presupuestal (código y nombre)	

Aplicaciones TI Utilizadas	

Información Adicional

SUNASA
SUPERINTENDENCIA NACIONAL DE ASEGURAMIENTO EN SALUD

PLANTILLA DE DOCUMENTACION DE SEGREGACION DE FUNCIONES

Gestión de Riesgos Operativos **Código del Formato:** **GRO-03**

Fecha de Elaboración	
Institución	
Tipo de Institución	
Codigo SUNASA	
Nombre del Proceso	
Responsable del Proceso	
Evaluador	

Actividades	Responsable Operativo	Autorización	Custodia de Activos	Registro	Actividad de Control
Nombre Actividad 01: Esterilización material obstétrico					
Función 01				Cargo, Área y/o Comité	
Función 02	Cargo, Área y/o Comité				
Función 03					
Nombre Actividad 02					
Función 01				Cargo, Área y/o Comité	
Función 02					Cargo, Área y/o Comité
Nombre Actividad 03					
Función 01					Cargo, Área y/o Comité
Función 02				Cargo, Área y/o Comité	

SUNASA REPÚBLICA DEL PERÚ V°B° U.R.A.R.

Resumen de las debilidades identificadas relacionadas a la segregación de funciones

•

SUNASA

PLANTILLA DE DENTIFICACION Y MEDICION DE RIESGOS, CONTROLES Y TRATAMIENTO POR ACTIVIDAD O SUB-PROCESO

Gestión de Riesgos Operativos

Código del Formato: **GRO-04**

Fecha de Elaboración	
Institución	
Tipo de Institución	
Codigo SUNASA	
Nombre del Proceso	
Responsable del Proceso	
Evaluador	

IDENTIFICACION DE LOS RIESGOS DEL SUB-PROCESO O ACTIVIDAD									Identificación de Controles Existentes			
Cuentas Asociadas / partida Presupuestal	Aseveración Contable (IAFAS)	Nombre Cuenta Contable o Partida Presupuestal	Nº del Riesgo	Descripción del Riesgo	Código del Evento	Evento	Código de Origen	Origen	Nº de Control	Descripción del Control Existente	Cargo del Responsable	Código de Control
					#N/A		#N/A					
					#N/A		#N/A					
					#N/A		#N/A					
					#N/A		#N/A					
					#N/A		#N/A					
					#N/A		#N/A					
					#N/A		#N/A					
					#N/A		#N/A					

		Características del Control				Medición de los Riesgos Existentes						Tratamiento del Riesgo	Localización del Impacto (marcar con una X en los camp				
Tipo de Control	Nivel de Control Existente	Frecuencia del Control	Documentos Revisados como parte del Control	Evidencias de Control	Disposición de diferencias y excepciones	Nº	Impacto	Nº	Probabilidad	Nivel de Riesgo	Criticidad	Tratamiento Adicional	Servicio al Cliente	Salud del Asegurado/ Paciente	Vida Humana	Privacidad	Impacto Financiero para Entidad
						#N/A		#N/A		#N/A	#N/A						
						#N/A		#N/A		#N/A	#N/A						
						#N/A		#N/A		#N/A	#N/A						
						#N/A		#N/A		#N/A	#N/A						
						#N/A		#N/A		#N/A	#N/A						
						#N/A		#N/A		#N/A	#N/A						
						#N/A		#N/A		#N/A	#N/A						
						#N/A		#N/A		#N/A	#N/A						

de los Riesgos os que aplique)				Plan de Adecuación		
Impacto Financiero Paciente/ Asegurado	Legal y Requerim. Regulatorio	Ventaja Competitiva	Imagen Pública	Plan de Acción	Responsable	Observaciones

SUNASA
SUPERINTENDENCIA NACIONAL DE ASEGURAMIENTO EN SALUD

DIAGRAMA DE FLUJO DE ACTIVIDADES O SUB-PROCESOS

Gestión de Riesgos Operativos

Código del Formato: **GRO-05**

Empresa: **Fecha de Elaboración:**

Proceso:

Actividad:

Area/ Cargo / Responsable:

Area 1	Area 2	Area 3	Area 4

SUNASA
SUPERINTENDENCIA DEL PERÚ
I.R.A.R.

SUNASA

PLANTILLA DE DINAMICAS CONTABLES
Gestión de Riesgos Operativos

Código del Formato: GRO-06

Fecha de Elaboración	
Institución	
Tipo de Institución	
Evaluador	
Codigo SUNASA	

Fecha de elaboración	
Nombre del Proceso	
Responsable del Proceso	

Código de Cuenta	Descripción de la Cuenta	Débito	Crédito

Código de Cuenta	Descripción de la Cuenta	Débito	Crédito

Código de Cuenta	Descripción de la Cuenta	Débito	Crédito

COMENTARIOS / OBSERVACIONES

SUNASA
I.R.A.R.

SUNASA

PLANTILLA DE TRATAMIENTO Y MONITOREO DE RIESGOS POR ACTIVIDAD O SUB-PROCESO

Gestión de Riesgos Operativos

Código del Formato: GRO-07

Fecha de Elaboración	
Institución	
Tipo de Institución	
Codigo SUNASA	
Nombre del Proceso	
Responsable del Proceso	
Evaluador	

Tratamiento de Riesgos del Sub-Proceso					Monitoreo de los Riesgos del Sub-Proceso			
Nº de Riesgo	Descripción del Riesgo	Area o Unidad Responsable	Nombre Gerente Responsable	Plan de Adecuación	Fecha de Inicio	Fecha de Término	Fecha de Seguimiento	Observaciones

SUNASA

PLANTILLA RESUMEN DE LOS ACTIVOS DE INFORMACION

Gestión de Riesgos Operativos

Código del Formato: **GRO-08**

Fecha de Elaboración	
Institución	
Tipo de Institución	
Evaluador	
Codigo SUNASA	

Fecha de elaboración	
Nombre del Proceso	
Responsable del Proceso	

Detalle de los Activos de Información Principales del Proceso						
Nº del Activo de Información	Nombre del Activo de Información	Descripción del Activo de Información	Responsable del Activo de Información	Ubicación del Activo de Información	Usuarios del Activo de Información	Observaciones

SUNASA I.R.A.R.

SUNASA
SUPERINTENDENCIA NACIONAL DE ASEGURAMIENTO EN SALUD

GUIAS METODOLOGICAS
Gestión de Riesgos Operativos

- Guía GRO- 11 ***Aseveraciones Contables sobre los Estados Financieros***
- Guía GRO- 12 ***Categorización de Eventos de Riesgos de Operación***
- Guía GRO- 13 ***Categorías de Riesgos de Operación- Origen***
- Guía GRO- 14 ***Categoría de Controles Estándares***
- Guía GRO- 15 ***Clasificación de los Controles***
- Guía GRO- 16 ***Niveles de Control de Riesgos de Operación***
- Guía GRO- 17 ***Impacto Cualitativo si se materializa un riesgo***
- Guía GRO- 18 ***Probabilidad Cualitativa de Ocurrencia de un determinado riesgo***
- Guía GRO- 19 ***Matriz de Criticidad de Riesgos Operativos***
- Guía GRO- 20 ***Tratamiento de Riesgos de Operación***
- Guía GRO- 21 ***Áreas de Impacto cuando se materializan los riesgos operativos***
- Guía GRO- 22 ***Guía para la Identificación de Activos de Información críticos del Proceso*** .

SUNASA
I.R.A.R.

SUNASA

ASEVERACIONES CONTABLES SOBRE LOS ESTADOS FINANCIEROS

Gestión de Riesgos Operativos **Código del Formato: GRO-11**

La siguiente tabla contiene la descripción de las aseveraciones contables con relación a los Estados Financieros de la Entidad.

- Es objetivo la veracidad y exactitud de las cifras mostradas en sus balances y estados de pérdidas y ganancias.

- El correcto registro de las transacciones permite a la Entidad ser líder en transparencia y exactitud de su información financiera.

- La Entidad considera muy importante que en función a la diversidad de tipos de errores que pueden ocurrir existan controles que deben estar eficazmente diseñados para prevenir y detectar errores de importancia o fraude.

En tal sentido el evaluador debe buscar las siguientes aseveraciones con relación a los Estados Financieros de la IAFAS que:

Códigos	Aseveración	Descripción
I	**Integridad**	No existen activos, pasivos, transacciones o hechos sin registrar, ni partidas sin revelar.
E	**Existencia**	Un activo o un pasivo existe a una fecha determinada.
O	**Ocurrencia**	Una transacción o un hecho realmente tuvo lugar durante el periodo.
V	**Valoración**	Un activo o un pasivo está registrado por un importe apropiado.
DO	**Derechos y Obligaciones**	Un activo o un pasivo pertenece a la compañía a una fecha determinada.
SA	**Salvaguarda de Activos**	Todos los activos deben estar protegidos de adquisiciones, usos o disposiciones no autorizadas.
RP	**Revelación y Presentación**	Un activo o un pasivo está adecuadamente clasificado, descrito y evidenciado en los Estados Financieros.

SUNASA
I.R.A.R.

CATEGORIZACION DE EVENTOS DE RIESGOS DE OPERACION - EVENTOS

Gestión de Riesgos Operativos **Código del Formato: GRO-12**

Tipo de Evento	Código	Ejemplos
Fraude Interno	**FI**	
Actividades No Autorizadas	FI- 1	
	FI- 1.1	Actividad/Transacciones/Tareas no reveladas (intencionalmente)
	FI- 1.2	Realizar Actividad/Transacciones/Tareas no autorizadas (con o sin pérdidas económicas)
	FI- 1.3	Valoración errónea de posiciones, stocks, activos (intencionalmente)
Hurto y Fraude	FI- 2	
	FI- 2.1	Fraude/Fraude crediticio/Depósitos sin valor
	FI- 2.2	Hurto/Extorsión/ Malversación/Robo
	FI- 2.3	Apropiación indebida de activos
	FI- 2.4	Destrucción maliciosa de activos
	FI- 2.5	Falsificación
	FI- 2.6	Suplantación
	FI- 2.7	Utilización de cheques sin fondo
	FI- 2.8	Contrabando
	FI- 2.9	Apropiación de cuentas/Fingimiento de personalidad
	FI- 2.10	Incumplimiento/Evasión de impuestos(intencionalmente)
	FI- 2.11	Sobornos/Cohechos/Colusión
	FI- 2.12	Abuso de información privilegiada (no a favor de la empresa)
Fraude Externo	**FE**	
Seguridad de Sistemas	**FE- 1**	
	FE- 1.1	Daños por ataques informáticos
	FE- 1.2	Robo de información (con o sin pérdidas económicas)
Hurto y Fraude	**FE- 2**	
	FE- 2.1	Hurto/Robo
	FE- 2.2	Suplantación
	FE- 2.3	Falsificación
	FE- 2.4	Circulación de cheques sin fondo
	FE- 2.5	Extorsión/Soborno/Cohecho/Colusión
	FE- 2.6	Apropiación indebida de activos de información
Relaciones laborales y seguridad en el puesto de	**RL**	
Relaciones Laborales	**RL- 1**	
	RL- 1.1	Asuntos relacionados a remuneración, beneficios sociales, extinción de contratos, indemnizaciones
	RL- 1.2	Organización de la actividad laboral/Huelgas
	RL- 1.3	Asuntos relacionados al proceso de seleccion, contratación e inducción
Salud y Seguridad en el puesto de trabajo	**RL- 2**	
	RL- 2.1	Responsabilidad común (resbalones, etc.)
	RL- 2.2	Eventos relacionados con las normas de higiene y seguridad en el trabajo
	RL- 2.3	Indemnizaciones a los trabajadores a consecuencia de un daño laboral
Diversidad y Discriminación	**RL- 3**	
	RL- 3.1	Todo tipo de discriminaciones (acoso sexual, racismo, maltrato, etc.)
Prácticas con clientes (asegurados, pacientes,	**PN**	
Adecuación, divulgación de información y confianza	**PN- 1**	
	PN- 1.1	Abusos de confianza/Incumplimiento de pautas
	PN- 1.2	Aspectos de adecuación/Divulgación de información (lavado de dinero, know your customer, etc.)
	PN- 1.3	Violación de la revelación de información sobre clientes
	PN- 1.4	Violación de privacidad
	PN- 1.5	Confusión de cuentas
	PN- 1.6	Abuso y aprovechamiento de información confidencial y privilegiada

CATEGORIZACION DE EVENTOS DE RIESGOS DE OPERACION - EVENTOS

Gestión de Riesgos Operativos **Código del Formato: GRO-12**

Tipo de Evento	Código	Ejemplos
	PN- 1.7	Ocultar información crítica
Prácticas inadecuadas de negocio o mercado	**PN- 2**	
	PN- 2.1	Prácticas inadecuadas de negociación/Mercado
	PN- 2.2	Manipulación del mercado
	PN- 2.3	Abuso de información privilegiada (en favor de la empresa)
	PN- 2.4	Lavado de dinero
	PN- 2.5	Actividades no autorizadas
	PN- 2.6	Conflicto de interés
Defectos del producto/Servicio	**PN- 3**	
	PN- 3.1	Productos defectuosos (no autorizados, etc.)
	PN- 3.2	Errores en el diseño y modelos
	PN- 3.3	Publicidad o Venta engañosa
Actividades de asesoramiento	**PN- 4**	
	PN- 4.2	Litigios sobre resultados de las actividades de asesoramiento
Selección, patrocinio y exposición	**PN- 5**	
	PN- 5.1	Ausencia o deficiencia en la investigación a clientes conforme a normas
	PN- 5.2	Superación de los límites de exposición frente a clientes
	PN- 5.3	Concentración de Clientes
Ejecución, entrega y gestión de	**EP**	
Recepción, ejecución y mantenimiento de operaciones	**EP- 1**	
	EP- 1.1	Comunicación defectuosa
	EP- 1.2	Errores de introducción de datos, mantenimiento o carga
	EP- 1.3	Incumplimiento de plazos o de responsabilidades
	EP- 1.4	Funcionamiento erróneo de modelos/Sistemas
	EP- 1.5	Error contable/atribución a entidades erróneas
	EP- 1.6	Errores en otras tareas
	EP- 1.7	Fallo en la entrega
	EP- 1.8	Falla en la gestión colateral
	EP- 1.9	Mantenimiento de datos
	EP- 1.10	Fallas en manejo de colaterales
	EP- 1.11	Falta de asignación de responsabilidades
	EP- 1.12	Falta de segregación de funciones
Seguimiento y comunicación de informes	**EP- 2**	
	EP- 2.1	Incumplimiento de la obligación de informar (fallas en el monitoreo, etc.)
	EP- 2.2	Inexactitud de informes externos (con o sin generación de pérdidas)
Admisión de clientes y documentación	**EP- 3**	
	EP- 3.1	Inexistencia de autorizaciones/rechazos de clientes
	EP- 3.2	Poderes incompletos/Faltantes
Gestión de cuentas de clientes	**EP- 4**	
	EP- 4.1	Acceso no autorizado a cuentas
	EP- 4.2	Registros incorrectos de clientes (con o sin generación de pérdidas)
	EP- 4.3	Pérdida o daño de activos de clientes por negligencia
	EP- 4.4	Información incompleta del Cliente
Contrapartes comerciales, distribuidores y proveedores	**EP- 5**	
	EP- 5.1	Prácticas inadecuadas de contrapartes distintas de clientes
	EP- 5.2	Otros litigios con contrapartes distintas de clientes
	EP- 5.3	Externalización de Procesos CORE o críticos
	EP- 5.4	Deficiencia en la Selección y Contratación de Proveedores
	EP- 5.5	Litigios con distribuidores/Proveedores
	EP- 5.6	Concentración de Proveedores

CATEGORIZACION DE EVENTOS DE RIESGOS DE OPERACION - EVENTOS

Gestión de Riesgos Operativos **Código del Formato: GRO-12**

Tipo de Evento	Código	Ejemplos
Daños a activos materiales	**DA**	
Desastres y otros acontecimientos	**DA- 1**	
	DA- 1.1	Desastres naturales (Inundación, Sismo, Incendio, endemias, epidemias, pandemias;etc.)
	DA- 1.2	Pérdidas humanas por causas externas (terrorismo, vandalismo, conmoción civil, huelgas, etc.)
	DA- 1.3	Daños al activo por causas externas o desastres naturales
Incidencias en el negocio y	**TI**	
Sistemas	**TI- 1**	
	TI- 1.1	Hardware
	TI- 1.2	Software
	TI- 1.3	Telecomunicaciones
	TI- 1.4	Interrupción/Incidencias en los suministros (energía, etc.)
	TI- 1.5	Otros

SUNASA
I.R.A.R.

SUNASA

CATEGORIAS DE ORIGEN DE RIESGOS DE OPERACION - ORIGEN

Gestión de Riesgos Operativos **Código del Formato: GRO-13**

Categoría	Código	Sub- Categoría	Descripción
PERSONAS	PE		Riesgo asociado con el personal propio de la Institución
	PE1	Personal Inadecuado	No se cuenta con personal adecuado para la ejecución de las funciones encargadas, en términos de formación académica, competencias, especialización, aptitudes, experiencia laboral previa, años de servicio, etc.
	PE2	Personal insuficiente	No se cuenta con la cantidad de personal suficiente para el desempeño de las funciones encargadas, o el procesamiento del volumen de transacciones requerido, durante el horario normal de labores.
	PE3	Desempeño Inadecuado	El personal no desempeña sus funciones satisfactoriamente de acuerdo a los requerimientos del puesto.
	PE4	Dependencia de personal clave	La satisfactoria ejecución de las actividades de la unidad o proceso depende del conocimiento o habilidades de un número limitado de colaboradores. Los conocimientos requeridos para el desempeño de una tarea están concentrados en pocas personas y no se encuentran debidamente documentados.
	PE5	Excesiva Rotación de personal	El personal que ejecuta una función o actividad es cambiado frecuentemente.
	PE6	Actitud Deshonesta	El personal no desarrolla sus actividades con honestidad, ni de acuerdo al Código de Etica, Reglamentos Internos de trabajo, MOF, ROF y Valores de la institución.
	PE7	Infraestructura y logística Inadecuada	Espacio físico o infraestructura o logística inapropiada para el desarrollo de las actividades propias del puesto o actividad.
	PE8	Inadecuado Clima Laboral	No se cuenta con incentivos o beneficios apropiados para el desempeño de sus funciones, conflictos no resueltos, falta de motivación, entre otros.
PROCESOS	PR		Es el Riesgo asociado con los Procesos Internos de la Institución
	PR1	Procesos mal definidos o ausencia de los mismos	Objetivos, funciones, estructura, políticas, procedimientos y controles mal definidos; Complejidad; Exceso de volumen; Falta de documentación. Inconsistencias en los procesos.
	PR2	Incumplimiento y errores en el proceso	Falta de cumplimiento del flujo definido; Error de registros.
	PR3	Falta o deficiencia de controles	Falta o deficiencia en mecanismo que permita prevenir o detectar oportunamente la ocurrencia de eventos no deseados.
TECNOLOGIA	TE		Es el Riesgo asociado con la Tecnología y Seguridad de la Información de la Institución
	TE1	Falta de Confidencialidad	Divulgación de información confidencial a personas no autorizadas.
	TE2	Falta de Integridad	La información proporcionada por los sistemas o reportes no es veraz, consistente o completa.
	TE3	Falta de Disponibilidad	Los sistemas no se encuentran disponibles en la oportunidad y con las funcionalidades en que son requeridos para el desarrollo de las funciones.
	TE4	Problemas de calidad del software	Falta de interoperabilidad de los sistemas, idoneidad,eficiencia, usabilidad, entre otros.
	TE5	Seguridad de Información	Falta o deficiencia de los accesos, soporte, back ups, plan de contingencia (DRP), entre otros.
	TE6	Sofwares y Hardwares no autorizados	Programas, Sistemas o Equipos que no han pasado por el protocolo de seguridad de información.
RELACION CON TERCEROS	RT		Es el Riesgo asociado por la interacción con personas ajenas a la institución
	RT1	Inapropiada provisión de bienes o servicios por parte de proveedores externos	Incumplimiento por parte del proveedor de condiciones de calidad, oportunidad y costo que afectan el desempeño de las actividades de la unidad o proceso. Concentración de proveedores, falta de identificación de proveedores críticos y planes de contingencia.

SUNASA I.R.A.R.

SUNASA

CATEGORIAS DE ORIGEN DE RIESGOS DE OPERACION - ORIGEN

Gestión de Riesgos Operativos **Código del Formato: GRO-13**

Categoría	Código	Sub- Categoría	Descripción
	RT2	Acciones legales adversas	Incumplimiento de condiciones contractuales; falta de contratos; Incumplimiento de normas legales; negligencia de lo ofrecido.
EVENTOS EXTERNOS	EE		Es el Riesgo asociado por eventos fuera del alcance de la institución
	EE1	Conducta indebida de terceros	Substracción ilícita de activos por terceros; Daño intencional a la institución por terceros
	EE2	Daños a la infraestructura y activos	Desastres naturales y civiles; Por incendio; endemias, epidemias, pandemias; Fallas en el transporte, energía y telecomunicación externa; entre otros.
	EE3	Cambios regulatorios	Cambios en la regulación del país; Cambios en los regímenes tributarios y de mercado
	EE4	Problemas políticos/gobierno	Bloqueo de negocio; Expropiación de activos; Guerra; Inestabilidad política.
	EE5	Eventos con impacto mediático	Noticias, denuncias y otros que afecten el servicio al cliente, salud del asegurado o paciente, vida humana, privacidad, impacto financiero, requerimientos legales-regulatorios, ventaja competitiva y/o imagen pública.

SUNASA I.R.A.R.

SUNASA

CATEGORIAS DE CONTROLES ESTANDARES

Gestión de Riesgos Operativos **Código del Formato: GRO-14**

Para cada instancia de control existente y/o por implementar, realizar una estimación cualitativa de la atenuación del Riesgo de Operación que se logra a través del control.

De la siguiente tabla seleccionar la descripción, que a su juicio mas se aproxime a este nivel de control.

Código	Controles
C1	Inventario Físico / Arqueo
C2	Inspección / Revisiones Internas
C3	Documentación de Transacciones
C4	Reporte de Conciliación
C5	Reporte de Excepciones
C6	Cruce de Información / Comparaciones
C7	Control de Acceso
C8	Verificación de Firmas
C9	Verificación de Autonomías / Autorización / Aprobación (VºBº)
C10	Verificación de Requisitos / Validaciones
C11	Almacenamiento Seguro
C12	Protección Física
C13	Indicadores de Gestión
C14	Respaldo (Back Up) de Información
C15	Bitácoras de accesos, cambios y operaciones en sistemas
C16	Planes de Continuidad de Negocios / Planes de Contigencia o alternos
C17	Plan de Mantenimiento
C18	Actualización de Hardware y Software
C19	Definición de perfiles de usuarios
C20	Segregación de Funciones Incompatibles
C21	Peritaje u Opinión de Expertos
C22	Capacitación de Personal
C23	Supervisión del Personal
C24	Evaluación de Desempeño
C25	Descripción de los Puestos de Trabajo
C26	Reclutamiento de Personal Calificado
C27	Otros

SUNASA I.R.A.R.

SUNASA

CLASIFICACION DE LOS CONTROLES

Gestión de Riesgos Operativos **Código del Formato: GRO-15**

Para cada instancia de control existente y/o por implementar, realizar una estimación cualitativa de la atenuación del Riesgo de Operación que se logra a través del control.

De la siguiente tabla seleccionar la descripción, que a su juicio mas se aproxime a este nivel de control.

Nivel	Descripción
Preventivo y/o Concurrente Manual	Un procedimiento o actividad que previene que un error o evento de riesgo ocurra y que se puede ejecutar durante la actividad. La ejecución está a cargo de alguna persona.
Preventivo y/o Concurrente de Aplicación	Un procedimiento o actividad que previene que un error o evento de riesgo ocurra y que se puede ejecutar durante la actividad. El control lo ejecuta un programa de una aplicación computarizada.
Detectivo Manual	Un procedimiento o actividad que identifica un error o evento de riesgo después que la transacción ha ocurrido. La ejecución está a cargo de alguna persona.
Detectivo De Aplicación	Un procedimiento o actividad que identifica un error o evento de riesgo después que la transacción ha ocurrido, pero el control lo ejecuta un programa de una aplicación computarizada.
Generales de TI	Controles fundamentales (accesos, cambios, planificación y monitoreo) sobre los procesos del área de tecnología de información.

SUNASA I.R.A.R.

SUNASA

NIVELES DE CONTROL DE RIESGOS DE OPERACION

Gestión de Riesgos Operativos **Código del Formato: GRO-16**

Para cada instancia de control existente y/o por implementar, realizar una estimación cualitativa de la atenuación del Riesgo de Operación que se logra a través del control.

De la siguiente tabla seleccionar la descripción, que a su juicio mas se aproxime a este nivel de control.

Puntos	Descripción
Estricto (Optimizado)	Riesgo transferido a terceros.
	Integrados con el monitoreo en tiempo real.
	Automatización y herramientas son usadas para apoyar los controles y permiten ejecutar cambios rápidos en las actividades de control.
	Definición explícita de supervisión cruzada continua.
	Atención especial de Auditores Internos, Externos y Reguladores
Alto (Monitoreado)	Automatización y herramientas son usadas para apoyar los controles.
	Existen pruebas periódicas para evaluar la efectividad del diseño y existen reportes para la gerencia.
	Existe una definición explícita de supervisión por Jefatura de Servicio / Gerencia dentro de la misma línea
	Perfiles de acceso específicos por persona
	Contraseñas alfa-numéricas que se cambian cada cierto tiempo.
	Mecanismos duales de autenticación
	Reportes de control revisados como parte de una rutina diaria
Regular (Estandarizado)	Están bien diseñados, en sus lugares y documentados.
	Existe supervisión de pares y/o a nivel jefaturas de Departamento
	Los perfiles de acceso son masivos, pero específicos por puesto
	Mecanismos de autenticación basados en contraseñas estáticas
	Mecanismos establecidos para obtener diversos reportes de control
	No es una actividad auditada regularmente a nivel de detalle
Bajo (Informal)	Están Bien diseñados.
	Están en sus lugares pero no están documentados.
	Dependen de los empleados.
	No hay capacitación ni comunicación formal.
	Existen posibilidades de control (ejemplo reportes), pero no se utilizan de manera regular; sólo ante incidentes
	Los perfiles de acceso son generales
Inexistente (No Confiable)	No están bien diseñados.
	No están en sus lugares.
	No existen controles definidos
	En caso de sistemas, no se cuenta con criterios de autenticación / autorización

SUNASA REPÚBLICA DEL PERÚ T.R.A.R.

SUNASA

IMPACTO CUALITATIVO EN LA IAFAS

Gestión de Riesgos Operativos **Código del Formato: GRO-17 A**

Para cada instancia de Riego de Operación identificada, realizar una estimación cualitativa del impacto financiero que tendría el evento.

De la siguiente tabla seleccionar la descripción, que a su juicio más se aproxime a este nivel de impacto financiero y consignar la correspondiente cantidad de puntos en la matriz de calificación de riesgos de operación:

Puntos	Nivel	Descripción
26	Extremo	Pérdida Financiera mayor a 1% del margen bruto o presupuesto
		Endeudamiento Patrimonial- Mayor a 2%
		Existencia de debilidad material. (3)
16	Mayor	Pérdida Financiera mayor a 0.7% a 1% del margen bruto o presupuesto
		Endeudamiento Patrimonial- Mayor a 1.6% y meno o igual a 2%
		Existencia de deficiencia significativa.(2)
5	Moderado	Pérdida Financiera mayor a 0.4% a 0.7% del margen bruto o presupuesto
		Endeudamiento Patrimonial- Mayor a 1.4% y menor o igual a 1.6%
		Existencia de deficiencia de control.(1)
2	Menor	Pérdida Financiera mayor a 0.1% a 0.4% del margen bruto o presupuesto
		Endeudamiento Patrimonial- Mayor a 1% y menor o igual a 1.4%
1	Insignificante	Pérdida Financiera menor al 0.1% del margen bruto o presupuesto
		Endeudamiento Patrimonial- menor o igual a 1%

SUNASA I.R.A.R.

Pérdida Financiera: Es la probabilidad de que ocurra un evento que tenga consecuencia financieras negativas, generando gastos en los Estados o Reportes financieros/control generados por riesgos operativos.

(1) Deficiencia de Control: Existe una deficiencia de control cuando el diseño u operación de un control no permite a la Gerencia o empleados prevenir o detectar errores oportunamente, en el desempeño de sus funciones. Se debe determinar si las excepciones de control son Deficiencias de Control. Analizar y evaluar los errores y excepciones de control identificados en la ejecución de las pruebas y a través de otras fuentes, para determinar si representan Deficiencias de Control.

- Una deficiencia en el diseño existe si (a) falta un control necesario para cumplir con los objetivos del control; o (b) un control existente no está bien diseñado y aunque el control opera según el diseño no se logra el objetivo del control.

- Una deficiencia operativa existe si (a) un control bien diseñado no opera según el diseño previsto; o (b) la persona que ejecuta el control no posea la autoridad o competencias necesarias para ejecutarlo efectivamente.

(2) Deficiencia Significativa: Una deficiencia significativa es una deficiencia de control, o combinación de deficiencias de control, que afectan adversamente la habilidad de la compañía para iniciar, autorizar, registrar, procesar o reportar información financiera externa confiable de acuerdo con principios de contabilidad generalmente aceptados, de manera que exista una probabilidad más que remota de que un error más que inconsecuente en los estados financieros anuales o interinos o reportes de control, no sea prevenido o detectado.

(3) Debilidad Material: Una deficiencia significativa que por sí misma, o en combinación con otras deficiencias significativas, resulta en una probabilidad más que remota de que un error importante para los estados financieros interinos o anuales o reportes de control, no sea prevenido o detectado.

SUNASA

PROBABILIDAD CUALITATIVA DE OCURRENCIA

Gestión de Riesgos Operativos **Código del Formato: GRO-18**

Para cada instancia de Riesgo de Operación identificada, realizar una estimación cualitativa de la probabilidad de ocurrencia que tendría el evento.

De la siguiente tabla seleccionar la descripción, que a su juicio mas se aproxime a este nivel de probabilidad y consignar la correspondiente cantidad de puntos en la matriz de calificación de riesgos de operación:

Puntos	Nivel	Descripción
5	Casi certeza	Eventos similares ocurren o pueden ocurrir todos los meses.
		Existencia de debilidad material. (3)
4	Probable	Eventos similares ocurren o pueden ocurrir cada 6 meses.
		Existencia de deficiencia significativa. (2)
3	Posible	Eventos similares ocurren o pueden ocurrir cada 1 año.
		Nivel de control Regular.
		Existencia de deficiencia de control.(1)
2	Improbable	Eventos similares ocurren pueden ocurrir cada 3 años.
		Nivel de control Alto.
1	Raro	Eventos similares ocurren o pueden ocurrir cada 5 años o no existe registro del evento.
		Nivel de control Estricto.

(1) Deficiencia de Control: Existe una deficiencia de control cuando el diseño u operación de un control no permite a la Gerencia o empleados prevenir o detectar errores oportunamente, en el desempeño de sus funciones. Se debe determinar si las excepciones de control son Deficiencias de Control. Analizar y evaluar los errores y excepciones de control identificados en la ejecución de las pruebas y a través de otras fuentes, para determinar si representan Deficiencias de Control.

- Una deficiencia en el diseño existe si (a) falta un control necesario para cumplir con los objetivos del control; o (b) un control existente no está bien diseñado y aunque el control opera según el diseño no se logra el objetivo del control.

- Una deficiencia operativa existe si (a) un control bien diseñado no opera según el diseño previsto; o (b) la persona que ejecuta el control no posea la autoridad o competencias necesarias para ejecutarlo efectivamente.

(2) Deficiencia Significativa: Una deficiencia significativa es una deficiencia de control, o combinación de deficiencias de control, que afectan adversamente la habilidad de la compañía para iniciar, autorizar, registrar, procesar o reportar información financiera externa confiable de acuerdo con principios de contabilidad generalmente aceptados, de manera que exista una probabilidad más que remota de que un error más que inconsecuente en los estados financieros anuales o interinos no sea prevenido o detectado.

(3) Debilidad Material: Una deficiencia significativa que por si misma, o en combinación con otras deficiencias significativas, resulta en una probabilidad más que remota de que un error importante para los estados financieros interinos o anuales no sea prevenido o detectado.

SUNASA

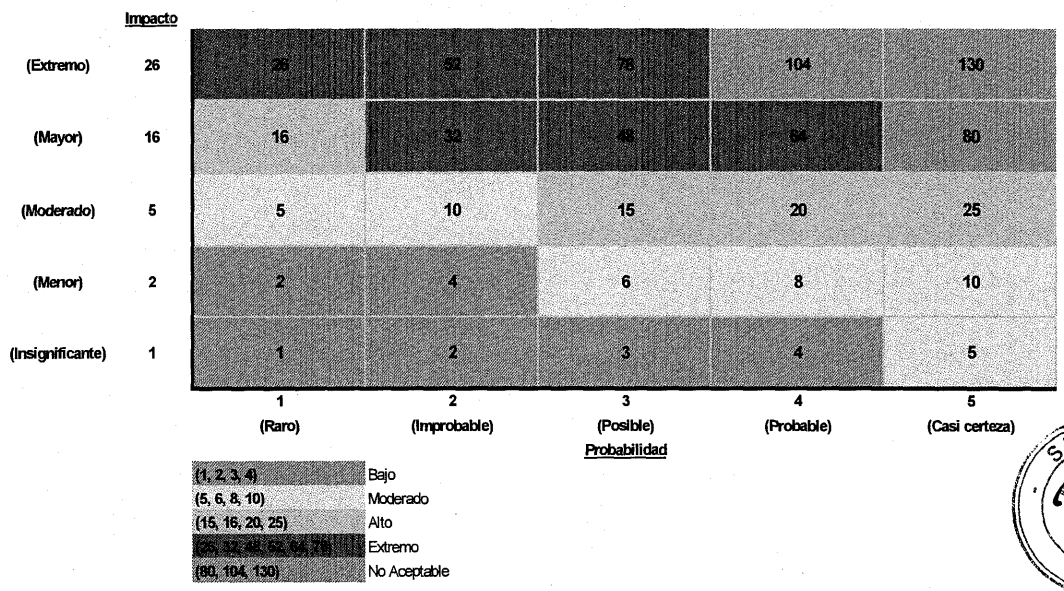
MATRIZ DE CRITICIDAD DE RIESGOS OPERATIVOS

Gestión de Riesgos Operativos **Código del Formato: GRO-19**

Para cada instancia del Riesgo de Operación Identificada, el nivel cualitativo de la misma se obtiene multiplicando los puntos asignados a impacto por los puntos asignados a probabilidad de ocurrencia.

El resultado se ubicara entre (impacto extremo y casi certeza de ocurrencia) y 1 (impacto insignificante y ocurrencia rara).

Matriz de Clasificación de Criticidad de Riesgos



Si bien cada riesgo de operación se evalúa de manera individual, la escala numérica permite una aproximación al nivel de riesgo operacional total (agregado) de un proceso y/o unidad.

Calificación	Criticidad	Descripción
1, 2, 3, 4	**Riesgo Bajo**	Requiere de una administración bajo los procedimientos de rutina establecidos.
5, 6, 8 y 10	**Riesgo Moderado**	Requiere de una administración y seguimiento permanente de parte de la Gerencia responsable. Adicional, los riesgos con puntos de 5 y 10 requieren un monitoreo permanente.
15, 16, 20 y 25	**Riesgo Alto**	Requiere de una evaluación cuidadosa y a corto plazo, de parte de la Gerencia responsable ("dueña" del riesgo), con seguimiento del Comité de Gestión de Riesgos de Operación.
26, 32, 48, 52, 64 y 78	**Riesgo Extremo**	Requiere de una evaluación cuidadosa e inmediata, de parte de la Gerencia responsable ("dueña" del riesgo), con seguimiento del Comité de Gestión de Riesgos de Operación.
80, 104 y 130	**Riesgo No Aceptable**	Requiere de algún tipo de acción o medida inmediata

SUNASA

TRATAMIENTO DE RIESGOS DE OPERACION

Gestión de Riesgos Operativos **Código del Formato: GRO-20**

Una vez identificado el nivel de Riesgo de Operación y los controles aplicados para su atenuación se debe decidir la opción de tratamiento.

De la siguiente tabla seleccionar la descripción, que a su juicio más se aproxime a la forma en que se tratará el riesgo identificado:

Puntos	Descripción
Evitar	El nivel de riesgo de la actividad es inaceptable
Transferir	Transferir a un tercero con capacidad financiera / especialización necesaria para administrar adecuadamente.
Reducir	Establecer controles para atenuación
Retener	Aceptar riesgo en su presente nivel. Establecer las medidas contingentes necesarias.
Aprovechar	Aceptar niveles de riesgo mayores al presente para aprovechar oportunidades detectadas

SUNASA

AREAS DE IMPACTO CUANDO SE MATERIALIZAN LOS RIESGOS OPERATIVOS

Gestión de Riesgos Operativos **Código del Formato: GRO-21**

La siguiente tabla contiene la descripción de las Áreas definidas como prioritarias, que pueden ser afectadas cuando se materializa un evento de Riesgo de Operación.

Esta información sirve para completar la Plantilla de Identificación de eventos de Riesgo de Operación.

Códigos	Nivel	Descripción
SC	**Servicio al Cliente**	La habilidad de la Entidad en proveer un servicio de excelencia a sus clientes-paciente/asegurado, a través de su personal, calidad de atención a los clientes-pacientes/asegurados y del suministro competitivo de productos, es crucial para su éxito. El servicio al cliente abarca tanto las expectativas que los clientes tienen de la Entidad así como la manera en que traten y atiendan a los clientes-pacientes/asegurados. La Entidad debe proveer un excelente servicio a sus clientes poniendo más atención en la calidad de servicio que en precios bajos. El servicio debe ser expeditivo, confiable y personalizado. Se espera que el personal conozca al cliente y al sector salud. Los sistemas de información y procesos de la Entidad tienen un rol clave en el suministro de esta calidad de servicio.
SA	**Salud del Asegurado o Paciente**	La Organizacion debe proteger y cuidar la salud, integridad física o mental y controlar, en lo posible, las enfermedades de los pacientes.
VH	**Vida Humana**	La Capacidad de la Entidad para evitar la pérdida de vida humana. Moralidad no relacionada con el curso natural de la enfermedad y que difiere de la evolución esperada.
PR	**Privacidad**	El mayor activo de la Entidad es la confianza de sus clientes-pacientes/asegurados. Es de suma importancia el ser un buen guardián de la información que posee acerca de sus clientes y de sus operaciones de negocio. La confidencialidad de la información específica de un cliente es su más alta prioridad.
IFE	**Impacto Financiero para la Entidad**	Las finanzas son la actividad primordial de la corporación, su razón de ser, así como, los efectos financieros de las decisiones y acciones deben tenerse en alta consideración.
IFP	**Impacto Financiero para el Paciente/Asegurado**	La materialización del riesgo puede generar un impacto financiero o desembolso al Paciente o Asegurado, además del impacto moral incluido en Servicio al Cliente.
LR	**Legal y Requerimiento Regulatorio**	La Entidad debe cumplir con todas las leyes y regulaciones aplicables. La exactitud y disponibilidad de información son requisitos para poder mantener necesarios niveles de cumplimiento y reporte. Los clientes de la Entidad podrían ver una infracción legal o regulatoria, relativamente pequeña, como una violación importante de la confianza depositada en ésta.
VC	**Ventaja Competitiva**	La Entidad debe obtener información de las necesidades de sus clientes y concerlos para obtener una ventaja competitiva y mejorar sus servicios.
IP	**Imagen Pública**	Un activo importante para una Entidad es su marca-nombre, así como su posición y reputación en el sector Salud. La revelación accidental, prematura o maliciosa de información, especialmente fuera de contexto, podría ser dañina para la reputación de la Entidad. El uso publicitado de información inexacta o no autorizada y los consecuentes efectos negativos podrían ser perjudiciales.

SUNASA I.R.A.R.

SUNASA

GUIA PARA LA IDENTIFICACION DE ACTIVOS DE INFORMACION CRITICOS DEL PROCESO

Gestión de Riesgos Operativos **Código del Formato: GRO-22**

1 **Identificar qué "información" importante utilizan los Usuarios del Proceso**
(Considerar que la información puede ser electrónica o física)

2 **Validar que la "información" esté debidamente protegida, ya que tiene un valor para la Entidad en términos de: imagen pública, servicio al cliente, privacidad, requerimientos legales, impacto financiero y/o ventaja competitiva?**

3 **¿Qué pasaría si esta "información" llegara a ser: ?**

- Conocida por individuos no autorizados (Confidencialidad),
- Indebidamente modificada o alterada de manera intencional o por accidente (Integridad) y/o
- No estuviera disponible cuando se requiera usarla (Disponibilidad).

4 **¿Podría la Entidad tener uno o varios de los siguientes impactos?:**

- Tener algún tipo de responsabilidad legal y/o perjuicio económico ante un cliente o empleado.
- Ser víctima de una estafa, operación fraudulenta o algún otro tipo de apropiación.
- Perder alguna ventaja competitiva y/o información propietaria.
- Afectar la privacidad de información del cliente/paciente/asegurado.
- Verse dañada la reputación ante los clientes.
- Producir un efecto directo de disminución de ingresos y/o aumento de costos.
- Generar inexactitudes en los estados financieros.
- Tomar decisiones erradas o no oportunas.
- Afectar la capacidad de proveer productos y servicios.