OGPP

REPUBLICA DEL PERU

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Resolución Ministerial

Lima, 04 de marzo de 2016 N° 081-2016-EF/10

CONSIDERANDO:

Que, el artículo 10 de la Ley N° 28716, Ley de Control Interno de las entidades del Estado, establece que la Contraloría General de la República, con arreglo a lo establecido en el artículo 14 de la Ley Nº 27785, dicta la normativa técnica de control que oriente la efectiva implantación y funcionamiento del control interno en las entidades del Estado, así como su respectiva evaluación; en ese sentido, dichas normas constituyen lineamientos, criterios, métodos y disposiciones para la aplicación y/o regulación del control interno en las principales áreas de su actividad administrativa u operativa de las entidades, incluidas las relativas a la gestión financiera, logística, de personal, de obras, de sistemas computarizados y de valores éticos, entre otras;

Que, mediante Resolución de Contraloría General N° 320-2006-CG se aprobaron las "Normas de Control Interno", con la finalidad de propiciar el fortalecimiento de los sistemas de control interno y mejorar la gestión pública;

Que, asimismo, con Resolución de Contraloría General N° 458-2008-CG, se aprobó la "Guía para la implementación del Sistema de Control Interno de las Entidades del Estado" como documento orientador para la gestión pública y el control gubernamental, sin perjuicio de la legislación que emitan los distintos niveles de gobierno, así como las normas que dicten los órganos rectores de los sistemas administrativos;

Que, en virtud de lo antes mencionado, mediante Resolución Ministerial N° 396-2012-EF/10, se conformó el Comité de Control Interno del Ministerio de Economía y Finanzas, el cual tiene a su cargo la elaboración del Sistema de Control Interno, su implementación, monitoreo y seguimiento; para cuyo efecto cuenta con una Secretaría Técnica ejercida por la Oficina General de Planificación y Presupuesto, órgano a cargo de emitir opinión técnica sobre directivas, lineamientos y otros instrumentos de gestión administrativa interna del Ministerio;

048235-16

200968-15

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Que, mediante la Cuarta Disposición Complementaria Final de la Ley N° 29953, Ley de Endeudamiento del Sector Público para el Año Fiscal 2013, se crea con carácter de permanente, el Comité de Riesgos en el Ministerio de Economía y Finanzas, cuyo Reglamento Operativo fue aprobado con Resolución Ministerial Nº 112-2013-EF/52, en el cual se establece que el Comité de Riesgos tiene competencia para revisar y evaluar los lineamientos y metodologías sobre la gestión del riesgo operacional que afecte o pueda afectar las finanzas públicas;

Que, el artículo 96 del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado con Decreto Supremo Nº 117-2014-EF, señala dentro de las funciones de la Dirección General de Endeudamiento y Tesoro Público, el conducir la gestión de riesgos, así como el diseñar y proponer las políticas, directrices y estrategias de gestión de riesgos financieros, operativos y contingentes fiscales de naturaleza jurídica y contractual, o derivados de desastres naturales, que afecten o puedan afectar a las finanzas públicas;

Que, para el cumplimiento de dichas funciones, la mencionada Dirección General cuenta dentro de su estructura orgánica con la Dirección de Gestión de Riesgos que tiene a su cargo el formular y proponer políticas, lineamientos, normas y estrategias de gestión de riesgos operacionales, así como formular y proponer modelos o metodologías de evaluación, clasificación y seguimiento de los riesgos operacionales, entre otras responsabilidades;

Que, en ese contexto, con Resolución Ministerial N° 270-2014-EF/10, se aprobó el Diagnóstico del Sistema de Control Interno del Ministerio de Economía y Finanzas y el Plan de Trabajo para la Implementación del Sistema de Control Interno del Ministerio de Economía y Finanzas, siendo que este último contiene las actividades a ser ejecutadas por los órganos y unidades orgánicas del Ministerio de Economía y Finanzas, estableciendo como actividad 76 por parte de la Dirección de Gestión de Riesgos de la Dirección General de Endeudamiento y Tesoro Público la siguiente: "Elaborar y aprobar los Lineamientos para la Gestión del Riesgo Operacional en el Ministerio de Economía y Finanzas";

Que, la gestión del riesgo operacional es un proceso continuo que permite identificar, valorar, mitigar y monitorear la posibilidad de ocurrencia de pérdidas financieras y no financieras debido a la inadecuación o fallas en los procesos internos, el personal, sistemas internos y tecnología de información, o a causa de acontecimientos externos, a fin que la presencia de tales eventos no afecte el desarrollo de las funciones y competencias de los diversos órganos del Ministerio, que impida la consecución de los objetivos del Ministerio;

Que, una adecuada gestión de los riesgos operacionales del Ministerio de Economía y Finanzas, que afectan o puedan afectar a las finanzas públicas, requiere de un enfoque integral en toda la organización, por lo que es necesario un trabajo conjunto y coordinado entre la Dirección de Gestión de Riesgos y la Oficina General de Planificación y Presupuesto;

Que, de esa manera, una buena gestión del riesgo operacional contribuye considerablemente al buen funcionamiento del Sistema de Control Interno en el Ministerio, siendo a su vez uno de sus componentes claves;

REPUBLICA DEL PERU

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
LIC. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Resolución Ministerial

Que, en ese sentido, la Dirección de Gestión de Riesgos de la Dirección General de Endeudamiento y Tesoro Público y la Oficina General de Planificación y Presupuesto han manifestado la necesidad de aprobar lineamientos que permitan implementar la Gestión del Riesgo Operacional de manera transversal, de modo que todos los órganos del Ministerio de Economía y Finanzas intervengan y contribuyan con su eficiente desarrollo; y,

De conformidad con la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo, la Resolución Ministerial N° 270-2014-EF/10, que aprueba el Diagnóstico del Sistema de Control Interno del Ministerio de Economía y Finanzas y el Plan de Trabajo para la Implementación del Sistema de Control Interno del Ministerio de Economía y Finanzas, y el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado con Decreto Supremo Nº 117-2014-EF;

SE RESUELVE:

Artículo 1.- Aprobar el documento "Lineamientos para la Gestión del Riesgo Operacional en el Ministerio de Economía y Finanzas", y sus anexos, cuyos textos forman parte integrante de la presente resolución ministerial, conforme al siguiente detalle:

- Anexo N° 01: "Metodología para la Gestión del Riesgo Operacional".
- Anexo N° 02: "Metodología para la Gestión del Riesgo en Tecnologías de la Información".

Artículo 2.- Publicar la presente Resolución Ministerial y sus anexos, en el Portal Institucional del Ministerio de Economía y Finanzas (www.mef.gob.pe), en el Intranet del Ministerio de Economía y Finanzas, y disponer su difusión a todo el personal del MEF mediante correo electrónico.

Regístrese y comuníquese.

ALONSO SEGURA VASI
Ministro de Economía y Finanzas

PERÚ | Ministerio de Economía y Finanzas

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
JUAN RAÚL LÓPEZ TORRES
FEDATARIO

LINEAMIENTOS
PARA LA GESTIÓN DEL RIESGO OPERACIONAL EN EL MINISTERIO DE ECONOMÍA Y FINANZAS

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Planificación y Modernización de la Gestión

ÍNDICE

LINEAMIENTOS PARA LA GESTIÓN DEL RIESGO OPERACIONAL EN EL MINSISTERIO DE ECONOMÍA Y FINANZAS

1. OBJETO

Establecer lineamientos generales y específicos para la gestión de los riesgos operacionales presentes en el Ministerio de Economía y Finanzas (MEF). Estos lineamientos servirán de medio de consulta para el personal que interviene en el proceso de gestión del riesgo operacional.

2. BASE LEGAL

2.1 Constitución Política del Perú.

2.2 Ley N° 29953 – Ley de Endeudamiento del Sector Público para el año fiscal 2013.

2.3 Decreto Supremo N° 117-2014-EF que aprueba el Reglamento de Organización y Funciones (ROF) del Ministerio de Economía y Finanzas.

2.4 Resolución Ministerial N° 112-2013-EF/52, que aprueba el Reglamento Operativo del Comité de Riesgos del Ministerio de Economía y Finanzas.

2.5 Resolución Ministerial Nº 270-2014-EF/10, que aprueba el Plan de Trabajo para la Implementación del Sistema de Control Interno en el Ministerio de Economía y Finanzas.

3. ALCANCE

Las instrucciones contenidas serán de aplicación general y de estricto cumplimiento por todo el personal del Ministerio de Economía y Finanzas (MEF) que interviene en la gestión del riesgo operacional.

4. DISPOSICIONES GENERALES

4.1 De las definiciones

4.1.1 Autoevaluación de Riesgos
Es el proceso por el cual se realizan dinámicas grupales con la finalidad de identificar, estimar, evaluar y tratar riesgos.

4.1.2 Coordinador de Control Interno
Personal de MEF responsable de la ejecución de las actividades conducentes al fortalecimiento e implementación del Sistema de Control Interno en el MEF, el cual también deberá apoyar al corresponsal de riesgo operacional en la recolección de información respecto a los riesgos operacionales identificados o a identificar.

4.1.3 Corresponsal de Riesgo Operacional
Personal del MEF responsable de implementar la gestión del riesgo operacional dentro del órgano o unidad orgánica del que forma parte.

4.1.4 Evento
Suceso o serie de sucesos derivados de los factores de riesgo operacional originados por la(s) misma(s) causa(s), que ocurre dentro un periodo de tiempo, afectando el curso normal de las diversas actividades del MEF.

4.1.5 Exposición al Riesgo
Medida que representa el grado de posibilidad de ocurrencia de un evento negativo o adverso, así como el impacto del mismo en el Ministerio al momento de materializarse.

4.1.6 Factores de Riesgo Operacional
Son aquellas categorías de fuentes originadoras de potenciales incidencias de riesgo operacional, relacionadas con fallas en las personas, procesos, sistemas internos y/o eventos externos.

4.1.7 Frecuencia
Es el número de ocurrencias de un evento en un periodo dado; también llamado Probabilidad, en términos cuantitativos.

4.1.8 Gestión del Riesgo Operacional
Es el proceso continuo efectuado por todos los niveles organizacionales del MEF que permite identificar, valorar y tratar riesgos operacionales, con la finalidad de coadyuvar en el logro de los objetivos del Ministerio.

4.1.9 Grado de exposición al riesgo
Es el nivel de riesgo que el MEF incurre en su búsqueda por cumplir con sus objetivos.

4.1.10 Incidencia de Riesgo Operacional
El evento que conduce a pérdidas o impide el logro de los objetivos de la organización y cuyo origen corresponde a factores de riesgo operacional.

4.1.11 Órganos de Alta Dirección
Son el Despacho Ministerial, el Despacho Viceministerial de Hacienda, el Despacho Viceministerial de Economía y la Secretaría General.

4.1.12 Órganos de Apoyo
Son la Oficina General de Administración (OGA), la Oficina General de Tecnologías de la Información (OGTI), la Oficina General de Servicio al Usuario (OGSU), Oficina General de Enlace, Oficina de Seguridad y Defensa Nacional (OSDENA) y Oficina de Comunicaciones.

4.1.13 Órganos de Asesoramiento
Son la Oficina General de Asesoría Jurídica (OGAJ) y la Oficina General de Planificación y Presupuesto (OGPP).

4.1.14 Órgano de Control Institucional
Es el órgano encargado de realizar el control gubernamental en el MEF, de conformidad con la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.

4.1.15 Órganos de Línea
Son las Direcciones Generales comprendidas en el Viceministerio de Hacienda y el Viceministerio de Economía de acuerdo al Reglamento de Organización y Funciones del MEF.

4.1.16 Planes de Acción
Programación de las actividades conducentes a reducir la exposición a los riesgos identificados y/o materializados. Los planes de acción son consolidados en el Plan de Gestión de Riesgos del MEF.

4.1.17 Riesgo Operacional
Es la posibilidad de ocurrencia de pérdidas o de incapacidad de cumplir correctamente con los objetivos del MEF debido a la inadecuación o a fallas en los procesos internos, el personal, sistemas internos y tecnologías de la información o bien a causa de eventos externos.

4.1.18 Riesgo en tecnologías de la información
La posibilidad de ocurrencia de pérdidas o de incapacidad de cumplir correctamente con los objetivos del MEF debido a los daños, interrupción, alteración o fallas derivadas de los sistemas físicos (hardware) e informáticos (software), aplicaciones de cómputo, redes y cualquier otro canal de distribución de la información, necesarios para la ejecución de procesos operacionales por parte de la institución.

Los riesgos en tecnologías de la información son parte de los riesgos operacionales asociados a actividades con soporte en recursos de tecnología de información, sistemas informáticos y tecnología inherente a dichos sistemas, los mismos que afectan el desarrollo de las actividades del Ministerio contra los principios de integridad, confidencialidad y disponibilidad de la información.

4.1.19 Severidad
Consecuencia o consecuencias de un evento, expresado en términos cualitativos, también llamado Impacto.

4.1.20 Tratamiento y Mitigantes del Riesgo
Conjunto de acciones de gestión de riesgos a realizar con respecto a los riesgos identificados. Dichas acciones incluyen el conjunto de directrices, procedimientos, técnicas, prácticas y

actividades a través de toda la organización, a todos los niveles y en todas las funciones, destinados a reducir el grado de exposición al riesgo.

4.1.21 Tolerancia al Riesgo
Es la desviación máxima en el grado de exposición al riesgo que el MEF tendría que aceptar.

4.2 De los lineamientos general para la gestión del riesgo operacional

4.2.1 Los órganos de la Alta Dirección del MEF, son los encargados de liderar y brindar los recursos necesarios para que los órganos del MEF, puedan realizar una correcta gestión del riesgo operacional

4.2.2 El MEF, conforme lo determine la Alta Dirección y el Comité de Riesgos, aplicará los lineamientos específicos y metodologías que formule la Dirección de Gestión de Riesgos para una adecuada gestión de riesgos

4.2.3 El MEF promoverá el fortalecimiento de la cultura de gestión del riesgo operacional y un ambiente interno que facilite su desarrollo adecuado. Para ello, el Comité de Riesgos será el encargado de promover una eficiente gestión del riesgo operacional.

4.2.4 Los Directores Generales, los Directores de Línea, los Corresponsales de Riesgo Operacional y personal involucrado en las diversas actividades del Ministerio, deberán gestionar el riesgo operacional en los procesos y servicios bajo su responsabilidad cumpliendo los lineamientos comprendidos en el presente documento.

4.2.5 La gestión de riesgo operacional es integral y abarca a toda la organización teniendo como base a los responsables a los diversos órganos que la componen.

El MEF a través de la Oficina General de Planificación y Presupuesto, en coordinación con la Dirección de Gestión de Riesgos (DGR), diseñará e implementará los mecanismos de monitoreo de los riesgos, y asegurará que se adopten las medidas de tratamiento necesarias para administrarlos, en forma consistente con los objetivos del MEF.

4.2.6 El MEF, a través de la Oficina General de Administración, brindará capacitación permanente en la Gestión de Riesgo Operacional a todo su personal, para lo cual procurará la inclusión de la temática en los instrumentos de gestión pertinentes (Plan de Desarrollo de Personas) en coordinación con la DGR, quien a su vez, deberá ser capacitada continuamente para realizar las acciones de asistencia y apoyo a

los distintos órganos y unidades orgánicas del MEF en la gestión de sus riesgos operacionales.

4.2.7 El MEF a través de programas de capacitación, concientización, talleres, seminarios, entre otros, promoverá en el personal altos estándares de ética e integridad y fortalecerá una cultura que enfatice la importancia de la gestión de los riesgos operacionales.

4.2.8 Es responsabilidad de todo el personal del MEF, independientemente de la relación contractual, bajo cualquier modalidad de contrato, coadyuvar en la gestión del Riesgo Operacional dentro del ámbito de su competencia.

4.2.9 El MEF, a través de la Oficina General de Administración, gestionará los riesgos operacionales asociados a las contrataciones y adquisiciones destinadas a los servicios críticos, con el fin que permitan a los proveedores coadyuvar en la gestión del Riesgo Operacional del MEF.

4.2.10 El MEF, a través de la Dirección de Gestión de Riesgos, promoverá gradualmente una cultura de gestión de riesgos operacionales que afecten o puedan afectar a las finanzas públicas en el MEF, mediante acciones coordinadas con otras Entidades del Sector.

4.2.11 Se reportará semestralmente los resultados de gestión y los riesgos operacionales identificados mediante el "Informe de Gestión de Riesgo Operacional", siendo la Dirección de Gestión de Riesgos responsable de elaborar dicho reporte. La Oficina General de Planificación y Presupuesto reportará también semestralmente el resultado del seguimiento de los planes de acción y del Plan de Gestión de Riesgos del MEF.

5. DISPOSICIONES ESPECÍFICAS

5.1 En cuanto a la gestión de incentivos:

5.1.1 Se debe establecer un sistema de incentivos no monetarios dirigidos a los Directores y corresponsales responsables de la gestión de los riesgos operacionales que afecten a los servicios que administran, tomando en cuenta la implementación efectiva de los planes de acción.

5.1.2 La Oficina de Recursos Humanos, en coordinación con la Dirección de Gestión de Riesgos y la Oficina General de Planificación y Presupuesto, diseñará una propuesta anual de incentivos no monetarios.

5.1.3 La Oficina General de Planificación y Presupuesto en coordinación con la Dirección de Gestión de Riesgos reportará

periódicamente a cada Director General los resultados que van obteniendo respecto al cumplimiento de sus planes de acción para la gestión del riesgo operacional.

5.1.4 Cada órgano o unidad orgánica es responsable de informar sobre incidencias de riesgos operacionales a través de sus corresponsables designados / certificados; así mismo, son responsables de informar acerca de situaciones que impidan la correcta implementación de medidas de tratamiento o mitigación para los riesgos calificados como extremos y altos.

5.2 **En cuanto al grado de exposición al riesgo y a la tolerancia al riesgo operacional:**

5.2.1 El MEF gestionará los riesgos operacionales a los que está expuesto, como producto de sus funciones y en cumplimiento de sus objetivos trazados, siendo la Dirección de Gestión de Riesgos la encargada de apoyar y asistir a los demás órganos en la gestión de sus riesgos operacionales y la Oficina General de Planificación y Presupuesto la encargada de monitorear los planes de acción para dicha gestión.

5.2.2 Los diferentes grados de exposición al riesgo son: Bajo, Moderado, Alto y Extremo y se describen en la Metodología para la Gestión del Riesgo Operacional.

5.2.3 El MEF podrá aceptar, como tolerancia al riesgo operacional para el cumplimiento de sus funciones, llegar a un límite de exposición de riesgo (luego de aplicadas las medidas del tratamiento y mitigación de riesgo) de hasta un nivel "Moderado" (zona amarilla).

5.2.4 La Dirección de Gestión de Riesgos y la Oficina General de Planificación y Presupuesto brindarán asistencia en la definición de las medidas de mitigación a los riesgos identificados, en forma participativa con los distintos órganos y unidades orgánicas, aprobándose de forma consensuada un Plan de Trabajo, que permita que la exposición al riesgo disminuya.

5.3 **De los relacionados al factor personas:**

5.3.1 El proceso de administración de personal deberá contemplar un proceso de inducción considerando los valores institucionales, el Código de Ética de la Función Pública[1], entre otros, contribuyendo con esto a mitigar parte de los riesgos operacionales generados por las personas.

---

[1] *Ley Nº 27815 - Ley del Código de Ética de la Función Pública*

5.3.2 El proceso de administración de personal, incluyendo su selección y evaluación deberá considerar los valores de transparencia, honestidad, integridad y otros factores, mitigando así los riesgos operacionales que puedan originarse por las personas.

5.3.3 Todo el personal del MEF, independientemente de su relación contractual, deberá tener claramente definidas sus funciones y responsabilidades del puesto y cargo que desempeña, con una segregación de funciones orientada a minimizar la exposición a los riesgos operacionales, para lo cual los instrumentos técnicos de gestión deben alinearse a los presentes lineamientos.

5.3.4 El personal del MEF deberá cumplir con sus funciones, manteniendo siempre una actitud proactiva frente a la gestión del riesgo operacional.

5.4 **De los relacionados al factor Procesos:**

5.4.1 El MEF deberá contar con un Plan de Continuidad del Negocio (o Plan de Continuidad Operativa) que tendrá como objetivo asegurar la continuidad de los procesos considerados críticos que soportan las operaciones y servicios que brinda el MEF.

5.4.2 Los servicios críticos del MEF, que dependan altamente de sistemas informáticos, deberán contar con planes de contingencia específicos los cuales deberán ser probados y documentados.

5.4.3 La prestación de servicios y abastecimiento para el desarrollo de los servicios críticos del Ministerio, por parte de un tercero, considerarán en sus contratos aspectos relacionados a los riesgos operacionales que podrían originarse por la prestación de dichos servicios, además de Planes de Continuidad del Negocio, de ser el caso.

5.4.4 Para considerar como medidas de mitigación implementadas para los principales riesgos, estas deberán estar definidas y contar con un procedimiento específico donde se describa la actividad a realizar, periodicidad y responsable de realizarla.

5.5 **De los relacionados al factor tecnologías de la información:**

5.5.1 La Oficina General de Tecnologías de la Información define los procedimientos específicos para la gestión de los riesgos en tecnologías de la información, de forma coordinada con la Dirección de Gestión de Riesgos, valiéndose de los criterios establecidos en los lineamientos y metodologías establecidas para la gestión de riesgos.

5.5.2 La prudente gestión de los riesgos asociados a la seguridad de información, se administra a través de las políticas y procedimientos para la Gestión de la Seguridad de la Información.

5.5.3 La gestión de los riesgos en tecnologías de la información que conlleven retrasos en un servicio o proceso es responsabilidad de cada órgano u unidad orgánica. Aquellos riesgos en tecnologías de la información inherentes a la gestión de la infraestructura, plataforma, o mantenimiento de los recursos de TI que se encarga de brindar el servicio o ser medio de soporte a la ejecución del proceso, serán de responsabilidad de la Oficina General de Tecnologías de la Información.

5.5.4 El MEF contará con un Sistema de Gestión de Seguridad de la Información conforme a la normatividad aplicable, de tal forma que se garantice la seguridad de la información en términos de confidencialidad, integridad y disponibilidad de los activos de información.

5.5.5 Los sistemas, medios de almacenaje y servicios de terceros que respaldan servicios críticos dentro del Ministerio deberán sujetarse a la Política de Seguridad de la Información del Ministerio.

5.6 **De los relacionados al factor eventos externos:**

5.6.1 Los riesgos derivados de desastres asociados a fenómenos naturales, disturbios, atentados, incendios, guerras externas e internas, cortes de servicios de comunicación e internet, hacking, entre otros, deberán mitigarse por medio del uso de seguros, planes de continuidad del negocio (o de continuidad operativa) u otros mecanismos que se estimen apropiados. Los seguros deberán tener la cobertura más amplia posible y deberán ser objeto de pago puntual y de procesos de renovación y contratación que garanticen la no interrupción de las coberturas.

5.6.2 El Grupo de Trabajo denominado Comité de Seguridad de la Información deberá establecer las condiciones mínimas a cumplir por los proveedores de servicios críticos del MEF, y el Oficial de Seguridad de la Información es responsable de asegurar el cumplimiento de las políticas de Seguridad de la Información.

5.7 **En cuanto a la identificación y la valorización de riesgos**

5.7.1 La Dirección de Gestión de Riesgos desarrollará las metodologías para la gestión de los riesgos operacionales y otra metodología específica para la gestión de los riesgos en tecnologías de la información. Asimismo, conducirá la

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
OGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Planificación y Modernización de la Gestión

formulación, operación y seguimiento del Plan de Continuidad del Negocio (o Continuidad Operativa) del MEF.

5.7.2 Las propuestas de modificación organizacional o de nuevos procesos serán sometidas a una evaluación de riesgos operacionales de acuerdo a las metodologías desarrolladas por la Dirección de Gestión de Riesgos.

5.7.3 El MEF, a través de sus órganos, realizará la autoevaluación de riesgos operacionales. Dicha autoevaluación será coordinada con la Dirección de Gestión de Riesgos y la Oficina General de Planificación y Presupuesto, y en ésta se identificarán y valorarán los riesgos operacionales inherentes a las funciones y las medidas de mitigación existentes definidos para dichos riesgos, teniendo en cuenta su diseño y efectividad, analizando la mejora o deterioro del perfil de riesgo para la determinación de las acciones a realizar.

5.8 **En cuanto al tratamiento y monitoreo del Riesgo Operacional**

5.8.1 Los Corresponsales de Riesgo Operacional, tienen a su cargo el monitoreo de la implementación de las medidas de mitigación para los riesgos identificados en los procesos de evaluación de riesgos operacionales. Dichos mitigantes serán ejecutados por los órganos del MEF, siendo supervisados por la Oficina General de Planificación y Presupuesto, quien proporcionará copia de los informes periódicos a la Alta Dirección, al Comité de Gestión de Riesgos, al Comité de Control Interno y a la Dirección de Gestión de Riesgos en calidad de Secretaría Técnica del Comité de Riesgos

5.8.2 Las incidencias de riesgo operacional serán evaluadas y tratadas por los órganos y/o dueños del proceso donde ocurrió; y la responsabilidad de monitorear el cumplimiento de los planes de acción será de acuerdo al grado de exposición al riesgo determinado.

5.9 **En cuanto a la información y comunicación del Riesgo Operacional**

5.9.1 El personal del MEF reportará a la Dirección de Gestión de Riesgos y a la Oficina General de Planificación y Presupuesto, las incidencias ocurridas, como producto del cumplimiento de sus funciones; el envío de dicha información deberá realizarse a través de los canales definidos por la metodología de gestión de riesgo operacional.

5.9.2 Los dueños de los procesos y/o Directores o Jefes de los Órganos o Unidades Orgánicas involucrados, remitirán a la Dirección de Gestión de Riesgos y a la Oficina General de Planificación y Presupuesto, información de manera periódica y

mediante los canales de transmisión establecidos, acerca de los riesgos monitoreados.

5.9.3 La Dirección de Gestión de Riesgos presentará un informe semestral o cuando lo solicite la Alta Dirección, conteniendo entre otros temas, aspectos relevantes de la gestión de riesgo operacional dentro del MEF, así como aspectos de gestión de la continuidad operativa.

5.9.4 La Oficina General de Planificación y Presupuesto presentará un informe semestral sobre la implementación por los órganos y entidades orgánicas de los planes de acción y del Plan de Gestión de Riesgos del MEF

5.9.5 Los proyectos de mejoras operativas que involucren una solución tecnológica, antes de su implementación y su respectiva evaluación de riesgos de acuerdo a las metodologías, deberán ser comunicados por los órganos involucrados a la Dirección de Gestión de Riesgos, para su opinión en cuanto sea pertinente. Previamente, deberán haber sido siempre discutidos y coordinados con la Oficina General de Tecnologías de la Información.

5.9.6 La Dirección de Gestión de Riesgos remitirá información relacionada a las incidencias ocurridas o riesgos identificados en el MEF, a los órganos competentes.

5.10 **En cuanto a la gestión del Riesgo en Tecnologías de la Información**

5.10.1 La Oficina General de Tecnologías de la Información participará de forma activa en la Gestión de Riesgos en Tecnologías de la Información proponiendo mecanismos de tratamiento y seguimiento, así como en la definición de medidas de mitigación y otros que sean necesarios para garantizar un nivel de riesgo acorde con el grado de exposición al riesgo del MEF.

5.10.2 El MEF elaborará un Plan de Recuperación Tecnológica para los aplicativos/servicios críticos coherente con el Plan de Continuidad del Negocio Global (o Continuidad Operativa), y un Sistema de Gestión de Seguridad de la Información tomando en cuenta los riesgos en tecnologías de la información.

5.10.3 La Oficina General de Tecnologías de la Información deberá hacer de conocimiento del personal del MEF las políticas, lineamientos, directrices y otras normativas relacionadas a la seguridad de la información en el MEF.

5.10.4 Los responsables de proyectos que involucren cambios significativos en el MEF y que hagan uso de una solución tecnológica deberán realizar un análisis de riesgos operacionales y después de su implementación; para ello utilizarán las

metodologías y formatos de evaluación elaborados por la Dirección de Gestión de Riesgos.

5.11 **En cuanto a la actualización**

5.11.1 La Dirección de Gestión de Riesgos propondrá los lineamientos para la Gestión del Riesgo Operacional y sus actualizaciones, las cuales serán remitidas al Comité de Riesgos para su revisión y a la Alta Dirección para su aprobación.

5.12 **En cuanto a la interpretación**

5.12.1 Las consultas referidas a la aplicación e interpretación de las normas, lineamientos y metodologías para la Gestión del Riesgo Operacional serán presentadas a la Dirección de Gestión de Riesgos.

6. RESPONSABILIDADES

6.1 **De la Alta Dirección:**

6.1.1 Es el responsable final de la gestión de los riesgos operacionales asociados a los servicios ofrecidos por las diversas áreas en los que opera el MEF.

6.1.2 Aprueba y emite los lineamientos de gestión de riesgo operacional y sus actualizaciones.

6.1.3 Garantiza la asignación de recursos necesarios para el adecuado desarrollo de la Gestión de Riesgos Operacionales, a fin de contar con la infraestructura, metodología y personal apropiados.

6.1.4 Promueve el proceso de gestión de riesgo operacional en el MEF.

6.1.5 Establece un sistema de gestión que fomente el adecuado funcionamiento de la gestión de riesgos operacionales.

6.2 **Del Comité de Riesgos:**

6.2.1 Revisa y evalúa las políticas, directrices, estrategias, lineamientos y metodologías sobre la gestión de riesgo operacional propuestas por la Dirección de Gestión de Riesgos, así como las actualizaciones de las mismas, de tal forma que se garantice una adecuada gestión de los riesgos operacionales.

6.2.2 Toma las acciones necesarias para asegurar la efectividad del proceso de gestión de riesgo operacional dentro del MEF.

6.2.3 Propone al Ministro las acciones necesarias para la implementación de medidas preventivas o correctivas requeridas para el adecuado cumplimiento de los objetivos del Ministerio, en materia de riesgos operacionales.

6.2.4 Revisa y propone las mejoras al Sistema de Gestión de Seguridad de la Información y el Plan de Continuidad del Negocio conducidos por la Oficina General de Tecnologías de la Información y la Dirección de Gestión de Riesgos respectivamente, en coordinación con los órganos competentes.

6.3 **De la Dirección de Gestión de Riesgos:**

6.3.1 Diseña y propone los lineamientos, directrices y estrategias de gestión de riesgo operacional.

6.3.2 Asiste a los diversos órganos involucrados en identificar y valorar los riesgos operacionales en coordinación con la Oficina General de Planificación y Presupuesto.

6.3.3 Desarrolla las metodologías para gestión del riesgo operacional y riesgos asociados a la tecnologías de la Información en coordinación con los órganos competentes; los mismos que incluyen entre otros la continuidad del negocio y la seguridad de la información.

6.3.4 Centraliza y sistematiza, en coordinación con la Oficina General de Planificación y Presupuesto, la información de los riesgos operacionales de todos los órganos del MEF.

6.3.5 Evalúa el riesgo operacional de los proyectos de mejoras operativas que involucren una solución tecnológica en coordinación con los órganos involucrados.

6.3.6 Elabora reportes sobre la gestión del riesgo operacional en el MEF.

6.3.7 Conduce el proceso de formulación y operación del Plan de Continuidad del Negocio del MEF y el seguimiento de su cumplimiento en lo referido a los riesgos operacionales.

6.3.8 Participa, en coordinación con la Oficina General de Tecnologías de la Información, en la elaboración del Plan de Seguridad de la Información en lo referido al análisis de riesgos en tecnología de la información.

6.3.9 Asiste a los órganos del MEF para la aplicación de la Metodología de Gestión del Riesgo Operacional y de Riesgos en Tecnologías de la Información.

6.3.10 Colabora con la Oficina General de Planificación y Presupuesto, en su calidad de Secretaría Técnica del Comité de Control Interno, para fortalecer el buen funcionamiento del Sistema de Control Interno en el MEF.

6.4 **De los Órganos del MEF:**

6.4.1 Identifican y valoran sus riesgos operacionales con la asistencia de la Dirección de Gestión de Riesgos y están encargados de implementar las medidas de mitigación en coordinación con la Oficina General de Planificación y Presupuesto.

6.4.2 Colaboran en la Gestión de los Riesgos Operacionales en coordinación con la Dirección de Gestión de Riesgos y con la Oficina General de Planificación y Presupuesto.

6.4.3 Son responsables de coordinar con los órganos pertinentes los recursos para la ejecución de las actividades conducentes a fortalecer o implementar la gestión de riesgos operacionales en sus respectivos órganos.

6.4.4 Son responsables de la gestión de sus riesgos operacionales.

6.5 **De los Corresponsales de Riesgo Operacional:**

6.5.1 Asistir al Director de cada órgano o unidad orgánica en la administración de los riesgos operacionales.

6.5.2 Autoevaluación de riesgos operacionales

i. Gestionar la identificación y valorización de riesgos a través del proceso de autoevaluación (con los expertos en el servicio).
ii. Garantizar la veracidad e integridad de los resultados de las autoevaluaciones de riesgos.
iii. Velar por el cumplimiento de los lineamentos para la gestión del Riesgo Operacional

6.5.3 Recolección de incidencias de riesgos operacionales

i. Gestionar la identificación y reporte de incidencias de riesgos operacional materializadas
ii. Monitorear e informar a la Dirección de Gestión de Riesgos respecto a cada incidente de Riesgo Operacional encontrado dentro del área de su competencia.

6.5.4 Medidas de mitigación propuestas

MINISTERIO DE ECONOMÍA Y FINANZAS 07 MAR. 2016

Dirección de Gestión de Riesgos - DGETP - MEF - GREGORIO BELAUNDE MATOSSIAN DIRECTOR

i. Identificar los riesgos que necesitan mitigantes adicionales de acuerdo a los lineamientos para la gestión del riesgo operacional del Ministerio.
ii. Realizar el monitoreo a la ejecución de las medidas de mitigación propuestas, informando periódicamente al Director, al Coordinador de Control Interno y a la Dirección de Gestión de Riesgos.
iii. Comunicar los cambios significativos en el plazo o forma de implementar las medidas de mitigación propuestas.

6.6 **De la Oficina General de Tecnologías de la Información:**

6.6.1 Implementar el Sistema de Gestión de la Seguridad de la Información en el Ministerio.

6.6.2 Gestionar la implementación de la política y procedimientos de Seguridad de la Información en el Ministerio.

6.6.3 Apoyar a la Dirección de Gestión de Riesgos en el proceso de identificación y valorización de riesgos operacionales relacionados con las tecnologías de la información.

6.7 **Comité de Control Interno:**

6.7.1 Comparte, a través de la Oficina General de Planificación y Presupuesto, Secretario Técnico del Comité, información relevante de incidencias de riesgos y otras situaciones de potenciales riesgos operacionales con la Dirección de Gestión de Riesgos.

6.7.2 Realiza periódicamente un proceso de revisión del Plan de Gestión de Riesgos y de seguimiento de la ejecución de los planes de acción, así como el monitoreo del cumplimiento de los lineamientos para la Gestión de Riesgo Operacional

6.8 **De la Oficina General Planificación y Presupuesto:**

6.8.1 Vela por que durante el desarrollo de los proyectos e iniciativas de mejora de procesos que se llevan a cabo en el MEF, se tomen en consideración los lineamientos definidos para la gestión del riesgo operacional.

6.8.2 Establece los procedimientos para monitorear en forma permanente los riesgos operacionales mediante el establecimiento de estrategias de verificación del desempeño de las medidas de mitigación implementadas, en forma consistente con los objetivos del MEF.

6.8.3 Realiza el seguimiento de las medidas de mitigación que son ejecutadas por los órganos competentes.

6.8.4 Elabora y monitorea, en coordinación con la Dirección de Gestión de Riesgos, el Plan de Gestión de Riesgos del MEF.

6.8.5 Pone en conocimiento de la Dirección de Gestión de Riesgos sobre el monitoreo de los planes de acción aplicados.

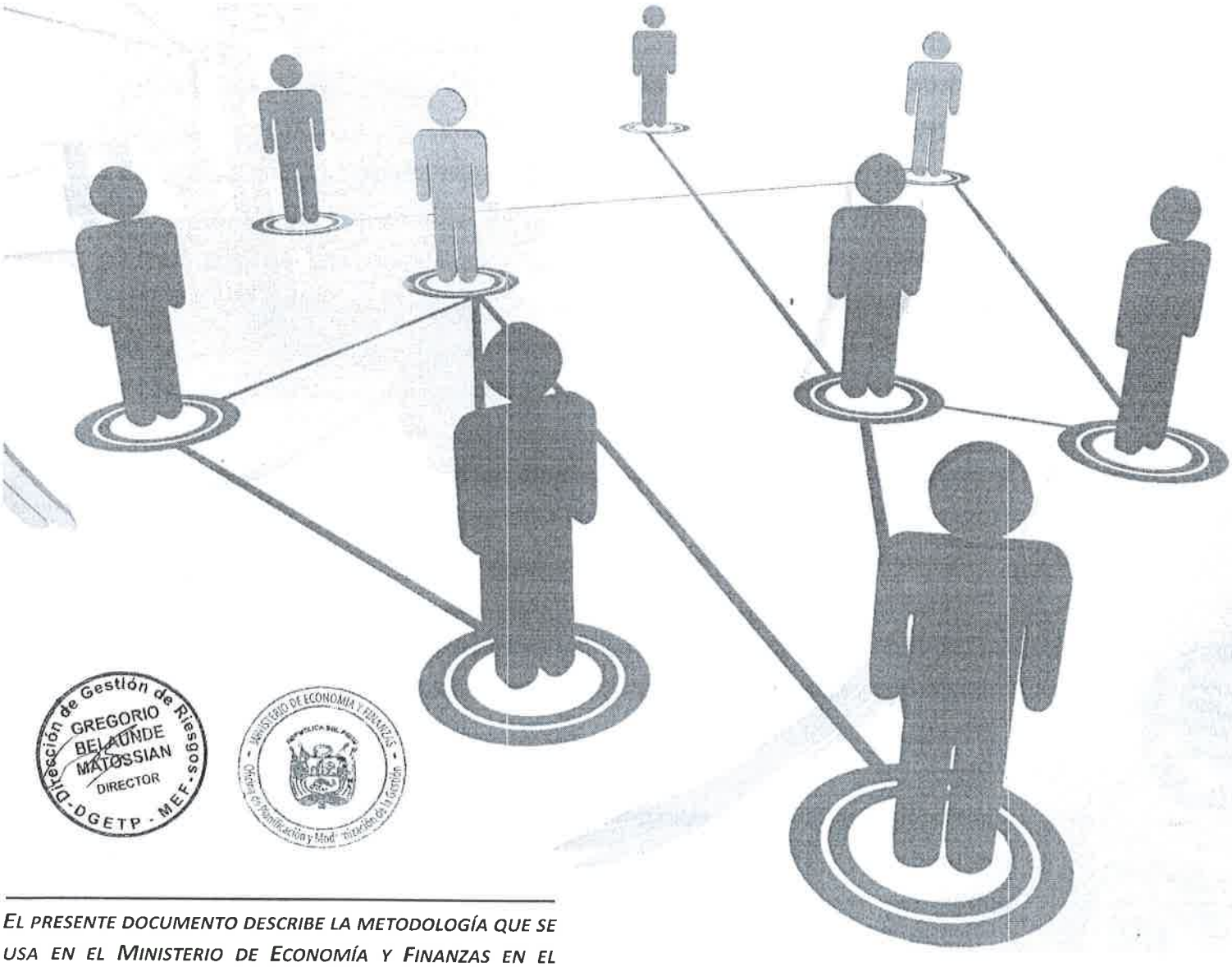
Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

PERÚ | Ministerio de Economía y Finanzas

ANEXO 1

METODOLOGÍA PARA LA GESTIÓN DEL RIESGO OPERACIONAL



EL PRESENTE DOCUMENTO DESCRIBE LA METODOLOGÍA QUE SE USA EN EL MINISTERIO DE ECONOMÍA Y FINANZAS EN EL MARCO DE LA GESTIÓN DEL RIESGO OPERACIONAL.

TABLA DE CONTENIDO

Introducción

El Ministerio de Economía y Finanzas (MEF), dentro de su estructura organizacional incluye a la Dirección de Gestión de Riesgos (DGR), como unidad orgánica encargada de formular y proponer modelos o metodologías de evaluación, clasificación y seguimiento de los riesgos operacionales que afecten o puedan afectar a las finanzas públicas[1].

El riesgo operacional es una categoría amplia, que a menudo parece abarcar todo menos los riesgos contingentes y financieros, como de mercado, liquidez, y de contraparte, y en este sentido debe entenderse a la gestión de riesgo operacional como un proceso evolutivo, donde todo el personal del Ministerio tiene una participación activa y con una curva de aprendizaje que dependerá de la capacidad para determinar y comprender los riesgos operacionales que afectan o pueden afectar el cumplimiento de sus objetivos misionales.

Es entonces necesario elaborar una metodología que permitan gestionar los riesgos operacionales apoyando así al proceso de interiorización de la cultura por la gestión del riesgo operacional en el Ministerio.

La Metodología para la Gestión del Riesgo Operacional del MEF, ha considerado como marco de desarrollo, los lineamientos descritos en los estándares internacionales, así como las notas técnicas y manuales elaboradas por el Departamento de Finanzas Públicas del Fondo Monetario Internacional. Adicionalmente tiene como basamento legal, la Resolución de Contraloría General N° 320-2006-CG, en particular lo referido a la Norma General para la Evaluación de Riesgos.

Este documento contiene dos capítulos: (a) el primero, referido al objeto, alcance y definiciones; y, (b) el segundo, muestra el paso a paso de cómo aplicar este documento, de acuerdo al proceso metodológico para la gestión del riesgo operacional.

Esta herramienta para la gestión de riesgos permitirá analizar lo que puede ocurrir y cuáles serían las consecuencias posibles, antes de decidir qué debe hacerse y cuando para reducir el riesgo operacional a un nivel aceptable.

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Planificación y Modernización de la Gestión

[1] Inciso a) y c) del Artículo 104 del ROF – MEF 2014

CAPITULO I – GENERALIDADES

1. Objetivo

Establecer la metodología destinada a gestionar el riesgo operacional en el Ministerio de Economía y Finanzas, definiendo para ello una estructura organizacional en la que participen las distintas direcciones/oficinas con funciones y responsabilidades específicas.

2. Alcance

De acuerdo al Reglamento de Organización y Funciones (ROF) del Ministerio de Economía y Finanzas, aprobado mediante D.S. Nº 117-2014-EF; la Dirección de Gestión de Riesgos tiene la función de formular y proponer políticas, lineamientos, normas y estrategias de gestión de los riesgos operacionales que afecten o puedan afectar a las finanzas públicas.

Gráfico 01: Esquema de la gestión de riesgo operacional del MEF

El alcance de la gestión del riesgo operacional y la aplicación de la presente metodología se circunscriben a los procesos, personas, tecnología y eventos externos que impacten negativamente en el Ministerio de Economía y Finanzas en el cumplimiento de sus objetivos.

3. Definiciones

Para efectos de la presente, se entiende por:

- Autoevaluación de Riesgos: Es el proceso por el cual se realizan dinámicas grupales con la finalidad de identificar, valorar y tratar riesgos.
- Base de Datos de Incidencias de Riesgos Operacionales: Es una herramienta de gestión que consiste en listar las incidencias que han tenido lugar en el MEF y que

hayan sido causadas por algún factor de riesgo operacional, obteniendo para ello información relevante acerca de la incidencia registrada.

- Cambio significativo: Aquel cambio en la estructura o procesos que podría poner en riesgo la normal atención de los servicios o cumplimiento de los objetivos del Ministerio.
- DGR: Dirección de Gestión de Riesgos
- MEF: Ministerio de Economía y Finanzas.
- Corresponsales de Riesgo Operacional: Personal del MEF responsable de implementar la gestión del riesgo operacional dentro del órgano o unidad orgánica del que forma parte.
- Especialista de Riesgos: Personal del Equipo de Trabajo de Riesgos Operacionales de la DGR encargado de realizar el taller de Identificación y autoevaluación de Riesgos, así como las acciones previas y posteriores a éste.
- Evento: Suceso o serie de sucesos derivados de los factores de riesgo operacional originados por la(s) misma(s) causa(s), que ocurre dentro un periodo de tiempo, afectando el curso normal de las diversas actividades del Ministerio.
- Exposición al Riesgo: Indicador que representa el grado de posibilidad de ocurrencia de un evento negativo o adverso, así como el impacto del mismo en el Ministerio al momento de materializarse.
- Factores de Riesgo Operacional: Son aquellas categorías de fuentes originadoras de potenciales incidencias de riesgo operacional, relacionadas con fallas en las personas, procesos, sistemas internos y/o eventos externos.
- Frecuencia (Probabilidad): Es el número de ocurrencias de un evento en un periodo dado. En una etapa inicial también es posible llamarlo probabilidad en un sentido más cualitativo.
- Gestión del Riesgo Operacional: Es el proceso continuo efectuado por todos los niveles organizacionales del Ministerio que permite identificar, valorar y tratar riesgos operacionales, con la finalidad de coadyuvar en el logro de los objetivos del Ministerio.
- Grado de exposición al riesgo: Es el nivel de riesgo que el Ministerio de Economía y Finanzas incurre en su búsqueda por cumplir con sus objetivos y misiones.
- Indicadores Clave de Riesgo: (KRI) Son unidades de medidas basadas en volumen o actividad que sirven como señales de alerta temprana para la gestión de riesgos, focaliza los cambios de las condiciones de riesgo, antes de que estas se materialicen y permiten tomar acciones.
- Incidencia de Riesgo Operacional: El evento que conduce a pérdidas o impide el logro de los objetivos de la organización y cuyo origen corresponde a factores de riesgo operacional.
- Matriz de Riesgo Operacional (Mapa de Riesgos): es la herramienta de Gestión de Riesgo Operacional que consiste en un cuadro de doble entrada (matriz) en el

cual se registran los riesgos identificados y se recopila información de acuerdo a criterios definidos por la DGR.

- Medios de Comunicación: Prensa escrita, radial, televisiva y redes sociales.
- Objetivos Estratégicos: Son objetivos de mediano y largo plazo que se encuentran alineados con la misión y visión del MEF.
- Objetivos Relacionados: Son los objetivos específicos de las distintas unidades del Ministerio que buscan el cumplimiento de un objetivo estratégico previamente establecido.
- OGTI: Oficina General de Tecnologías de la Información.
- OGPP: Oficina General de Planificación y Presupuesto.
- Órganos de Alta Dirección: Son el Viceministerio de Hacienda, Viceministerio de Economía y la Secretaría General.
- Órgano de Control Institucional: Es el órgano encargado de realizar el control gubernamental en el Ministerio, de conformidad con la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.
- Órganos de Línea: Son las Direcciones Generales comprendidas en el Viceministerio de Hacienda y el Viceministerio de Economía de acuerdo al Reglamento de Organización y Funciones del Ministerio.
- Órganos de Administración Interna: Se divide en:

  Órganos de Asesoramiento: Son la Oficina General de Planificación y Presupuesto (OGPP), Oficina General de Asesoría Jurídica (OGAJ) y la Oficina de Seguridad y Defensa Nacional (OSDENA).

  Órganos de Apoyo: Son la Oficina General de Administración (OGA), la Oficina General de Tecnologías de la Información (OGTI), la Oficina General de Servicio al Usuario (OGSU), Oficina General de Enlace (OGEN), y Oficina de Comunicaciones.

- Participantes: Son los dueños del proceso u otra persona que domine el proceso, con los cuales el Especialista de Riesgo Operacional realiza el Taller de Autoevaluación e Identificación de Riesgos.
- PEI: Plan Estratégico Institucional.
- Planes de Acción: Programación de las actividades conducentes a tratar los riesgos.
- POI: Plan Operativo Institucional.
- Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- Riesgo Intrínseco (Inherente): Es el nivel de exposición o nivel de riesgo total, al cual está expuesto una institución, medido de forma cualitativa mediante su frecuencia y severidad (o probabilidad e impacto).

07 MAR. 2016

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

- Riesgo Operacional: Es la posibilidad de ocurrencia de pérdidas o de incapacidad de cumplir correctamente con los objetivos del Ministerio debido a la inadecuación o a fallas en los procesos internos, el personal, sistemas internos y tecnologías de la información o bien a causa de eventos externos.
- Riesgo Objetivo: Es el nivel de exposición remanente o exposición final, que persiste aún después que se han ejecutado las medidas de tratamiento adicionales a las medidas de tratamiento existentes.
- Riesgo Reputacional: La posibilidad de incidencias relacionadas a las operaciones de las Direcciones u Oficinas que afectan a la imagen del Ministro y/o del Ministerio. Deriva de la materialización del riesgo operacional.
- Riesgo Residual: Es el nivel de exposición remanente o exposición final, que persiste aún después que se han ejecutado las medidas de tratamiento a los riesgos identificados previamente (riesgo absoluto).
- Semaforización: Es la técnica por la cual se emplea los colores del semáforo, en nuestro caso, (negro, rojo, amarillo y verde) para indicar, de forma gráfica, la gradualidad de una situación que está siendo evaluada, por ejemplo el nivel de riesgo.
- Severidad (Impacto): Consecuencia o consecuencias de un evento, expresado en términos cualitativos, también llamado Impacto.
- Sistema Administrativo: Según la Ley Orgánica del Poder Ejecutivo (LOPE), en el MEF se manejan cinco (5) sistemas los cuales son: Sistema Nacional de Presupuesto Público, Sistema Nacional de Tesoro Público, Sistema Nacional de Endeudamiento Público, Sistema Nacional de Contabilidad Pública y Sistema Nacional de Inversión Pública.
- Taller de Autoevaluación de Riesgos: Es el proceso por el cual se realizan dinámicas grupales bajo la conducción del Equipo de Trabajo de Riesgos Operacionales, con el objetivo de identificar y evaluar riesgos.
- Tolerancia al Riesgo: Es la desviación máxima en el grado de exposición al riesgo que el Ministerio está dispuesto a aceptar.
- Tratamiento del Riesgo: Proceso por el que se decide las acciones de gestión de riesgos a realizar con respecto al riesgo identificado.

CAPITULO II – DE LA METODOLOGIA

La metodología para la Gestión del Riesgo Operacional busca guiar la gestión del riesgo operacional en el MEF, para lo cual deberá ser implementada y utilizada por el personal del Ministerio, en coordinación con el Equipo de Trabajo de Riesgos Operacionales de la DGR.

Para gestionar adecuadamente los riesgos operacionales en el MEF, se deberán implementar los componentes de acuerdo al grafico siguiente:

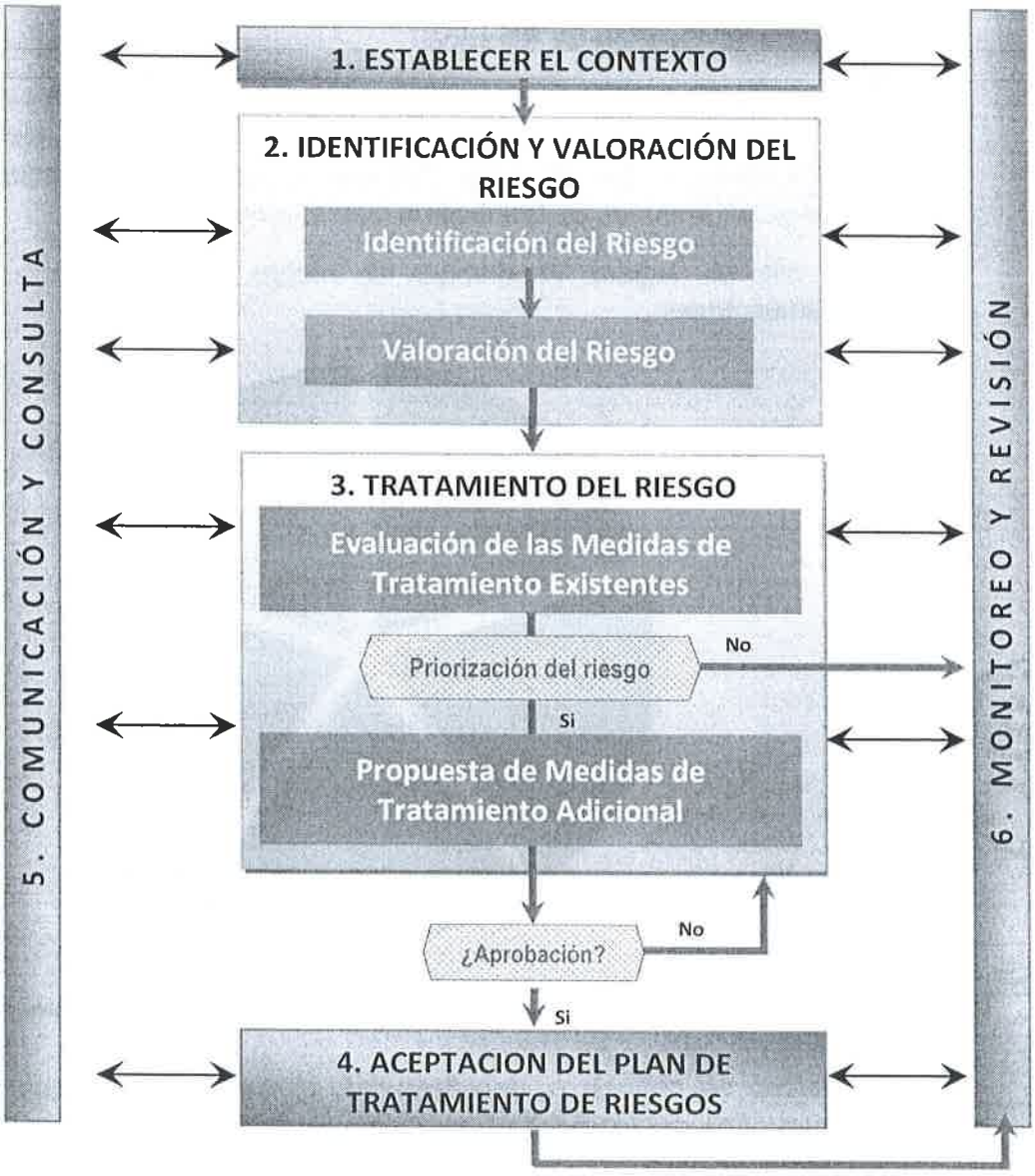


Gráfico N° 2: Esquema General de la Metodología

1. Establecer el Contexto

1.2 Ambiente Interno

El Ambiente Interno busca incorporar la filosofía de gestión del riesgo operacional en la cultura organizacional del MEF; para ello este componente será desarrollado bajo un enfoque de mejora continua y este proceso debe ser extendido progresivamente a todo el Ministerio.

Para el desarrollo del Ambiente Interno en los procesos del Ministerio, se debe considerar los siguientes aspectos[2]:

1.2.1 Filosofía de Gestión de Riesgos

La filosofía de gestión de riesgos permitirá a los colaboradores del MEF crear una conciencia de prevención de riesgos, generando en ellos, actitudes y emprendimiento de acciones dirigidas a prevenir y gestionar el riesgo operacional, además de fortalecer la cultura de riesgos.

Para ello se seguirá un enfoque de mejora continua que contará con las siguientes fases:

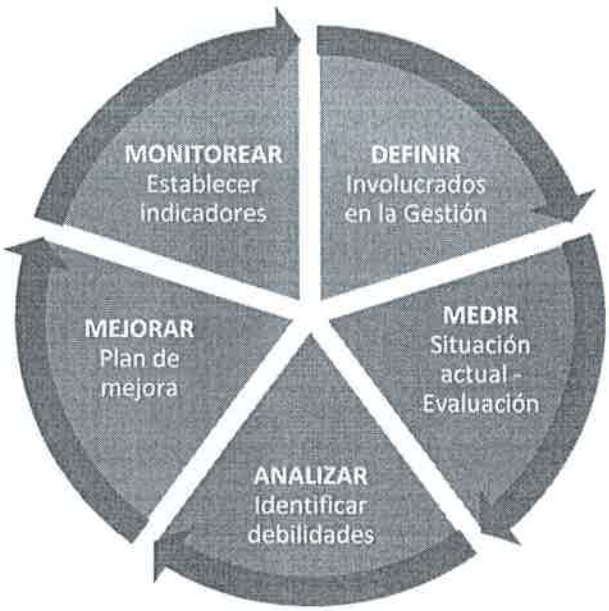


Gráfico N° 3: Fases de la Filosofía de la Gestión de Riesgos

- Definir: se definen e identifican los actores, responsables, participantes, entre otros involucrados en la gestión de riesgos.
- Medir: se determina el grado de conocimiento del personal, sobre temas de prevención y gestión de riesgos, para lo cual se debe realizar un diagnóstico de la situación actual de la cultura de riesgo en el MEF[3].

[2] *Gestión de Riesgos Corporativos-Marco Integrado/Técnicas de Aplicación – COSO ERM, 2004.*

- Analizar: se analiza la información obtenida de la fase "medición" y se identifica los puntos débiles de la cultura de riesgos en el MEF.
- Mejorar: se diseñan los planes y/o estrategias para fortalecer los puntos débiles identificados en la fase anterior, así como reforzar aquellos que lo necesiten.
- Monitorear: se realiza evaluaciones de forma periódica, tales como encuestas y/o seguimiento de indicadores.

1.2.2 Integridad y valores éticos

El desarrollo de la integridad y de los valores éticos constituye parte de la creación y reforzamiento de un ambiente interno adecuado para el desarrollo de una gestión de riesgos operacionales; en tal sentido, la eficacia de la gestión de riesgos no deberá sobreponerse a la integridad y los valores éticos. Para ello, los colaboradores del MEF deberán tener siempre en cuenta la siguiente normativa:

- La Ley N° 27815 – "Ley del Código de Ética de la Función Pública" sus modificatorias y su reglamento.
- La Resolución Ministerial N° 523-2010-EF/43 que aprueba la Directiva de Normas Técnicas y Lineamientos para la Conducta y Desempeño Ético del Personal del MEF.

1.2.3 Estructura organizacional comprometida

El desarrollo de un Ambiente Interno adecuado necesita de una estructura organizacional adecuada, que permita elevar la gestión de riesgos a todas las direcciones, para ello se cuenta con el apoyo de la Dirección de Gestión de Riesgos (DGR) y el Comité de Riesgos del MEF, así como de la Oficina General de Planificación y Presupuesto (OGPP) en su calidad de Secretaría Técnica del Sistema de Control Interno y el Comité del Sistema de Control Interno del Ministerio.

Asimismo, es indispensable contar con el compromiso de la Alta Dirección, las Direcciones Generales, cada Dirección y Oficina, del MEF, para lograr que:

- Los colaboradores guíen sus acciones de forma correcta desde el punto de vista legal y moral.
- No existan aspectos que no hayan sido normados o no se hayan definido pautas específicas para tal fin.
- Se fomente la búsqueda de ayuda en caso sea necesario, informando de los problemas, antes de que el impacto negativo en el Ministerio sea mayor.

[3] *Para realizar la medición de la situación actual de cultura de riesgo en el MEF, podría utilizarse el modelo de la cultura de riesgo desarrollado por PricewaterhouseCoopers (PwC) basado en cuatro atributos: Liderazgo y estrategia; responsabilidad y recompensa; personas y comunicación y gestión de riesgos e infraestructura, ver Apéndice 1, - Encuesta de la Cultura de Gestión de Riesgos del MEF.*

1.3 Establecimiento de Objetivos

La gestión del riesgo operacional deberá ser coherente con los objetivos estratégicos, la misión y la visión del Ministerio (PEI, POI); para ello será necesario el establecimiento claro de los objetivos estratégicos y una adecuada definición del grado de exposición y tolerancia al riesgo, acorde con los objetivos trazados.

Los objetivos estratégicos son establecidos a nivel de los Órganos de Alta Dirección y de los Órganos de Línea; estos objetivos son plasmados en el documento Plan Estratégico Institucional (PEI) y el Plan Operacional Institucional (POI).

El monitoreo del cumplimiento de los objetivos descritos en el PEI y el POI es realizado mediante los indicadores de desempeño, definidos por las Direcciones Generales y Oficinas Generales del MEF, que se encuentran descritos en dichos documentos.

En tal sentido, la gestión de riesgo operacional, tomará en cuenta los objetivos establecidos en los documentos PEI y POI; sin embargo, la DGR y los corresponsales de riesgo, deberán tomar en cuenta que el PEI, el POI y otros documentos de gestión no son la única fuente de identificación de los servicios esenciales que brinda el MEF y por ende de identificación de los riesgos operacionales.

1.4 Grado de exposición y tolerancia por riesgo operacional

Para una adecuada gestión del riesgo operacional es necesario definir el grado de exposición por riesgo operacional al que están expuestos los diferentes objetivos del MEF y los servicios que brinda el MEF, lo que permitirá determinar si dichos objetivos y servicios requiere tomar medidas para reducir o mitigar el riesgo para lograr un riesgo residual más bajo, así como identificar los riesgos cuyo nivel de riesgo no se podrá reducir.

Por otro lado, la tolerancia al riesgo, la cual está definida en los lineamientos para la Gestión del Riesgo Operacional, determina los niveles de desviación de la exposición al riesgo, en el cumplimiento de un objetivo establecido o servicio esencial y define los responsables en la toma de acciones inmediatas, todo ello con el objetivo de lograr por lo menos retornar el riesgo identificado hacia los niveles residuales determinados por grado de exposición al riesgo operacional.

En la tabla siguiente, se describe las acciones a seguir de acuerdo al nivel de exposición al riesgo operacional determinado, y el cual se ve reflejado en la matriz de riesgo operacional.

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
07 MAR. 2016
LIC. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Tabla de Acciones por Grados de Exposición al Riesgo

ÓRGANOS	ACCIONES	EXPOSICIÓN AL RIESGO
ÓRGANOS DE LÍNEA ÓRGANOS DE ASESORAMIENTO ÓRGANOS DE APOYO	- Implementar tratamientos y mitigantes, si fuera necesario. - Otro mitigante que establezca la Unidad Orgánica, o el Órgano.	Bajo (verde)
ÓRGANOS DE LÍNEA ÓRGANOS DE ASESORAMIENTO ÓRGANOS DE APOYO	- Implementar tratamientos y mitigantes. - Otro mitigante que establezca el Órgano o la Alta Dirección.	Medio (amarillo)
ÓRGANOS DE ALTA DIRECCIÓN ÓRGANOS DE LÍNEA ÓRGANOS DE ASESORAMIENTO ÓRGANOS DE APOYO	- Implementar tratamientos y mitigantes inmediatos. - Otro mitigante que establezca la Alta Dirección	Alto (rojo)
ÓRGANOS DE ALTA DIRECCIÓN ÓRGANOS DE LÍNEA ÓRGANOS DE ASESORAMIENTO ÓRGANOS DE APOYO	- Implementar tratamientos y mitigantes inmediatos.	Extremo (negro)

2. Identificación y Valoración del Riesgo

La dinámica de este componente se basa en una identificación de los riesgos y luego en una valoración de los riesgos identificados, y su ejecución es un trabajo en equipo entre el personal de cada Órgano del Ministerio, en coordinación con el Equipo de Trabajo de Riesgos Operacionales.

La dinámica incluye siempre una primera etapa de identificación y valoración efectuada con las unidades orgánicas (Direcciones y Oficinas), y una segunda etapa de consolidación a efectuar con los Directores Generales y los Despachos de Alta Dirección para uniformizar la visión de los riesgos entre los diferentes órganos del Ministerio a fin de buscar soluciones comunes. La dinámica debe repetirse parcialmente cada vez que se produce cambios en la organización del MEF u otro cambio significativo.

La metodología usa la técnica de semaforización,[4] la que permite el desarrollo de la Matriz de Riesgos, considerando el siguiente Mapa de Calor y Zonas de Riesgo.

[4] *La técnica de semaforización, es una técnica que consiste en utilizar colores (al igual que el semáforo) para expresar la gradualidad en la medida de un riesgo.*

MAPA DE CALOR					
FRECUENCIA (Probabilidad)	Muy Frecuente	(amarillo)	(rojo)	(negro)	(negro)
	Frecuente	(amarillo)	(rojo)	(negro)	(negro)
	Poco Frecuente	(verde)	(amarillo)	(rojo)	(negro)
	Raro	(verde)	(verde)	(amarillo)	?
		Menor	Moderada	Significativa	Catastrófica
		SEVERIDAD (Impacto)			

Grafico 04: Mapa de Calor

Un evento de frecuencia rara y severidad catastrófica plantea un desafío particular: podría estar en la zona negra para la priorización, pero el costo de la implementación del tratamiento es tan alto que conviene preguntarse si se debe hacer o no, por ejemplo la construcción de un bunker subterráneo para mitigar el riesgo de guerras altamente destructivas (depende del país).

ZONAS DE RIESGO			
(verde)	(amarillo)	(rojo)	(negro)
Bajo	**Medio**	**Alto**	**Extremo**
Requiere seguimiento	Requiere atención	Requiere atención prioritaria	Requiere atención prioritaria e inmediata

Grafico 05: Zonas de Riesgo

Cada zona de Riesgo resulta de un cruce entre la Frecuencia (Probabilidad) y el Severidad (Impacto) tal como se ha determinado en el Mapa de Calor.

2.1 Identificación del Riesgo

De acuerdo al Análisis de Procesos y de los diferentes servicios que brinda el Órgano y la Unidad Orgánica, se identifica los riesgos asociados a ellos, los cuales puedan alterar su *"modus operandus"* normal y su continuidad para el logro de los objetivos misionales.

Las principales herramientas usadas para la identificación de los riesgos operacionales son:

2.2.1 Recopilación de Información para la identificación de los riesgos

Se deberá obtener información preliminar (Mapa de Procesos y ROF, Informes de órganos internos e instituciones externas, Reportes de incidencias / Base de datos

de incidencias de riesgos operacionales), que permita al Especialista de Riesgos entender el proceso o servicio bajo alcance, conocer las incidencias de riesgos y las vulnerabilidades detectadas, y así definir pautas para la identificación de riesgos en los talleres con los usuarios finales. También se deberá realizar una revisión del inventario histórico de riesgos de las áreas involucradas en el proceso o en el servicio.

Para ello será importante contar con los insumos de información siguientes:

Mapa de Procesos y ROF, ayuda al personal de la DGR, comprender la interrelación de las tareas del personal, entradas, salidas, reglas y recursos, y de esta forma, identificar los riesgos operacionales para luego registrarlos en la Matriz de Riesgos. Estudio y revisión de Manual de Organización y Funciones y el Manual de Procedimientos, además de las políticas de las áreas involucradas en el proceso[5] o servicio seleccionado a analizar y cualquier otra información que se considere relevante como las normativas vigentes para ese proceso o dicho servicio.

Informes de órganos internos e instituciones externas, emitidos por la Dirección de Gestión de Riesgos o por los Órganos de Control y/o Auditoría tanto interna (Órgano de Control Institucional) como externa (Contraloría General de la República); estos informes serán empleados para sustraer los riesgos o vulnerabilidades descritos en dichos informes y posteriormente alimentar con dicha información la Matriz de Riesgos Operacionales del MEF.

Reportes de incidencias / Base de datos de incidencias de riesgos operacionales, solicitar el envío del reporte de incidencias (Apéndice N° 3) y/o riesgos a los Directores, dueños del proceso o servicio y/o colaboradores de las Direcciones u Oficinas que evidencien un incidente o identifiquen un riesgo.

La Base de Datos de Incidencias de Riesgos Operacionales es alimentada con los reportes de incidencias y/o identificación de riesgos y concentra el registro de incidencias que ocurrieron y que fueron reportadas por los colaboradores del Ministerio, siendo también útil para reevaluar la frecuencia con la que ocurre un incidente y la severidad.

2.2.2 Talleres de Autoevaluación con Usuarios

Tienen como objetivo identificar riesgos que impacten negativamente en las operaciones del proceso o servicio bajo alcance y las causas que lo originan. Este componente no busca determinar la medida del riesgo o las acciones que se tomarán para tratarlo, por lo que es necesario que no se desestime ningún riesgo que intuitivamente parezca pequeño ya que puede estar correlacionado con otro de mayor importancia o puede ser que, luego de analizarlo y valorarlo, resulte significativo.

[5] De acuerdo a la "Guía práctica para el relevamiento de la información, caracterización de los Procesos y su narración a través de Procedimientos" aprobada por R.D. N° 551-2013-EF/43.01, los procesos, según su función, se clasifican en procesos estratégicos, procesos principales (misionales) y procesos de soporte.

Se empieza con la identificación de los riesgos de un proceso o servicio y sus causas; así como otras características relevantes. Para poder llevar a cabo esta etapa se deberá desarrollar las siguientes actividades:

- Inducción a la metodología: el Especialista de Riesgos expone los criterios metodológicos a considerarse durante las etapas de la gestión de riesgos.
- El Especialista de Riesgos coordina con el dueño del proceso o servicio para que él u otra persona que domine el proceso, exponga la secuencia del mismo y a medida que se recorre el flujo permita a los participantes señalar la problemática que puede generar riesgos operativos. Para esto se podrían plantear las siguientes preguntas:
  - ¿Qué podría ocurrir si se materializa el riesgo?
  - ¿Por qué podría ocurrir?
  - ¿Cómo podría ocurrir?
- Los usuarios finales en coordinación con el Especialista de Riesgos deben registrar los riesgos operacionales que vayan identificando, así como su causa, evento, consecuencia y observaciones (si hubiese), en el Formato FT-01, columnas **1, 2, 3, 6, 7, 8,** y **9**, que se encuentra como Apéndice Nro. 5.

2.2 Valoración del Riesgo

Identificados los riesgos que afectan a los procesos del MEF, es necesario estimar su frecuencia (probabilidad) y severidad (impacto) para determinar el **riesgo intrínseco** asociado a ellos.

- El especialista de Riesgos instruye a los participantes para que asignen valores de frecuencia (probabilidad) y severidad (impacto) en ausencia de medidas de tratamiento, de acuerdo a los parámetros de Frecuencia y Severidad del Apéndice N° 2. Dicha información debe ser registrada, en el Formato de trabajo FT-01, columnas **10, 11**, que se encuentra en el Apéndice Nro.5.
- La exposición intrínseca, es la exposición al riesgo sin tomar en cuenta las medidas de tratamiento implementadas. La fórmula para el cálculo de este nivel de riesgo es la siguiente:

Exposición Intrínseca o Nivel de Riesgo Intrínseco	=	*Frecuencia Intrínseca * Severidad Intrínseca*

Ello permitirá definir cuáles son los riesgos críticos y establecer la criticidad para el MEF que deberán ser objeto de una vigilancia interna prioritaria independientemente de la calidad de las medidas de tratamiento existentes, pues estas pueden desaparecer o deteriorase en todo momento en razón de reorganizaciones u otros eventos que modifiquen el entorno de la entidad.

Por cada riesgo identificado se dirá así en qué zona de riesgo se encuentra según el Mapa de Calor.

3. Tratamiento del Riesgo

El tratamiento del riesgo mediante medidas existentes permite reducir el nivel de riesgo intrínseco para llegar a un nivel de riesgo residual. Es necesario tratar de reducir aún más el nivel de riesgo residual, con medidas adicionales de tratamiento, para llegar a un nivel de riesgo residual objetivo (o riesgo objetivo).

Este proceso del tratamiento del riesgo se describe en la gráfica siguiente:

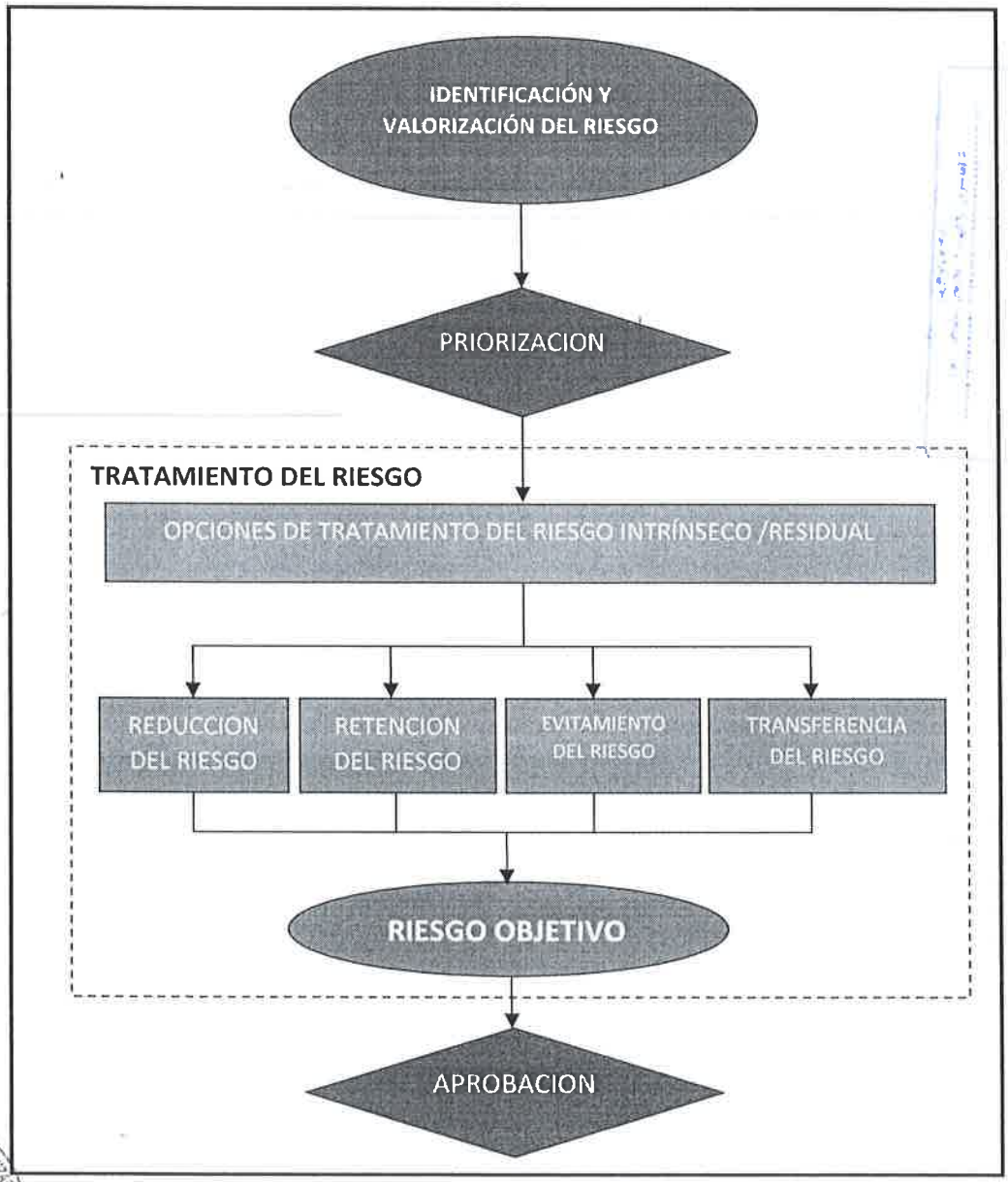


Grafico N° 6: Esquema general del tratamiento del riesgo

3.1 Evaluación de las Medidas de Tratamiento del Riesgo (MTR) existentes

Se toma como input las medidas de tratamiento de riesgos que actualmente existen, y se procede a su evaluación y cómo estas varían la estimación del riesgo intrínseco.

Como resultado de esta evaluación, se obtendrá el **Riesgo Residual**, que define la situación presente de los riesgos en el MEF.

- El Especialista de Riesgos apoya en la identificación de las medidas de tratamiento actuales para la mitigación de los riesgos intrínsecos. Los Riesgos que no tuvieran medidas de tratamiento implementadas, no podrán tener variación de estimación del riesgo intrínseco.
- El Especialista de Riesgos debe indicar a los participantes el método que se va a emplear para evaluar el **diseño y la efectividad** de las medidas de tratamiento existentes, luego debe coordinar con el grupo de usuarios finales para llegar a un consenso sobre las características de las medidas de tratamiento actuales.

➢ **Diseño:** Este criterio está orientado a determinar la solidez institucional de la medida de tratamiento; la ejecución de la medida de tratamiento podrá ser así evaluada, considerando 2 parámetros:

Diseño	Explicación
"Bueno"	- Sustentado en RD, RM, o DS. - Incluido en el Procedimiento. - Documentado
"Malo"	- Se realiza de manera informal o a criterio del personal.

➢ **Efectividad:** La efectividad está orientada a reducir el nivel de severidad con que impacta una incidencia (reducir el impacto) o reducir su frecuencia (probabilidad), la efectividad podrá ser evaluada, considerando 2 parámetros:

Efectividad	Explicación
"Efectivo"	La medida de tratamiento reduce la frecuencia o la severidad.
"No efectivo"	La medida de tratamiento no reduce ni la frecuencia ni la severidad.

- El Especialista de Riesgos debe registrar la información recopilada, ya que esta permitirá calcular la frecuencia residual y la severidad residual.

Exposición Residual o Nivel de Riesgo Residual	=	*Frecuencia Residual * Severidad Residual*

- El nivel de riesgo residual debe ser reevaluado periódicamente y calculado nuevamente tras la implementación de los planes de acción definidos en la siguiente etapa.

- Dicha información debe ser registrada, en el Formato de trabajo FT-01, columnas **13, 14, 15, 16** y **17,** que se encuentra como Apéndice Nro. 5.
- El resultado obtenido se compara con la siguiente tabla para determinar la priorización del riesgo, en cuanto a su tratamiento.

Riesgo	Interpretación
Extremo (negro)	Requiere tratamiento adicional en el corto plazo
Alto (rojo)	Requiere tratamiento adicional en el mediano plazo
Medio (amarillo)	Requiere tratamiento adicional en largo plazo
Bajo (verde)	No requiere tratamiento adicional

Grafico 07: Priorización del Riesgo

3.2 Propuesta de Medidas de Tratamiento Adicionales

Para esta etapa es necesario contar con la Matriz de Riesgos Residuales e involucra la selección, desarrollo e implementación de una o más medidas de tratamiento adicionales para modificar los riesgos residuales y su exposición. Las medidas de tratamiento irán enfocadas en reducir la probabilidad de ocurrencia de los eventos o en reducir la severidad del impacto cuando ocurran, o en ambos aspectos.

El tratamiento del riesgo implica un proceso cíclico de:

- Valoración del tratamiento del riesgo, a la luz de la valoración del riesgo identificado.
- Decisión sobre si los niveles de riesgo residual son tolerables;
- Si no son tolerables, generación de propuestas de nuevas medidas de tratamiento para el riesgo; y
- Valoración de la eficacia de dicho tratamiento.

De acuerdo a la evaluación efectuada a los riesgos operacionales, se tomarán las siguientes opciones de tratamiento como referenciales ya que finalmente pueden implementarse otras que se ajusten mejor a las características del riesgo. Además son las que también se aplican de manera más o menos consciente con las medidas de tratamiento existentes.

a) **Reducir (mitigar) el riesgo:** Acción por la cual se busca reducir el nivel de riesgo con la implementación de medidas de tratamiento. Esta medida normalmente está asociada a riesgos con eventos de regular frecuencia y regular severidad.

b) **Retención (aceptación) del riesgo:** Acción por la cual se decide no tomar acción sobre el riesgo ya que no es material. Normalmente estos riesgos están asociados a eventos de poca frecuencia y baja severidad.

c) **Evitar el riesgo:** Decisión de los Órganos de Alta Dirección o de la Direcciones Generales de suspender el proceso, cambio, o cualquier otra acción que planeaba ejecutarse por considerarlo de un riesgo elevado.

d) **Transferir (compartir) el riesgo:** Acción que busca trasladar el riesgo de manera parcial o total a un tercero. Esta acción es usualmente asociada con la contratación de pólizas de seguros que permiten trasladar parcialmente el riesgo a una compañía de seguros o externalizar procesos, también se puede transferir el riesgo, por ejemplo, a los proveedores o usuarios externos de los servicios que brinda el MEF.

El Especialista de Riesgos instruye acerca de las opciones de tratamiento disponibles para tratar los riesgos, estas opciones finalmente son elegidas por los participantes de cada taller teniendo en cuenta que debe ser apropiado y realizable técnicamente; también se deben considerar las metas y objetivos de la organización para seleccionar opciones de mitigación de los riesgos, las cuales a su vez serán coordinadas con la Oficina General de Planificación y Presupuesto (OGPP), en su calidad de secretaría técnica del Comité de Control Interno.

La Oficina General de Planificación y Presupuesto (OGPP), en coordinación con el Especialista de Riesgos, apoyarán la articulación de las **medidas de tratamiento propuestas** para asegurar que las políticas, estándares, procedimientos y planes de acción definidos sean apropiadamente ejecutados, mejorando así el diseño y efectividad de las operaciones.

Las actividades de las medidas de tratamiento propuestas deberán estar preferentemente incorporadas en todos los procesos y actividades de apoyo en el ámbito de la Mejora Continua. Incluyen las Medidas de Tratamiento de Riesgos generales así como las de aplicación a los sistemas de información, además de la tecnología de información relacionada.

Las medidas de tratamiento propuestas deben ser registradas, en el Formato de trabajo FT-01, columnas **19, 22** y **23,** que se encuentra como Apéndice Nro. 5. Para ello tener en cuenta lo siguiente:

3.2.1 Tipos de Medidas de Tratamiento:

Las medidas de tratamiento definidas podrán ser clasificadas como:

i. Preventivas
Son aquellas medidas que intentan disuadir la ocurrencia de aquellas incidencias con impacto negativo. Estos tipos de medidas tienen un carácter proactivo frente al riesgo.

Ejemplos claros de medidas preventivas son los documentos de segregación de funciones (MOF), autorizaciones y permisos adecuadamente registrados, entre otros.

ii. Detectivas
Son aquellas medidas que intentan detectar actos o incidencias con impacto negativo; estas medidas muestran evidencia de la existencia de algún error en las operaciones y/o en los servicios.

Ejemplos claros de estas medidas o "controles" detectivos son las, conciliaciones bancarias, inventario de documentos y/o auditorias, entre otras.

iii. Correctivas

Son aquellas medidas que intentan corregir un error acontecido o una incidencia con impacto negativo ocurrido. Estas medidas son empleadas para hechos o incidencias ocurridas, por lo tanto podrán estar incorporadas en la Base de Datos de Incidencias de Riesgos Operacionales.

Las medidas correctivas podrán ser los planes de acción definidos en la fase de tratamiento por su carácter de atención a incidencias ocurridas.

3.2.2 Priorizar acciones para la atención del riesgo

- La prioridad de atención (en condiciones normales) de los riesgos identificados y evaluados, será dada desde la zona de mayor nivel de riesgo hacia las zonas de menor nivel de riesgo (negro, rojo, amarillo y verde, en ese orden); debiendo tomar acciones inmediatas para aquellos riesgos que se encuentren en la zona de mayor nivel de riesgo (zona negra o riesgo extremo).
- Para el caso en que un conjunto de riesgos, se encuentren en una misma zona de riesgo, la DGR podrá proponer a las Direcciones, Oficinas y/o dueños del proceso, los riesgos que deberían tener prioridad en su atención y/o atender a aquellos riesgos que presenten un mayor nivel de severidad.
- Alternativamente, la Alta Dirección y las Direcciones/Oficinas Generales, podrán solicitar la atención inmediata de aquellos riesgos que consideren críticos.
- El tipo de tratamiento seleccionado para tratar los riesgos debe ser apropiado y técnicamente realizable y debe ser coordinado con la DGR, por medio del Equipo de Trabajo de Riesgo Operacional y con la Oficina General de Planificación y Presupuesto (OGPP) originándose para ello Planes de Acción.

En el siguiente gráfico se esquematiza la priorización para la atención de riesgos: Comenzando por la Esfera 1, campo negro, el cual requiere atención prioritaria e inmediata, seguido por la Esfera 2, campo rojo, el cual requiere atención prioritaria, siguiendo con la Esfera 3, campo amarillo, el cual requiere atención, y finalmente la Esfera 4, campo verde, el cual requiere seguimiento.

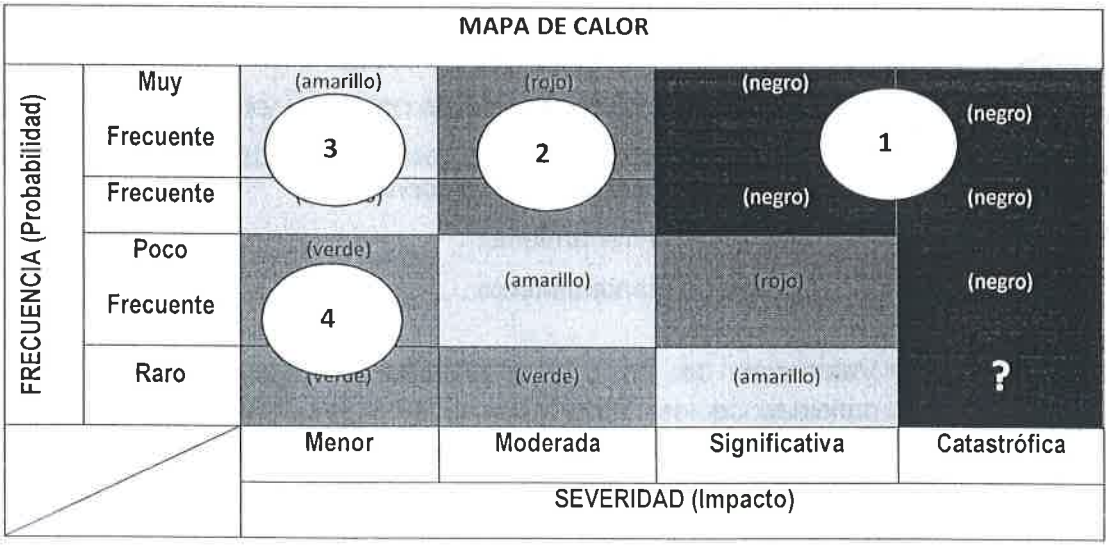


Grafico 08: Mapa de calor con prioridad de atención

3.2.3 Evaluación de las opciones de medidas de tratamiento recomendadas

Las medidas de tratamiento recomendadas deben ser evaluadas respecto a la factibilidad (compatibilidad, aceptación del usuario) y la efectividad (ganancia en la mitigación de riesgos) de cada medida. El objetivo es seleccionar las medidas de tratamiento más apropiadas para minimizar los riesgos.

3.2.4 Evaluación costo-beneficio de las respuestas al riesgo

i) La implementación de las respuestas al riesgo y el cumplimiento de los planes de acción generan costos; en tal sentido, la elección de una respuesta al riesgo deberá considerar los beneficios derivados de dicha respuesta, para ello se deberán tener en consideración, entre otros, los siguientes aspectos: Nivel de riesgo, costo de la respuesta al riesgo, costo del mantenimiento de la respuesta y la efectividad de la respuesta al riesgo; dicha evaluación podrá realizarse de manera cuantitativa o cualitativa. Asimismo, dicha selección debe situar el riesgo residual dentro de las tolerancias al riesgo establecido.

ii) El análisis costo/beneficio debe ser cualitativo. El propósito es demostrar que con la implementación de las medidas de tratamiento se reducen los niveles de riesgo. Un análisis costo/beneficio para las nuevas medidas de tratamiento propuestas o la ampliación de los existentes comprende:

- Determinación del impacto de la implementación o ampliación de medidas de tratamiento.
- Determinación del impacto de la no implementación o ampliación de medidas de tratamiento.
- Estimación de los costos de la implementación, lo cual incluye, sin que se limite a:
  - Compras de hardware y software
  - Reducción de la efectividad operacional si el desempeño del sistema se reduce por el incremento de la seguridad.
  - Costos de implementación de políticas y procedimientos adicionales
  - Costos de contratación de personal adicional para la implementación de políticas, procedimientos o servicios
  - Costos de entrenamiento
  - Costos de mantenimiento

- Valoración de los costos y beneficios de la implementación contra la criticidad de los datos y del sistema para determinar la importancia de la implementación de nuevas medidas de tratamiento, dados sus costos e impacto relativo.

iii) Las medidas de tratamiento propuestas deberán ser evaluadas de acuerdo al siguiente parámetro.

- **Recursos:** Se estimará los recursos necesarios para implementar las medidas de tratamiento de acuerdo a la siguiente tabla:

Bajo	- Inversión no significativa. - Requiere horas de trabajo adicionales. - Requiere compra de algún equipo auxiliar de reposición o consumibles.
Medio	- Inversión que se maneja a nivel de Dirección General. - Requiere días de trabajo adicional- Inversión en equipos menores. - Contratación de mano de obra o servicios temporales.
Alto	- Inversión aprobada por la Alta Dirección. - Se incluye en el presupuesto. - Inversión en mano de obra, equipos o servicios de gran costo.

Dicha información debe ser registrada, en el Formato de trabajo FT-01, columna **21,** que se encuentra como Apéndice Nro. 5.

3.2.5 Planes de Acción

- Los planes de acción son actividades dirigidas a tratar los riesgos logrando reducir su frecuencia, reducir su severidad o una combinación de ambas. El tratamiento seleccionado ante un riesgo, debe ser expresado en planes de acción, siempre que sea posible.
- Un Plan de Acción es un documento que registra actividades sincronizadas a ejecutarse para la realización exitosa de una medida de tratamiento. En su forma macro se define como Plan de Gestión de Riesgos Operacionales, que es un documento consolidado.
- Los planes de acción son determinados por la Dirección y/o dueño del proceso donde se identificó el riesgo o donde ocurrió la incidencia; todo ello en coordinación con el Equipo de Trabajo de Riesgos Operacionales, la Oficina General de Planificación y Presupuesto (OGPP) en su calidad de Secretaria Técnica de Sistema de Control Interno y la Oficina General de Tecnologías de la Información (OGTI) cuando corresponda.
- Los planes de acción serán documentados y monitoreados por la Dirección de Gestión de Riesgos, por medio del Equipo de Trabajo de Riesgos Operacionales y en coordinación con la Oficina General de Planificación y Presupuesto (OGPP) en su calidad de Secretaria Técnica de Sistema de Control Interno; debiendo considerar el riesgo evaluado, la acción que se realizará, el responsable de la acción y el plazo para su implementación. Para tal fin se utilizará la **Ficha de Plan de Acción** expuesta en el Apéndice N° 6.

3.2.6 Riesgo Objetivo:

En esta valoración se toma como input (entradas) el riesgo intrínseco y el residual, los cuales están en la Fila 12 y Fila 18, respectivamente del Apéndice N° 5, así como las medidas de tratamiento propuestas con los planes de acción de cada medida. Las nuevas medidas de tratamiento o la ampliación de las medidas existentes en términos de reducción de la frecuencia o severidad mitigan el riesgo porque:

- Eliminan algunas de las vulnerabilidades del sistema (defectos o debilidades), por consiguiente se reducen el número de posibles fuentes de amenazas / vulnerabilidades.
- Reducen la magnitud de los impactos adversos.

El Especialista de Riesgos debe registrar la información recopilada, ya que esta permitirá calcular la frecuencia objetivo y la severidad objetivo.

Exposición Objetivo o Nivel de Riesgo Objetivo	= *Frecuencia objetivo * Severidad Objetivo*

4. Aceptación del Plan de Tratamiento de Riesgos

En esta etapa, el órgano sometido al análisis de riesgos y a su respectivo tratamiento debe determinar el nivel de impacto y riesgo aceptable. Es por ello que se debe preguntar si hay riesgos que a pesar de haber sido tratados han cumplido con el objetivo de mitigación objetivo.

Si la respuesta es NO se debe volver hacer un tratamiento y si es SI se acepta el riesgo con sus medidas de tratamiento, responsabilidad, tiempo y costos, etc. Estos planes en caso de ser necesarios serán presentados periódicamente en sesión de Comité de Riesgos para su respectiva aprobación. Esta decisión no es puramente técnica. Pueden influir las decisiones políticas y gerenciales o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios[6].

Para la etapa de aceptación se debe considerar que:

a) Para ejecutar esta acción es necesario contar con el Plan de Tratamiento de riesgos y valoración de riesgos residuales revisados por el órgano bajo alcance.
b) Los decisores en esta etapa, pueden ser el Comité de Riesgos del MEF, o el mayor nivel jerárquico, de acuerdo al alcance definido, en función de si hay otros órganos involucrados o no.
c) Producto de esta etapa, obtendremos el Plan de Tratamiento de Riesgos, y la lista de riesgos aceptados con la respectiva justificación para aquellos que no cumplen con el criterio de aceptación normal.

[6]Magerit v3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

5. Comunicación y Consulta

La información es esencial en todos los niveles del Ministerio para identificar, valorar y dar respuesta a los riesgos; en ese marco, la información debe presentarse en forma oportuna, mediante los mecanismos adecuados y en un nivel de detalle necesario para poder ser transmitido a los Despachos de Alta Dirección, Directores Generales, Directores y al personal, así como a interesados externos, tales como usuarios de los servicios que brinda el Ministerio, proveedores y organismos encargados de controlar los bienes y recursos públicos del país, entre otros.

a) Partes Involucradas:

Para una efectiva gestión de riesgos operacionales estableceremos como partes involucradas al Comité de Riesgos, Despachos de Alta Dirección, Directores Generales, Directores y al personal, así como a interesados externos, tales como usuarios de los servicios que brinda el MEF, proveedores, inversores, entes reguladores, entre otros.

b) Información:

La Dirección de Gestión de Riesgos a través del Equipo de Trabajo de Riesgos Operacionales, emitirá informes relacionados a la gestión de riesgos operacionales y continuidad del negocio los cuales serán canalizados hacia el Director General de la DGETP con copia al Director General de la OGPP. Como parte de la información relevante debe considerarse las incidencias por riesgo operacional registradas, según los lineamientos correspondientes. Asimismo, el Comité de Riesgos deberá ser informado de las Incidencias de Riesgos Operacionales significativas

En cumplimiento con el párrafo anterior, el Equipo de Trabajo de Riesgos Operacionales, administrará una Base de Datos de Incidencias de Riesgos Operacionales, relacionada a las actividades del MEF; asimismo, elaborará y mantendrá las matrices de riesgos operacionales del Ministerio actualizadas en forma periódica (Ver Apéndice 6), en coordinación con la Oficina General del Planificación y Presupuesto (OGPP) en su calidad de Secretaria Técnica del Sistema de Control Interno y con los Corresponsales de Gestión de Riesgo Operacional del Ministerio.

c) Medios de Comunicación:

Los medios sugeridos a usar para comunicar el proceso de gestión serán los informes, oficios, circulares, capacitaciones, presentaciones, campañas de concientización que son de fácil desarrollo y permiten llegar a todo el público objetivo.

d) Comunicación

El Ministerio, a través de la DGR, comunica de manera clara la filosofía y enfoque de la gestión de riesgos operacionales; para esto se vale de las comunicaciones descendentes de la filosofía y lo que se espera de los colaboradores, además del flujo de información ascendente. Todo ello contribuye a introducir y afianzar la cultura de gestión de riesgos en el MEF. Para esto la DGR puede utilizar, entre otros mecanismos, los siguientes:

i. Realizar sesiones informativas con los colaboradores del MEF para comentar los riesgos y las respuestas al riesgo que se hayan llevado a cabo.
ii. Informar sobre los riesgos de las Direcciones u Oficinas por medio de comunicaciones a los colaboradores.
iii. Facilitar a todos los colaboradores del MEF los lineamientos, metodologías, procedimientos y estándares para la gestión de riesgos operacionales.
iv. Inducción para los nuevos colaboradores sobre la filosofía de gestión de riesgos del MEF.

La comunicación de las incidencias de riesgo operacional, planes de acción, nuevas medidas u otros que estén relacionados a la gestión del riesgo operacional, debe ser efectuada adecuadamente; para ello se han creado los canales apropiados que permitan reportar a los receptores correctos, quienes tomarán las acciones que correspondan; en ese sentido, se presenta los siguientes mecanismos a emplear:

i. La creación de un buzón de riesgo operacional, donde los Directores, Corresponsales de Riesgo Operacional y colaboradores del Ministerio puedan remitir sus reportes y dudas sobre incidencias - riesgos operacionales; dicho buzón se manejará a través de la cuenta de correo riesgos@mef.gob.pe, y su acceso será asignado al Jefe del Equipo de Trabajo de Riesgos Operacionales. Formato de reporte expuesto en el Apéndice N° 3.
ii. Reuniones de trabajo, donde se exponga los temas relevantes de la gestión del riesgo operacional, se presenten incidencias, se definan planes de acción, nuevos controles y/o se atiendan nuevas consultas y/o incidencias relacionadas al riesgo operacional.

e) Plan de Comunicación

El plan de comunicación se debe realizar interna (oficinas, direcciones, personal, funcionarios, directores generales, directores, alta dirección) y externamente (ciudadanos, proveedores, entes reguladores, inversores, etc.), teniendo en cuenta las definiciones sobre la existencia del riesgo, los objetivos de la gestión, el debido informe de los avances del proceso y todo aquello que se considere necesario.

Asimismo, debe ser diseñado de forma tal que permita crear conciencia en seguridad y evidencie la existencia de riesgos tecnológicos; si está bien estructurado permitirá lograr los objetivos de la gestión de forma satisfactoria, obtener información de soporte al análisis y colaborar en la planificación del proceso de gestión de riesgos.

Su estructura principal deberá contener tres etapas:

i. Comunicación inicial: en esta se incluye conceptos generales sobre riesgos, sus implicaciones, las ventajas de la gestión, entre otros aspectos.
ii. Comunicación sobre la marcha: Durante esta etapa se busca mostrar los avances del proceso de gestión de riesgos operacionales para obtener retroalimentación y conseguir el apoyo y participación de todos los involucrados en el MEF.
iii. Comunicación de resultados: Con esta etapa de la comunicación se busca compartir y difundir los resultados obtenidos teniendo en cuenta los debidos filtros de información de acuerdo al público objetivo.

Las anteriores etapas de comunicación aplican igual a nivel interno o externo dependiendo de las determinaciones del MEF.

f) Cuestionarios sobre de Gestión de Riesgos Operacionales

El Equipo de Trabajo de Riesgos Operacionales, podrá diseñar e implementar cuestionarios de gestión de riesgo operacional, y encuestas de los riesgos operacionales, con el fin de promover la gestión del riesgo operacional en el ministerio.

Para ello, deberá considerar aspectos relacionados a las fases de identificación, evaluación, control y comunicación de la gestión del riesgo operacional. Ver Apéndice N° 7 – Cuestionario de Gestión de Riesgos Operacionales.

6. Monitoreo y Revisión

Comprende las acciones para guiar y orientar que las medidas de tratamiento para los riesgos se ejecuten de acuerdo a los planes de acción definidos, así como el reporte de las deficiencias encontradas y su corrección.

Para desarrollar el monitoreo de la implementación de los planes de acción la Oficina General de Planificación y Presupuesto (OGPP) en su calidad de Secretaria Técnica del Sistema de Control Interno en coordinación con la DGR deberá elaborar un cronograma de monitoreo de acuerdo a los tiempos que se definieron en los planes de acción. Este cronograma deberá manejar tiempos de prevención y ejecución. Por ejemplo, se deberá empezar con el plan de acción que tenga el tiempo menor de implementación, si en este caso es de 1 mes (30 días) , el tiempo de prevención será a los 15 días y el tiempo de ejecución será a los 30 días.

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
LIC. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Apéndice N° 1.- Encuesta de la Cultura de Gestión de Riesgos del MEF

N°	Definiciones	1	2	3	4	5
1	Considero que las políticas establecidas en la Gestión de Riesgos Operacionales, dirigen la conducta de los empleados de la MEF hacia una cultura de prevención de riesgos.					
2	Conozco y entiendo la misión y los objetivos definidos por el Equipo de Trabajo y/o Dirección al que pertenezco, así como de la Dirección/Oficina General y la del MEF.					
3	Los Jefes, Directores y el Director General muestran una actitud coherente con el Código de Ética de la Función Pública e influyen en su personal a cargo.					
4	La capacitación recibida en Gestión de Riesgo Operacional fue suficiente para aplicar la gestión de riesgo operacional en mi área de trabajo.					
5	El personal del ministerio identifica los riesgos operacionales y los informa a sus Jefes inmediatos; y posteriormente a la Dirección de Gestión de Riesgos y a la OGPP.					
6	El personal del ministerio hace uso de los reportes de incidencias para reportar los riesgos identificados y/o las incidencias ocurridas.					
7	En mi trabajo, cuando el Jefe, Director y/o Director General me solicita información y/o realizar un trabajo que tiene algunas complicaciones o es poco claro, consulto con él/ella y/o demás jefes, acerca del trabajo encomendando, logrando así tener una fluidez de la información en ambos sentidos.					
8	En mi trabajo, cuando tengo temas difíciles o de poco conocimiento técnico y legal, busco ayuda con mis compañeros y/o hago consulta con los documentos oficiales del MEF.					
9	Conozco y entiendo mis funciones descritas en el MOF, ROF y las aplico diligentemente en mi trabajo.					
10	Conozco y entiendo el código de ética, las políticas relacionadas con mi trabajo así como otro documento oficial relevante del MEF.					
11	Conozco y brindo información acerca de las medidas de tratamiento de riesgos que han sido definidos en los procesos y servicios que forman parte de mi trabajo.					
12	Conozco los riesgos que hace han identificado, dentro de los procesos y servicios de la Dirección/ Oficina del Ministerio en la cual trabajo.					
13	El personal del Ministerio toma acciones de respuesta, en coordinación con el Jefe de Equipo, Director y/o Director General, para hacer frente a un riesgo identificado, como producto del cumplimiento de sus funciones.					

Leyenda: *Utilizar el criterio 1 en las preguntas del 1-4 y el criterio 2 en las preguntas del 5-13*

Puntaje	Criterio 1	Criterio 2
-2	Muy en Desacuerdo	No ha sucedido
-1	Desacuerdo	Pocas veces
0	Neutral	Frecuentemente
1	De acuerdo	Casi siempre
2	Muy de acuerdo	Siempre

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
LIC. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Rango	Descripción	Acciones
[-2.0 - 0.0 >	Muy mala	Tomar acciones inmediatas
[0.0 - 0.5 >	Mala	Replantear los planes
[0.5 - 1.0 >	Regular	Tomar acciones por precaución
[1.0 - 1.5 >	Buena	Fortalecer puntos débiles
[1.5 - 2.0]	Ideal	Continuar con la gestión

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Apéndice N° 2.- Determinación de la Frecuencia y Severidad

Tabla N° 1
Clasificación de Frecuencias

Valor	Descriptivo	Frecuencia (Probabilidad)
4	**Muy Frecuente**	El evento ocurre constantemente
3	**Frecuente**	El evento ocurre varias veces pero no llega a ser una constante
2	**Poco Frecuente**	El evento ocurre con baja frecuencia
1	**Raro**	El evento puede ocurrir excepcionalmente.

Tabla N° 2
Clasificación de la Severidad (impactos)

Evaluación de la Severidad (Impacto)	Severidad (Impacto) en la reputación y/o legal	Severidad (Impacto) en las Operaciones
Catastrófica 4	Pérdida de confianza del mercado internacional en el Gobierno Creación de comisiones de Investigación por parte del Congreso a la gestión de la Alta Dirección. Alta cobertura de medios de comunicación nacionales y cobertura por medios de comunicación extranjeros. Sanciones legales que afecten al personal del Ministerio.	Paralización de algún sistema administrativo de rectoría del MEF por más de cuatro días. Gran cantidad de tiempo del personal de la Alta Dirección dedicado a manejar el impacto.
Significativa 3	Se debilita la confianza del mercado internacional sobre el Gobierno. Interpelación Ministerial. Reclamo mayoritario de la ciudadanía. Alta cobertura de medios de comunicación nacionales.	Paralización de algún sistema administrativo de rectoría del MEF por más de dos días y menos de cuatro. Se dedican grandes cantidades de tiempo del personal directivo a manejar el impacto.
Moderada 2	Recibe atención de la Alta Dirección. No se afecta la confianza del mercado internacional. Hallazgos de la Contraloría sobre la gestión interna del MEF. Cobertura moderada de medios de comunicación nacionales.	Paralización de algún sistema administrativo de rectoría del MEF por un día completo hasta dos días. Se dedica una cantidad moderada de tiempo del personal directivo y operativo a manejar el impacto.
Menor 1	Recibe atención de alguna Dirección u Oficina General, y/o la Alta Dirección. Poca cobertura de medios de comunicación. Investigación interna en cada Dirección u Oficina General.	Paralización de algún sistema administrativo de rectoría del MEF durante las horas laborables de un día. Se dedica poca cantidad de tiempo del personal operativo a manejar el impacto.

Apéndice N° 3.- Formato de Reporte de Incidencias / Riesgo

REPORTE DE INCIDENCIA Y/O RIESGOS

DIRECCION QUE REPORTA		FECHA DE OCURRENCIA	
REPORTADO POR		FECHA DE IDENTIFICACION	
FECHA DE ENVIO		TIPO DE INCIDENCIA	

DETALLE DE LA INCIDENCIA:

¿QUE PASO? ¿COMO SUCEDIÓ? (DESCRIPCION TOTAL DEL EVENTO) DESCRIBE LOS IMPACTOS OPERATIVOS, FINANCIEROS, REPUTACIONAL, ETC.

¿POR QUÉ SUCEDIÓ? ¿CUALES FUERON LAS CAUSAS? - FALLAS EN LOS SISTEMAS / PROCESOS / PERSONAS / EVENTOS EXTERNOS	
1	
2	
3	
4	
5	
6	
7	

¿CUALES FUERON LAS ACCIONES TOMADAS EN EL MOMENTO PARA SUBSANAR LA SITUACION?	
1	
2	
3	
4	
5	
6	
7	

OBSERVACIONES:

Dirección de Gestión de Riesgos - GREGORIO DE LAUNDE MATOSSIAN - DIRECTOR - DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS - Dirección General de Programación y Modernización de la Gestión

Apéndice N° 4.- Formato de Base de Datos de Incidencias de Riesgos Operacionales

Código de identificación del evento	Fecha de Registro del Adm. de Rop	Órgano o Unidad orgánica que reporta	Responsable del Órgano o Unidad Orgánica que reporta	Lugar Físico	Fecha de ocurrencia InCidencia	Fecha de descubrimiento	Mes	Descripción Breve de la incidencia	Descripción amplia de la incidencia	Servicio / Aplicativo / Órgano afectado	Proceso Asociado (*)	Identificación del Riesgo (**)	Factor de Riesgo (**)	Tipo de Impacto de la Incidencia	Detalle del Impacto	Sustento	¿Qué falló?	Acciones de tratamiento ejecutadas o a ejecutar (propuestas)	Fecha de ejecución de las acciones	Información Adicional

(*) Proceso según clasificación de la OGPP, de corresponder, o descripción corta del servicio involucrado.
(**) En caso la incidencia cuente con un riesgo operacional relacionado, se debe ingresar el riesgo registrado en la Matriz de Riesgos Operacioales.

Dirección de Gestión de Riesgos - DGETP - MEF - soGasos
GREGORIO BERMUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Planificación y Modernización de la Gestión

PERÚ | Ministerio de Economía y Finanzas

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es "COPIA FIEL DEL ORIGINAL" que ha servido a la vista
07 MAR. 2016
LIC. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Apéndice N° 5.- Matriz de Riesgo Operacional

Formato FTU 01

Para la identificación de riesgos operacionales

Elaboración de la matriz de riesgos operacionales del Ministerio de Economia y Finanzas

Nombre de Direccion
Nombre de Oficina General
Nombre de Oficina de Linea
Lugar y Fecha

	Identificacion del Riesgo								*Calculo Riesgo Intrinseco*			*Eval de las Medidas de Trat. de Riesgo existentes*			*Calculo Riesgo Residual*			*Eval. de las Medidas de Trat. de Riesgo adicionales*			*Calculo Riesgo Objetivo*				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Nro.	Proceso o Servicio	Descripción larga del riesgo	Factor	Sub Factor	Causa	Evento	Consecuencia	Observaciones	Frecuencia Intrinseca	Severidad Intrinseca	Riesgo (F x S)	Medida de Tratamiento de Riesgos (MTR) existente	Diseño de la MTR	Efectividad de la MTR	Fecuencia Residual	Severidad Residual	Riesgo residual	Medida de Tratamiento de Riesgos (MTR) propuesta	Plan	Recursos	Fecuencia Objetivo	Severidad Objetivo	Riesgo objetivo	Diferencia	Tipo Ev
			Campo utilizado para el trabajo de gabinete no incluye al usuario final	Campo utilizado para el trabajo de gabinete no incluye al usuario final							Campo Calculado						Campo Calculado					Campo Calculado	Campo Calculado	

Las columnas 4, 5 y 26, deberan ser trabajadores por lo gestores del Taller (ETRO).
Las columnas 12, 18, 24 y 25 son campos calculados, basados en las tablas de valoraciòn establecidas en la metodologia.

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Planificación y Modernización de la Gestión

Apéndice N° 6.- Ficha de Plan de Acción

PLAN DE ACCIÓN - RIESGOS OPERACIONALES

Plan Nro.	
Fecha:	

Dirección General / Oficina General / Despacho Alta Dirección	
Dirección / Oficina	
Riesgo Asociado	

Nro.	Actividad a Realizar	Responsable	Recursos	Costos Estimados (*)	Fecha Inicio	Fecha Fin	Resultado Esperado	Meta Física (*)	Fecha de verificación de la implementación	Fecha Cierre
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

(*) Información a ser completada siempre y cuando se pueda consignar una meta física que pueda ser expresada cuantitativamente; de no ser el caso dejar vacías las celdas.

Apéndice N° 7.- Cuestionario de Gestión de Riesgos Operacionales

Fases	Descripción de la pregunta *	Objetivos de la Pregunta *	Proposiciones	SI	NO	PA
Identificación	El personal debe ser motivado por sus Jefes inmediatos, para adecuar sus actividades a la gestión de riegos operacionales.	Asegurar que las Direcciones impulsen al personal a identificar riesgos operacionales.	Mi Jefe nos impulsa y motiva a identificar riesgos operacionales en las actividades que hacemos en el día a día; ya sean propias o de mis compañeros.			
	El personal debe relacionar sus actividades con la fase de identificación, lo cual es fundamental que el personal realice el ejercicio de identificar las fallas, ya sean por cuenta propia o por terceros.	Asegurar que el personal se involucre en la identificación de los riesgos operacionales y los haga inherentes a sus actividades del día a día.	Cuando ocurre una incidencia que obstaculiza realizar mis actividades de forma normal, aviso del hecho a mi Jefe inmediato y/o informo a la DGR acerca del hecho.			
	El personal debe solicitar a la DGR asesoramiento en temas de identificación de riesgos.	Asegurar el interés del personal en gestionar sus riesgos operacionales	Estoy en constante comunicación con la DGR y hago consultas relacionadas a la forma de identificar los riesgos operacionales.			
Valorización	El personal debe conocer por lo menos, sus principales riesgos que tienen un alto impacto (severidad), dado que ameritan la creación de un Indicador clave de riesgo.	Asegurar que el personal tome conciencia de los riesgos de impacto alto para sus Direcciones y para el Ministerio en general.	Conozco los riesgos que tienen un nivel de gran impacto para la Dirección a la cual pertenezco así como para el Ministerio.			

	El personal debe hacer uso de la Metodología de la Gestión del Riesgo Operacional para la evaluación de los riesgos, así como los cuadros proveídos.	Asegurar que el personal utilice la Metodología de la Gestión del Riesgo Operacional.	Utilizo los cuadros de frecuencia y severidad que nos ha proveído la DGR, para ser empleados en la evaluación de los riesgos que identifico.			
	El personal debe hacer el ejercicio de analizar y evaluar, de forma cualitativa los impactos que tiene un incidente.	Asegurar que el personal realice el ejercicio de analizar las consecuencias frente a hechos de carácter negativo.	Siempre que ocurre un incidencia que impide continuar con mis labores y/o afecte en la reputación de mi Dirección o del MEF y/o impida cumplir con mis metas, analizo cuales fueron las consecuencias como producto de dicha incidencia.			
Tratamiento	El personal debe tener una participación activa en el tratamiento de los riesgos e incidencias.	Asegurar que el personal esté involucrado en la propuesta de acciones para mitigar el riesgo (Plan de Acción).	Siempre que identifico un riesgo, propongo a mi Jefe inmediato y/o a la DGR; una medida para tratarlo y mitigarlo.			
	El personal debe actuar en forma coordinada con sus jefes inmediatos, de tal forma se logre una cohesión en el tratamiento al riesgo.	Asegurar que el personal responda ante una situación negativa (tratamiento).	Las incidencias negativas que ocurren en mi Dirección, son tratadas de forma inmediata y coordinada con mi Jefe inmediato.			
	Contrastar el nivel de riesgo que tienen los procesos de una Dirección con los mitigantes predefinidos y/o definidos.	Observar deficiencias en el establecimiento de mitigantes así como la necesidad de definirlos.	Pienso que las acciones que actualmente realizamos en mi trabajo, son suficientes para mitigar los riesgos que afectan a mi Dirección.			

07 MAR. 2016

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS - Oficina de Planificación y Modernización de la Gestión

Comunicación	El personal debe comunicarse constantemente para aclarar las dudas que tengan el personal, acerca de la gestión de riesgos operacionales.	Asegurar la comunicación en la dirección desde el personal hacia la DGR.	Remito correos de consulta y/o consulto con la DGR acerca de los riesgos que afectan a mi Dirección.			
	La DGR debe de asegurar que la comunicación y/o solicitudes que realice, llegue al público objetivo.	Asegurar que la comunicación remitida por la DGR llegue hacia el público objetivo	Recibo correos y/o llamadas por parte de la DGR, solicitándome información y/o mayor detalle de los riesgos que se han identificado, ya sea en forma interna o externa.			
	Los empleados deben utilizar las herramientas que diseñe la DGR, en relación a la gestión de riesgos operacionales.	Asegurar que el personal emplee los formatos diseñados para la comunicación de riesgos.	Utilizo el formato de reporte de incidencias, para informar a la DGR, acerca de los riesgos y/o incidencias ocurridas.			

(*) Información reservada para el Equipo de Trabajo de Riesgos Operacionales.

Significado de las respuestas:
SI: El personal realiza las acciones que se describen en la proposición correspondiente.
NO: El personal no realiza las acciones que se describen en la proposición correspondiente:
PA: El personal realiza, de forma parcial, las actividades que se describen en la proposición correspondiente.

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF - SOBSEN

MINISTERIO DE ECONOMÍA Y FINANZAS
Dirección de Planificación y Modernización de la Gestión

Apéndice N° 8.- Ejemplos de eventos de riesgo operacional

FRECUENCIA (PROBABILIDAD)	MENOR	MODERADA	SIGNIFICATIVA	CATASTRÓFICA
MUY FRECUENTE	- Luminaria malograda. - Carencia de materiales de escritorio para trabajar.			
FRECUENTE	- Corte de Internet (Menor 1hr) - Caída del Correo Institucional. - Ausencia del personal. - Caída del Sistema de Trámite Documentario.	- Manifestaciones sociales en los alrededores de la Sede MEF.		
POCO FRECUENTE	- Emisión de documentos con errores materiales. - Ascensores averiados. - Fallas en las Impresoras y/o Scanner en una oficina.	- Caída de internet en las zonas de operación de los CONECTAMEF.	- Renuncia de personal clave.	- Terremoto de gran magnitud en Lima y Callao - Ruptura de Fibra Óptica (Prolongada) - Ataque terrorista a la Sede MEF. - Corte total de fluido eléctrico en Lima (Mayor a 2 días) -Incendio/ inundación de toda la sede principal del MEF
RARO	- Avería de todos los marcadores de asistencia del personal.	- Fallas en todos los terminales de Bloomberg	- Caída en simultaneo de de Aplicativos SIAF-SIAD-SGPP-SIGA - Corte Internet (Mayor 8 hr)	- Meteoritos - Guerras altamente destructivas
		SEVERIDAD (IMPACTO)		

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que ha servido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Hoja de Control de Cambios

Nº de Versión	Fecha de presentación del documento	Cambios	Equipo responsable de la modificación
Versión 1	27-07-2011	Elaboración inicial del documento	ETRO
Versión 2.0	28-11-2014	Se realizo una actualización en base a la elaboración de la matriz de riesgos operacionales del MEF.	ETRO

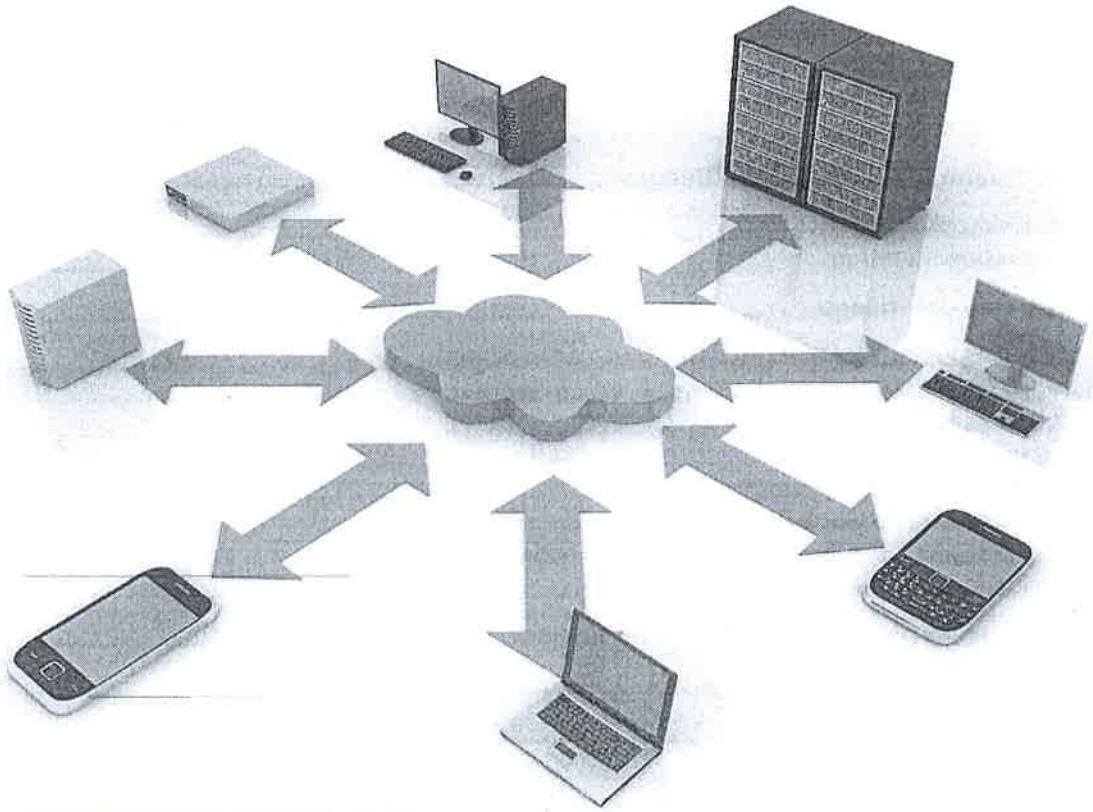
Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO SELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Planificación y Modernización de la Gestión

PERÚ | Ministerio de Economía y Finanzas

ANEXO 2

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS EN TECNOLOGÍAS DE LA INFORMACIÓN



El presente documento describe la metodología que se usará en el Ministerio de Economía y Finanzas en el marco de la gestión de riesgos en tecnologías de la información, como parte de la gestión del riesgo operacional.

TABLA DE CONTENIDO

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Introducción

El Ministerio de Economía y Finanzas (MEF), dentro de su estructura organizacional incluye a la Dirección de Gestión de Riesgos (DGR), como unidad orgánica encargada de formular y proponer modelos o metodologías de evaluación, clasificación y seguimiento de los riesgos financieros, operacionales y contingentes que afecten o puedan afectar a las finanzas públicas[1].

La Tecnología de la Información (TI), se encuentra estrechamente ligada a la operación diaria del MEF, coadyuvando al logro de las metas y objetivos institucionales. En ese sentido es necesario considerar los riesgos a los que están expuestos los activos de TI y la información con la que interactúan, ya que la materialización de estos riesgos puede implicar pérdidas significativas y causar serios inconvenientes a nivel misional y estratégico.

Es entonces necesario elaborar una metodología que permitan gestionar los riesgos en tecnologías de la información apoyando así a la gestión integral del riesgo operacional.

La Metodología para la Gestión de Riesgos en Tecnologías de la Información del MEF, ha considerado como marco de desarrollo, los lineamientos descritos en los estándares internacionales ISO 31000, ISO 27005, haciendo un híbrido que permita modelar la naturaleza del MEF, en cuanto a gestión de riesgos se refiere y su fácil aplicación e implementación progresiva.

Este documento contiene dos capítulos: (a) el primero, referido al objeto, términos, consideraciones y marcos de referencia para su desarrollo; y, (b) el segundo, muestra el paso a paso de cómo aplicar este documento, de acuerdo al proceso metodológico para la gestión del riesgo en tecnologías de la información (comunicación y consulta, establecer el contexto, valoración del riesgo, tratamiento del riesgo, aceptación del plan de acción, y monitoreo y revisión).

Esta herramienta para la gestión de riesgos permitirá analizar lo que puede ocurrir y cuáles serían las consecuencias posibles, antes de decidir qué debe hacerse y cuando para reducir el riesgo en tecnologías de la información a un nivel aceptable.

[1] *Inciso a) y c) del Artículo 104 del ROF – MEF 2014, aprobado mediante Decreto Supremo N° 117-2014-EF*

CAPITULO I – GENERALIDADES

1. Objeto

Establecer las guías metodológicas que faciliten la gestión de riesgos en tecnologías de la información, definiendo para ello una estructura comunicación y coordinación en la que participen todos los órganos y unidades orgánicas del Ministerio de Economía y Finanzas (MEF).

1.1. Los Riesgos en TI, dentro del contexto de Gestión de Riesgos en el MEF

La gestión de los riesgos en tecnologías de la información, es una actividad continua que aporta valor a la gestión tecnológica, ya que permite mediante procesos de identificación, análisis y valoración de riesgos, determinar cuánto valen y cómo se encuentran protegidos los activos de TI. Además las actividades de tratamiento permitirán elaborar un plan de acción que implantado y ejecutado satisfaga los niveles de riesgo que tolera el MEF en aspectos tecnológicos; las acciones de monitoreo y revisión apoyan al enfoque de mejora continua que se define en el numeral 1.3.

La gestión de riesgos en TI requiere una organización comprometida y la participación informada de todo el personal que trabaja con los activos de tecnologías de la información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general de los activos para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

La gestión de riesgos operacionales en el MEF además de gestionar los riesgos relacionados a personas, procesos y eventos externos, enfoca su atención a la tecnología de la información (Figura 01).

Figura 01:- Ubicación del riesgo en TI en la gestión de riesgos del MEF

1.2. Beneficios de implementar Gestión de riesgos en TI

Cuando la gestión del riesgo de TI se implemente y se mantenga de acuerdo con esta metodología, ello permitirá al MEF, entre otros:

- Coadyuvar en alcanzar los objetivos institucionales;
- Fomentar la gestión proactiva;
- Mejorar el gobierno de tecnologías de la información;
- Establecer una base confiable para la toma de decisiones y la planificación;
- Mejorar los controles existentes en tecnologías de la información;
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo en TI;
- Mejorar la eficacia y la eficiencia operativa;
- Fortalecer los procesos misionales.
- Mejorar la prevención de pérdidas y la gestión de incidentes en TI;
- Mejorar la cultura de gestión de riesgos de TI en el MEF.
- Ser consciente de la necesidad de identificar y tratar los riesgos en TI en toda la organización.

1.3. La metodología de riesgos en TI como proceso

La metodología de trabajo propuesta, deberá ser repetitivo pues los activos de TI se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

Para ello se define el Ciclo de Deming aplicado a la gestión de riesgos de tecnología de la información (Figura 02):

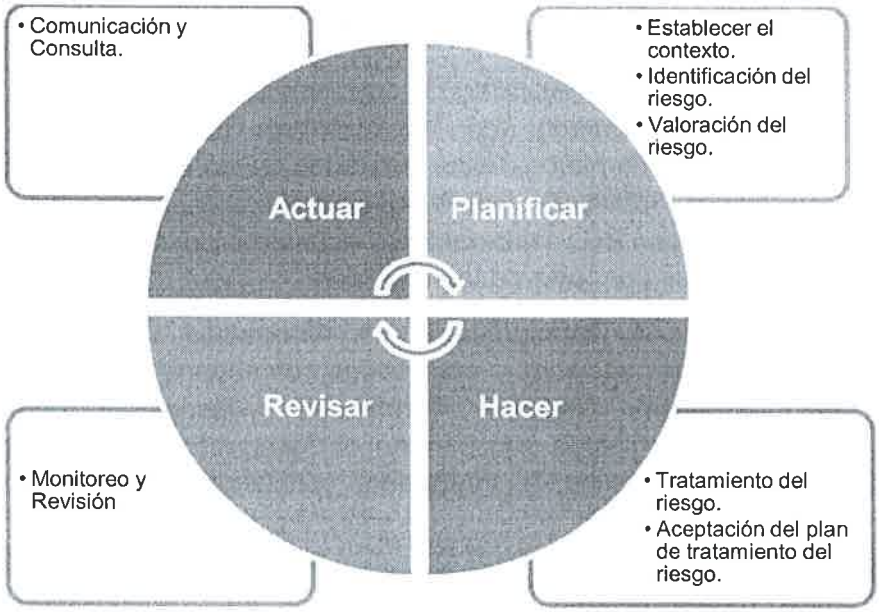


Figura 02:- Ciclo Deming aplicado a la gestión de riesgos de TI.

2. Términos y definiciones

2.1. **Activos de Tecnologías de la Información**: Son los elementos de hardware o software que permiten el procesamiento automatizado de la información. Alcanza a los equipos de comunicación y equipos auxiliares de apoyo.

2.2. **Amenaza**: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial).

2.3. **Análisis de riesgos:** Proceso sistemático (metodología) que comprende la identificación y valoración de los riesgos. Producto de esta etapa es la determinación de los riesgos intrínsecos.

2.4. **Exposición al Riesgo:** Medida que representa el grado de probabilidad de ocurrencia de un evento negativo o adverso, así como el impacto del mismo en el MEF al momento de materializarse.

2.5. **Frecuencia (Probabilidad):** Es el número de ocurrencias de un evento en un periodo dado. En una etapa inicial también es posible llamarlo probabilidad en un sentido más cualitativo.

2.6. **Identificación del riesgo:** Acción para encontrar, listar y caracterizar elementos de riesgo (activos, amenazas, vulnerabilidades), valorar los activos y sus dependencias.

2.7. **Seguridad de la Información:** Conjunto de acciones destinadas a asegurar la confidencialidad, integridad y disponibilidad de los activos de información y tecnologías para su procesamiento, apoyando finalmente a la continuidad de las operaciones del MEF.

2.8. **Severidad (Impacto):** Resultado negativo (daño a los activos de tecnologías de la información) de un riesgo que se ha hecho presente a causa de acciones o condiciones naturales o deliberadas, expresado en términos cualitativos, también llamado Impacto.

2.9. **Riesgo en TI:** La posibilidad de ocurrencia de pérdidas o de incapacidad de cumplir correctamente con los objetivos del MEF debido a los daños, interrupción, alteración o fallas derivadas de los sistemas físicos (hardware) e informáticos (software), aplicaciones de cómputo, redes y cualquier otro canal de distribución de la información, necesarios para la ejecución de procesos operacionales por parte de la institución.

Los riesgos en tecnologías de la información son parte de los riesgos operacionales asociados a actividades con soporte en recursos de tecnología de información, sistemas informáticos y tecnología inherente a dichos sistemas, los mismos que afectan el desarrollo de las actividades del MEF contra los principios de integridad, confidencialidad y disponibilidad de la información.

2.10. **Riesgo Operacional:** Es la posibilidad de ocurrencia de pérdidas o de incapacidad de cumplir correctamente con los objetivos del MEF debido a la inadecuación o a fallas en los procesos internos, el personal, sistemas internos y tecnologías de la información o bien a causa de eventos externos.

2.11. **Riesgo Objetivo:** Es el nivel de exposición remanente o exposición final, que persiste aún después que se han ejecutado las medidas de tratamiento adicionales a las medidas de tratamiento existentes.

2.12. **Riesgo Residual:** Es el nivel de exposición remanente o exposición final, que persiste aún después que se han ejecutado las medidas de tratamiento a los riesgos identificados previamente (riesgo absoluto).

2.13. **Valoración del riesgo:** Acción para asignar valores a la frecuencia y severidad de un riesgo y determinar el riesgo intrínseco y su valor.

2.14. **Tolerancia al Riesgo:** Es la desviación máxima en el grado de exposición al riesgo que el MEF está dispuesto a aceptar.

2.15. **Tratamiento de los riesgos:** Acciones de selección e implementación de medidas para protegerse del riesgo; en este etapa se decide las acciones de gestión de riesgos que se realizan o a realizar con respecto al riesgo identificado (para llegar a un riesgo residual y luego a un riesgo objetivo).

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS

3. Marco de Referencia

3.1. ISO 31000:2009 Gestión del Riesgo, Principios y Directrices

3.2. Norma Técnica Peruana ISO/IEC 27005:2009 Gestión del Riesgo en Seguridad de la Información.

3.3. Metodología para la Gestión del Riesgo Operacional en el Ministerio de Economía y Finanzas.

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

CAPITULO II – DE LA METODOLOGIA

1. Proceso metodológico

La metodología para la gestión del riesgo en tecnologías de la información busca gestionar el riesgo en los activos de TI en el Ministerio de Economía y Finanzas.

El proceso para el análisis y la gestión del riesgo en tecnologías de la información como parte del riesgo operacional, debería:

- Ser parte de la gestión integral de riesgos del MEF,
- Estar incluido en la cultura y las prácticas, y
- Estar adaptado a los procesos de misionales del MEF.

El proceso comprende las actividades que se describen en los numerales 2 al 7 de este capítulo, el mismo que se ilustra en la figura siguiente:

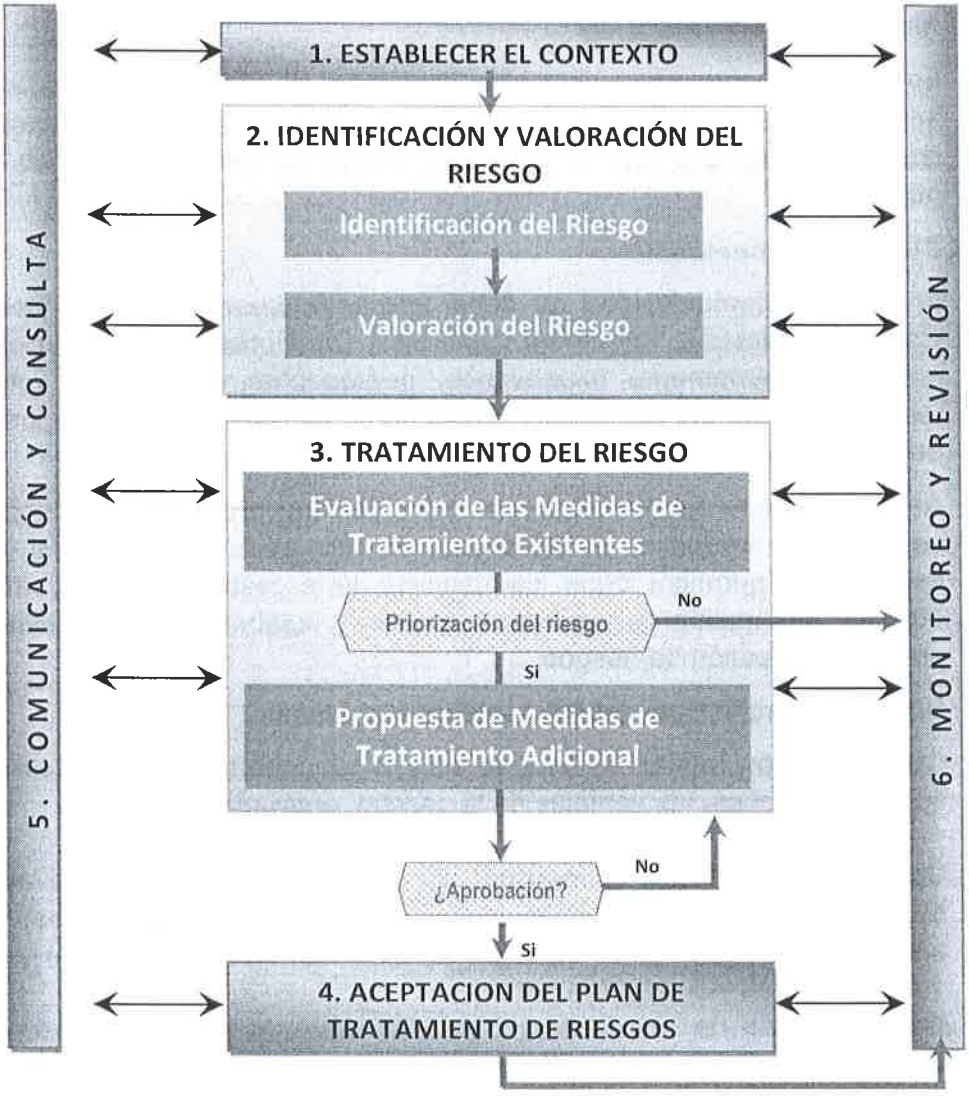


Figura 03: Esquema General de la Metodología

2. Comunicación y consulta

La información es esencial en todos los niveles del MEF para identificar, evaluar y dar respuesta a los riesgos; en ese marco, la información debe presentarse en forma oportuna, mediante los mecanismos adecuados y en un nivel de detalle necesario para poder ser transmitido a las partes involucradas externas e internas. Este intercambio de información debería tener lugar durante todas las etapas de la implementación de la gestión del riesgo en TI y su comprensión continúa de las partes involucradas.

2.1. Partes involucradas

Para una efectiva gestión de riesgos en tecnologías de la información, estableceremos como partes involucradas a la Alta Dirección, el Comité de Riesgos, Directores Generales, Directores y a todo el personal del MEF, así como a interesados externos, tales como usuarios de los servicios que brinda el MEF, proveedores, inversores, entre otros.

2.2. Medios de comunicación

Los medios sugeridos a usar para comunicar el proceso de gestión serán los informes, oficios, circulares, capacitaciones, presentaciones, campañas de concientización que son de fácil desarrollo y permiten llegar a todo el público objetivo.

2.3. Plan de Comunicación

El plan de comunicación se debe aplicar internamente (Alta Dirección, el Comité de Riesgos, Directores Generales, Directores y a todo el personal del MEF) y externamente (ciudadanos, proveedores, inversores, entre otros), teniendo en cuenta las definiciones sobre la existencia del riesgo, los objetivos de la gestión, y todo aquello que se considere necesario.

Asimismo, debe ser diseñado de forma tal que permita crear conciencia en seguridad y evidencie la existencia de riesgos tecnológicos; si está bien estructurado permitirá lograr los objetivos de la gestión de forma satisfactoria, obtener información de soporte al análisis y colaborar en la planificación del proceso de gestión de riesgos.

Su estructura principal deberá contener tres etapas:

Comunicación inicial: en esta se incluye conceptos generales sobre riesgos, sus implicaciones, las ventajas de la gestión, entre otros aspectos.

Comunicación sobre la marcha: Durante esta etapa se busca mostrar los avances del proceso de gestión de riesgos en TI para obtener retroalimentación y conseguir el apoyo y participación de todos los involucrados en el MEF.

Comunicación de resultados: Con esta etapa de la comunicación se busca compartir y difundir los resultados obtenidos teniendo en cuenta los debidos filtros de información de acuerdo al público objetivo.

Las anteriores etapas de comunicación aplican igual a nivel interno o externo.

2.4. Consideraciones

Es necesaria la participación de personal de la OGTI, quienes brindarán información de los activos de acuerdo a su detalle y uso, amenazas, vulnerabilidades, frecuencias e impactos que permitan realizar el levantamiento de información necesario para el análisis y evaluación de los riesgos.

Estas actividades están relacionadas a lo referido en los Pasos del 01 al 10 (Ver apéndice).

Se deberá interactuar también con los responsables de dirección u oficinas y corresponsales de riesgos, de acuerdo al alcance definido, para validar la información trabajada conjuntamente con el personal de la OGTI, de acuerdo a la responsabilidad que se le asigne.

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

MINISTERIO DE ECONOMÍA Y FINANZAS

3. Establecimiento del contexto

3.1. Ambiente Interno

El componente "Ambiente Interno" busca incorporar la filosofía de gestión de riesgos en la cultura organizacional del MEF, para ello, éste proceso debe ser extendido progresivamente a todo el MEF.

Para el desarrollo del componente "Ambiente Interno", se debe considerar los siguientes aspectos[2]:

3.1.1. Filosofía de Gestión de Riesgos

La filosofía de gestión de riesgos permitirá a los colaboradores del MEF, crear una conciencia de prevención de riesgos, generando en ellos actitudes y emprendimiento de acciones dirigidas a prevenir y gestionar el riesgo en TI además de fortalecer la cultura de riesgos.

3.1.2. Integridad y valores éticos

El desarrollo de la integridad y de los valores éticos, constituye parte de la creación y reforzamiento de un ambiente interno adecuado para el desarrollo de una gestión de riesgos; en tal sentido, la eficacia de la gestión de riesgos no deberá sobreponerse a la integridad y los valores éticos. Para ello, los colaboradores del MEF deberán tener siempre en cuenta la siguiente normativa:

- La Ley Nº 27815 – "Ley del Código de Ética de la Función Pública" sus modificatorias y su reglamento.
- La Resolución Ministerial Nº 523-2010-EF/43 que aprueba la Directiva de Normas Técnicas y Lineamientos para la Conducta y Desempeño Ético del Personal del MEF.

3.1.3. Consideraciones normativas y de gestión

De acuerdo a la naturaleza de la metodología, es necesario tener en cuenta los documentos que normas la gestión del MEF, como, Plan Operativo Institucional del MEF, Plan Estratégico Institucional, Plan Operativo Informático, entre otros.

3.1.4. Estructura organizacional comprometida

El ambiente interno, se basa en la estructura organizacional que permita elevar la gestión de riesgos a todas las direcciones, para ello se cuenta con el apoyo de la Dirección de Gestión de Riesgos (DGR), la Oficina General de Planificación y Presupuesto (OGPP) y el Comité de Riesgos del MEF.

Asimismo, es indispensable contar con el compromiso de la Alta Dirección, los Directores Generales y los Directores del MEF, para lograr que:

- Los colaboradores guíen sus acciones de forma correcta desde el punto de vista legal y moral.

[2] *Gestión de Riesgos Corporativos-Marco Integrado/Técnicas de Aplicación – COSO ERM, 2004.*

- No existan aspectos que no hayan sido normados o no se hayan definido pautas específicas para tal fin.
- Se fomente la búsqueda de ayuda en caso sea necesario, informando de los problemas, antes de que el impacto negativo en el MEF sea mayor.

3.2. Establecimiento de Objetivos

El objetivo de la gestión de riesgos en TI es facilitar a la organización en el logro de su misión, permitiendo:

- ✓ Reducir los impactos de los riesgos en TI identificados, de manera justificada, asegurando el normal funcionamiento de los activos de tecnología de la información que apoyan a los servicios del MEF.
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos en niveles bajos.
- ✓ Facilitar el monitoreo y seguimiento de los riesgos de TI
- ✓ Concientizar al personal de la organización de la existencia de riesgos y de la necesidad de gestionarlos.

3.3. Alcance

El alcance de la gestión del riesgo en tecnologías de la información y la aplicación de la presente metodología abarca a todo el MEF, aplicado de manera progresiva hacia sus direcciones generales, oficinas generales, direcciones, oficinas, procesos o servicios según se defina, alineado a la estructura jerárquica organizacional del MEF (Apéndice 01).

4. Identificación y Valoración de Riesgos

La dinámica de este componente se basa en una identificación de los riesgos y luego en una valoración de los riesgos identificados, y su ejecución es un trabajo en equipo entre el personal de cada Órgano del MEF, en coordinación con el Equipo de Trabajo de Riesgos Operacionales.

La dinámica incluye siempre una primera etapa de identificación y valoración efectuada con las unidades orgánicas (Direcciones y Oficinas), y una segunda etapa de consolidación a efectuar con los Directores Generales y los Despachos de Alta Dirección para uniformizar la visión de los riesgos entre los diferentes órganos del MEF, a fin de buscar luego soluciones comunes. La dinámica debe repetirse parcialmente cada vez que se produce cambios en la organización del MEF u otro cambio significativo.

La metodología usa la técnica de semaforización,[3] la que permite el desarrollo de la Matriz de Riesgos, considerando el siguiente Mapa de Calor y Zonas de Riesgo.

MAPA DE CALOR					
FRECUENCIA (Probabilidad)	Muy Frecuente	(amarillo)	(rojo)	(negro)	(negro)
	Frecuente	(amarillo)	(rojo)	(negro)	(negro)
	Poco Frecuente	(verde)	(amarillo)	(rojo)	(negro)
	Raro	(verde)	(verde)	(amarillo)	?
		Menor	Moderada	Significativa	Catastrófica
		SEVERIDAD (Impacto)			

Figura 04: Mapa de Calor

Un evento de frecuencia rara y severidad catastrófica plantea un desafío particular: podría estar en la zona negra para la priorización, pero el costo de la implementación del tratamiento es tan alto que conviene preguntarse si se debe hacer o no, por ejemplo la construcción de un bunker subterráneo para mitigar el riesgo de guerras altamente destructivas (depende del país).

[3] *La técnica de semaforización, es una técnica que consiste en utilizar colores (al igual que el semáforo) para expresar la gradualidad en la medida de un riesgo.*

ZONAS DE RIESGO			
(verde)	(amarillo)	(rojo)	(negro)
Bajo	**Medio**	**Alto**	**Extremo**
Requiere seguimiento	*Requiere atención*	*Requiere atención prioritaria*	*Requiere atención prioritaria e inmediata*

Figura 05: Zonas de Riesgo

Cada zona de Riesgo resulta de un cruce entre la Frecuencia (Probabilidad) y el Impacto (Severidad) tal como se ha determinado en el Mapa de Calor.

4.1. Identificación de Riesgos

PASO 1: Inventario de Activos

a) Se deben identificar el conjunto de activos de tecnologías de la información, entendiéndose como activo cualquier elemento que interactué con la información y que represente valor para el MEF. Estos activos serán aquellos que queden enmarcados dentro de la definición del alcance.

b) El inventario de activos de tecnologías de la información permitirá identificar los activos y clasificarlos en:

- Información (Datos)
- Software
- Hardware
- Comunicaciones
- Infraestructura (Instalaciones)

c) El formato para elaborar el inventario de activos de tecnologías de la información está definido en el Apéndice N° 02 – *Columna 1 al 10*, teniendo en cuenta:

- Las consideraciones para realizar el inventario de activos de tecnologías de la información, se describe en el Apéndice N° 03.
- Las instrucciones para el llenado del inventario de activos de tecnologías de la información, se detalla en el Apéndice 04
- Las instrucciones para la codificación de activos de tecnologías de la información se encuentran en el Apéndice 05.

PASO 2: Valoración de Activos

a) Identificados los activos se procederá a valorarlos de acuerdo con los criterios de confidencialidad, integridad, y disponibilidad, como indica el Apéndice N° 06 - Tabla de valoración de activos de tecnologías de la información. Estas actividades serán registradas en las *Columnas del 11 al 13* y su cálculo automático se visualizara en la *Columna 14* del Apéndice N° 02.

PASO 3: Identificación de Amenazas

a) Consiste en determinar las amenazas que pueden afectar a cada activo de TI que se encuentra bajo alcance. Las amenazas son "cosas que pueden ocurrir". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a los activos y causar un daño potencialmente negativo.

b) Se debe entender que las amenazas pueden ser de origen natural o humano y pueden ser accidentales o deliberadas. Deberán identificarse tanto las fuentes de amenazas accidentales como las deliberadas. Una amenaza puede surgir desde adentro o desde afuera de la entidad. Se debe identificar las amenazas de manera genérica y por tipo (por ejemplo acciones no autorizadas, daño físico, fallas técnicas).

c) El Apéndice 07 presenta una relación de Amenazas Tipos, que nos servirá como guía para nuestro análisis.

d) Identificadas las Amenazas se procederá a registrar sus componentes (Modo Potencial de Falla, Intención, Fuente, Causa o motivo del modo potencial de efecto falla, Efecto del modo potencial de falla) utilizando las *Columna 5 al 10* del Apéndice N° 09.

PASO 4: Identificación de Vulnerabilidades

a) Se deberán identificar las vulnerabilidades que las amenazas puedan explotar para causar daño a los activos de TI de la entidad.

b) Se puede identificar vulnerabilidades en las áreas siguientes:

- Procesos y procedimientos
- Rutinas administrativas
- Personal
- Entorno Físico
- Configuración del sistema de información
- Hardware, Software o equipo de comunicación
- Dependencia de partes externas, entre otros.

c) Una vulnerabilidad que no tiene amenaza correspondiente puede no requerir la implementación de una medida de tratamiento, pero se debería reconocer y monitorear para observar sus cambios. Se debe de tomar en consideración que una medida de tratamiento implementada de manera incorrecta o que funcione mal puede ser en sí mismo una vulnerabilidad.

d) El Apéndice 08, presenta una relación de Vulnerabilidades Tipos, que nos servirá como guía para nuestro análisis.

e) Identificadas las Vulnerabilidades se procederá a su registro utilizando la *Columna 12* del Apéndice N° 09.

4.2. Valoración del Riesgo

PASO 5: Determinación de la Frecuencia

a) Se evaluará el nivel de frecuencia, de acuerdo a la tabla de criterios definidos en el Apéndice N° 10 (TABLA DE NIVEL DE FRECUENCIA).

b) Posterior a ello el valor deberá ser registrado en la *Columna 13* del Apéndice N° 09.

PASO 6: Determinación de la Severidad

a) Se debe desarrollar y especificar criterios de impacto en términos del grado de daño en costos y en dificultad de cumplir objetivos misionales en el MEF, causados por un evento que degrade los activos de TI, considerando lo siguiente:

- Nivel de clasificación del activo de TI impactado
- Infracción a la seguridad de la información (por ejemplo pérdida de confidencialidad, integridad y disponibilidad)
- Operaciones impedidas (internas o de terceros)
- Perturbación de los planes y plazos
- Daño a la reputación
- Infracciones a estipulaciones legales, regulatorias o contractuales

b) De las amenazas identificadas, se evaluará su nivel de severidad, de acuerdo a la tabla de criterios definido en el Apéndice N° 10 (TABLA DE NIVEL DE SEVERIDAD).

c) Posterior a ello el valor deberá ser registrado en la *Columna 14* del Apéndice N° 09.

PASO 7: Determinación del Riesgo Intrínseco

La exposición intrínseca, es la exposición al riesgo sin tomar en cuenta las medidas de tratamiento implementadas. La fórmula para el cálculo de este nivel de riesgo es la siguiente:

Exposición Intrínseca o Nivel de Riesgo Intrínseca	=	*Frecuencia Intrínseca * Severidad Intrínseca*

Donde la *Frecuencia Intrínseca* es la determinada en el Paso 5, y la *Severidad Intrínseca* es la determinada en el Paso 6.

5. Tratamiento del Riesgo

5.1. Análisis de las medidas de tratamiento existentes

El tratamiento del riesgo mediante medidas existentes permite reducir el nivel del riesgo intrínseco para llegar a un nivel de riesgo residual. Es necesario tratar de reducir aún más el nivel de riesgo residual, con medidas adicionales de tratamiento, para llegar a un nivel de riesgo residual objetivo (o riesgo objetivo).

Este proceso cíclico implica la dinámica general del tratamiento del riesgo:

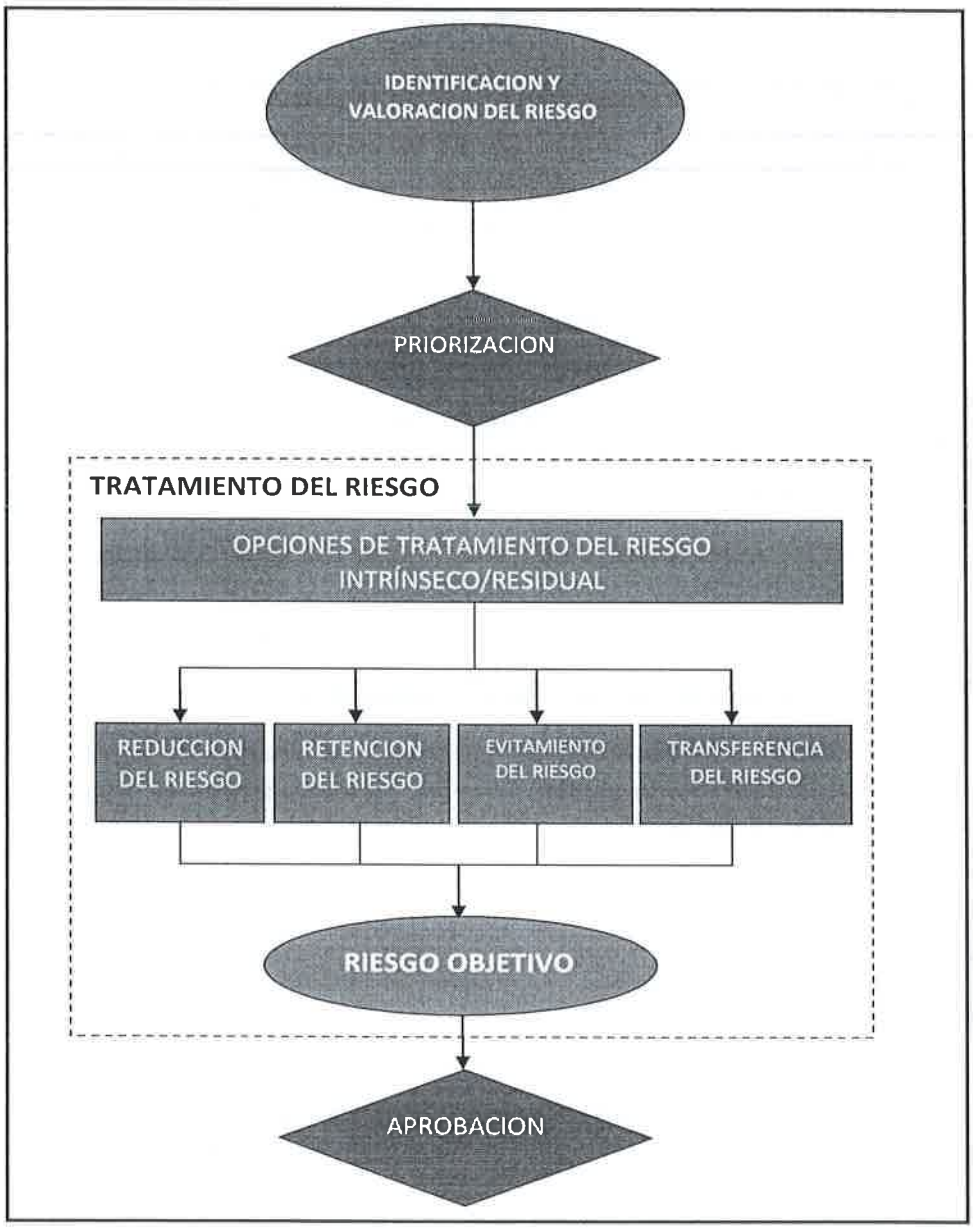


Figura 06: Esquema de general del tratamiento del riesgo

PASO 8: Identificación y evaluación de medidas de tratamiento existentes (implementadas)

a) Se describirá la medida de tratamiento aplicada a la amenaza identificada, considerando la efectividad de la medida de tratamiento de acuerdo a su evaluación.

b) Las medidas de tratamiento definidas deberán ser evaluadas de acuerdo a 2 parámetros:

- **Ejecución:** Está orientada a reducir el nivel de frecuencia con que ocurre una incidencia; a mayor nivel de ejecución de una medida de tratamiento, menor será la frecuencia residual con que pueda ocurrir una incidencia.

  La ejecución de la medida de tratamiento podrá ser evaluada, considerando 3 niveles de ejecución:

Ejecución	Explicación
3. Alta	*Se ejecuta por encima de un 80%*
2. Media	*Se ejecuta entre un 30% y 80%*
1. Baja	*Se ejecuta por debajo del 30%*

***Tabla 01**:* Parámetro de ejecución.

- **Efectividad:** La efectividad está orientada a reducir el nivel de severidad con que impacta una incidencia (reducir el impacto), a mayor nivel de efectividad, menor será el nivel de severidad residual con la que pueda impactar una incidencia.

  La efectividad de la medida podrá ser evaluada, considerando 3 niveles de efectividad:

Efectividad	Explicación
3. Fuerte	*La medida de tratamiento reduce considerablemente el impacto o severidad.*
2. Moderada	*La medida de tratamiento reduce de manera moderada el impacto o severidad.*
1. Débil	*La medida de tratamiento reduce débilmente el impacto o severidad.*

***Tabla 02**:* Parámetro de efectividad.

c) La eficacia de la medida de tratamiento, estará definida como una función de la ejecución de la medida y de su efectividad, medida en forma cualitativa, de acuerdo a los parámetros definidos de ejecución y efectividad. Se usa la siguiente fórmula para definir la medida de tratamiento:

*Eficacia de la medida de tratamiento = Ejecución * Efectividad*

Se considera **Fuerte**, cuando logra llevar la exposición al riesgo a un nivel menor. **Moderada**, cuando reduce la exposición al riesgo, pero aún podría existir exposición no manejable. **Débil**, cuando no logra ningún cambio.

De acuerdo a dichos parámetros, se puede obtener los siguientes resultados:

Resultados de la aplicación de la ejecución y efectividad		
*Ejecución*Efectividad*	*Frecuencia residual*	*Severidad Residual*
*3*3*	*La frecuencia se reducirá hasta un valor de 1*	*La severidad se reducirá hasta un valor de 1*
*3*2*	*La frecuencia se reducirá hasta un valor de 1*	*La severidad se reducirá un valor de 1**
*3*1*	*La frecuencia se reducirá hasta un valor de 1*	*La severidad mantendrá el valor original*
*2*3*	*La frecuencia se reducirá un valor de 1**	*La severidad se reducirá hasta un valor de 1*
*2*2*	*La frecuencia se reducirá un valor de 1**	*La severidad se reducirá un valor de 1**
*2*1*	*La frecuencia se reducirá un valor de 1**	*La severidad mantendrá el valor original*
*1*3*	*La frecuencia mantendrá el valor original*	*La severidad se reducirá hasta un valor de 1*
*1*2*	*La frecuencia mantendrá el valor original*	*La severidad se reducirá un valor de 1**
*1*1*	*La frecuencia mantendrá el valor original*	*La severidad mantendrá el valor original*

Tabla 03: Resultados de la aplicación de la ejecución y la efectividad.

(*) Para los casos en que el valor de la frecuencia o severidad (evaluado en el riesgo absoluto) sea igual a 1 se mantendrá dicho valor.

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

PASO 9: Determinación de Riesgos Residuales

a) Se calculará el nivel del riesgo actual de acuerdo a la siguiente fórmula:

Exposición Residual o Nivel de Riesgo Residual	=	*Frecuencia Residual * Severidad Residual*

b) El resultado obtenido se compara con la siguiente tabla para determinar la evaluación del riesgo:

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
07 MAR. 2016
LIC. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Riesgo	Interpretación
Extremo (negro)	Requiere tratamiento adicional en el corto plazo
Alto (rojo)	Requiere tratamiento adicional en el mediano plazo
Medio (amarillo)	Requiere tratamiento adicional en largo plazo
Bajo (verde)	No requiere tratamiento adicional

Figura 07: Tabla de Priorización

5.2 Propuesta de Medidas Adicionales de Tratamiento

Involucra la selección, desarrollo e implementación de las medidas de tratamiento para modificar los riesgos residuales y su exposición; estas irán también enfocadas en reducir la probabilidad de ocurrencia, en reducir la severidad del impacto o en ambos aspectos.

Para esta etapa es necesario contar con la Matriz de Riesgos Residuales

PASO 10: Selección de medidas de Tratamiento de Riesgos

Estas medidas se clasifican en general según la tipología siguiente, que también es la que se aplica de manera más o menos consciente con las medidas de tratamiento existentes.

5.2.1 Reducir el riesgo:

Acción por la cual se busca reducir el nivel de riesgo con la implementación de medidas de tratamiento. Esta medida normalmente está asociada a riesgos con eventos de regular frecuencia y regular severidad.

5.2.2 Retención del riesgo:

Acción por la cual se decide no tomar acción sobre el riesgo ya que no es material. Normalmente estos riesgos deben ser monitoreados, tanto más porque el riesgo intrínseco puede ser elevado, y la medida que asegura un nivel de riesgo bajo podría desaparecer o volverse inútil por un cambio de entorno u organizacional.

5.2.3 Evitar el riesgo:

Decisión de los Órganos de Alta Dirección o de la Direcciones Generales de suspender el servicio, cambio, o cualquier otra acción que planeaba ejecutarse por considerarlo de un riesgo elevado.

5.2.4 Transferir (compartir) el riesgo:

Acción que busca trasladar el riesgo de manera parcial o total a un tercero. Usualmente es asociada con la contratación de pólizas de seguros que permiten trasladar parcialmente el riesgo a una compañía

de seguros o externalizar el servicio; también se puede transferir el riesgo, por ejemplo, a los proveedores o usuarios externos de los servicios que brinda el MEF.

PASO 11: Priorizar acciones para la atención del riesgo

5.2.5 Enfoque para implementar medidas de tratamiento

Cuando se deben tomar medidas de tratamiento, se aplica la siguiente regla:

"Concentrarse en los grandes riesgos que demanden altos esfuerzos de mitigación al más bajo costo y con el mínimo impacto sobre los objetivos (misión) del negocio."

Con base en el reporte de valoración de riesgos, las acciones se deben priorizar. Será dada desde la zona de mayor nivel de riesgo hacia las zonas de menor nivel de riesgo (negro, rojo, amarillo y verde, en este orden). La consecución de recursos debe concentrarse en aquellos riesgos de nivel inaceptable, debiendo tomar acciones inmediatas para aquellos riesgos que se encuentren en la zona de mayor nivel de riesgo (zona negra o riesgo extremo).

Las amenazas/vulnerabilidades asociadas requieren acciones correctivas inmediatas.

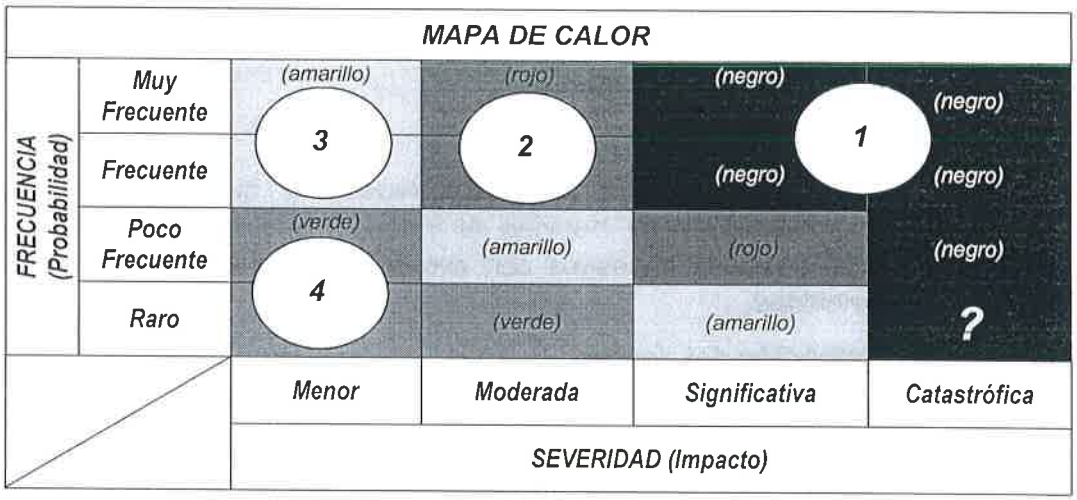


Figura 08: Mapa de calor con prioridad de atención

PASO 12: Evaluación de las opciones de medidas de tratamiento propuestas

Las medidas de tratamiento recomendadas en los talleres de autoevaluación de riesgos no necesariamente son las más apropiadas y factibles de implementar. Se debe evaluar la factibilidad (compatibilidad, aceptación del usuario) y la efectividad (ganancia en la mitigación de riesgos) de cada medida recomendada. El objetivo es seleccionar las medidas de tratamiento más apropiadas para minimizar los riesgos.

PASO 13: Evaluación de las respuestas al riesgo

a) La implementación de las respuestas al riesgo y el cumplimiento de los planes de acción generan costos; en tal sentido, la elección de una respuesta al riesgo deberá considerar los beneficios derivados de dicha respuesta, para ello se deberán tener en consideración, entre otros, los siguientes aspectos: Nivel de riesgo, costo de la respuesta al riesgo, costo del mantenimiento de la respuesta y la efectividad de la respuesta al riesgo; dicha evaluación podrá realizarse de manera cuantitativa o cualitativa. Asimismo, dicha selección debe situar el riesgo residual dentro de las tolerancias al riesgo establecidas.

b) La evaluación puede ser de tipo cuantitativo o cualitativo. El propósito es demostrar que con la implementación de las medidas de tratamiento se reducen los niveles de riesgo. Un análisis para las nuevas medidas de tratamiento propuestas o la ampliación de los existentes pueden comprender lo siguiente:

- Determinación del impacto de la implementación o ampliación de medidas de tratamiento.
- Determinación del impacto de la no implementación o ampliación de medidas de tratamiento.
- Estimación de los costos de la implementación, lo cual incluye, sin que se limite a:
  - Compras de hardware y software
  - Reducción de la efectividad operacional si el desempeño del sistema se reduce por el incremento de la seguridad.
  - Costos de implementación de políticas y procedimientos adicionales
  - Costos de contratación de personal adicional para la implementación de políticas, procedimientos o servicios
  - Costos de entrenamiento
  - Costos de mantenimiento
- Valoración de los costos y beneficios de la implementación contra la criticidad de los datos y del sistema para determinar la importancia de la implementación de nuevas medidas de tratamiento, dados sus costos e impacto relativo.

PASO 14: Elección de medidas de tratamiento propuestas

Con base en el resultado del análisis costo/beneficio, se determinará las medidas de tratamiento más efectivo para reducir los riesgos que atenten contra los objetivos (misión) del MEF. Las medidas de tratamiento seleccionadas deben obedecer a una combinación de medidas técnicas, operativas y administrativas para asegurar una apropiada protección de activos de TI y de la organización.

PASO 15: Planes de Acción

El tratamiento propuesto ante los riesgos, debe ser expresado en planes de acción, siempre que sea posible. Los planes de acción son actividades dirigidas

a tratar los riesgos logrando reducir su frecuencia, reducir su severidad o una combinación de ambas. El plan de acción debe contener al menos:

- Actividades a realizar.
- Responsable.
- Recursos.
- Fecha de inicio.
- Fecha de entrega.
- Resultado esperado.
- Fecha de verificación de la implementación.
- Fecha de cierre.

El Apéndice 11, muestra el formato para la formulación de los Planes de Acción.

PASO 16: Implementación de las medidas de tratamiento propuestas

Dependiendo de cada situación particular, las medidas de tratamiento a implementarse pueden bajar los niveles de riesgo pero no eliminarlos. El tratamiento de los riesgos objetivos se describe a continuación.

5.2.6 Riesgo Objetivo:

El MEF debe analizar la extensión de la reducción de riesgo generada por las nuevas medidas de tratamiento o la ampliación de las medidas existentes en términos de reducción de la probabilidad/frecuencia o impacto/severidad de las amenazas. La implementación de medidas de tratamiento propuestas o la ampliación de las existentes mitigan el riesgo porque:

- Eliminan algunas de las vulnerabilidades del sistema (defectos o debilidades), por consiguiente se reducen el número de posibles parejas de fuentes de amenazas / vulnerabilidades.
- Adicionan al objetivo para reducir la capacidad y motivación de las fuentes de amenaza.
- Reducen la magnitud de los impactos adversos.

El riesgo remanente después de la implementación de nuevas medidas de tratamiento o la ampliación de los existentes es el riesgo objetivo. Prácticamente no hay activos de TI libre de riesgos, y no todas las medidas implementadas eliminan los riesgos.

PASO 17: Determinación (Cálculo) del Riesgo Objetivo

La exposición final, es la exposición al riesgo que persiste, aun después de que se han ejecutado medidas de tratamiento definidas previamente. Se denominara exposición objetivo o nivel de riesgo objetivo, se calcula con la formula siguiente:

Exposición Objetivo o Nivel de Riesgo Objetivo	=	*Frecuencia objetivo * Severidad Objetivo*

Para determinar el valor de la frecuencia objetiva y severidad objetiva se utiliza el Apéndice 10 y la información será ingresada en las columnas 35 al 41 del Apéndice 09.

6. Aceptación del plan de tratamiento de riesgos

En esta etapa, el órgano sometido al análisis de riesgos y a su respectivo tratamiento debe determinar el nivel de impacto y riesgo aceptable, es por ello que se debe preguntar si hay riesgos que a pesar de haber sido tratados han cumplido con el objetivo de mitigación. Si la respuesta es NO, se debe volver hacer un tratamiento y si es SI se acepta el riesgo con sus medidas de tratamiento, responsabilidad, tiempo y costos, "etc. Esta decisión no es puramente técnica. Puede influir las decisiones políticas, gerenciales o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios"[4].

PASO 18: Aprobación del Plan de Tratamiento de Riesgos

a) Para ejecutar esta acción es necesario contar con el Plan de tratamiento de riesgos y valoración de riesgos residuales revisados por el órgano sometido bajo alcance.
b) Producto de esta etapa, obtendremos el Plan de Tratamiento de Riesgos, y la lista de riesgos aceptados con la respectiva justificación para aquellos que no cumplen con el criterio de aceptación normal.

7. Monitoreo y Revisión

Es el proceso que consiste en la evaluación de la implementación de los planes de acción para el adecuado funcionamiento de la gestión de riesgos en TI; incluye el reporte de las deficiencias encontradas y su corrección.

Comprende las acciones para asegurar que todas las medidas de tratamiento de riesgos se ejecuten de acuerdo a los planes de acción definidos. Este monitoreo deberá realizarse de acuerdo a:

PASO 19: Monitorear la ejecución de las medidas de tratamiento del riesgo y planes de acción.

Comprende las acciones para guiar y orientar que las medidas de tratamiento para los riesgos se ejecuten de acuerdo a los planes de acción definidos, así como el reporte de las deficiencias encontradas y su corrección.

[4] *Magerit v3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*

Para desarrollar el monitoreo de la implementación de los planes de acción la Oficina General de Planificación y Presupuesto (OGPP) en coordinación con la Dirección de Gestión de Riesgos (DGR) deberá elaborar un cronograma de monitoreo de acuerdo a los tiempos que se definieron en los planes de acción. Este cronograma deberá manejar tiempos de prevención y ejecución. Por ejemplo, se deberá empezar con el plan de acción que tenga el menor tiempo de implementación, si en este caso es de 1 mes (30 días), el tiempo de prevención será a los 15 días y el tiempo de ejecución será a los 30 días.

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

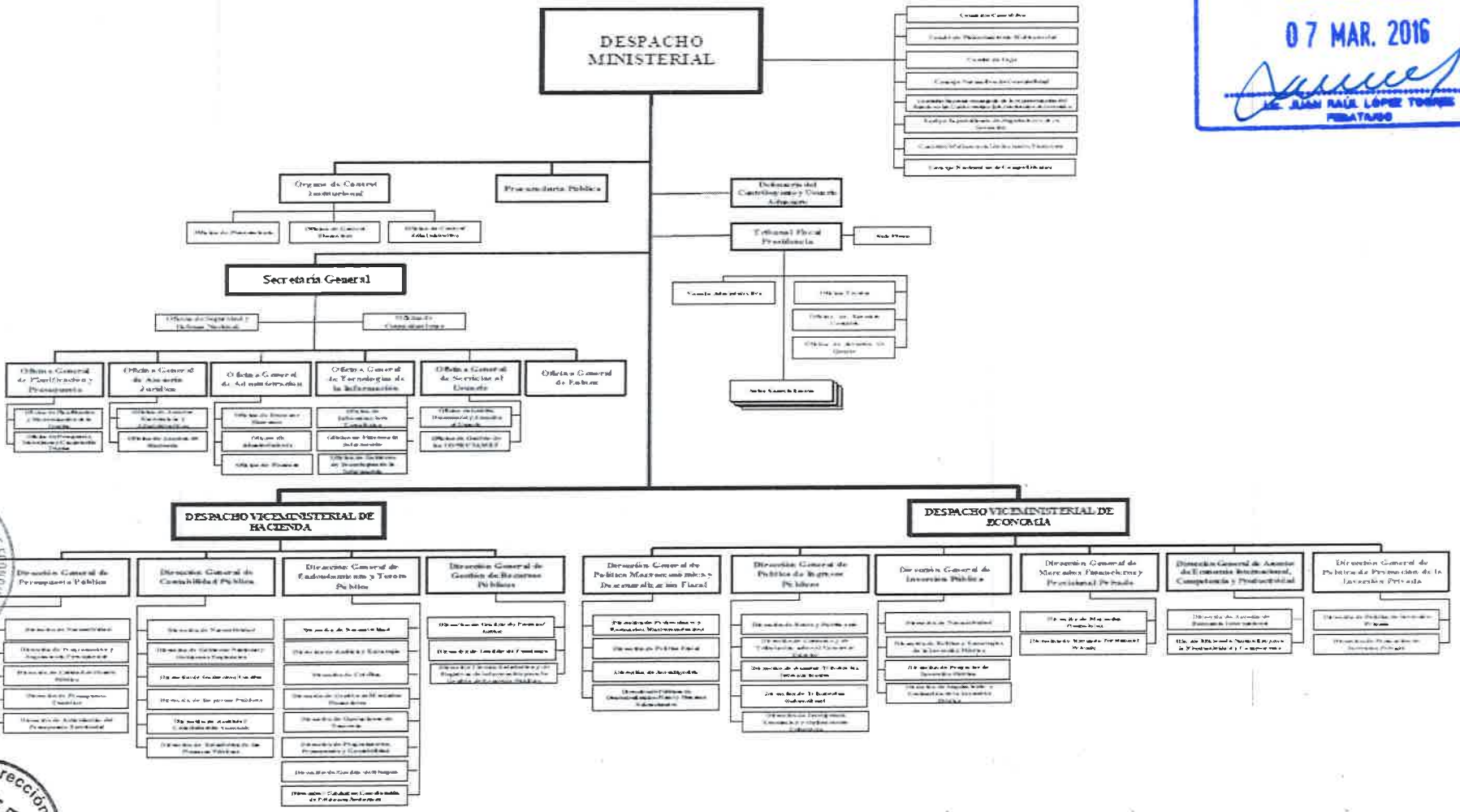
MINISTERIO DE ECONOMÍA Y FINANZAS

APÉNDICE

- ***Apéndice 01:*** *Organigrama del MEF*
- ***Apéndice 02:*** *Formato para trabajar el Inventario de Activos de TI*
- ***Apéndice 03:*** *Consideraciones para realizar el inventario de activos de TI*
- ***Apéndice 04:*** *Instrucciones para el llenado del inventario de activos de TI*
- ***Apéndice 05:*** *Instrucciones para la codificación de los activos de TI*
- ***Apéndice 06:*** *Tabla de valoración de activos de TI*
- ***Apéndice 07:*** *Amenazas Tipos*
- ***Apéndice 08:*** *Vulnerabilidades Tipos*
- ***Apéndice 09:*** *Formato para trabajar el Análisis y Evaluación de Riesgos en TI*
- ***Apéndice 10:*** *Tablas de Nivel de Frecuencia y Nivel de Severidad*
- ***Apéndice 11:*** *Formato para trabajar las medidas de tratamiento*

APENDICE 01

ORGANIGRAMA DEL MINISTERIO DE ECONOMIA Y FINANZAS (ROF 2014)



APENDICE 02

FORMATO PARA TRABAJAR EL INVENTARIO DE ACTIVOS DE TI

SUBPROCESO :		RESPONSABLE :		FECHA:	

1	2	3	4	5	6	7	8	9	10	11	12	13	14
IDENTIFICACION DE ACTIVOS								RESPONSABILIDAD		VALORIZACION DEL ACTIVO			
										C	I	D	
CLASIFICACION	TIPO	N°	NOMBRE DEL ACTIVO	CODIGO	DESCRIPCION	FUNCION	UBICACIÓN	PROPIETARIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

APENDICE 03

CONSIDERACIONES PARA REALIZAR EL INVENTARIO DE ACTIVOS DE TI

1. IDENTIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

En esta actividad se busca identificar los activos de tecnologías de la información relevantes dentro del alcance definido, determinando sus características, atributos, y su clasificación por tipos.

2. METODOS DE IDENTIFICACIÓN DE ACTIVOS DE TI

Se deben identificar el conjunto de activos de tecnologías de la información, entendiéndose como activo cualquier elemento que interactué con la información y que represente valor para el Ministerio. Estos activos serán aquellos que queden enmarcados dentro de la definición del alcance.

El inventario de activos de tecnologías de la información permitirá identificar los activos y clasificarlos en:

- Información (Datos)
- Software
- Hardware
- Comunicaciones
- Infraestructura (Instalaciones)

a) Información (Datos)

Independientemente al estado físico o lógico donde se encuentre, se refiere principalmente a:

- Información utilizada para la operatividad del proceso o servicio bajo alcance.
- Información estratégica necesaria para lograr los objetivos propuestos.
- Información personal, como puede ser definido específicamente en el sentido de las leyes nacionales sobre la privacidad de datos.

Ejemplos: Base de Datos, Proyectos de Resolución, Manuales técnicos de la infraestructura tecnológica, entre otros.

b) Software

Se refiere principalmente a:

Sistema Operativo: Software base de operaciones desde la cual todos los otros programas se ejecutan. Ejemplo: Windows (XP, Vista, 7, 8), Linux, Leopard X, IOS, otros.

Servicio, mantenimiento y administración: Software que complementa los servicios del sistema operativo y no está directamente al servicio de los usuarios o aplicaciones (aunque por lo general es esencial e incluso indispensable para el funcionamiento global del sistema de información). Ejemplo: Drivers, otros.

Estándar o paquetes: Son productos completos comercializados como tales (en lugar de una sola vez o desarrollos específicos). Ellos proporcionan servicios para los usuarios y las aplicaciones, pero no son personalizadas o específicas

como las aplicaciones empresariales. Ejemplo: Antivirus, Ofimática (Office 2010), software de diseño (Autocad), otros.

Sistemas de Gestión de Base de Datos: Es aquel software cuyo objetivo es servir de interfaz entre la base de datos, el usuario y las aplicaciones. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta. Permiten definir los datos a distintos niveles de abstracción y manipular dichos datos, garantizando la seguridad e integridad de los mismos. Ejemplo: Oracle, DB2, PostgreSQL, MySQL, MS SQL Server, etc.

Empresarial estándar: Este es un programa comercial diseñado para dar a los usuarios acceso directo a los servicios y funciones que requieren de su sistema de información en su contexto profesional. Hay una muy amplia, teóricamente ilimitada, gama de campos. Ejemplo: SAP, ERP, Software de contabilidad, otros.

Empresarial específico: Este es un software en el que diversos aspectos (sobre todo soporte, mantenimiento, actualización, etc.) han sido específicamente desarrollados para dar a los usuarios acceso directo a los servicios y funciones que requieren de su sistema de información. Hay una gama muy amplia, teóricamente ilimitado, de campos. Ejemplo: SIAF, SIAD, STD, otros.

c) Hardware

Se refiere principalmente a:

Equipo para el tratamiento de la data: Equipo de procesamiento de información automática que incluye los elementos necesarios para operar de forma independiente. Ejemplo: Mainframes, servidores, otros.

Equipo transportable: Laptop, asistente digital personal (PDA), tablets, otros.

Equipo fijo: PC (Computadora personal), máquinas de cajero automático (ATM), otros.

Periférico de proceso: Equipo conectado a una computadora a través de un puerto de comunicación (enlace serial, paralela, etc.) para transportar o transmitir datos. Ejemplo: Impresora, escáner, lector, fotocopiador, otros.

Soporte de Información:

Medio Electrónico; ejemplo: CD-ROM, USB, cartucho de copia de seguridad, desmontable, disco duro removible, cinta estática, otros.

Medio No Electrónico; ejemplo: Papel, diapositivas, transparencias, documentación, fax, videos, fotos, otros.

d) Comunicaciones

Se refiere principalmente a:

Medios de comunicación: Son las características de los protocolos de comunicación. Ejemplo: TCP/IP, otros.

Soporte: Son las características físicas y técnicas de los equipos de comunicación. Ejemplo: Cableado (Ethernet, Gigabit Ethernet, etc.), inalámbrico (Wifi, WIMAX, etc.), fibra óptica, otros.

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
07 MAR. 2016
Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

Relé pasivo o activo: Este subtipo incluye todos los dispositivos que no son las terminaciones lógicas de comunicaciones, pero son dispositivos intermedios o relé. Ejemplo: Accespoint, router, hub, switch, otros.

e) Infraestructura (Instalaciones)

El sitio comprende todos los lugares que contienen el alcance o la parte del alcance, y los medios físicos necesarios para su funcionamiento, principalmente:

Entorno externo: Esto afecta a todos los lugares en los que los medios de gestión de riesgos ("Controles") no pueden ser aplicados. Ejemplos: casas del personal, los locales de otra organización, área urbana, otros.

Local: Este lugar está delimitado por el perímetro de la organización en contacto con el exterior, esto puede ser un límite físico de protección obtenido mediante la creación de barreras físicas o medios de vigilancia alrededor de los edificios. Ejemplos: Edificios e instalaciones.

Zona: Una zona está formada por una frontera física protectora, particiones que forman los locales de la organización; se obtiene mediante la creación de barreras físicas alrededor de la infraestructura de la organización de procesamiento de información. Ejemplos: oficinas, zona de acceso reservado, zona segura.

Comunicaciones: Se refiere a las zonas especiales donde se ubican los equipos de comunicaciones y relacionados. Ejemplos: Centrales telefónicas, otros.

Utilitarios: Son los equipos que sirven de soporte o brindan energía a los sistemas de información, sin estar directamente relacionados con los datos o información, considerando si algún fallo en estos equipos afectaría a los activos principales. Ejemplos: fuentes de alimentación de energía eléctrica, equipos de climatización, equipos de aire acondicionado, otros.

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
07 MAR. 2016
FEDATARIO

MINISTERIO DE ECONOMÍA Y FINANZAS
REPÚBLICA DEL PERÚ

APENDICE 04

INSTRUCCIONES PARA EL LLENADO DEL INVENTARIO DE ACTIVOS DE TI

1. **N°:**

   Se indica el número consecutivo (1,2,…,n).

2. **NOMBRE DE ACTIVO**:

   Se indica el nombre del activo.

3. **CÓDIGO:**

   Se indica el código asignado según lo descrito en el Apéndice N° 05.

4. **DESCRIPCIÓN:**

   Se detallará las características y atributos del activo. Ejemplo: Equipo Proliant HP 505, procesador Xeon 3.5, 8MB memoria RAM, etc.

5. **FUNCIÓN:**

   Se describe la funcionalidad del activo dentro del sistema de información

6. **UBICACIÓN:**

   Se identificará la ubicación del activo.

7. **PROPIETARIO DEL ACTIVO**:

   Es el responsable del activo.

8. **USUARIO DEL ACTIVO:**

   Es el responsable por el uso adecuado de los activos.

9. **VALORACIÓN DEL ACTIVO**:

   Es el resultado promedio de los valores de las dimensiones de la información (C, I, D). Cada dimensión de seguridad de la información será valorada según lo descrito en el Apéndice N° 06.

APENDICE 05

INSTRUCCIONES PARALACODIFICACIÓN DE LOS ACTIVOS DE TI

Para la codificación de los activos se asignará un código según el tipo de activo y el proceso donde se encuentre, de acuerdo al siguiente detalle:

NUMERO DE PROCESO	ABREVIATURA DEL TIPO DE ACTIVO	NUMERO CONSECUTIVO
Se indica el número de proceso asignado según el Mapa de Procesos General.	DIN -Datos(Información) SOF-Software HAR -Hardware RED –Red de Comunicaciones SIT -Sitios	001,002, …,00X

Ejemplo: Proceso: Identificación y Registro (12)
Activo: Software
Número consecutivo: 012
Codificación del activo será: **12-SOF-012**

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
REPÚBLICA DEL PERÚ

APENDICE 06

TABLA DE VALORACIÓN DE ACTIVOS DE TI

DIMENSIÓN	CRITERIO	VALOR
CONFIDENCIALIDAD	**INFORMACIÓN DE CARÁCTER: RESERVADO** El activo es definido por una disposición legal u obligación contractual y/o puede ser conocida por un número reducido de personas o entidades autorizadas.	10
	INFORMACIÓN DE CARÁCTER: CONFIDENCIAL El activo es definido por una disposición legal u obligación contractual y/o es utilizada por el personal del proceso con autorización gerencial para el cumplimiento de sus funciones.	8
	INFORMACIÓN DE CARÁCTER: INTERNO El activo es definido por una disposición administrativa interna de la ENTIDAD y puede ser de conocimiento de toda la entidad.	5
	INFORMACIÓN DE CARÁCTER: PÚBLICO El activo puede ser de conocimiento público en general.	1
INTEGRIDAD	**MODIFICACIÓN NO PERMITIDA** El activo se encuentra definido por una disposición legal u obligación contractual para no ser modificado o es política de la entidad.	10
	MODIFICACIÓN AUTORIZADA El activo puede ser modificado por disposición legal o con autorización de nivel gerencial.	5
	MODIFICACIÓN LIBRE El activo puede ser modificado por el propietario del mismo.	1
DISPONIBILIDAD	**DISPONIBILIDAD PERMANENTE** El activo requiere estar disponible en todo momento y con interrupciones programadas de corto tiempo (Requerido por cada activo), debido a una disposición legal u obligación contractual o por políticas de la entidad.	10
	DISPONIBILIDAD PROGRAMADA El activo requiere estar disponible sólo en periodos programados por una disposición administrativa interna y aprobada a nivel gerencial.	5
	DISPONIBILIDAD MÍNIMA El activo puede no estar disponible en todo momento, sólo en casos específicos.	1

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
LIC. JUAN RAUL LÓPEZ TORRES
FEDATARIO

AMENAZAS TIPO

Nro	Amenaza	Tipo
1	Incendio	Daño físico
2	Daño por agua	
3	Contaminación	
4	Accidente mayor	
5	Destrucción del equipo o los medios	
6	Polvo, corrosión, congelación	
7	Fenómeno Climático	Eventos naturales
8	Fenómeno sísmico	
9	Fenómeno volcánico	
10	Fenómeno meteorológico	
11	Inundación	
12	Fallas del sistema de aire acondicionado o del suministro de agua	Pérdida de servicios esenciales
13	Perdida del suministro de electricidad	
14	Falla del equipo de telecomunicaciones	
15	Radiación electromagnética	Perturbación debido a radiación
16	Radiación térmica	
17	Pulsos electromagnéticos	
18	Intercepción de señales de interferencia comprometedoras	Compromiso de la información
19	Espionaje remoto	
20	Interceptación de comunicaciones	
21	Robo de medios o documentos	
22	Robo de equipos	
23	Hallazgo de medios reciclados o descartados	
24	Divulgación	
25	Datos de fuentes no confiables	

Código	Amenaza	Tipo
26	Adulteración del Hardware	
27	Adulteración del software	
28	Detección de posición	
29	Falla de equipo	Fallas técnicas
30	Mal funcionamiento del equipo	
31	Saturación del sistema de información	
32	Mal funcionamiento del software	
33	Uso no autorizado del equipo	Accionesno autorizadas
34	Copia fraudulenta del software	
35	Uso de software falsificado o copiado	
36	Corrupción de datos	
37	Procesamiento ilegal de datos	
38	Error en el uso	Compromiso de funciones
39	Abuso de derechos	
40	Falsificación de derechos	
41	Negación de acciones	
42	Ruptura en la disponibilidad del personal	
43	Hacking	Hacker, cracker
44	Ingeniería social	
45	Intrusión en el sistema, incursiones	
46	Acceso no autorizado al sistema	
47	Crimen informático (acoso cibernético)	Criminal informático
48	Acto fraudulento (reproducción de archivos, suplantación, intercepción)	
49	Soborno informático	
50	Falsificación o usurpación de la dirección	
51	Intrusión en el sistema	

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
07 MAR. 2016

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MAYOSSIAN
DIRECTOR
DGETP - MEF

Código	Amenaza	Tipo
52	Bomba/Terrorismo	Terrorismo
53	Equipo de guerra informática	
54	Ataque al sistema (ej.DDOS)	
55	Penetración en el sistema	
56	Adulteración del sistema	
57	Ventaja de defensa	Espionaje
58	Ventaja política	
59	Explotación económica	
60	Robo de información	
61	Intrusión en la privacidad personal	
62	Asalto a un empleado	Gente de adentro de la institución (empleados mal capacitados, resentidos, maliciosos, negligentes, deshonestos o despedidos)
63	Chantaje	
64	Búsqueda de información propietaria	
65	Abuso informático	
66	Fraude y robo	
67	Soborno por información	
68	Ingreso de datos falsificados o corruptos	
69	Intercepción	
70	Códigos maliciosos (ej. virus, troyano)	
71	Venta de información personal	
72	Disfunciones del sistema (bugs)	
73	Intrusión en el sistema	
74	Sabotaje al sistema	

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
LIC. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

APENDICE 08

VULNERABILIDADES TIPO

Código	Vulnerabilidad	Categoría
1	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Hardware
2	Falta de esquemas de reemplazo periódicos	
3	Susceptibilidad a la humedad, al polvo y a la suciedad	
4	Sensibilidad a la radiación electromagnética	
5	Falta de control eficiente del cambio de configuración	
6	Susceptibilidad a variación de voltaje	
7	Susceptibilidad a variaciones de temperatura	
8	Almacenamiento no protegido	
9	Falta de cuidado al descartarlo	
10	Copia no controlada	
11	Pruebas al software inexistentes o insuficientes	Software
12	Errores conocidos en el software	
13	No hacer "logout" cuando se sale de la estación de trabajo	
14	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
15	Falta de evidencia de auditoria	
16	Asignación equivocada de derechos de acceso	
17	Software ampliamente distribuido	
18	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	
19	Interfaz de usuario complicada	
20	Falta de documentación	
21	Seteo incorrecto de parámetros	
22	Fechas incorrectas	
23	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	
24	Tablas de claves no protegidas	
25	Mala administración de claves	

Código	Vulnerabilidad	Categoría
26	Habilitación de servicios innecesarios	
27	Software inmaduro o nuevo	
28	Especificaciones no claras o incompletas para los desarrolladores	
29	Falta de control de cambios eficaz	
30	Descarga y uso incontrolado de software	
31	Falta de copias de respaldo	
32	Falta de protección física del edificio, puertas y ventanas	
33	No producir informes de gestión	
34	Falta de pruebas de envió o recepción de mensaje	Red
35	Líneas de comunicación no protegidas	
36	Tráfico delicado no protegido	
37	Juntas malas en el cableado	
38	Punto de falla única	
39	Falta de identificación y autentificación de destinador y destinatario	
40	Arquitectura de red insegura	
41	Transferencia de claves en claro	
42	Gestión inadecuada de la red (capacidad de recuperación del ruteo)	
43	Conexiones no protegidas de la red publica	
44	Ausencia del personal	Personal
45	Procedimientos inadecuados del reclutamiento	
46	Capacitación de seguridad insuficiente	
47	Uso incorrecto del software y hardware	
48	Falta de conciencia de seguridad	
49	Falta de mecanismos de monitoreo	
50	Trabajo no supervisado del personal externo o de limpieza	
51	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es COPIA FIEL DEL ORIGINAL que he tenido a la vista
07 MAR. 2016
JUAN RAÚL LÓPEZ PORTILLO PERALTA

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

Código	Vulnerabilidad	Categoría
52	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Sitio
53	Ubicaciones en un área susceptible a las inundaciones	
54	Red inestable de energía eléctrica	
55	Falta de protección física del edificio, puertas y ventanas	
56	Falta de un procedimiento formal para el registro y baja de usuarios	Organización
57	Falta de proceso formal para revisar el derecho de acceso (supervisión)	
58	Disposiciones inexistentes o insuficientes (respecto de la seguridad) En contratos con clientes y/o terceros	
59	Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información	
60	Falta de auditorías regulares (supervisión)	
61	Falta de procedimientos de identificación y evaluación del riesgo	
62	Falta de informes de fallas registradas en los registros del Administrador y del operador	
63	Respuesta inadecuada del mantenimiento del servicio	
64	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	
65	Falta de procedimiento de control de cambios	
66	Falta de procedimiento formal para el control de la documentación de la empresa	
67	Falta de procedimiento formal para la supervisión del registro de la empresa	
68	Falta de proceso formal para autorización de información pública disponible	
69	Falta de asignación apropiada de responsabilidades de seguridad en la información	
70	Falta de planes de continuidad	
71	Falta de una política de uso de correos electrónicos	
72	Falta de procedimientos para introducir software en sistemas operativos	
73	Faltas de registro en los historiales del administrador y del operador	
74	Falta de procedimientos para manejo de la información clasificada	
75	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos	
76	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	
77	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
07 MAR. 2016

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF - sobs

MINISTERIO DE ECONOMÍA Y FINANZAS

Código	Vulnerabilidad	Categoría
78	Falta de política formal sobre el uso de computadoras portátiles	
79	Falta de control de activos que se encuentran fuera del local	
80	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"	
81	Falta de autorización al acceso a las instalaciones de procesamiento de la información	
82	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	
83	Falta de revisiones regulares de la gestión	
84	Falta de procedimientos para reportar debilidades en la seguridad	
85	Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales	

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
D-DGETP - MEF-sogos

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

APENDICE 09

FORMATO PARA TRABAJAR EL ANÁLISIS Y EVALUACIÓN DE RIESGOS EN TI

INICIO PROCESO:		PROCESO:		RESPONSABLE:		CARGO:		FECHA ELABORACION:	

EVALUACION DEL RIESGO																		TRATAMIENTO DEL RIESGO										APROBACION DE PLANES DE ACCION	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
N°	IDENTIFICACION DEL ACTIVO			AMENAZA						IMPACTO						PROBABILIDAD						NIVEL DE RIESGO INICIAL						NIVEL DE RIESGO OBJETIVO				APROBACION DE RIESGO OBJETIVO	
	NOMBRE	CATEGORIA	VALOR TOTAL DEL ACTIVO	Nivel Potencial de Daño (Tabla 7 Anx)	INTENCION			FUENTE	Causa y motivo del riesgo originado en dicha fuente	Efecto del riesgo potencial de daño	FRECUENCIA	VULNERAB.	ESTIMACION DEL NIVEL DE RIESGO INTRINSECO	EVALUACION DEL RIESGO INTRINSECO	CONTROLES (Existentes del activo o control)	MEDIDAS DE TRATAMIENTO EXISTENTES	EJECUCION (Si/No)	EFECTIVIDAD (Si/No)	PROBAB.	NIVEL DE EXPOSICION	FRECUENCIA REGIONAL	VULNERAB. REGIONAL	ESTIMACION DEL RIESGO INICIAL	EVALUACION DEL RIESGO INICIAL	MEDIDAS DE TRATAMIENTOS PROPUESTOS	RECURSOS	PCM PLAN DE ACCION	FRECUENCIA OBJETIVO	VULNERAB. OBJETIVO	ESTIMACION DEL RIESGO OBJETIVO	EVALUACION DEL RIESGO OBJETIVO	RESULTADO	COMENTARIOS
					DELIBERADA	ACCIDENTAL	AMBIENTAL																									

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

OGETIC - Dirección de Gestión de Riesgos - MEF
GREGORIO

CAMPOS DEL FORMATO DE ANALISIS Y EVALUACION DE RIESGOS

EVALUACIÓN DEL RIESGO

1. NUMERO

IDENTIFICACIÓN DEL ACTIVO

2. NOMBRE
3. CÓDIGO(S)
4. VALOR REAL DEL ACTIVO

AMENAZA

5. Modo Potencial de Efecto Falla
6. INTENCIÓN
9. FUENTE
10. Causa o motivo del modo potencial de efecto falla
11. IMPACTO Efecto del modo potencial de falla
12. FRECUENCIA
13. SEVERIDAD
14. ESTIMACION DEL RIESGO INTRINSECO
15. EVALUACION DEL RIESGO INTRINSECO

TRATAMIENTO DEL RIESGO

16. VULNERABILIDAD (Debilidad del activo o control)
17. MEDIDAS DE TRATAMIENTO EXSITENTES
18. EJECUCION (Severidad)
19. EFECTIVIDAD (Frecuencia)
20. EFICACIA
21. NIVEL DE EFICACIA
22. FRECUENCIA RESIDUAL
23. SEVERIDAD RESIDUAL

NIVEL DE RIESGO RESIDUAL

24. ESTIMACION DEL RIESGO RESIDUAL
25. EVALUACION DEL RIESGO RESIDUAL
26. MEDIDAS DE TRATAMIENTOS PROPUESTAS
27. RECURSOS
28. PLAN DE ACCION

NIVEL DE RIESGO OBJETIVO

29. FRECUENCIA OBJETIVO
30. SEVERIDAD OBJETIVO
31. ESTIMACIÓN DEL RIESGO OBJETIVO
32. EVALUACION DEL RIESGO OBJETIVO

APROBACIÓN DE PLANES DE ACCIÓN

APROBACIÓN DE RIESGO OBJETIVO

33. RESULTADO
34. COMENTARIOS

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF

APENDICE 10

NIVEL DE FRECUENCIA

Valor	*Descriptivo*	*Frecuencia (Probabilidad)*
4	*Muy Frecuente*	*El evento ocurre constantemente*
3	*Frecuente*	*El evento ocurre varias veces pero no llega a ser una constante*
2	*Poco Frecuente*	*El evento ocurre con baja frecuencia*
1	*Raro*	*El evento puede ocurrir excepcionalmente.*

NIVEL DE SEVERIDAD

Criterio	*Descripción*	*Valor*
CATASTRÓFICA	*Afecta la Continuidad del Negocio del MEF / Paralización de servicios críticos por encima de los tiempos tolerables*	*4*
SIGNIFICATIVA	*Afecta la Continuidad de un área o servicio especifico del MEF / Paralización de servicios específicos en los tiempos promedios tolerables*	*3*
MODERADA	*Puede afectar a un proceso de soporte del MEF que puede recuperarse dentro de los tiempos tolerables*	*2*
MENOR	*Su afectación es recuperada en un corto tiempo*	*1*

Dirección de Gestión de Riesgos
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR
DGETP - MEF-sobs

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es COPIA FIEL DEL ORIGINAL que he tenido a la vista
07 MAR. 2016
JUAN RAÚL LÓPEZ TORRES
FEDATARIO

APENDICE 11

FORMATO DE TRABAJO DE LAS MEDIDAS DE TRATAMIENTO – PLAN DE ACCION

Ministerio de Economía y Finanzas

PLAN DE ACCIÓN - MEDIDAS DE TRATAMIENTO

Plan Nro.	1
Fecha	

Unidad Orgánica/ Orgáno	
Codigo del riesgo(s) asociado(s)	

Nro.	Actividad a Realizar	Responsable	Recursos	Costos Estimados	Fecha Inicio	Fecha fin	Resultado Esperado	Meta Física	Fecha de verificación de la implementación	Fecha Cierre
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Firma del Corresponsal de Riesgos

Firma del Director

Dirección de Gestión de Riesgos - DGETP - MEF
GREGORIO BELAUNDE MATOSSIAN
DIRECTOR

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
07 MAR. 2016
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO