METODOLOGÍA
MEDICIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
SGSI-ME-02

Elaborado por:	Revisado por:	Aprobado por:
.....	.....	.....
Nombre y Firma	Nombre y Firma	Nombre y Firma

1. OBJETIVO:

Establecer los criterios para identificar, registrar y medir la gestión y efectividad del Sistema de Gestión de Seguridad de la Información (SGSI) según los requisitos y controles definidos en la norma técnica peruana NTP ISO/IEC 27001:2014.

Con el fin de poder establecer el nivel de efectividad y mejora continua del SGSI implementado, el CGSI ha establecido la ejecución anual de la medición de indicadores de gestión de seguridad de la información que deben ser presentados en la Revisión por la Dirección.

2. ALCANCE:

La presente metodología aplica a todas las áreas de la SUNAT que estén involucradas en la medición del SGSI.

3. DOCUMENTOS ASOCIADOS:

- Programas de Gestión de Medición del Sistema de Gestión de Seguridad de la Información SGSI-ME-02.FO-01.
- Determinación de Medidas y Mediciones del Sistema de Gestión de Seguridad de la Información SGSI-ME-02.FO-02.
- Evaluación de Objetivos y Metas del Sistema de Gestión de Seguridad de la Información SGSI-ME-02.FO-03.

4. DOCUMENTOS DE REFERENCIA:

NTP ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.

.

5. DEFINICIONES Y SIGLAS:

Definiciones

5.1 Atributo: Propiedad o característica de un objeto que se puede distinguir cuantitativa o cualitativamente por medios humanos o automatizados.

5.2 Propietario del Riesgo: Persona o entidad que tiene la responsabilidad y la autoridad para gestionar un riesgo.

5.3 Indicador: Medida que provee una estimación o evaluación de atributos específicos derivados de un modelo analítico con respecto a la necesidad definida de información.

5.4 Indicador de Gestión: Componente o coeficiente resultante de los cálculos según la medición

establecida en los controles sobre los requisitos definidos en el SGSI.

5.5 Medición: Proceso de obtención de información acerca de la eficacia del SGSI y los controles utilizando un método de medición, una función de medición, un modelo de análisis y criterios de decisión.

5.6 Mejora Continua: Actividad recurrente para mejorar el desempeño de los procesos en forma coherente con los requisitos y políticas de la organización.

5.7 Método de Medición: Una secuencia lógica de las operaciones, descritas de forma genérica, utilizadas en la cuantificación de un atributo con respecto a una escala específica.

Nota: El tipo de método de medición depende de la naturaleza de las operaciones utilizadas para cuantificar un atributo. Se pueden distinguir dos tipos:

- Subjetivo: cuantificación mediante opinión humana;
- Objetivo: cuantificación sobre la base de reglas numéricas.

5.8 Resultados de la Medición: Uno o más indicadores y sus interpretaciones asociadas que conducen a la necesidad de información.

Siglas

5.9 OFSI: Oficial de Seguridad de la Información.

5.10 CGSI: Comité de Gestión de Seguridad de la Información.

5.11 RDMM: Responsable de Desarrollar las Medidas y Mediciones.

5.12 SGSI: Sistema de Gestión de Seguridad de la Información.

5.13 SUNAT: Superintendencia Nacional de Aduanas y de Administración Tributaria.

5.14 SN: Superintendente Nacional.

6. METODOLOGÍA:

6.1. Condiciones Generales:

6.1.1. El Programa de Gestión para la Medición del SGSI se desarrolla en concordancia con la política y el alcance del SGSI, lo cual permite determinar los objetivos, metas y programas de gestión.

6.1.2. La operación de medición de la seguridad de la información incluye

actividades que son esenciales para asegurar que los resultados de la medición desarrollada proporcionan información precisa con respecto a la eficacia del SGSI implementado, los controles o el grupo de los controles y las necesidades de acciones de mejora apropiadas. Esta actividad incluye lo siguiente:

- Integrar procedimientos de medición en el funcionamiento general del SGSI.
- Recolectar, almacenar y verificar los datos.

6.1.3. En el análisis y evaluación de los indicadores, los datos recolectados deberán ser analizados para desarrollar resultados de la medición y estos deberán ser comunicados. Esta actividad incluye lo siguiente:

- Analizar los datos y desarrollar los resultados de las mediciones; y
- Comunicar los resultados de las mediciones a las partes interesadas pertinentes.

6.1.4. Para realizar el procedimiento de medición se debe tener en cuenta los siguientes criterios.

Objeto de la medición	Objeto (entidad) que se caracterizan a través de la medición de sus atributos. Un objeto puede incluir procesos, planes, proyectos, recursos y sistemas o componentes de estos.
Atributo	Propiedad o característica de un objeto de medición que se puede distinguir cuantitativamente o cualitativamente por medios humanos o automatizados.
Método de medición	Secuencia lógica de operaciones utilizadas para cuantificar un atributo con respecto a una escala especificada.
Medida base	Una medida base se define en términos de un atributo y el método de medición especificado para cuantificarlo (ej. Número de personas capacitadas, número de sitios, costo acumulado a la fecha). Como se recogen los datos, se asigna un valor a la medida base.
Función de medición	Algoritmo o cálculo realizado para combinar dos o más medidas. La escala y unidad de la medida derivada depende de las escalas y unidades de las medidas base, de las cuales está compuesta, así como también de cómo son combinadas por la función.
Indicador	Medida que provee una estimación o evaluación de los atributos especificados derivados de un modelo analítico con respecto a una definida necesidad de información. Los indicadores son la base para el análisis y la toma de decisiones. El modelo analítico es un algoritmo o cálculo que combina una o más medidas base o derivada con un criterio de decisión asociado. Se basa en la comprensión, o la suposición de, la relación esperada entre la medida base y/o su comportamiento a lo largo del tiempo. Un modelo analítico produce estimaciones o evaluaciones relevantes a una

	definida necesidad de información.
Criterio de Decisión	Umbrales, objetivos o modelos utilizados para determinar la necesidad de una acción o investigación, o para describir el nivel de confianza en un determinado resultado. Criterios de decisión para ayudar a interpretar los resultados de la medición.

6.2. Desarrollo, Operación, Análisis y Evaluación de las Medidas y Mediciones

RDMM:

1. Elabora una vez al año el Programa de Gestión para la Medición del SGSI en el documento Programas de Gestión de Medición del Sistema de Gestión de Seguridad de la Información SGSI-ME-02.FO-01, cuando sea necesario, se incluye el sustento de actividades.
2. Comunica a todos los involucrados, vía mail, el documento Programas de Gestión de Medición del Sistema de Gestión de Seguridad de la Información SGSI-ME-02.FO-01.
3. Desarrolla los criterios definidos en el ítem 6.1.4. Para el desarrollo de las medidas utiliza el documento Determinación de Medidas y Mediciones del Sistema de Gestión de Seguridad de la Información SGSI-ME-02.FO-02.

OFSI:

4. Analiza y evalúa utilizando el documento Evaluación de Objetivos y Metas del Sistema de Gestión de Seguridad de la Información SGSI-ME-02.FO-03.

5. ¿El indicador del resultado es rojo?
   - Si: Ir al ítem 5.1.
   - No: Ir al ítem 5.2.

5.1. Generar una medida correctiva siguiendo lo especificado en el Procedimiento de Acciones Correctivas del Sistema de Gestión de Seguridad de la Información SGSI-PR-04, ir al ítem 5.2.

5.2. Informar al CGSI, los resultados de la medición, para su aprobación y conocimiento.

CGSI:

6. Aprobar el resultado de la medición, siguiendo lo especificado en el Procedimiento de Revisión por la Dirección del Sistema de Gestión de Seguridad de la Información SGSI-PR-02.

7. CONTROL DE CAMBIOS:

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial	01	04/02/2019	Oficial de Seguridad de la Información