ES COPIA AUTENTICADA

ROGER A. SICCHA MARTINEZ
Director General
Oficina General de Administración
MINISTERIO DE ECONOMÍA Y FINANZAS

Resolución Directoral

Lima, *06 de abril de 2016* *N° 120-2016-EF/43.01*

CONSIDERANDO

Que, de conformidad con lo establecido en el literal d) del artículo 64 del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado mediante Decreto Supremo N° 117-2014-EF, se establece que corresponde a la Oficina General de Tecnologías de la Información, el formular y proponer políticas y normas de seguridad informática, e implementar soluciones de protección de las redes, equipos y sistemas de información del Ministerio, en concordancia con las políticas de seguridad establecidas;

Que, mediante Resolución Ministerial N° 081-2014-EF/44 se aprobó el documento de gestión denominado "Política de Seguridad de la Información del Ministerio de Economía y Finanzas", con el objetivo de establecer el marco general de gestión para proteger adecuadamente la información y que define un conjunto de principios, lineamientos y responsabilidades para tal propósito;

Que, mediante Resolución Ministerial N° 004-2016-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de gobierno electrónico, por considerar la seguridad de la información, como un componente crucial para dicho objetivo;

Que, en ese sentido, resulta necesario aprobar la "Metodología de Gestión de Riesgos de Seguridad de la Información", que tiene por objetivo definir un enfoque sistemático y ordenado para abordar la gestión de riesgos y determinar las necesidades y requerimientos relacionados con la seguridad de la información, como parte del Sistema de Gestión de Seguridad de la Información;

Que, mediante Resolución Ministerial N° 223-2013-EF/41, se incorpora en la Directiva N° 004-2012-EF/41.02 "Lineamientos para la elaboración de Directivas en el Ministerio de Economía y Finanzas", aprobada con Resolución Ministerial N° 359-2012-EF/41, el numeral 5.5 concerniente a la aprobación de documentos técnicos normativos que no sean directivas internas, tales como Manuales, Instructivos y otros de similar naturaleza, que emitan o propongan los propongan los órganos de administración interna, en materias de sus respectivas competencias para ser aprobados por el Director General de la Oficina General de Administración;

De conformidad con lo dispuesto en el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado con Decreto Supremo N° 117-2014-EF/43, y en la Resolución Ministerial N° 223-2013-EF/41.

SE RESUELVE:

Artículo 1.- Aprobar la "Metodología de Gestión de Riesgos de Seguridad de la Información", que como anexo forma parte integrante de la presente resolución.

Artículo 2.- Publicar la presente resolución 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.

REPUBLICA DEL PERU

MINISTERIO DE ECONOMÍA Y FINANZAS

Oficina General de Tecnologías de la Información

METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Oficina de Gobierno de Tecnologías de la Información

2016

HISTORIAL DE REVISIONES

Versión	Fecha	Detalle de cambios realizados	Elaborado por:	Revisado por:	Aprobado por:
01	11.02.2016	Adaptación de entregable elaborado por firma consultora M&T Consulting (en coordinación con la Dirección de Gestión de Riesgos) mediante contratación ADS-046-2015-EF/43.	Delfor Chacón C. José Visalot T.	Julio Molina G.	Percy Caro C.

Contenido

MINISTERIO DE ECONOMÍA Y FINANZAS · REPÚBLICA DEL PERÚ · Oficina de Gobierno de Tecnologías

1. INTRODUCCIÓN

El Ministerio de Economía y Finanzas (MEF), como toda organización en general, enfrenta diversos factores e influencias adversas de origen tanto interno como externo que podrían hacer incierto el logro de sus objetivos institucionales. El efecto de esta incertidumbre sobre dichos objetivos es conocido como "riesgo"[1].

El manejo adecuado del riesgo requiere que éste se identifique, se analice y luego se evalúe si el riesgo deba ser modificado mediante un tratamiento apropiado a fin de minimizar los impactos negativos o maximizar las oportunidades[2], según los criterios pertinentes que se hayan establecido en cada organización individual. Asimismo, la gestión de riesgos puede tener aplicación en varios campos de la actividad organizacional tales como la continuidad de las operaciones, la recuperación de desastres de tecnologías de la información, o la seguridad de la información.

En el presente documento se define un enfoque sistemático y ordenado con el que en el Ministerio se abordará la gestión de riesgos para efectos de determinar las necesidades y requerimientos relacionados con la seguridad de la información. De esta manera, la metodología descrita brindará soporte al funcionamiento efectivo del sistema de gestión de seguridad de la información del MEF en conformidad con las normas técnicas peruanas relevantes en la materia, y de manera particular, en concordancia con los lineamientos para la gestión del riesgo operacional y la metodología para la gestión de riesgos en tecnologías de la información que ha formulado la Dirección de Gestión de Riesgos del Ministerio.

[1] De acuerdo a la definición de "riesgo" en la norma técnica peruana sobre gestión del riesgo, NTP-ISO 31000:2011.

[2] De acuerdo a lo indicado en la norma técnica peruana sobre requisitos de los sistemas de gestión de seguridad de la información, NTP-ISO/IEC 27001:2014.

MINISTERIO DE ECONOMÍA Y FINANZAS · DESPACHO VICEMINISTERIAL · OFICINA DE GOBIERNO DE TECNOLOGÍAS

2. OBJETO

Establecer y describir los criterios, prácticas y procedimientos para la adecuada gestión de riesgos y oportunidades relacionadas con la seguridad de la información en el Ministerio.

3. BASE LEGAL

3.1. Resolución de Contraloría General Nº 320-2006-CG, que aprueba las Normas de Control Interno de aplicación en las entidades del Estado.

3.2. Resolución Ministerial N° 649-2012-EF/10, que aprueba la conformación del grupo denominado "*Comité de Gestión de la Seguridad de la Información*" en el Ministerio de Economía y Finanzas.

3.3. Resolución Ministerial N° 081-2014-EF/44, que aprueba la "Política de Seguridad de la Información del Ministerio de Economía y Finanzas".

3.4. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

4. ALCANCE

Los lineamientos metodológicos contenidos en el presente documento serán de aplicación en las actividades de valoración y tratamiento de riesgos de seguridad de la información, en concordancia con los requisitos de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

5. DEFINICIONES

a) Activo: Todo aquello que tenga valor para la organización.

b) Activo de información: Activo constituido por información relevante para los procesos organizacionales, así como todo elemento de registro, procesamiento, almacenamiento o transmisión de esta información. Para efectos de la presente metodología, los términos "*activo*" y "*activo de información*" se entenderán como sinónimos.

c) Amenaza: Causa potencial de un evento no deseado que puede resultar en daño a los activos de una organización.

d) Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y estimar su magnitud.

e) Clasificación de los activos de información: Categorización de los activos que tienen valor para la organización.

MINISTERIO DE ECONOMÍA Y FINANZAS · Oficina de Gobierno de Tecnologías · PERÚ

f) Control: Medida (proceso, política, regla, práctica u otra acción) que modifica un riesgo.

g) Confidencialidad: Característica por la cual se garantiza que la información no sea accesible ni sea divulgada a individuos, entidades o procesos no autorizados.

h) Criterio de aceptación del riesgo: Condición, establecida formalmente por la organización, que ayuda a determinar cuáles son aquellos riesgos con los que puede convivir la organización.

i) Custodio: Identifica a la persona o unidad organizativa que tiene la responsabilidad de mantener los niveles de protección adecuados en base a las especificaciones dadas por el propietario.

j) Disponibilidad: Característica por la cual se garantiza que se pueda disponer de un activo y éste se encuentre listo para ser utilizado cuando lo requiera una persona o unidad organizativa autorizada.

k) Estimación del riesgo: Asignación de valores a la probabilidad de ocurrencia del evento no deseado y al impacto respectivo, con el fin de valorar la magnitud del riesgo.

l) Evaluación de riesgos: Proceso de comparación del riesgo estimado con los criterios de aceptación establecidos en la organización, a fin de determinar si el riesgo y/o su magnitud es aceptable o tolerable.

m) Identificación de riesgos: Proceso para encontrar, reconocer y caracterizar los elementos de riesgo.

n) Impacto: Consecuencia adversa para la organización que resulta de la pérdida en la confidencialidad, integridad y disponibilidad de la información.

o) Integridad: Característica por la cual se garantiza que se salvaguarda la exactitud y cabalidad de los activos.

p) Inventario de activos: Registro conformado por los activos de información que tienen valor para la organización y que están dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) existente.

q) Incidente de seguridad de la información: Evento no deseado que tiene probabilidad de comprometer las operaciones de la organización y poner en riesgo la seguridad de su información.

r) Nivel de exposición al riesgo: Grado de magnitud de un riesgo expresado en términos de la combinación de su probabilidad y sus consecuencias (impacto).

s) Oportunidad: Evento que podría tener un efecto positivo sobre los objetivos organizacionales, conduciendo a la obtención de beneficios o recompensas.

t) Probabilidad de ocurrencia del riesgo: Medida del grado de posibilidad de que una amenaza explote una vulnerabilidad.

u) Propietario del activo: Persona o unidad organizativa que, con la aprobación gerencial respectiva, tiene la responsabilidad de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

v) Propietario del riesgo: Persona o unidad organizativa con responsabilidad y autoridad para gestionar un riesgo.

w) Respuesta al riesgo: Decisión o estrategia para tratar el riesgo, pudiendo ser: aceptar, evitar, transferir o reducir el riesgo.

x) Riesgo: Es la probabilidad de que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos.

y) Riesgo efectivo: Nivel de riesgos que se posee actualmente.

z) Riesgo residual: Riesgo remanente después de ser tratado.

aa) Tratamiento de riesgos: Proceso de selección e implementación de controles para minimizar el riesgo.

bb) Usuarios de los activos de información: Personas que usan los activos de información de la organización en sus actividades diarias.

cc) Vulnerabilidad: Debilidad de un activo que pueden ser explotadas por una o más amenazas.

dd) CGSI: Comité de Gestión de Seguridad de la Información

ee) EGR: Equipo de Gestión de Riesgos, conformado por el Oficial de Seguridad de la Información y por principales representantes de cada proceso en el alcance.

ff) OSI: Oficial de Seguridad de la Información

gg) OGTI: Oficina General de Tecnologías de la Información

hh) SGSI: Sistema de Gestión de Seguridad de la Información

ii) MEF: Ministerio de Economía y Finanzas

6. CONSIDERACIONES GENERALES

6.1. El ámbito dentro del cual se ejecutarán las acciones de la gestión de riesgos de seguridad de la información estará limitado al alcance vigente del Sistema de Gestión de Seguridad de la Información del Ministerio.

6.2. Los riesgos serán gestionados en un ciclo de mejora continua que se repetirá periódicamente (p.ej. anualmente) o cuando ocurra un cambio significativo en el proceso dentro del alcance, de tal forma que se asegure el control continuo de los riesgos de seguridad de la información a niveles aceptables.

En casos excepcionales, que comprendan cambios significativos en la entidad, en sus procesos o la ocurrencia de algún evento relevante que justifique su ejecución, se podrá realizar una gestión de riesgos no planificada.

6.3. La actualización de la presente Metodología de Gestión de Riesgos de Seguridad de la Información se realizará como consecuencia el ciclo natural de mejora del proceso de gestión de riesgos en el Ministerio, o por cambios en los siguientes aspectos del entorno organizacional, según sea necesario y apropiado:

a) políticas, estrategias y objetivos institucionales;

b) funciones y estructura organizacional;

c) contexto normativo y reglamentario;

d) enfoque de la evaluación de riesgos (métodos cualitativos o cuantitativos);

e) criterios de clasificación y valoración de activos;

f) criterios de evaluación del riesgo;

g) criterios de aceptación del riesgo.

6.4. Cualquier servicio referido a la gestión de riesgos de seguridad de la información que se realice en el Ministerio, debe tomar como referencia lo dispuesto por la presente metodología.

7. ROLES Y FUNCIONES

7.1. Propietarios de los activos de información

a) Tomar medidas para minimizar el riesgo por pérdida o exposición de los activos de información que están bajo su responsabilidad.

b) Promover la participación activa del personal en la identificación, análisis evaluación y tratamiento de riesgos de seguridad de la información.

c) Realizar el inventario de los activos de información y mantenerlo actualizado.

d) Clasificar la información de acuerdo con los niveles de clasificación que se establezcan.

e) Autorizar accesos sobre la información de las que son propietarios, ratificar periódicamente estos accesos e informar inmediatamente a las áreas competentes sobre el personal que no debería tener acceso a la misma.

f) Proponer medidas de control sobre la información a su cargo.

g) Definir la criticidad de la información a su cargo y los niveles mínimos de servicio cuando se requiere recuperar información en caso de desastres.

h) Revisar y dar la conformidad a la matriz de riesgos.

7.2. Custodios de los activos de información

a) Implementar los controles propuestos para la protección de los activos asignados para su custodia, según el plan de tratamiento de riesgos.

b) Reportar oportunamente incidentes y debilidades de seguridad de la información.

c) Apoyar activamente en las actividades de identificación, análisis, evaluación y tratamientos de riesgos de seguridad de la información, relacionados a tecnología.

7.3. Oficial de Seguridad de la Información (OSI)

a) Liderar los talleres a desarrollarse para la identificación, análisis y evaluación de riesgos de seguridad de la información.

b) Conformar para cada uno de los procesos del alcance del SGSI, un Equipo de Valoración y Tratamiento de Riesgos, el cual estará integrado por los propietarios y custodios de los activos de información y personal de apoyo involucrado.

c) Capacitar o gestionar la capacitación del Equipo de Valoración y Tratamiento de Riesgos, participar y asegurar su disponibilidad para el desarrollo de dichas actividades.

d) Presentar a los propietarios de riesgos el resultado de la gestión de riesgos (Plan de Tratamiento de Riesgos), para obtener su aprobación.

e) Revisar los resultados de la gestión de riesgos en un ciclo de mejora continua que se repetirá anualmente, y de manera excepcional si es que un evento significativo o cambio en la institución generara esta necesidad.

7.4. Equipo de Valoración y Tratamiento de Riesgos (EVTR)

- Participar de los talleres de gestión de riesgos que se lleven a cabo.
- Conocer la presente metodología de gestión de riesgos y oportunidades.
- Participar de la elaboración o actualización de los formatos de gestión de riesgos.
- Definir las estrategias a seguir a fin de gestionar los riesgos identificados.
- Proponer controles a ser evaluados dentro del marco de plan de tratamiento de riesgos.

8. PROCESO METODOLÓGICO

En el marco de la presente metodología, la gestión de riesgos consta de 5 actividades que se llevan a cabo de manera secuencial de la manera mostrada en la siguiente tabla:

Tabla 1: Actividades de la Gestión de Riesgos

Proceso	Fases	Actividades
Gestión de Riesgos	Preparación	Parametrización
	Valoración	Inventario de Activos
		Análisis de Riesgos
		Evaluación de Riesgos
	Tratamiento	Tratamiento de Riesgos

8.1. Parametrización

a) Nivel de aceptación del riesgo

EL MEF reconoce los siguientes niveles de riesgos: Extremo, Alto, Medio y Bajo. En la etapa de análisis y evaluación del riesgo, se han considerado como aceptables los riesgos definidos como Medio y Bajo. Es decir, aquellos riesgos

que no ocasionan un impacto significativo sobre el desempeño e integridad de los procesos.

Los riesgos tipificados con valor Extremo y Alto son considerados para ser tratados de acuerdo con lo descrito en el presente documento, salvo en los casos que se detallan en la siguiente sección.

b) Criterios de aceptación del riesgo

Se ha considerado que los riesgos identificados como Extremos o Altos al término de la actividad de Evaluación de Riesgos podrán ser aceptados sin requerir de un tratamiento, solo bajo las siguientes condiciones particulares:

a) El costo de tratar el riesgo se estima como mayor a la pérdida o impacto económico generado por la ocurrencia del mismo.

b) El costo de implementar el control o controles está fuera de presupuesto del año en curso.

c) No se dispone de recursos o se sufre recortes de presupuesto por decisión de la alta dirección.

8.2. Inventario de Activos

Se deberá iniciar con la elaboración del inventario de activos de información de los procesos considerados dentro del alcance del SGSI. A los activos de información identificados se les asignará un valor en base a los criterios de confidencialidad, integridad y disponibilidad sobre los mismos.

a) Identificación de los activos

Para cada proceso identificado, preparar la lista de los activos de Información (ver formato ***SGSI-FORM-01 Inventario de Activos de Información***) con los siguientes datos:

a) Código del activo

b) Nombre único del activo

c) Descripción del activo

d) Categoría del Activo: indica la naturaleza del activo (ver tabla 2).

e) Tipo: entendido como sub categoría del activo (ver tabla 2).

f) Clasificación: respecto al grado de secreto del uso del activo (ver tabla 3).

g) Frecuencia de uso: diario, semanal, quincenal, mensual, anual, eventual (ver tabla 4).

h) Tipo de Ubicación: física, lógica.

i) Ubicación: Descripción de la ubicación indicada.

j) Propietario: Persona responsable de la gestión, producción, mantenimiento, uso y seguridad de los activos.

k) Custodio: Persona responsable de la seguridad de información del activo durante el uso y custodia del mismo.

l) Requerimiento legal, reglamentario o contractual: si el activo está relacionado o sujeto a alguno se debe indicar.

Tabla 2: Categorías y tipos de activos

Categoría	Tipo de Activo
Información	Información electrónica
	Información escrita
	Información hablada
	Otro tipo de información
Software	Software comercial o herramientas, utilitarios
	Software desarrollado por terceros
	Software desarrollado internamente
	Software de administración de Base de Datos
	Otro software
Físicos (Hardware, comunicaciones e Infraestructura)	Equipo de procesamiento
	Equipo de comunicaciones
	Medio de almacenamiento
	Mobiliario y equipamiento
	Otros equipos
Servicios	Procesamiento y comunicaciones
	Servicios generales
	Otros servicios
Personal	Clientes (usuarios)
	Empleados
	Personal Externo
Imagen y reputación	Imagen y reputación

MINISTERIO DE ECONOMÍA Y FINANZAS · Oficina de Gobierno de Tecnologías

Tabla 3: Clasificación

Clasificación	Detalle
Público	Son todos aquellos activos que se presumen públicos, y que pueden ser accedidos tanto por miembros de la organización como por personas externas a ella (**público en general**), sin estar sujetos a ningún control.
Uso interno	Son todos aquellos activos que son accedidos exclusivamente por **personal interno de la institución** y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas de acceso.
Confidencial	Son todos aquellos activos que pertenecen a un **proceso o unidad orgánica** y que por su naturaleza son reservados exclusivamente al personal del área o proceso específico y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas de acceso.
Restringida	Es toda información cuyo contenido es restringido a un grupo determinado de individuos, seleccionados a partir de un proyecto específico o que pertenecen a un **grupo o nivel específico de poder** dentro de la organización.

Tabla 4: Frecuencia de uso

Frecuencia de Uso	Valor
Muy Frecuente (Diario y Semanal)	4
Frecuente (Quincenal)	3
Poco Frecuente (Mensual y Anual)	2
Raro (Eventual)	1

b) Valoración de activos

Se estima el valor del activo como el promedio de sumar los valores del nivel de relevancia respecto a la confidencialidad, integridad y disponibilidad (ver formato SGSI-FORM-01 Inventario de Activos de Información):

$$\text{Valor del Activo} = \frac{\text{(Confidencialidad + Integridad + Disponibilidad)}}{3}$$

Por ello, para determinar el nivel de relevancia de cada uno de las tres aristas de valoración del activo, se emplea la siguiente escala de valor (ver tabla 5).

Tabla 5: Escala de valor de los activos

Valor	Confidencialidad	Disponibilidad	Integridad
5 (Muy Alto)	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría **irreversiblemente** a la organización.	Se requiere que el activo **nunca** esté indisponible, pues su carencia afectaría **irreversiblemente** a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **0%**, pues la vulneración de su integridad afectaría **irreversiblemente** a la organización.
4 (Alto)	La información asociada al activo es **restringida** y solo personal de un proyecto específico puede acceder a ella, pues su divulgación afectaría **gravemente** a la organización.	Se considera que como máximo el activo puede estar indisponible por **una hora**, pues su carencia afectaría **gravemente** a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **15%**, pues la vulneración de su integridad afectaría **gravemente** a la organización.
3 (Medio)	La información asociada al activo es **confidencial** y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría **considerablemente** a la organización.	Se considera que como máximo el activo puede estar indisponible por **un día**, pues su carencia afectaría **considerablemente** a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **50%**, pues la vulneración de su integridad afectaría **considerablemente** a la organización.
2 (Bajo)	La información asociada al activo es **de uso interno** y solo personal del MEF puede acceder a ella, pues su divulgación afectaría **parcialmente** a la organización.	Se considera que como máximo el activo puede estar indisponible por **una semana**, pues su carencia afectaría **parcialmente** a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **85%**, pues la vulneración de su integridad afectaría **parcialmente** a la organización.
1 (Muy Bajo)	La información asociada al activo es **pública** y cualquiera puede acceder a ella, pues **no impacta** a la organización.	Se considera que como máximo el activo puede estar indisponible por **tiempo indefinido**, pues su carencia **no impacta** a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **100%**, pues la vulneración de su integridad **no impacta** a la organización.

Con base en el promedio obtenido (valor del activo en términos de confidencialidad, integridad y disponibilidad) y el rango de tasación establecido por el MEF para la selección de aquellos activos que serán considerados para continuar con la gestión de riesgos de seguridad de información, se identifican a los activos de valor más significativo (ver tabla 6).

MINISTERIO DE ECONOMÍA Y FINANZAS · Oficina de Gobierno de Tecnologías

Tabla 6: Tasación del activo

Valor	Tasación
4.001 – 5.000	Muy Alto
3.001 – 4.000	Alto
2.001 – 3.000	Medio
1.001 – 2.000	Bajo
1.000 – 1.000	Muy Bajo

Se deja establecido seleccionar aquellos activos cuyo valor es "Alto" y "Muy Alto" para pasar a la siguiente etapa de análisis.

8.3. Análisis de Riesgos

Una vez que se completa el inventario de activos de información, se procede al análisis de riesgos, donde se seleccionarán solo los activos de información cuyo valor resultó ser crítico. Y para estos activos de información se deberá identificar las posibles amenazas a las que están expuestos los mismos, así como también las vulnerabilidades y controles existentes.

a) Identificar las amenazas y sus fuentes

En base a la lista de activos que han sido identificados como relevantes, se realizará la identificación de las amenazas asociadas a cada uno de ellos (ver tabla 7).

Tabla 7: Tipos de Amenazas

No	Amenaza	Tipo
1	Acceso no autorizado a la información	Amenazas a la Información
2	Modificación no autorizada de la información	
3	Eliminación no autorizada de la información	
4	Robo de activos contenedores de información	
5	Inadecuada eliminación de activos contenedores de información	
6	Corrupción de datos por error de procesamiento	
7	Uso extra laboral de la información	
8	Ataques de Hacking/cracking sobre la información	
9	Virus informáticos que alteran o eliminan la información	
10	Fuga de Información	
11	Adulteración intencional del software (bombas lógicas, sabotaje)	Amenazas al Software
12	Cambios no autorizados sobre el software (mantenimientos)	

No	Amenaza	Tipo
13	Actualizaciones no controladas del software (parches)	
14	Instalación de software no licenciado o autorizado	
15	Copia no controlada del código fuente del software	
16	Saturación de la operación del software	
17	Hacking/cracking	
18	Virus informáticos	
19	Error Humano en los cambios sobre el software (bugs)	
20	Incompatibilidad en la operación con otros software	
21	Corto Circuito	Amenazas a Activos Físicos (Hardware, Comunicaciones e Infraestructura)
22	Filtraciones de Agua	
23	Filtración de Polvo	
24	Corrosión de equipos	
25	Congelación de equipos	
26	Desconexión de equipos	
27	Saturación de humedad en ambientes	
28	Fallas del sistema de aire acondicionado	
29	Radiación electromagnética	
30	Robo de equipos o de sus componentes	
31	Incumplimiento del plan de mantenimiento	
32	Uso inadecuado de los equipos	
33	Des configuración del equipo	
34	Obsolescencia de los componentes del equipo	
35	Falla de servicios para las telecomunicaciones	Amenazas a Servicios
36	Degradación de servicios para las telecomunicaciones	
37	Falla de la provisión de energía eléctrica	
38	Incumplimiento de fechas por parte de proveedores	
39	Provisión de servicios defectuosos (personal)	
40	Provisión de recursos defectuosos (materiales)	
41	Falla en servicios de información provistos por clientes	
42	Contaminación del ambiente por gases	Amenazas a Personal
43	Uso de credenciales falsificadas	
44	Bloqueo del acceso al centro de trabajo	
45	Dificultad en el desplazamiento hacia el centro de trabajo	

MINISTERIO DE ECONOMÍA Y FINANZAS · REPÚBLICA DEL PERÚ · Oficina de Gobierno de Tecnologías

No	Amenaza	Tipo
46	Asaltos/secuestros	
47	Enfermedad	
48	Sismo	Amenazas a Ubicaciones Físicas
49	Inundación	
50	Hundimiento de suelos	
51	Incendio	
52	Destrucción intencional de los ambientes (protestas)	

b) Identificar controles existentes y planificados

Luego se identifican los controles con que cuenta la institución y aquellos que al menos debería tener para implementar un adecuado nivel de seguridad de información del activo evaluado. Cada control cuenta con un nivel de capacidad respecto a su propia implementación:

Tabla 8: Nivel de Capacidad

Nivel de Capacidad	
Optimizado (5)	El control cuenta con marcos de uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones, a partir de las cuales se aplican mejoras.
Predecible (4)	El control cuenta con marcos de uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones
Definido (3)	El control implementado cuenta con una especificación o marco de su uso o aplicación permanente con hitos y responsables designados.
Documentado (2)	El control implementado cuenta con una declaración en una que obliga a su aplicación permanente.
Realizado (1)	Control implantado no riguroso ni documentado.

Para cada uno de estos controles se deben definir los siguientes atributos:

a) Descripción del control.

b) Tipo de control: preventivo, de detección o correctivo.

c) Nivel de Capacidad (ver tabla 8).

d) Cláusula, Objetivo de control y Control relacionado a la ISO 27002.

Estos controles son agrupados en base a su tipo; de manera que obtenemos tres Niveles de Capacidad promedio, cada uno de los cuales corresponde a los controles preventivos, de detección y correctivos, respectivamente.

Considerando estos valores, se determina el Nivel de Vulnerabilidad del activo frente a las amenazas:

$$\text{Nivel de Vulnerabilidad} = 6 - \frac{\text{Cap. de ctrls. preventivos + Cap. de ctrls. de detección + Cap. de ctrls. correctivos)}}{3}$$

c) Identificar los niveles de amenaza

Para determinar el nivel de amenaza, se emplea la siguiente escala de valor:

Tabla 9: Nivel de Amenaza

	Nivel de Amenaza
5	Una o más veces a la semana
4	Una vez al mes
3	Una vez al año
2	Ha sucedido alguna vez
1	Nunca ha ocurrido

d) Estimar de la probabilidad de ocurrencia del riesgo

La Probabilidad de Ocurrencia es el promedio de sumar los valores del nivel de Vulnerabilidad y el Nivel de Amenaza (***ver formato SGSI-FORM-02 Análisis de Riesgos de Seguridad de la Información***):

$$\text{Probabilidad de Ocurrencia} = \frac{\text{(Nivel de Vulnerabilidad + Nivel de Amenaza)}}{2}$$

e) Tasar la probabilidad de ocurrencia del riesgo

Para determinar si una amenaza es significativa respecto a un activo, se identifica la Probabilidad de Ocurrencia dentro del rango del nivel de ocurrencia establecido (ver formato SGSI-FORM-02 Análisis de Riesgos de Seguridad de la Información):

Tabla 10: Tasación de la Probabilidad

Valor	Tasación
4.001 – 5.000	Muy Frecuente (Muy alto)
3.001 – 4.000	Frecuente (Alto)
2.001 – 3.000	Poco Frecuente (Medio)
1.001 – 2.000	Raro (Bajo)

MINISTERIO DE ECONOMÍA Y FINANZAS · Oficina de Gobierno de Tecnologías

Se ha establecido seleccionar aquellos riesgos cuya probabilidad es Muy frecuente (Muy Alto) y Frecuente (Alto), para pasar a la siguiente etapa: Evaluación.

8.4. Evaluación de Riesgos

Una vez completado el análisis de riesgos, se procederá a la evaluación de riesgos donde se utilizará como información de entrada los riesgos seleccionados en la actividad precedente, para luego valorizar el impacto que podría causar cada una de las amenazas identificadas.

a) Evaluar el impacto sobre la institución

Para cada amenaza identificada se valoriza los impactos que estas tendrán sobre los activos de información (ver formato ***SGSI-FORM-03 Evaluación de Riesgos de Seguridad de la Información***). Para la determinación del Nivel de Impacto se promedian los valores de cada aspecto a considerar: imagen institucional (o económico), operacional y legal.

Tabla 11: Impactos de las Amenazas

Valor	Impacto (Severidad)		
	Imagen Institucional	Operacional	Legal
	Pérdida de imagen	Paralización de operaciones de la Institución	Incumplimiento de leyes, reglamentos o contratos
Catastrófica (4)	Pérdidas de imagen institucional	No se pueden recuperar las operaciones	Se afecta la permanencia de la institución
Significativa (3)	Pérdidas de imagen de altos cargos.	Las operaciones tardan meses en reanudarse	Se afecta la permanencia de una de las áreas de la institución
Moderada (2)	Pérdidas de imagen de un área	Las operaciones tardan días en reanudarse	Se afecta a una de los autoridades de la institución
Menor (1)	Pérdidas de imagen del personal regular de la Institución.	Se opera parcialmente	Se afecta al personal regular de la institución

b) Estimar el nivel de exposición al riesgo

El Nivel de Exposición al Riesgo es el promedio de multiplicar los valores calculados en los pasos anteriores (ver formato SGSI-FORM-03 Evaluación de Riesgos de Seguridad de la Información):

a) Nivel de Impacto (Severidad).
b) Probabilidad de Ocurrencia del Riesgo (Frecuencia).

MINISTERIO DE ECONOMÍA Y FINANZAS · REPÚBLICA DEL PERÚ · Oficina de Gobierno de Tecnologías

De esta forma, se calcula en Nivel de Riesgo Real o Nivel de Exposición al Riesgo, según el producto indicado:

Nivel de Exposición al Riesgo	=	(Nivel del Impacto * Probabilidad de Ocurrencia del Riesgo)

c) Tasar el nivel de exposición al riesgo

Para determinar el nivel de riesgo, se identifica el Nivel de Exposición al Riesgo dentro del rango indicado (ver formato SGSI-FORM-03 Evaluación de Riesgos de Seguridad de la Información):

Tabla 12: Tasación del nivel de exposición al riesgo

Valor	Tasación
16 - 20	Extremo
11 – 15	Alto
6 –10	Medio
1 – 5	Bajo

Se ha establecido seleccionar aquellos riesgos cuyo valor es Extremo y Alto, para pasar a la siguiente etapa: Tratamiento. Debe considerarse también la aplicación del **Nivel de aceptación de riesgos**, definido en el presente documento (ver Sección 8.1).

8.5. Tratamiento de Riesgos

a) Propuesta de tratamiento de los riesgos

La institución debe determinar qué niveles de riesgos serán considerados como significativos, es decir, serán seleccionados para ser tratados, siguiendo un criterio similar al de las fases anteriores.

Una vez efectuado el análisis y la evaluación del riesgo, se debe decidir cuáles acciones se han de tomar con los activos que están sujetos a riesgos reales y significativos para la institución. Para ello se puede aplicar una de las estrategias que se muestran en la siguiente tabla:

Tabla 13: Tipo de Control

Medida frente al Riesgo	
Retener o Aceptar	Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas.

Medida frente al Riesgo	
Reducir	Reducir el impacto o la probabilidad de ocurrencia mediante la implementación de un control de seguridad de la información. Se utiliza cuando al implementar el control trae beneficios mayores a la inversión de su implementación.
Evitar	Eliminar la fuente del proceso que genera la amenaza. Se utiliza cuando el nivel de riesgo es alto, la actividad del proceso o sistema que lo genera no es de gran impacto en términos de negocio para la Entidad, de modo que puede ser retirada funcionalmente.
Transferir	Transferir el impacto del riesgos a terceros (empresas aseguradoras o proveedores de servicio). Se utiliza cuando no se puede mitigar la probabilidad de ocurrencia de un riesgo pero el impacto es inminente.

Cada estrategia tomada está asociada a una serie de atributos, para cada una de ellas detallamos lo siguiente:

a) Retener (Aceptar): La aceptación del riesgo debe ser realizada formalmente por la institución, ya que su elección implica que la institución es consciente de las posibles amenazas a las que se encuentra expuesta y que está optando por no tomar medidas frente a estas. Para ello, debe estar sujeta a una serie de criterios formales, detallados en la sección 8.1 Criterios de Aceptación de Riesgo.

b) Reducir: Esta estrategia implica la implementación de controles, los cuales la institución se compromete a establecer; para cada uno de ellos se debe indicar lo siguiente: Nombre del Control, Tipo de Control, Nivel de Capacidad, Responsable, Costo, Fechas de inicio y fin de implementación.

c) Evitar: Debido a las implicancias de evitar un riesgo, esta medida también debe contar con ciertos atributos que la describan: Detalle de la medida (Observaciones), Responsable, Costo, Fechas de inicio y fin de realización.

d) Transferir: Finalmente, la elección de transferir el riesgo, que conlleva a la relación con una entidad externa, requiere del siguiente detalle: Medida (Observaciones), Responsable, Costo, Fechas de inicio y fin de realización.

b) Plan de tratamiento de riesgos

Producto de esta selección se genera el Plan de Tratamiento haciendo uso del formato ***SGSI-FORM-04 Plan de Tratamiento del Riesgo Gestión de oportunidades.***

Seguidamente, tal como lo estipula la norma técnica peruana NTP-ISO/IEC 27001:2014, se elabora la Declaración de Aplicabilidad. Para ello se hace uso del formato ***SGSI-FORM-05 Declaración de Aplicabilidad***, el que contiene la relación de los controles necesarios y la justificación para su inclusión, sea que estén implementados o no, y la justificación de la exclusión de los controles indicados en el Anexo A de dicha norma técnica.

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

NOTA: Para el caso de la estrategia de Reducir usada en el Plan de Tratamiento de Riesgos, los propietarios de los riesgos aceptan los controles propuestos y los riesgos residuales (riesgos que surgen después de la aplicación de los controles planificados) mediante la firma del formato SGSI-FORM-07 Acta de Aprobación del Plan de Tratamiento de Riesgos y Riesgos Residuales.

9. GESTIÓN DE OPORTUNIDADES

A partir del análisis de contexto que consiste en determinar el entorno externo y el interno, comprendemos la realidad en la cual operará el SGSI. Luego, de manera similar a la gestión de riesgos, se identifican posibles fuentes de oportunidad que permitan alcanzar o lograr los objetivos de la organización, se analizan los potenciales beneficios e impactos de las oportunidades identificadas, se fijan prioridades y se establecen los planes de acción o proyectos para implementar las oportunidades.

Las acciones mencionadas de gestión de oportunidades se llevan a cabo por el mismo equipo que efectúa la gestión de riesgos, y ambos tipos de actividades pueden efectuarse paralelamente.

La gestión de oportunidades se lleva a cabo empleando el formato ***SGSI-FORM-06 Matriz de Tratamiento de Oportunidades***. Los campos se completan de la siguiente manera:

Tabla 14: Gestión de oportunidades

Nombre del Campo	Descripción del Campo
Código de la oportunidad	Se asigna un código con el siguiente formato: **OP- XX** (donde XX, es el número correlativo de la oportunidad correspondiente).
Descripción de la oportunidad	Narrativa descriptiva de la oportunidad identificada.
Área de Impacto	Identificación del área de impacto, en donde la oportunidad puede llevarse a cabo. Las áreas de impacto posible son: - Impacto Legal - Impacto Imagen - Impacto Operacional
Objetivo Organizacional	Descripción del objetivo estratégico organizacional al que brindará soporte la oportunidad identificada.
Tratamiento de la oportunidad	Existe 2 opciones de tratamiento de la oportunidad: - **Explotar**: Tratar de hacer que la oportunidad definitivamente suceda. Se deben tomar medidas para asegurar que los beneficios de la oportunidad se realicen. - **Ignorar**: Menores oportunidades pueden ser ignoradas, mediante la adopción de un enfoque reactivo sin tomar acciones explícitas.

Nombre del Campo	Descripción del Campo
Responsable	Definir el responsable de implementar la oportunidad.
Fecha de Cumplimiento	Indicar la fecha en que la oportunidad estará implementada.
Resultados Evaluados	Indicar el resultado de la evaluación de la implementación de la oportunidad.
Recursos	Indicar los recursos requeridos para ejecutar la oportunidad.

A continuación, en el mismo formato "*SGSI-FORM-06 Matriz de Tratamiento de Oportunidades*", se formula el plan de acción para la oportunidad identificada, indicando las actividades a realizar, fecha de inicio y fin, los resultados de la aplicación del plan y la evidencia correspondiente.

10. RESPONSABILIDADES

10.1. La Oficina de Gobierno de TI de la OGTI, es la responsable de velar por el cumplimiento de la presente Metodología, así como su elaboración, publicación y difusión.

11. CONSIDERACIONES COMPLEMENTARIAS

11.1. Los formatos aprobados en los procedimientos vigentes que tenga relación con la gestión de riesgo de la seguridad de la información, se adecuarán a los planteados en la presente metodología.

12. ANEXOS

12.1. SGSI-FORM-01 Inventario de Activos de Información del Sistema de Gestión de la Seguridad de la Información del MEF. (Anexo N°01)

12.2. SGSI-FORM-02 Análisis de Riesgos de Seguridad de la Información. (Anexo N°02).

12.3. SGSI-FORM-03 Evaluación de Riesgos de Seguridad de la Información. (Anexo N°03)

12.4. SGSI-FORM-04 Plan de Tratamiento de Riesgos. (Anexo N°04)

12.5. SGSI-FORM-05 Declaración de Aplicabilidad. (Anexo N°05)

12.6. SGSI-FORM-06 Matriz de Tratamiento de Oportunidades. (Anexo N°06)

12.7. SGSI-FORM-07 Acta de Aprobación del Plan de Tratamiento de Riesgos y los Riesgos Residuales. (Anexo N°07)

MINISTERIO DE ECONOMÍA Y FINANZAS · Oficina de Gobierno de Tecnologías

Anexo N° 01

SGSI-FORM-01 Inventario de Activos de Información del Sistema de Gestión de la Seguridad de la Información del MEF

	Inventario de Activos de Información del Sistema de Gestión de la Seguridad de la Información del MEF	CODIGO SGSI-FORM-01	REVISION 6
		FECHA 27/11/2015	PAGINA 1

1. Proceso: _____ 4. Cargo del Responsable: _____ 7. Fecha: _____

2. Área: _____ 5. Teléfono del Responsable: _____

3. Responsable del Área: _____ 6. Email del Responsable: _____

COD.	ACTIVO	DESCRIPCIÓN	CATEGORÍA DEL ACTIVO	TIPO DE UBICACIÓN (FÍSICA O LÓGICA)	UBICACIÓN	CLASIFICACIÓN				FRECUENCIA DE USO				PROPIETARIO	CUSTODIO	REQUISITOS LEGALES, REGULATORIOS Y CONTRACTUALES	VALOR DEL ACTIVO Y NIVEL DE TASACIÓN				
						PÚBLICA	INTERNA	CONFIDENCIAL	RESTRINGIDA	Muy Frecuente	Frecuente	Poco Frecuente	Raro				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	NIVEL DE TASACIÓN
ACTIVOS DE INFORMACIÓN																					
ACTIVOS DE SOFTWARE																					
ACTIVOS FÍSICOS																					
SERVICIOS																					
PERSONAL (CLIENTES, EMPLEADOS, PERSONAL EXTERNO)																					
IMAGEN Y REPUTACIÓN																					

CATEGORIAS Y TIPOS DE ACTIVOS

CATEGORÍA	CÓDIGO	Tipo de Activo
Activos de Información	I1	Información electrónica
	I2	Información escrita
	I3	Información hablada
	I4	Otro tipo de información
Activos de Software	SW1	Software comercial o herramientas, utilitarios
	SW2	Software desarrollado por terceros
	SW3	Software desarrollado internamente
	SW4	Software de administración de Base de Datos
	SW5	Otro software
Activos Físicos	F1	Equipo de procesamiento
	F2	Equipo de comunicaciones
	F3	Medio de almacenamiento
	F4	Mobiliario y equipamiento
	F5	Otros equipos
Servicio (Terceros)	S1	Procesamiento y comunicaciones
	S2	Servicios generales
	S3	Otros servicios
Personal	P1	Clientes
	P2	Empleados
	P4	Personal Externo
Imagen y Reputación	IR1	Imagen y Reputación

VALOR DEL ACTIVO	
VALOR DEL ACTIVO	**CONFIDENCIALIDAD**
5 (Muy Alto)	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría irreversiblemente a la organización.
4 (Alto)	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, pues su divulgación afectaría gravemente a la organización.
3 (Medio)	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la organización.
2 (Bajo)	La información asociada al activo es de uso interno y solo personal del MEF puede acceder a ella, pues su divulgación afectaría parcialmente a la organización.
5 (Muy Bajo)	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la organización
VALOR DEL ACTIVO	**INTEGRIDAD**
5 (Muy Alto)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0%, pues la vulneración de su integridad afectaría irreversiblemente a la organización.
4 (Alto)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 15%, pues la vulneración de su integridad afectaría gravemente a la organización.
3 (Medio)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50%, pues la vulneración de su integridad afectaría considerablemente a la organización.
2 (Bajo)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85%, pues la vulneración de su integridad afectaría parcialmente a la organización.
5 (Muy Bajo)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100%, pues la vulneración de su integridad no impacta a la organización.
VALOR DEL ACTIVO	**DISPONIBILIDAD**
5 (Muy Alto)	Se requiere que el activo nunca esté indisponible, pues su carencia afectaría irreversiblemente a la organización.
4 (Alto)	Se considera que como máximo el activo puede estar indisponible por una hora, pues su carencia afectaría gravemente a la organización.
3 (Medio)	Se considera que como máximo el activo puede estar indisponible por un día, pues su carencia afectaría considerablemente a la organización.
2 (Bajo)	Se considera que como máximo el activo puede estar indisponible por una semana, pues su carencia afectaría parcialmente a la organización.
5 (Muy Bajo)	Se considera que como máximo el activo puede estar indisponible por tiempo indefinido, pues su carencia no impacta a la organización.

MINISTERIO DE ECONOMÍA Y FINANZAS
REPÚBLICA DEL PERÚ
Oficina de Gobierno de Tecnologías

Valor del Activo

Se estima el Valor del Activo del promedio de sumar los valores del nivel de importancia de la Confidencialidad, Integridad y Disponibilidad.

Nivel de Tasación

Valor del Activo	Nivel de Tasación
4,01 a 5,00	Muy Alto
3,01 a 4,00	Alto
2,01 a 3,00	Medio
1,01 a 2,00	Bajo
1	Muy Bajo

Niveles de Clasificación

Categorización de los activos que tienen valor para la Entidad. Dicha tipificación se divide en:

Restringida: Es toda información cuyo contenido es restringido a un grupo determinado de individuos, seleccionados a partir de un proyecto específico o que pertenecen a un grupo o nivel específico de poder dentro de la organización.

Confidencial: Son todos aquellos activos que pertenecen a un proceso o unidad orgánica y que por su naturaleza son reservados exclusivamente al personal del área o proceso específico y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas de acceso.

Uso Interno: Son todos aquellos activos que son accedidos exclusivamente por personal interno de la institución y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas

Anexo N° 02

SGSI-FORM-02 Análisis de Riesgos de Seguridad de la Información

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

CODIGO	REVISION
SGSI-FORM-02	1
FECHA	PAGINA
27/11/2015	1

1. Proceso: _____
2. Área: _____
3. Responsable del Área: _____
4. Cargo del Responsable: _____
5. Teléfono del Responsable: _____
6. Email del Responsable: _____

Fecha: _____

Nº	ACTIVO	AMENAZA		MECANISMO DE PROTECCIÓN EXISTENTE						Nivel de Vulnerabilidad	RIESGO	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad		Probabilidad Ocurrencia del Riesgo	Nivel de Probabilidad Ocurrencia
AMENAZAS A LOS ACTIVOS DE INFORMACIÓN												
AMENAZAS A LOS ACTIVOS DE SOFTWARE												
AMENAZAS A ACTIVOS FÍSICOS												
AMENAZAS A LOS SERVICIOS												
AMENAZAS AL PERSONAL												
AMENAZAS A LAS UBICACIONES FÍSICAS												

ANÁLISIS DE RIESGOS

CONTENIDO
RIESGOS

N°
Indicar el número correlativo y secuencial del activo.

Activo
Indicar los principales activos que pueden ser afectados por alguna amenaza, cuyo nivel de tasación sea "Alto".

Amenaza
Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

Nivel de Amenaza (Escala de Likert)
Estimación de la probabilidad de ocurrencia de la amenaza:

5 Muy Alto (Una o más veces a la semana)
4 Alto (Una vez al mes)
3 Medio (Una vez al año)
2 Bajo (Ha sucedido alguna vez)
1 Muy bajo (Nunca ha ocurrido)

Nivel de Capacidad
Nivel de Capacidad que los mecanismos de protección (preventivos, detectivos y correctivos) existentes han alcanzado:

5 Optimizado: El control cuenta con marcos do uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones, a partir de las cuales se aplican mejoras.
4 Predecible: El control cuenta con marcos de uso, hitos, responsables y se monitorea a través de la recopilación y análisis de mediciones
3 Definido: El control implementado cuenta con una especificación o marco de su uso o aplicación permanente con hitos y
2 Documentado: El control implementado cuenta con una declaración en una que obliga a su aplicación permanente.
1 Realizado: Control implantado no riguroso ni documentado

Vulnerabilidad
Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

Nivel de Vulnerabilidad (Escala de Likert)
Grado de exposición que posee el activo frente a una amenaza:

5 Muy Alto (Impactaría irreversiblemente)
4 Alto (Impactaría gravemente)
3 Medio (Impactaría considerablemente)
2 Bajo (Impactaría parcialmente)
1 Muy Bajo (No Impactarla)

Nivel de Impacto Economica, Legal y Operacional (Escala de Likert)

5 Muy Alto (Impactaría irreversiblemente)
4 Alto (Impactarla gravemente)
3 Medio (Impactaría considerablemente)
2 Bajo (Impactarla parcialmente)
1 Muy Bajo (No impactaria)

Riesgo
Es la probabilidad de que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos.

Probabilidad de Ocurrencia
Se estima la Probabilidad de Ocurrencia del promedio de los valores resultantes del Nivel de Vulnerabilidad y el

Nivel de Probabilidad de Ocurrencia

Valor	Tasación
4.001 – 5.000	Muy Alto
3.001 – 4.000	Alto
2.001 – 3.000	Medio
1.001 – 2.000	Bajo
1.000 – 1.000	Muy Bajo

ANÁLISIS DE RIESGOS

CONTENIDO

CLASIFICACIÓN DE LAS AMENAZAS

1 **Amenazas Naturales**
Inundaciones, Tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales.

2 **Amenazas en Instalaciones**
Fuego, explosión, caída de energía, daño de agua, pérdida de acceso, fallas mecánicas.

3 **Amenazas Humanas**
Huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave.

4 **Amenazas Tecnológicas**

5 **Amenazas Operacionales**

6 **Amenazas Sociales**
Motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo.

CLASIFICACIÓN DE LAS VULNERABILIDADES

1 **Seguridad de los Recursos Humanos**
Falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de

2 **Control de Acceso**

3 **Seguridad Física y Ambiental**
Control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, suceptibilidad de equipos a variaciones de voltaje.

4 **Gestión de Operaciones y Comunicación**
Complicadas interfases para usuarios, control de cambio inadecuado, gestión de red inadecuada carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión.

5 **Mantenimiento, Desarrollo y Adquisición de Sistemas de Información**
Protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos.

Anexo N° 03

SGSI-FORM-03 Evaluación de Riesgos de Seguridad de la Información

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO	REVISIÓN
OGSI-FORM-03	1
FECHA	PÁGINA
27/11/2015	[illegible]

1. Proceso: ____________
2. Área: ____________
3. Responsable del Área: ____________
4. Cargo del Responsable: ____________
5. Teléfono del Responsable: ____________
6. Email del Responsable: ____________
7. Fecha: ____________

COD	ACTIVO	AMENAZA	CRITERIOS DE EVALUACIÓN						RIESGO EFECTIVO	
			Impacto							
			Impacto Legal	Impacto Económico /Imagen Institucional	Impacto Operacional	Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Relevancia del Activo (Valor del Activo)	Nivel de Exposición al Riesgo	Nivel de Riesgo
AMENAZAS A LOS ACTIVOS DE INFORMACIÓN										
AMENAZAS AL SOFTWARE										
AMENAZAS A ACTIVOS FÍSICOS										
AMENAZAS A SERVICIOS										
AMENAZAS AL PERSONAL										
AMENAZAS A LA IMAGEN										

MINISTERIO DE ECONOMÍA Y FINANZAS - REPÚBLICA DEL PERÚ - Oficina de Gobierno de Tecnologías

EVALUACIÓN DE RIESGOS

CONTENIDO

N°
Indicar el número correlativo y secuencial del activo.

Activo
Indicar los principales activos que pueden ser afectados por alguna amenaza, cuyo nivel de tasación sea "Alto".

Amenaza
Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

Nivel de Amenaza (Escala de Likert)
Estimación de la probabilidad de ocurrencia de la amenaza:

5 Muy Alto (Una vez a la semana)
4 Alto (Una vez al mes)
3 Medio (Una vez cada 6 meses)
2 Bajo (Una vez al año)
1 Muy bajo (Una vez cada 5 años)

Vulnerabilidad
Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

Nivel de Vulnerabilidad (Escala de Likert)
Grado de exposición que posee el activo frente a una amenaza:

5 Muy Alto (Impactaría irreversiblemente)
4 Alto (Impactaría gravemente)
3 Medio (Impactaría considerablemente)
2 Bajo (Impactaría parcialmente)
1 Muy Bajo (No impactaría)

Nivel de Impacto Economica, Legal y Operacional (Escala de Likert)

5 Muy Alto (Impactaría irreversiblemente)
4 Alto (Impactaría gravemente)
3 Medio (Impactaría considerablemente)
2 Bajo (Impactaría parcialmente)
1 Muy Bajo (No impactaría)

Riesgo
Probabilidad de que una amenaza se materialice sobre una vulnerabilidad de un activo de Información, causando un determinado impacto en la Institución.

Probabilidad de Ocurrencia
Se estima la Probabilidad de Ocurrencia del promedio de los valores resultantes del Nivel de Vulnerabilidad y el Nivel de Amenaza.

Nivel de Probabilidad de Ocurrencia

Valor	Tasación
4.001 – 5.000	Muy Alto
3.001 – 4.000	Alto
2.001 – 3.000	Medio
1.001 – 2.000	Bajo
1.000 – 1.000	Muy Bajo

Anexo N° 04
SGSI-FORM-04 Plan de Tratamiento de Riesgos

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO: SGSI-F-SRGO4 | REVISIÓN: 1 | FECHA: 27/1/2015 | PÁGINA: 1

1. Proceso:
2. Área:
3. Responsable del Área:
4. Cargo del Responsable:
5. Teléfono del Responsable:
6. Email del Responsable:
Fecha:

ITEM	ACTIVO	AMENAZA	RIESGO INHERENTE: Nivel de Exposición al Riesgo	RIESGO INHERENTE: Nivel de Riesgo	CONTROL PROPUESTO	DESCRIPCIÓN / OBSERVACIONES	CUMPLIMIENTO CONTROL (Si/No)	COSTO ANUAL	TIEMPO ANUAL	OPCIÓN PARA EL TRATAMIENTO	RIESGO RESIDUAL: VULNERABILIDAD: Nivel de Exposición al Riesgo	RIESGO RESIDUAL: VULNERABILIDAD: Nivel de Vulnerabilidad	RIESGO RESIDUAL: VULNERABILIDAD: Probabilidad de Ocurrencia de Riesgo	RIESGO RESIDUAL: IMPACTO: Impacto Legal	RIESGO RESIDUAL: IMPACTO: Impacto Económico	RIESGO RESIDUAL: IMPACTO: Impacto Operacional	RIESGO RESIDUAL: IMPACTO: Nivel de Imagen	RIESGO RESIDUAL: Nivel de Exposición al Riesgo (Valor de Activo)	RIESGO RESIDUAL: Nivel de Exposición al Riesgo	RIESGO RESIDUAL: Nivel de Tolerancia	IMPLEMENTACIÓN: RESPONSABLE	IMPLEMENTACIÓN: FECHA INICIO	IMPLEMENTACIÓN: FECHA FIN
	AMENAZAS A LOS ACTIVOS DE INFORMACIÓN																						
	AMENAZAS A LOS ACTIVOS DE SOFTWARE																						
	AMENAZAS A LOS ACTIVOS FISICOS																						
	AMENAZAS A LOS SERVICIOS																						
	AMENAZAS AL PERSONAL (CLIENTES, EMPLEADOS, PERSONAL EXTERNO)																						

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

TRATAMIENTO DE RIESGOS

CONTENIDO

CONTROLES PROPUESTOS

Control Propuesto

Función de protección propuesta para reducir el riesgo identificado.

Descripción / Observación

Descripción u observación de la función de protección propuesta.

Opción para el Tratamiento

R Reducir (Reducir el impacto o la probabilidad de ocurrencia a niveles aceptables mediante la implementación de controles de seguridad de la información)
A Aceptar (Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas)
E Evitar (Reducir a su mínima expresión la posibilidad de ocurrencia de la amenaza)
T Transferir (Transferir el impacto del riesgo a terceros (empresas aseguradoras o proveedores de servicio))

Costo Aproximado

Estimación del costo para implementar la función de protección propuesta.

4 Mayor a S/.100,000
3 De S/.30,000 a S/.100,000
2 De S/.15,000 a S/. 30,000
1 Menor a S/.15,000
D Desconocido

Tiempo Aproximado

Estimación del tiempo de implementación de la función de protección propuesta.

C Corto plazo (Menos de 3 meses)
M Mediano plazo (De 3 a 12 meses)
L Largo plazo (Más de 1 año)
D Desconocido

Riesgo Residual

Riesgo remanente después de un tratamiento del riesgo.

Nivel de Riesgos

Se estima el Nivel de Tolerancia al Riesgo del promedio de sumar los valores del nivel de Relevancia del Activo, el nivel de Probabilidad de Ocurrencia del Riesgo y el Nivel de Impacto.

Nivel de exposición al Riesgo	Nivel de Tolerancia
3.334 - 5.000	Alto
1.667 - 3.333	Medio
1.000- 1.666	Bajo

MINISTERIO DE ECONOMÍA Y FINANZAS · REPÚBLICA DEL PERÚ · Oficina de Gobierno de Tecnologías

Anexo N° 05
SGSI-FORM-05 Declaración de Aplicabilidad

MINISTERIO DE ECONOMÍA Y FINANZAS
REPÚBLICA DEL PERÚ
Oficina de Gobierno de Tecnologías

DECLARACIÓN DE APLICABILIDAD

CÓDIGO	REVISIÓN
SGSI-FORM-05	1
FECHA	PÁGINA
27/11/2015	1

Cláusula	Objetivo de Control	Control	Aplica	Detalle de los Controles	Justificación de la
A.5 Política de seguridad de la información	A.5.1 Dirección de la Gerencia para la Seguridad de la Información	A.5.1.1 Políticas para la seguridad de la información			
		A.5.1.2 Revisión de las políticas para la seguridad de información			
A.6 Organización de la Seguridad de la Información	A.6.1 Organización interna	A.6.1.1 Roles y Responsabilidades para la Seguridad de la Información			
		A.6.1.2 Segregación de Funciones			
		A.6.1.3 Contacto con autoridades			
		A.6.1.4 Contacto con grupos especiales de interés			
		A.6.1.5 Seguridad de la Información en la Gestión de Proyectos			
	A.6.2 Dispositivos Móviles y Teletrabajo	A.6.2.1 Política de Dispositivos Móviles			
		A.6.2.2 Teletrabajo			
A.7 Seguridad de los Recursos Humanos	A.7.1 Antes del Empleo	A.7.1.1 Selección			
		A.7.1.2 Términos y condiciones del empleo			
	A.7.2 Durante el Empleo	A.7.2.1 Responsabilidades de la gerencia			
		A.7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información			
		A.7.2.3 Proceso disciplinario			
	A.7.3 Terminación y cambio de empleo	A.7.3.1 Terminación o cambio de responsabilidades del empleo			
A.8 Gestión de Activos	A.8.1 Responsabilidad por los activos	A.8.1.1 Inventario de activos			
		A.8.1.2 Propiedad de los activos			
		A.8.1.3 Uso aceptable de los activos			
		A.8.1.4 Retorno de activos			
	A.8.2 Clasificación de la información	A.8.2.1 Clasificación de la información			
		A.8.2.2 Etiquetado de la información			
		A.8.2.3 Manejo de activos			
	A.8.3 Manejo de los medios	A.8.3.1 Gestión de medios removibles			
		A.8.3.2 Disposición de medios			
		A.8.3.3 Transferencia de medios físicos			
A.9 Control de accesos	A.9.1. Requisitos de la empresa para el control de	A.9.1.1 Política de control de accesos			
		A.9.1.2 Acceso a redes y servicios de red			
	A.9.2 Gestión de acceso de usuario	A.9.2.1 Registro y baja de usuarios			
		A.9.2.2 Aprovisionamiento de acceso a usuarios			
		A.9.2.3 Gestión de derechos de accesos privilegiados			
		A.9.2.4 Gestión de información de autentificación secreta de usuarios			
		A.9.2.5 Revisión de Derechos de acceso de usuarios			
		A.9.2.6 Remoción o ajuste de derechos de acceso			
	A.9.3 Responsabilidades de los usuarios	A.9.3.1 Uso de información de autenticación secreta			
	A.9.4 Control de acceso a sistema y aplicación	A.9.4.1 Restricción de acceso a la información			
		A.9.4.2 Procedimientos de ingreso seguro			
		A.9.4.3 Sistema de gestión de contraseñas			
		A.9.4.4 Uso de programas utilitarios privilegiados			
		A.9.4.5 Control de acceso al código fuente de los programas			

MINISTERIO DE ECONOMÍA Y FINANZAS · Oficina de Gobierno de Tecnologías

A.10 Criptografía	A.10.1 Controles Criptográficos	A.10.1.1 Política sobre el uso de controles criptográficos			
		A.10.1.2 Gestión de claves			
A.11 Seguridad Física y ambiental	A.11.1 Áreas Seguras	A.11.1.1 Perímetro de seguridad física			
		A.11.1.2 Controles de Ingreso Físico			
		A.11.1.3 Asegurar oficinas, áreas e instalaciones			
		A.11.1.4 Protección contra amenazas externas y ambientales			
		A.11.1.5 Trabajo en áreas seguras			
		A.11.1.6 Áreas de despacho y cargas			
	A.11.2 Equipos	A.11.2.1 Emplazamiento y protección de los equipos			
		A.11.2.2 Servicios de suministro			
		A.11.2.3 Seguridad del cableado			
		A.11.2.4 Mantenimiento de equipos			
		A.11.2.5 Remoción de activos			
		A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones			
		A.11.2.7 Disposición o reutilización segura de equipos			
		A.11.2.8 Equipos de usuario desatendidos			
		A.11.2.9 Política de escritorio limpio y pantalla limpia			
A.12 Seguridad de las Operaciones	A.12.1 Procedimientos y Responsabilidades Operativas	A.12.1.1 Procedimientos operativos documentados			
		A.12.1.2 Gestión del cambio			
		A.12.1.3 Gestión de la capacidad			
		A.12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones			
	A.12.2 Protección contra códigos maliciosos	A.12.2.1 Controles contra códigos maliciosos			
	A.12.3 Respaldo	A.12.3.1 Respaldo de la información			
	A.12.4 Registros y monitoreo	A.12.4.1 Registro de Eventos			
		A.12.4.2 Protección de información de registros			
		A.12.4.3 Registros del administrador y del operador			
		A.12.4.4 Sincronización del reloj			
	A.12.5 Control del software operacional	A.12.5.1 Instalación de software en sistemas operacionales			
	A.12.6 Gestión de vulnerabilidad técnica	A.12.6.1 Gestión de vulnerabilidades técnicas			
		A.12.6.2 Restricciones sobre la instalación de sofware			
	A.12.7 Consideraciones para la auditoría de los	A.12.7.1 Controles de auditoría de sistemas de información			
	A.13.1 Gestión de seguridad de la red	A.13.1.1 Controles de la red			
		A.13.1.2 Seguridad de servicios de red			
		A.13.1.3 Segregación en redes			
	A.13.2 Transferencia de información	A.13.2.1 Políticas y procedimientos de transferencia de la información			
		A.13.2.2 Acuerdo sobre transferencia de información			
		A.13.2.3 Mensajes electrónicos			
		A.13.2.4 Acuerdos de confidencialidad o no divulgación			
A.14 Adquisición, desarrollo y mantenimiento de sistemas	A.14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad de información			
		14.1.2 Aseguramiento de servicios de aplicación en redes públicas			
		14.1.3 Protección transacciones de servicios de aplicación			
	A.14.2. Seguridad en los procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro			
		14.2.2 Procedimientos de control de cambio en sistemas			
		14.2.3 Revisión técnica de aplicaciones luego de cambios en la plataforma operacional			
		14.2.4 Restricciones sobre cambios a paqueles de software			
		14.2.5 Principios de Ingeniería de sistemas seguros			
		14.2.6 Ambiente de desarrollo seguro			
		14.2.7 Desarrollo subcontratado			
		14.2.8 Prueba de la seguridad del sistema			
		14.2.9 Prueba de la aceptación del sistema			
	A.14.3 Información de prueba	A.14.3.1 Protección de datos de prueba			

A.15 Relaciones con los proveedores	A.15.1 Seguridad de la información en las relaciones con los proveedores	15.1.1 Política de seguridad de información para las relaciones con proveedores				
		15.1.2 Abordar la seguridad en los acuerdos con proveedores				
		15.1.3 Cadena de suministro de tecnología de la información y comunicación				
	A.15.2 Gestión de entrega de servicios del proveedor	15.2.1 Monitoreo y revisión de servicios de proveedores				
		15.2.2 Gestión de cambios para servicios de proveedores				
A.16 Gestión de Incidentes de Seguridad de la Información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos				
		16.1.2 Reporte de eventos de seguridad de información				
		16.1.3 Reporte debilidades de seguridad de la información				
		16.1.4 Evaluación y decisión sobre los eventos de seguridad de información				
		16.1.5 Respuesta a incidentes de seguridad de información				
		16.1.6 Aprendizaje de incidentes de seguridad de información				
		16.1.7 Recolección de evidencia				
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio	A.17.1 Continuidad de seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de información				
		17.1.2 Implementación de la continuidad de la seguridad de información				
		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de información				
	A.17.2 Redundancias	A.17.2.1 Instalaciones de procesamiento de la informacón				
A.18 Cumplimimento	A.18.1 Cumplimiento con requisitos legales y contractuales	18.1.1 Identificación de la ley aplicable y los requisitos contractuales				
		18.1.2 Derechos de propiedad intelectual				
		18.1.3 Protección de registros				
		18.1.4 Privacidad y protección de información de identificación personal				
		18.1.5 Regulación de controles criptográficos				
	A.18.2 Revisiones de seguridad de la información	18.2.1 Revisión independiente de la seguridad de información				
		18.2.2 Cumplimiento con las políticas y normas de seguridad				
		18.2.3 Revisión del cumplimiento técnico				

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

Anexo N° 06
SGSI-FORM-06 Matriz de Tratamiento de Oportunidades

TRATAMIENTO DE OPORTUNIDADES

CÓDIGO	REVISIÓN
SGSI-FORM-06	1
FECHA 27/11/2015	PÁGINA 1

CÓDIGO DE LA OPORTUNIDAD	DESCRIPCIÓN DE LA OPORTUNIDAD	AREA DE IMPACTO	OBJETIVO ORGANIZACIONAL	TRATAMIENTO DE OPORTUNIDAD	RESPONSABLE	FECHA DE CUMPLIMIENTO	RESULTADOS EVALUADOS	RECURSOS

MINISTERIO DE ECONOMÍA Y FINANZAS · Oficina de Gobierno de Tecnologías

	PLAN DE ACCIÓN POR CADA OPORTUNIDAD	CÓDIGO SGSI-FORM-06	REVISIÓN 1
		FECHA 27/11/2015	PÁGINA 1

CÓDIGO DE LA OPORTUNIDAD	ACTIVIDADES	FECHA DE INICIO	FECHA DE FIN	RESULTADO	RESPONSABLE	EVIDENCIA

Anexo N° 07
SGSI-FORM-07 Acta de Aprobación del Plan de Tratamiento de Riesgos y los Riesgos Residuales

Fecha 05 feb. 16

Acta de Aprobación del Plan de Tratamiento de Riesgos y Riesgos Residuales

Los Propietarios de los riesgos de seguridad de la información identificados en el Ministerio de Economía y Finanzas, declaran:

- ✓ Comprendemos y aprobamos el **Plan del Tratamiento del Riesgo** y, por tanto, nos comprometemos a la implementación de los controles indicados en este documento.
- ✓ Reconocemos que la implementación de controles para el tratamiento de riesgos es un proceso que reducirá la probabilidad o el impacto de los riesgos, por lo que su ejecución no hace que el MEF sea invulnerable frente a los riesgos residuales.
- ✓ Aceptamos los riesgos residuales, producto de la implementación de los controles, decisión tomada con entera responsabilidad y en forma voluntaria.
- ✓ Declaramos que la aceptación de estos riesgos residuales expirará en un año a partir de la fecha de firma de este documento, dado que tendrán que ser evaluados en una nueva gestión de riesgos, para el próximo periodo de operación del SGSI.

N°	Nombre del Propietario del Riesgo	Cargo	Firma

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías