INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

ESQUEMA 1

DE NORMA IRAM-ISO/IEC 27004

Tecnología de la información

Gestión de la seguridad de la información - Medición

Information technology
Information security management – Measurement

LAS OBSERVACIONES DEBEN

ENVIARSE CON EL FORMULARIO DE LA

ETAPA DE DISCUSIÓN PÚBLICA

DOCUMENTO EN ESTUDIO

Septiembre de 2010

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de la Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

Esta norma IRAM es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

Esta norma es una adopción idéntica de la norma ISO/IEC 27004:2009.

Sólo se han realizado los cambios editoriales siguientes:

Se agregó un anexo informativo con la bibliografía considerada y otro donde se indican los organismos de estudio de la norma.

Prefacio ISO

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas par realizar acuerdos en los campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1.

Las normas internacionales se elaboran de acuerdo a las reglas dadas en las directivas de ISO/IEC, parte 2.

La tarea principal del comité técnico conjunto es la de preparar normas internacionales. Los proyectos de normas internacionales adoptadas por el comité técnico conjunto son circulados a los organismos nacionales y sometidos a votación. La publicación como Norma Internacional requiere la aprobación de al menos el 75% de los organismos nacionales.

Es importante señalar la posibilidad de que algunos elementos de esta norma internacional pueden estar sujetos a derechos de patente. ISO e IEC no son responsables de la identificación de alguno o todos de esos derechos de patentes.

La norma ISO/IEC 27004 fue preparada por el comité técnico conjunto ISO/IEC JTC1, Tecnología de la información, subcomité SC 27, Técnicas de seguridad en TI.

Introducción

0.1 General

Esta norma proporciona una guía para el desarrollo y uso de mediciones y medidas para evaluar la efectividad de un Sistema de Gestión de Seguridad de la Información (SGSI) y controles o grupos de control, según lo especificado en IRAM-ISO/IEC 27001.

Esto incluiría la política, gestión de riesgos de seguridad de la información, objetivos de control, controles, procesos y procedimientos, y respalda al proceso de evaluación, ayudando a determinar si es necesario que alguno de los procesos del SGSI o los controles se modifiquen o mejoren. Se recomienda tener en cuenta que ninguna medición de los controles puede garantizar la seguridad completa.

La implementación de este enfoque constituye un Programa de medición de seguridad de la información. Este programa asistirá a la alta dirección en la identificación y evaluación de los no cumplimiento e ineficacia de los procesos y controles del SGSI, y en la priorización de las acciones asociadas con la mejora o cambio de estos procesos y/o controles. También puede asistir a la organización para demostrar el cumplimiento con la norma IRAM-ISO/IEC 27001 y proveer evidencia adicional para la revisión de la alta dirección y los procesos de gestión de riesgos de seguridad de la información.

Esta norma asume que el punto de partida para el desarrollo de medidas y mediciones es un entendimiento fehaciente de los riesgos de seguridad de la información que enfrenta una organización, y que las actividades de evaluación de riesgo de la organización se han realizado de manera correcta (por ejemplo basadas en la norma ISO/IEC 27005), como lo requiere la norma IRAM-ISO/IEC 27001. El Programa de medición de la seguridad de la información impulsará a la organización a proveer información confiable a las partes interesadas relevantes concernientes a sus riesgos de seguridad de la información y el estado del SGSI implementado para manejar esos riesgos.

Efectivamente implementando, el Programa de medición de la seguridad de la información aumentará la confianza de las partes interesadas en los resultados de las mediciones y permite a las partes interesadas hacer uso de éstas mediciones para efectuar mejoras continuas a la seguridad de la información y al SGSI.

Los resultados de medición acumulados permitirán la comparación del progreso para alcanzar los objetivos de seguridad de la información sobre un período de tiempo como parte del proceso de mejora continua del SGSI de la organización.

0.2 Visión general de la alta dirección

IRAM-ISO/IEC 27001 requiere que la organización “lleve a cabo revisiones periódicas de la efectividad del SGSI teniendo en cuenta los resultados de la efectividad de las mediciones” y que “se mida la efectividad de los controles para verificar que se cumpla con los requerimientos de seguridad”. La IRAM-ISO/IEC 27001 también requiere que la organización “defina cómo medir la efectividad de los controles o grupo de controles seleccionados; y que especifique cómo estas mediciones se utilizarán para evaluar la efectividad de los controles para producir resultados comparables y reproducibles”.

El enfoque adoptado por la organización para cumplir con los requerimientos de mediciones especificados en la IRAM-ISO/IEC 27001 variará basado en un número de factores significativos, incluyendo los riesgos de seguridad de la información que enfrenta la organización, su tamaño, los recursos que tiene disponibles y los requerimientos legales, regulatorios y contractuales aplicables. Son importan-

tes la cuidadosa selección y justificación de los métodos utilizados para cumplir con los requerimientos de las mediciones, de manera de asegurar que no se dedicarán recursos excesivos a dichas actividades del SGSI en detrimento de otras. Idealmente, las actividades de medición actuales se integrarán en operaciones regulares de la organización con mínimos requerimientos adicionales de recursos.

Esta norma brinda recomendaciones concernientes a las siguientes actividades como base para que una organización cumpla con sus requerimientos de medición especificados en IRAM-ISO/IEC 27001:

a) Desarrollar mediciones (por ejemplo: mediciones base, mediciones derivadas e indicadores);

b) Implementar y operar un Programa de mediciones de seguridad de la información;

c) Recolectar y analizar los datos;

d) Preparar los resultados de las mediciones;

e) Comunicar los resultados de las mediciones desarrolladas a las principales partes interesadas;

f) Utilizar los resultados de las mediciones como factores contribuyentes a las decisiones relacionadas con el SGSI.

g) Utilizar los resultados de las mediciones para identificar necesidades de mejorar el SGSI implementado, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos; y

h) Facilitar una mejora continua del Programa de mediciones de seguridad de la información

El tamaño de la organización es uno de los factores que impactará en la habilidad para cumplir con el proceso de medición. Generalmente, el tamaño y la complejidad del negocio, en combinación con la importancia de la seguridad de la información, afectan el alcance de las mediciones necesarias, tanto en términos de números de mediciones a seleccionar y en la frecuencia de recolección y análisis de los datos. Por ejemplo, para PyMES (Pequeñas y Medianas Empresas) podría ser suficiente un programa de medición de la seguridad de la información menos exhaustivo, mientras que las grandes organizaciones implementarán y operarán múltiples Programas de medición de la seguridad de la información.

Un solo Programa de medición de la seguridad de la información puede ser suficiente para pequeñas organizaciones, mientras que para grandes empresas la necesidad puede ser de múltiples Programas de mediciones de seguridad de la información.

La guía provista por esta norma resultará en la producción de documentación que contribuirá a la demostración de que se mide y evalua la efectividad de los controles se encuentra medida y evaluada.

Índice

Tecnología de la información

Gestión de la seguridad de la información - Medición

1 ALCANCE

Esta norma provee una guía en el desarrollo y uso de medidas y mediciones, de manera de evaluar la efectividad de un Sistema de Gestión de Seguridad de la Información (SGSI) implementado y de los controles o grupos de controles, como los especificados en la IRAM-ISO/IEC 27001.

Esta norma es aplicable a organizaciones de todo tipo y tamaño.

NOTA. El presente documento utiliza las formas verbales para la expresión de **provisiones**(por ejemplo: *debe, no debe, se recomienda, no se recomienda, no necesita, "puede y no puede*) que están especificadas en las directivas ISO-IEC, Parte 2, 2004, Anexo H. Ante cualquier duda, se recomienda consultar IRAM-ISO/IEC 27000 anexo A.

NOTA IRAM. *Shall y shall not* se han traducido del inglés como "debe y no debe". (Ver ISO/IEC 27000).

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Todo documento normativo que se menciona a continuación es indispensable para la aplicación de este documento.

Cuando en el listado se mencionan documentos normativos en los que se indica el año de publicación, esto significa que se debe aplicar dicha edición, en caso contrario, se debe aplicar la edición vigente, incluyendo todas sus modificaciones.

IRAM-ISO/IEC 27001:2007 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

ISO/IEC 27000:2009 - Information technology. Security techniques. Information security management systems. Overview and vocabulary.

3 TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento, se aplican los términos y definiciones de ISO/IEC 27000 y los siguientes.

3.1 modelo analítico (analytical model)
cálculo o algoritmo asociado con los criterios de decisión, que combina una o más medidas base y/o derivadas.

[ISO/IEC 15939:2007]

3.2 atributo (attribute)
propiedad o característica de un objeto que puede distinguirse cuantitativa o cualitativamente por medios manuales o automatizados

[ISO/IEC 15939:2007]

3.3 medida base (base measure)
medida definida en términos de un atributo y el método para cuantificarlo

[ISO/IEC 15939:2007]

NOTA. Una medida base es funcionalmente independiente de otras medidas.

3.4 dato (data)
grupo de valores asignados a mediciones base, derivadas y/o indicadores.

[ISO/IEC 15939:2007]

3.5 criterios de decisión (decisión criteria)
umbrales, objetivos o patrones utilizados para determinar la necesidad de una acción o de investigación adicional, o para describir el nivel de confianza de un resultado dado

[ISO/IEC 15939:2007]

3.6 medida derivada (derived measure)
medida que se define como la función de dos o más valores de medidas base

[ISO/IEC 15939:2007]

3.7 indicador [indicator]
medida que provee una estimación o evaluación de atributos específicos, derivados de un modelo analítico con respecto a la necesidad de información definida

3.8 necesidad de información (information need)
criterio necesario para manejar objetivos, metas, riesgos y problemas

[ISO/IEC 15939:2007]

3.9 medida (measure)
variable a la cual se le asigna un valor como el resultado de una medición

[ISO/IEC 15939:2007]

NOTA. El término *medidas* se utiliza para referirse de manera colectiva a las medidas base, medidas derivadas e indicadores.

Ejemplo: Una comparación entre una tasa de defectos medida y una tasa de defectos planificada, junto con la evaluación de si la diferencia indica o no un problema.

3.10 medición (measurement)
proceso de obtención de información sobre la efectividad del SGSI y de los controles utilizando un método de medición, una función de medición, un modelo analítico y criterios de decisión

3.11 función de medición (measurement function)
algoritmo o cálculo realizado para combinar dos o más medidas base.

[ISO/IEC 15939:2007]

3.12 método de medición (measurement method)
secuencia lógica de operaciones, descritas de manera genérica, utilizados para cuantificar un atributo con respecto a una escala especificada
[ISO/IEC 15939:2007]

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: la cuantificación involucra el juicio humano;
- objetivo: la cuantificación se basa en reglas numéricas.

3.13 resultados de la medición
(measurement results)
uno o más indicadores y su interpretación asociada, dirigidos a una necesidad de información

3.14 objeto (object)
elemento caracterizado a través de la medición de sus atributos

3.15 escala (scale)
conjunto de valores ordenados, continuos o discretos, o un conjunto de categorías con las cuales se relaciona el atributo

[ISO/IEC 15939:2007]

NOTA. El tipo de escala depende de la naturaleza de la relación entre los valores en la escala. Normalmente se definen cuatro tipos de escala:

- nominal: los valores de la medición son categóricos;
- ordinal: los valores de la medición son clasificados;
- intervalo: los valores de la medición tienen iguales distancias correspondientes a iguales cantidades del atributo;
- proporción: los valores de la medición tienen iguales distancias correspondientes a iguales cantidades del atributo, donde a ningún atributo le puede corresponder el valor cero.

Estos son sólo ejemplos de tipos de escala.

3.16 unidad de medición (unit of measurement)
cantidad particular, definida y adoptada por convención, con la cual se comparan otras cantidades del mismo tipo de manera de expresar su magnitud relativa a dicha cantidad

[ISO/IEC 15939:2007]

3.17 validación (validation)
confirmación, a través de la provisión de evidencia objetiva, de que se han cumplido con los requerimientos relativos a un uso o aplicación específicos.

3.18 verificación (verification)
confirmación, a través de la provisión de evidencia objetiva, de que se han cumplido con requerimientos especificados

[IRAM-ISO 9000:2005]

NOTA. Esto también se puede llamar *prueba de cumplimiento.*

4 ESTRUCTURA DE ESTA NORMA

Esta norma provee una explicación de las medidas y actividades de medición necesarias para evaluar la efectividad de los requisitos del SGSI, para la gestión de controles de seguridad adecuados y proporcionales como los requeridos por IRAM-ISO/IEC 27001:2007, 4.2.

Esta norma se encuentra estructurada de la siguiente manera:

- visión general del Programa de medición de la seguridad de la información y el modelo de medición de la seguridad de la información (capítulo 5);

- responsabilidades de la alta dirección por las mediciones de seguridad de la información (capítulo 6); y

- estructuras de medición y procesos a ser implementados en el Programa de medición de la seguridad de la información (capítulos 7 al 10). Por ejemplo:

    - planificación .y desarrollo;

    - implementación y operación;

    - mejora de los procesos de medición; y

    - comunicación de los resultados de la medición.

Además, el anexo A provee una plantilla de ejemplo de estructura de medición cuyos componentes son los elementos del Modelo de medición de la seguridad de la información (ver capítulo 7). El anexo B provee ejemplos de estructuras de medición para controles específicos o procesos de un SGSI, utilizando la plan-plantilla provista en el anexo A.

El objetivo de estos ejemplos es ayudar a la organización sobre cómo implementar las Mediciones de seguridad de la información y cómo registrar las actividades de medición y sus resultados.

5 VISIÓN GENERAL DE LA MEDICIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1 Objetivos de la medición de seguridad de la información

Los objetivos de la medición de seguridad de la información dentro del contexto del SGSI incluyen:

a) evaluar la efectividad de los controles o grupos de controles implementados (ver *4.2.2 d*) en la figura 1);

b) evaluar la efectividad del SGSI implementado (ver *4.2.3 b*) en la figura 1);

c) verificar el grado de cumplimiento de los requerimientos de seguridad identificados (ver *4.2.3 c*) en la figura 1);

d) facilitar la mejora del desempeño de la seguridad de la información en términos de los riesgos generales de negocio de la organización;

e) proveer resultados de las mediciones para asistir a la revisión por la alta dirección y facilitar la toma de decisiones relacionada con el SGSI y justificar las necesidades de mejoras del SGSI implementado;

La figura 1 ilustra la relación cíclica entrada-salida de las actividades de medición en relación al ciclo Planear-Hacer-Verificar-Actuar (PHVA), especificado en IRAM-ISO/IEC 27001. Los números de cada figura representan los subcapítulos correspondientes de IRAM-ISO/ IEC 27001:2007.

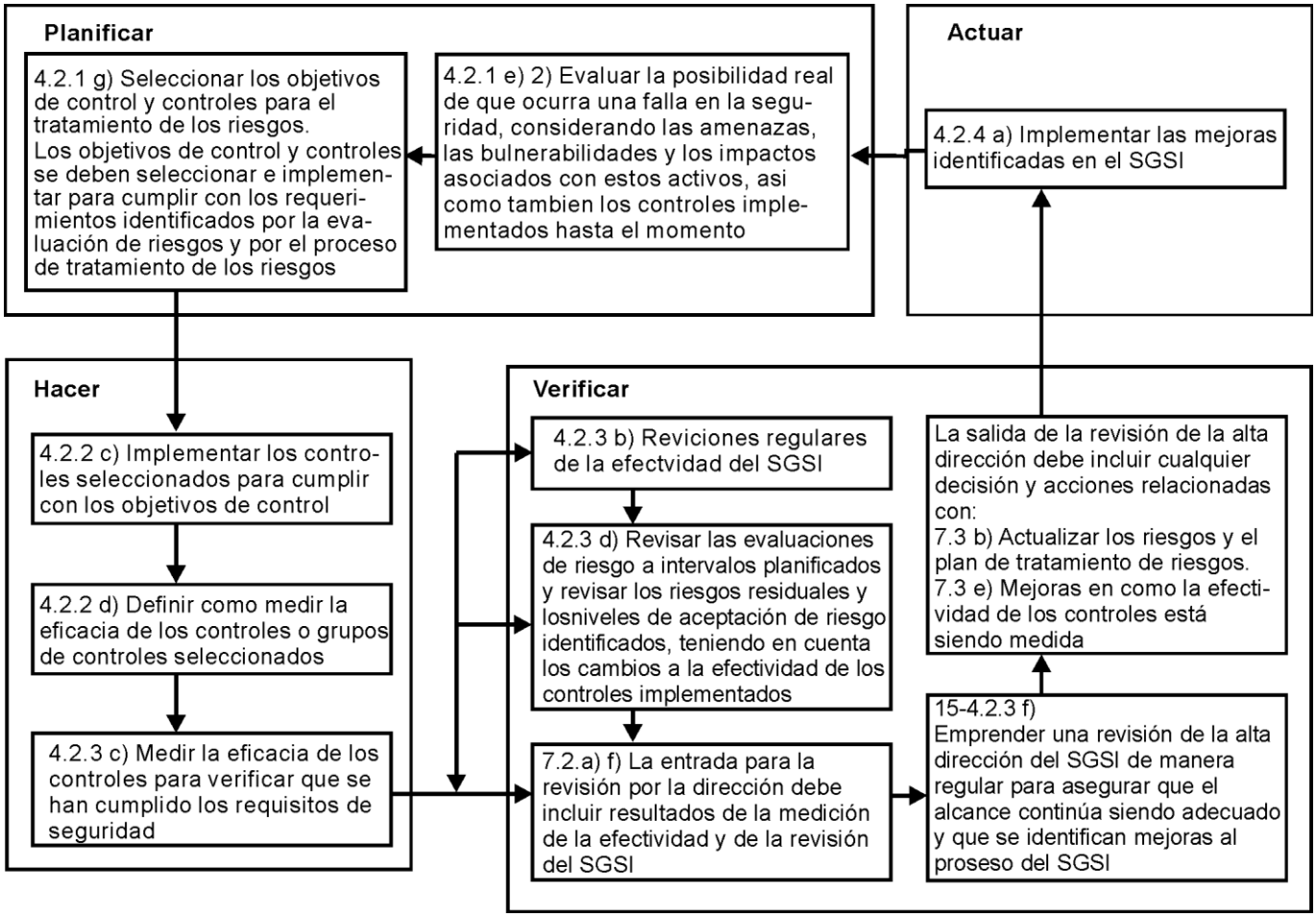


Figura 1 – Entradas y salidas de las mediciones en un ciclo SGSI-PHVA de gestión de seguridad de la información

Se recomienda que la organización establezca los objetivos de las mediciones basados en una serie de consideraciones, incluyendo:

a) el rol de la seguridad de la información como soporte de las actividades de negocio de la organización y los riesgos a los que ésta se enfrenta;

b) requerimientos legales, regulatorios y contractuales aplicables;

c) estructura organizacional;

d) costos y beneficios de implementar mediciones de seguridad de la información;

e) criterios de aceptación de riesgos de la organización; y

f) la necesidad de comparar varios SGSI's dentro de la organización.

5.2 Programa de medición de la seguridad de la información

Se recomienda que la organización establezca y gestione su Programa de medición de la seguridad de la información, de manera de alcanzar los objetivos de medición establecidos y adopte el modelo PHVA dentro de sus actividades generales de medición. Se recomienda que la organización desarrolle e implemente estructuras de medición de manera de obtener resultados repetibles, objetivos y útiles, basados en el Modelo de medición de la seguridad de la información (ver 5.4).

Se recomienda que el Programa de medición de la seguridad de la información y la estructura de medición desarrollada, aseguren que la organización efectivamente alcance sus mediciones objetivas y repetibles, y provea resultados de las mediciones para las partes interesadas correspondientes, de manera de identificar las necesidades de mejora del SGSI implementado, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos.

Se recomienda que un Programa de medición de la seguridad de la información incluya los siguientes procesos:

a) desarrollo de medidas y mediciones (ver capítulo 7);

b) operación de la medición (ver capítulo 8);

c) análisis de datos y reporte de los resultados de la medición (ver capítulo 9); y

d) valoración y mejora del Programa de medición de la seguridad de la información (ver capítulo 10).

Se recomienda que la estructura operacional y organizacional de un Programa de medición de la seguridad de la información se determine teniendo en cuenta la escala y complejidad del SGSI del cual es parte. En todos los casos, se recomienda que los roles y responsabilidades por el Programa de medición de la seguridad de la información se asignen explícitamente a personal competente.

Se recomienda que las medidas seleccionadas e implementadas por el Programa de medición de la seguridad de la información se relacionen directamente con las operaciones de un SGSI, y con otras medidas, como así también con los procesos de negocio de la organización. Las mediciones pueden integrarse a actividades operativas o realizarse a intervalos regulares determinados por la alta dirección del SGSI.

5.3 Factores de éxito

Los siguientes son factores que contribuyen al éxito del Programa de medición de la seguridad de la información de manera de facilitar la mejora continua del SGSI:

a) compromiso de la alta dirección soportado por los recursos apropiados;

b) existencia de los procesos y procedimientos del SGSI;

c) un proceso repetible capaz de capturar y reportar datos significativos de manera de proveer tendencias sobre un período de tiempo;

d) medidas cuantificables basadas en los objetivos del SGSI;

e) datos de fácil obtención que puedan ser utilizados en las mediciones;

f) valoración de la efectividad del Programa de medición de la seguridad de la información y la implementación de mejoras identificadas;

g) recolección, análisis, y reporte periódico y consistente de datos de mediciones de una forma que sea significativa;

h) uso de los resultados de las mediciones por las partes interesadas correspondientes, para identificar necesidades de mejora del SGSI implementado, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos;

i) aceptación de la respuesta de los resultados de las mediciones por las partes interesadas correspondientes; y

j) evaluaciones de la utilidad de los resultados de las mediciones y de las implementaciones de las mejoras identificadas.

Una vez implementado de manera exitosa, un Programa de medición de la seguridad de la información puede:

1) demostrar el cumplimiento de la organización con los requerimientos legales y regulatorios aplicables y con las obligaciones contractuales;

2) dar soporte a la identificación de problemas de seguridad de la información desconocidos o no detectados previamente;

3) asistir en satisfacer las necesidades de reportes de la alta dirección, al establecer medidas para actividades históricas y actuales; y

4) ser utilizado como datos de entrada para el proceso de gestión de seguridad de la información, las auditorías internas del SGSI y las revisiones de la alta dirección.

5.4 Modelo de medición de la seguridad de la información

NOTA. Los conceptos del modelo de medición de la seguridad de la información y de la estructura de medición adoptados en esta norma, se basan en los indicados en ISO/IEC 15939. El término “producto de información” utilizado en ISO/IEC 15939 es un sinónimo de “resultados de la medición” utilizado en esta norma, y “proceso de medición” utilizado en ISO/IEC 15939 es un sinónimo de “programa de medición” utilizado en esta norma.

5.4.1 Visión general

El modelo de medición de la seguridad de la información es una estructura que vincula una necesidad de información con los objetos de medición pertinentes y sus atributos. Los objetos de medición pueden incluir procesos, procedimientos, proyectos y recursos planificados o implementados.

El modelo de medición de seguridad de la información describe cómo los atributos concernientes son cuantificados y convertidos en indicadores, los cuales proveen la base para la toma de decisiones. La figura 2 representa el modelo de medición de la seguridad de la información.

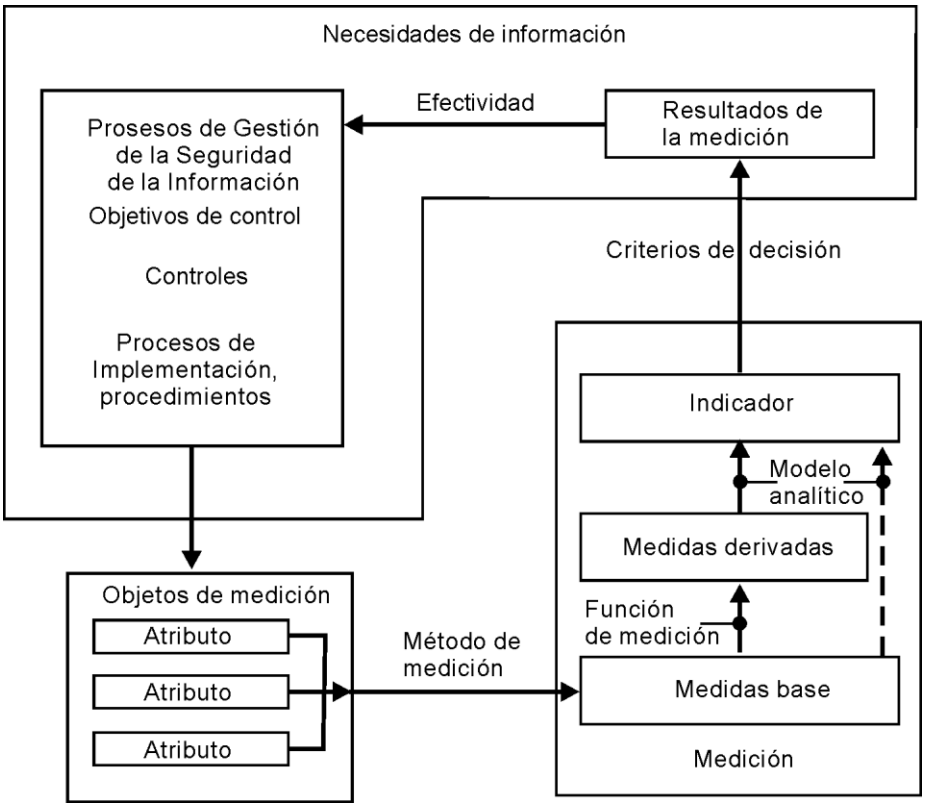


Figura 2 – Modelo de medición de la seguridad de la información

NOTA. El capítulo 7 provee información detallada sobre los elementos individuales del modelo de medición de la seguridad de la información.

Los subcapítulos que siguen dan una introducción a los elementos individuales del modelo. Ellos también proveen ejemplos de cómo se utilizan éstos elementos individuales.

Las necesidades de información o propósito de medición utilizados en los ejemplos de las tablas 1 a 4 de los subcapítulos siguientes, son para evaluar el nivel de concientización del personal correspondiente respecto del cumplimiento de las políticas de seguridad organizacionales (objetivo de control A.8.2, y controles A.8.2.1 y A.8.2.2 de IRAM-ISO/IEC 27001: 2007).

5.4.2 Medidas base y método de medición

Una medida base es la medida más simple que se puede obtener. La misma resulta de la aplicación de métodos de medición sobre los atributos seleccionados de un objeto de medición. Un objeto de medición puede tener muchos atributos, de los cuales sólo algunos pueden tener valores útiles a ser asignados a una medida base. Un dado atributo puede ser utilizado por muchas medidas base diferentes.

Un método de medición es una secuencia lógica de operaciones utilizado para cuantificar un atributo con respecto a una escala específica. La operación puede envolver actividades como contar las ocurrencias u observar el paso del tiempo.

Un método de medición se puede aplicar a atributos de un objeto de medición. Ejemplos de objetos de medición incluyen (pero no se limitan a):

- rendimiento de los controles implementados en el SGSI;
- estado de los activos de información protegidos por los controles;
- rendimiento de los procesos implementados en el SGSI;
- comportamiento del personal que forma parte del SGSI implementado;
- actividades de las unidades organizacionales responsables por la seguridad de la información; y
- grado de satisfacción de las partes interesadas.

Un método de medición puede utilizar objetos de medición de mediciones y atributos de una variedad de fuentes, tales como:

- resultados de la evaluación y el análisis de riesgos;
- cuestionarios y entrevistas personales;
- reportes de auditoría internos y/o externos;
- registros de eventos, tales como eventos del sistema, reportes estadísticos y pistas de auditorías;
- reportes de incidentes, particularmente aquellos de mayor impacto;
- resultados de pruebas, por ejemplo: pruebas de penetración, ingeniería social, herramientas de cumplimiento y de auditoría de seguridad; o
- registros de la seguridad de la información de la organización relacionados con los procedimientos y los programas, por ejemplo, los resultados del entrenamiento de concientización en seguridad de la información.

Las tablas 1 a 4, presentan la aplicación del modelo de seguridad de la información para los siguientes controles:

- El “Control 1” se refiere a que el control A.8.2.1 “Responsabilidad de la alta dirección” de la IRAM-ISO/IEC 27001:2007 (*La alta dirección debe requerir a los empleados, contratistas y usuarios de terceras partes, aplicar seguridad de acuerdo con las políticas y procedimientos establecidos por la organización*); se implemente de la siguiente manera: *Todo el personal relacionado con el SGSI debe firmar acuerdos de usuario antes de que se le permita acceso a un sistema de información*;

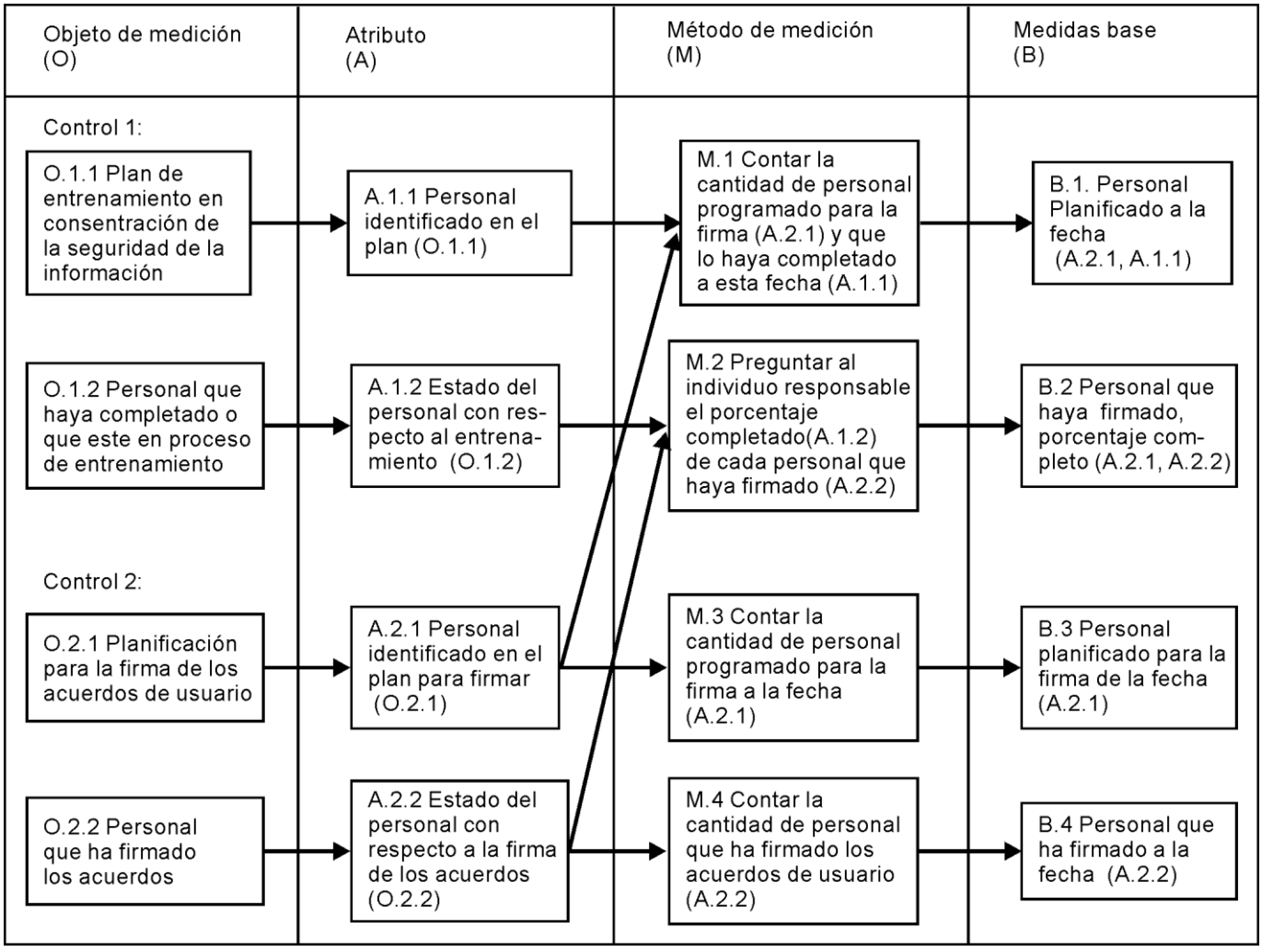
– El *Control 2* se refiere a que el control A.8.2.2 *Concientización, educación y entrenamiento en seguridad de la información* de la IRAM-ISO/IEC 27001:2007 (*Todos los empleados de la organización, y, donde sea pertinente, contratistas y usuarios de terceras partes deben recibir el entrenamiento en concientización apropiados y actualizaciones regulares en políticas y procedimientos organizacionales, como sea pertinente para la función de su trabajo*); se implemente de la siguiente manera: *Todo el personal relacionado con el SGSI debe recibir entrenamiento en concientización de la seguridad de la información antes de que se le permita el acceso a un sistema de información*.

Las estructuras de medición correspondientes está contenida en B.1.

NOTA. Las tablas 1 a 4 consisten en varias columnas (tabla 1, cuatro columnas, tabla 2 a la 4, tres columnas) a las cuales se les asigna una letra. A cada espacio dentro de las columnas individuales se le asigna un número. Las combinaciones de letras y números se utilizan en espacios subsiguientes para referirse a espacios anteriores. Las flechas designan los flujos de datos entre elementos individuales del modelo de medición de seguridad de la información, dentro del ejemplo específico.

La tabla 1 incluye un ejemplo de las relaciones entre un objeto de medición, un atributo, un método de medición y una medida base para medir los objetos establecidos por los controles implementados descriptos anteriormente.

Tabla 1 – Ejemplo de medida base y método de medición



5.4.3 Medida derivada y función de medición

Una medida derivada es una combinación de dos o más medidas base. Una medida base dada puede servir como entrada para varias medidas derivadas.

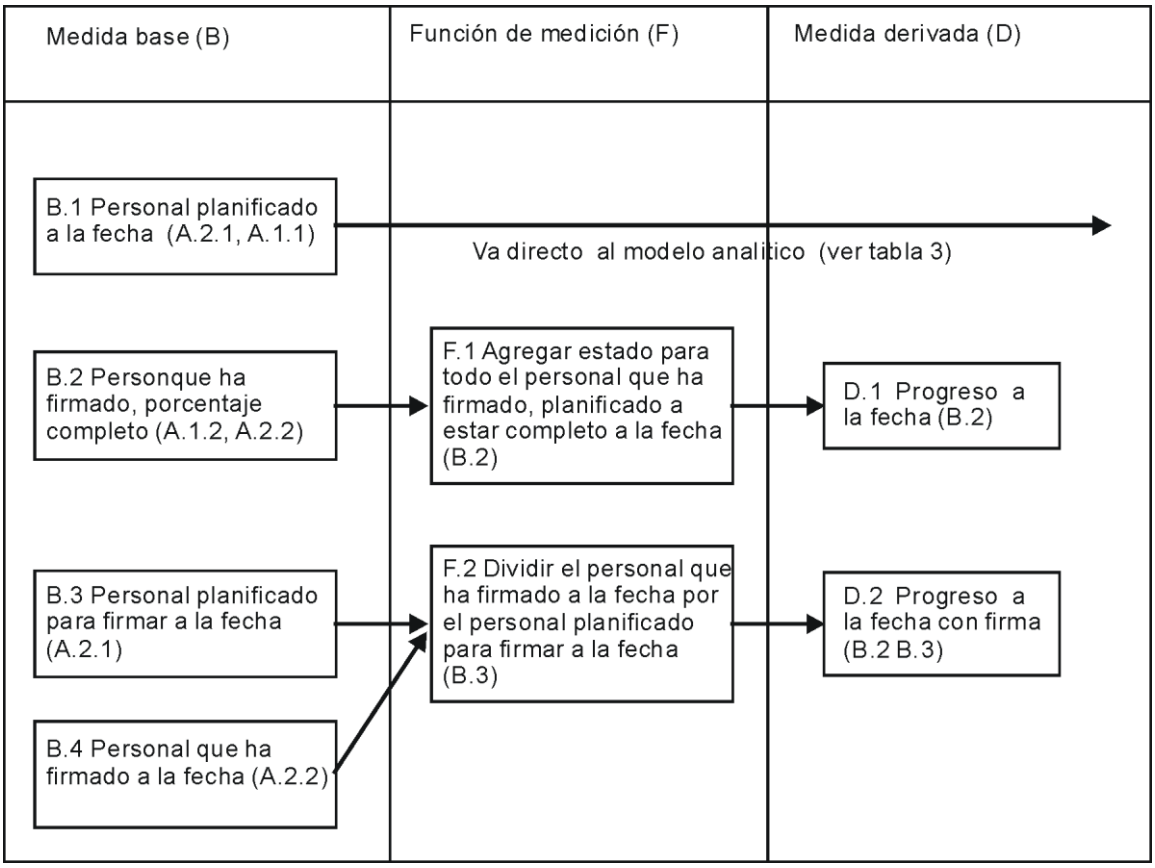
Una función de medición es un cálculo utilizado para combinar medidas base de manera de crear una medida derivada.

La escala y unidad de la medida derivada depende de las escalas y unidades de las medidas base de las cuales se compone, así como también de cómo se encuentren combinadas por la función de medición.

La función de medición puede involucrar una variedad de técnicas, tales como promediar las medidas base, aplicando ponderación a las medidas base, o asignando valores cualitativos a las medidas base. La función de medición puede combinar medidas base utilizando diferentes escalas, tales como resultados de evaluaciones porcentuales o cualitativas.

En la tabla 2 se presenta un ejemplo de la relación de más elementos de la aplicación del modelo de medición de seguridad de la información, por ejemplo medida base, función de medición y medida derivada.

Tabla 2 – Ejemplo de medida derivada y función de medición

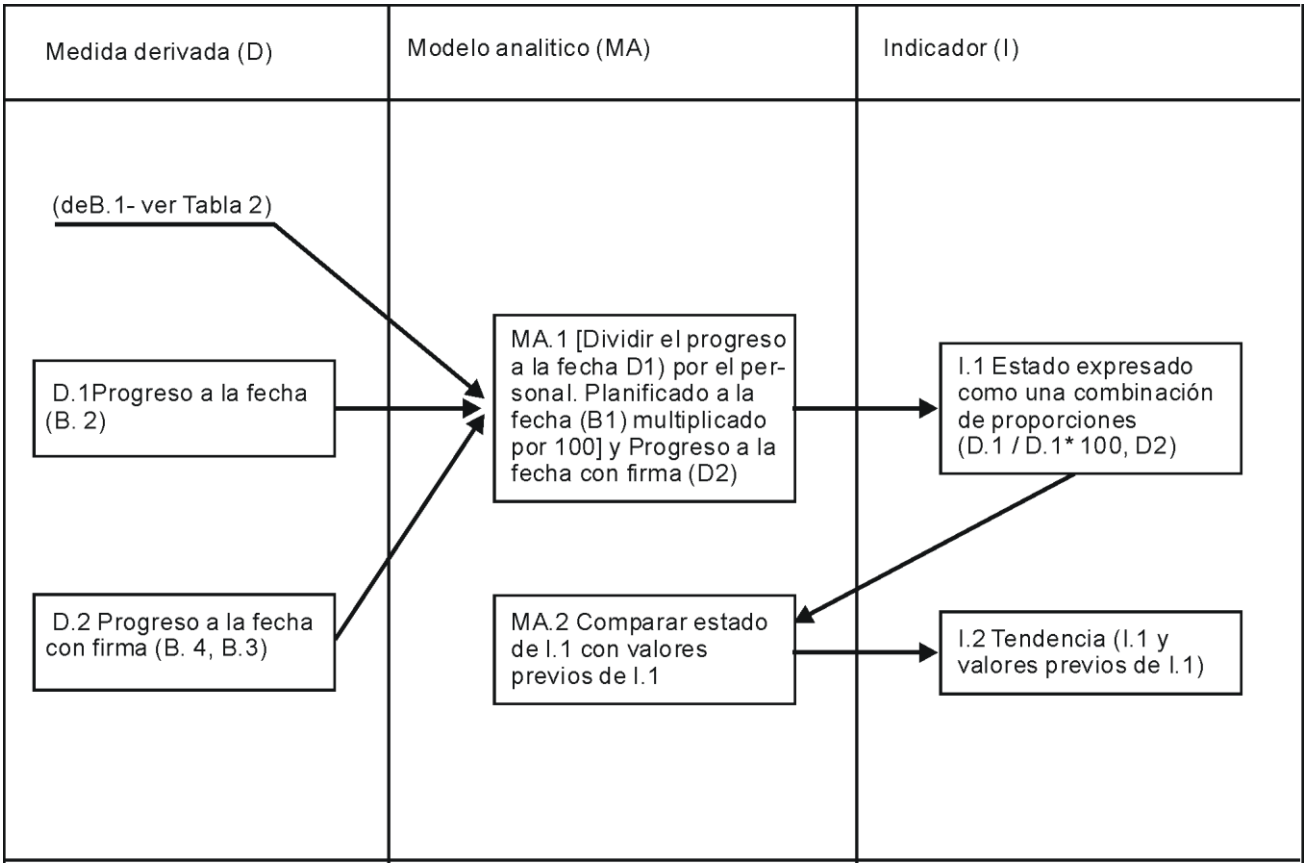


5.4.4 Indicadores y modelo analítico

Un indicador es una medida que provee una estimación o valoración de atributos específicos derivados de un modelo analítico con respecto a necesidades de información definidas. Los indicadores se obtienen aplicando un modelo analítico a las medidas base y/o derivadas, y combinándolas con los criterios de decisión. La escala y el método de medición afectan la elección de técnicas analíticas utilizadas para producir los indicadores.

En la tabla 3 se presenta un ejemplo de las relaciones entre las medidas derivadas, el modelo analítico y los indicadores, para la aplicación del modelo de medición de la seguridad de la información.

Tabla 3 – Ejemplo de un indicador y un modelo analítico



NOTA. Si un indicador se representa en forma gráfica o cuando se utilizan copias monocromáticas, se recomienda que sea utilizable por personas con limitaciones visuales. Para hacer eso posible se recomienda que se agregue una descripción del color, de las formas, la tipografía u otros métodos visuales.

5.4.5 Resultados de las mediciones y criterios de decisión

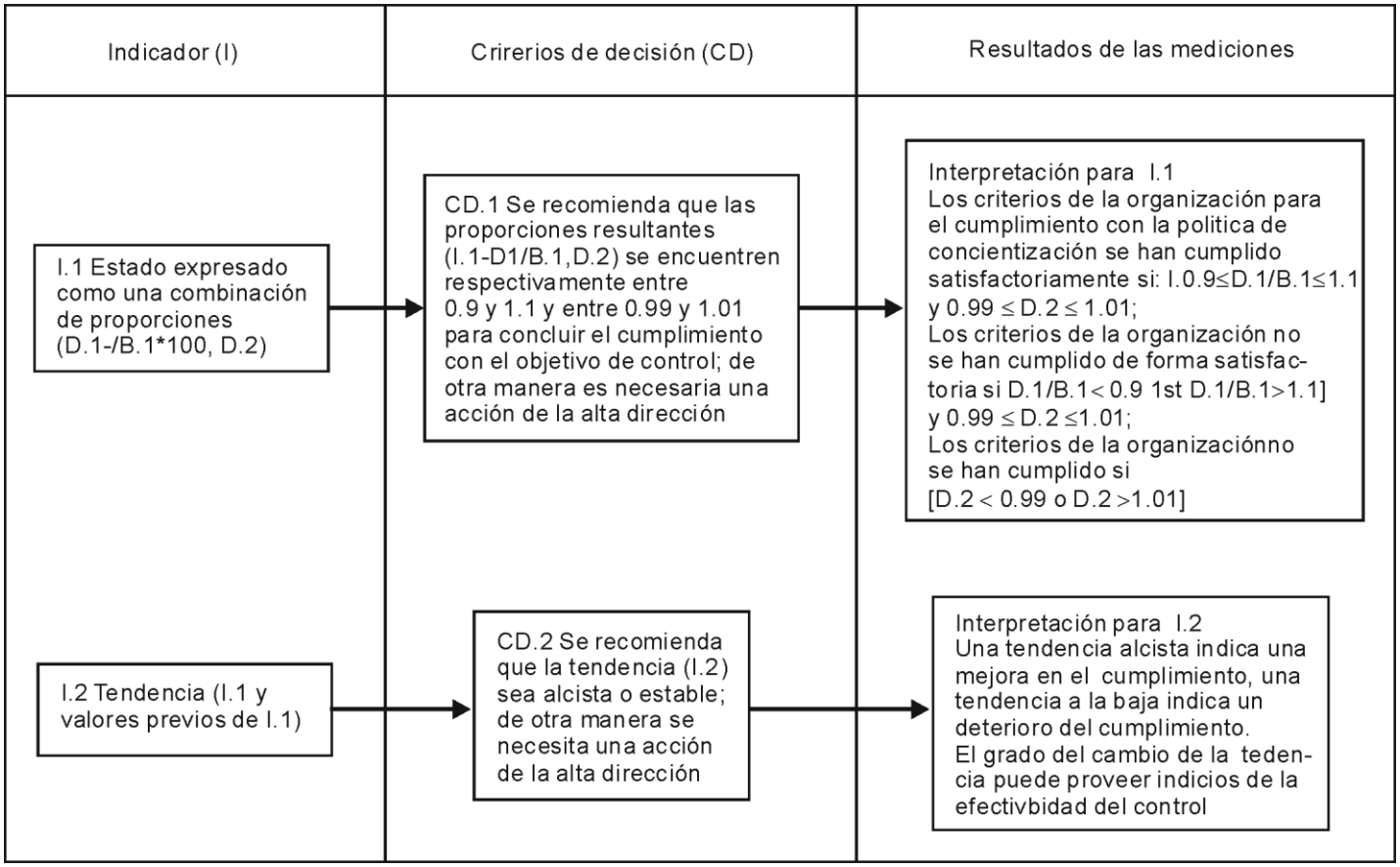
Los resultados de la medición se desarrollan interpretando los indicadores aplicados, basados en criterios de decisión definidos, y se recomienda que se considere en el contexto de los objetivos de medición generales de evaluación de la efectividad del SGSI. Los criterios de decisión se utiliza para determinar la necesidad de una acción o de más investigación, así como también para describir el nivel de confiabilidad de los resultados medidos. Los criterios de decisión se podría aplicar a una serie de indicadores, por ejemplo, para realizar análisis de tendencia basado en indicadores recibidos en diferentes puntos en el tiempo.

Las metas proveen especificaciones detalladas de rendimiento, aplicables a la organización o a

partes de la misma, derivadas de los objetivos de seguridad de la información y que necesitan ser establecidas y cumplidas de manera de alcanzar dichos objetivos.

La tabla 4 presenta un ejemplo de la relación de los elementos finales de la aplicación del modelo de medición de seguridad de la información (por ejemplo: indicador, criterios de decisión y resultados de medición).

Tabla 4 – Ejemplo de resultados de medición y modelo analítico



6 RESPONSABILIDADES DE LA ALTA DIRECCIÓN

6.1 Visión general

La alta dirección es responsable por el establecimiento del Programa de medición de la seguridad de la información, incluyendo a las diferentes partes interesadas (ver 7.5.8) en las actividades de medición, por la aceptación de los resultados de la medición como entrada para la revisión de la alta dirección y por su utilización en las actividades de mejora dentro del SGSI.

Para alcanzar esto, se recomienda que la alta dirección:

a) establezca objetivos para el Programa de medición de la seguridad de la información;

b) establezca una política para el Programa de medición de seguridad de la información;

c) establezca los roles y responsabilidades para el Programa de medición de la seguridad de la información;

d) proporcione recursos adecuados para realizar las mediciones, incluido el personal,

los fondos, las herramientas y la infraestructura;

e) asegure que se alcancen los objetivos del Programa de medición de la seguridad de la información;

f) asegure que las herramientas y el equipo utilizado para recolectar datos se mantenga de manera adecuada;

g) establezca el propósito de medición para cada estructura de medición;

h) asegure que la medición provea suficiente información para las partes interesadas relacionadas, en cuanto a la efectividad del SGSI y las necesidades de mejora del SGSI implementado, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos; y

i) asegure que la medición provea suficiente información a las partes interesadas con respecto a la efectividad de los controles o grupos de controles implementados y sus necesidades de mejora.

Se recomienda que la alta dirección asegure, mediante una apropiada asignación de roles y responsabilidades de medición, que los resultados de la gestión no se vean influenciados por los propietarios de la información (ver 7.5.8). Esto se puede alcanzar mediante la segregación de tareas o, de no ser posible, a partir del uso de documentación detallada que permita revisiones independientes.

6.2 Gestión de los recursos

Se recomienda que la alta dirección asigne y provea los recursos para dar soporte a las funciones esenciales de medición, tales como la recolección, el análisis, el almacenamiento, el reporte y la distribución de los datos. Se recomienda que la asignación de recursos incluya:

a) individuos con responsabilidad por todos los aspectos del Programa de medición de la seguridad de la información;

b) soporte financiero apropiado; y

c) soporte de infraestructura apropiado, como la infraestructura física y las herramientas utilizadas para realizar el proceso de medición.

NOTA. El capítulo 5.2.1 de la IRAM-ISO/IEC 27001:2007 especifica los requerimientos concernientes a la provisión de recursos para la implementación de un SGSI.

6.3 Entrenamiento, concientización y competencia en mediciones

Se recomienda que la alta dirección asegure que:

a) las partes interesadas (ver 7.5.8) se entrene adecuadamente para cumplir con sus roles y responsabilidades en el Programa de medición de la seguridad de la información implementado, y se encuentren calificados apropiadamente para cumplir con sus roles y responsabilidades; y

b) las partes interesadas entiendan que sus tareas incluyen el hacer sugerencias de mejora en el Programa de medición de la seguridad de la información implementado.

7 DETERMINACIÓN DE MEDIDAS Y MEDICIONES

7.1 Visión general

Este capítulo provee una guía sobre cómo desarrollar medidas y mediciones con el propósito de evaluar la efectividad del SGSI implementado y los controles o grupos de controles, e identificando conjuntos específicos de estructuras de medición. Se recomienda que se establezcan y documenten las actividades necesarias para desarrollar medidas y mediciones, incluyendo las siguientes:

a) definición del alcance de la medición (ver 7.2);

b) identificación de una necesidad de información (ver 7.3);

c) selección del objeto de medición y sus atributos (ver 7.4);

d) desarrollo de las estructuras de medición (ver 7.5);

e) aplicación de las estructuras de medición (ver 7.6);

f) establecimiento de los procesos y herramientas de recolección de datos y análisis (ver 7.7); y

g) establecimiento del enfoque y la documentación de la implementación de las mediciones (ver 7.8).

Cuando se establezcan éstas actividades, se recomienda que la organización tenga en cuenta los recursos financieros, humanos y de infraestructura (físicos y herramientas).

7.2 Definición del alcance de las mediciones

Dependiendo de las capacidades y recursos de una organización, el alcance inicial de las actividades de medición de la organización estará limitado a elementos tales como controles específicos, activos de información protegidos por estos controles, actividades específicas para la seguridad de la información a las cuales la alta dirección le otorga mayor prioridad. Con el tiempo, se ampliará el alcance de las actividades de medición de manera de incluir más elementos del SGSI implementado y controles o grupos de control, teniendo en cuenta las prioridades de las partes interesadas.

Se recomienda que se identifiquen las partes interesadas relacionadas y que las mismas participen en la definición del alcance de la medición. Las partes interesadas relacionadas pueden ser unidades organizacionales internas o externas a la organización, como gerentes de proyecto, gerentes de sistemas de información, o quienes toman las decisiones sobre la seguridad de la información. Se recomienda que se definan y comuniquen a estas partes interesadas, los resultados de las mediciones específicas, que tengan que ver con la efectividad de los controles individuales o grupos de controles.

La organización puede considerar definir un límite al número de resultados de las mediciones a ser informadas a quienes toman las decisiones, dentro de un período de tiempo determinado, de manera de asegurar su capacidad de afectar a la mejora del SGSI, basados en los resultados de las mediciones informados. Un excesivo número de resultados de mediciones informados impactará en la habilidad de quienes toman las decisiones para concentrar esfuerzos y priorizar futuras actividades de mejora. Se recomienda priorizar los resultados de las mediciones basado en la importancia de las necesidades de información correspondientes y en los objetivos asociados del SGSI.

NOTA. El alcance de la medición se relaciona con el alcance del SGSI establecido de acuerdo con IRAM-ISO/IEC 27001:2007 4.2.1 a).

7.3 Identificación de necesidad de información

Se recomienda que cada estructura de medición corresponda a, por lo menos, una necesidad de información. En el anexo A se presenta un ejemplo de necesidad de información, describiendo como punto de inicio el propósito de la medición y como fin los criterios de decisión relevantes.

Se recomienda que para identificar las necesidades de información pertinentes se desarrollen las siguientes actividades:

a) examinar el SGSI y sus procesos, tales como las siguientes:

   1) políticas y objetivos del SGSI, objetivos de control y controles;

   2) requerimientos legales, regulatorios, contractuales y organizacionales de seguridad de la información;

   3) resultados del proceso de gestión de riesgos de la seguridad de la información, como los descriptos en IRAM-ISO/IEC 27001.

b) priorizar las necesidades de información identificadas, basadas en criterios, tales como las siguientes:

1) prioridades del tratamiento de los riesgos;

2) recursos y capacidades de una organización;

3) intereses de las partes interesadas;

4) política de seguridad de la información;

5) información requerida para cumplir con los requerimientos legales, regulatorios y contractuales;

6) valor de la información en relación con el costo de la medición;

c) seleccionar un subconjunto de información requerida a ser utilizada en actividades de medición a partir de la lista de prioridades; y

d) documentar y comunicar las necesidades de información seleccionada a todas las partes interesadas relevantes.

Se recomienda que todas las mediciones aplicadas a un SGSI, controles o grupos de controles implementados, se realicen basados en la necesidad de información seleccionada.

7.4 Selección de objeto y atributos

Se recomienda que se identifiquen cada objeto de medición y sus atributos se identifiquen en el contexto general y el alcance del SGSI. Se recomienda que se haga notar que un objeto de medición puede tener varios atributos aplicables.

Se recomienda que el objeto y sus atributos que se van a utilizar para la medición, se seleccionen en base a la prioridad de las necesidades de información correspondientes.

Los valores que se asignen a una medida base se obtienen aplicando un método de medición apropiado para los atributos seleccionados. Se recomienda que dicha selección asegure que:

- se puede identificar una medida base pertinente y un método de medición apropiado; y
- se pueden desarrollar resultados de mediciones significativos, basados en los valores obtenidos y las medidas desarrolladas.

Las características de los atributos seleccionados determinan el tipo del método de medición a utilizar para obtener los valores que se van a asignar a las medidas base (ejemplo, cualitativos o cuantitativos).

Se recomienda que se documenten el objeto y los atributos seleccionados, junto con las razones para dicha selección.

Se recomienda que se utilicen datos que describan el objeto de medición y los atributos correspondientes, como los valores a ser asignados a las medidas base. Ejemplos de objetos de medición incluyen pero no se limitan a:

- productos y servicios;
- procesos;
- activos aplicables como instalaciones, aplicaciones y sistemas de información como los identificados en la IRAM-ISO/IEC 27001: 2005, (Inventario de activos, A.7.1.1);
- unidades de negocio;
- ubicaciones geográficas; y
- servicios provistos por terceras partes.

Se recomienda que se revisen los atributos de manera de asegurar que:

a) se han seleccionado atributos apropiados para medir; y

b) se ha definido la recolección de datos para asegurar que se encuentre presente un número suficiente de atributos que permita una medición efectiva.

Se recomienda que sólo se seleccionen los atributos que son pertinentes a la medida base. A pesar de que se recomienda que la selección tome en consideración el grado de dificultad en obtener los atributos a ser medidos, es conveniente que la misma no se realice únicamente

sobre datos de fácil obtención o sobre los atributos fáciles de medir.

7.5 Desarrollo de la estructura de medición

7.5.1 Visión general

Este subcapítulo (7.5) describe el desarrollo de la estructura de medición, desde 7.5.2 (la selección de la medida) hasta 7.5.8 (las partes interesadas).

7.5.2 Selección de la medida

Se recomienda identificar las medidas que satisfagan potencialmente la necesidad de información seleccionada, y que ellas se definan con detalle suficiente de manera de colaborar con la selección de medidas a ser implementadas. Las medidas recientemente identificadas pueden involucrar la adaptación de medidas existentes.

NOTA. La identificación de medidas base se encuentra muy relacionada con la identificación del objeto de medición y sus atributos.

Se recomienda seleccionar las medidas identificadas que satisfagan potencialmente las necesidades de información. Se recomienda que también se considere la información de contexto necesaria para interpretar o normalizar las medidas.

NOTA. Se pueden seleccionar muchas combinaciones diferentes de medidas (por ejemplo: medidas base, medidas derivadas e indicadores) para cubrir necesidades de información específicas.

Se recomienda que las medidas seleccionadas reflejen la prioridad de las necesidades de información. Los ejemplos de criterios que podrían utilizarse para la selección de medidas incluyen:

- facilidad para la recolección de los datos;
- disponibilidad de los recursos humanos para recolectar y gestionar los datos;
- disponibilidad de las herramientas apropiadas;
- número de indicadores potencialmente correspondientes respaldados por las medidas base;
- facilidad para la interpretación;
- número de usuarios de los resultados de medición desarrollados;
- evidencia de cómo las medidas se adecuan a los propósitos o necesidad de información; y
- costos de recolectar, gestionar y analizar los datos.

7.5.3 Método de medición

Se recomienda que para cada medida base individual se defina un método de medición. Dicho método de medición se utiliza para cuantificar un objeto de medición, a través de la transformación de los atributos en que se van a asignar a la medida base.

Un método de medición puede ser subjetivo u objetivo. Los métodos subjetivos se basan en la cuantificación, involucrando el juicio humano, mientras que los métodos objetivos utilizan la cuantificación basada en reglas numéricas, el cual se puede implementar por medios humanos o automáticos.

El método de medición cuantifica los atributos como valores al aplicar la escala apropiada. Cada escala utiliza unidades de medición. Sólo se comparan directamente las cantidades expresadas en la misma unidad de medición.

Para cada método de medición, se recomienda que se establezca y documente un proceso de medición. Se recomienda que dicha verificación asegure un nivel de confianza en el valor que será obtenido al aplicar el método de medición al atributo del objeto de medición, y asignarlo a una medida base. Donde sea necesario asegurar validez de los valores, se recomienda que se normalicen y verifiquen a intervalos definidos las herramientas utilizadas para medir atributos.

Se debe tener en cuenta la precisión del método de medición y se recomienda registrar la desviación o varianza asociada.

Se recomienda que el método de medición sea consistente a través del tiempo, de manera que los valores asignados a la medida base, tomadas en tiempos distintos, sean comparables, y que los valores asignados a una medida derivada y a un indicador también sean comparables.

7.5.4 Función de medición

Por cada medida derivada individual, se recomienda que se defina una función de medición, la cual sea aplicable a dos o más valores asignados a medidas base. Dicha función de medición se utiliza para transformar los valores asignados a una o más medidas base, al valor que se va asignar a una medida derivada. En algunos casos, una medida base puede contribuir directamente al modelo analítico además de una medida derivada.

Una función de medición (por ejemplo, un cálculo) puede involucrar una variedad de técnicas, tales como: promediar todos los valores asignados a las medidas base, aplicar ponderaciones a los valores asignados a las medidas base, o asignar valores cualitativos a los valores asignados a las medidas base, antes de utilizarlas para calcular el valor a ser asignado a una medida derivada. La función de medición puede combinar valores a ser asignados a medidas base utilizando diferentes escalas, como porcentajes o resultados de evaluaciones cualitativas.

7.5.5 Modelo analítico

Por cada indicador, se recomienda que se defina un modelo analítico con el propósito de transformar uno o más valores asignados a una medida base y/o derivada, en valores que se van a asignar al indicador.

El modelo analítico combina medidas relevantes, de una manera que produzca una salida que tenga significado para las partes interesadas.

Se recomienda que se tenga en consideración los criterios de decisión que se aplicarán a un indicador, cuando se defina el modelo analítico.

Algunas veces un modelo analítico puede ser tan simple como transformar un valor asignado a una medida derivada, en un valor a ser asignado a un indicador.

7.5.6 Indicadores

Los valores a ser asignados a los indicadores se producirán agregando valores establecidos a las medidas derivadas e interpretando éstos valores basados en los criterios de decisión. Se recomienda que se defina un formato para la presentación del indicador como parte del formato del informe (ver 7.7), por cada indicador que se informe al cliente.

Los formatos para la presentación de los indicadores presentarán visualmente las medidas y proveerán una explicación detallada de los indicadores. Se recomienda que se adapten los formatos para la presentación de los indicadores para cumplir con las necesidades de información del cliente.

7.5.7 Criterios de decisión

Se recomienda que se definan y documenten los criterios de decisión correspondiente a cada indicador, basado en los objetivos de seguridad de la información, para proveer una guía de acción a las partes interesadas. Se recomienda que dicha guía se enfoque hacia las expectativas de progreso y los umbrales para iniciar acciones de mejora, basados en el indicador.

Los criterios de decisión establecen una meta a través de la cual se mide el éxito (ver 5.3) y proveen una guía para interpretar el indicador en relación con su proximidad con dicha meta.

Es necesario definir las metas para cada ítem con respecto al rendimiento de los procesos del SGSI y los controles, para el cumplimiento de objetivos, y para la efectividad del SGSI que se está evaluado.

La alta dirección puede decidir no definir metas para los indicadores hasta tanto no se recolecten los datos iniciales. Una vez que se

identifiquen las acciones correctivas basadas en los datos iniciales, se pueden definir los criterios de decisión apropiados y los hitos de implementación que sean realistas para el SGSI específico. Si los criterios de decisión no se pueden establecer en este punto, se recomienda que la alta dirección evalúe si el objeto de medición y las medidas correspondientes realmente proveen el valor esperado por la organización.

Se puede facilitar el establecimiento de los criterios de decisión si se encuentran disponibles los datos históricos que corresponden a las medidas desarrolladas o seleccionadas. Las tendencias observadas en el pasado proveerán la percepción de los rangos de rendimiento que han existido previamente y una guía en la creación de criterios de decisión realistas. Los criterios de decisión se pueden calcular o basar en un entendimiento conceptual de un comportamiento esperado. Los criterios de decisión se pueden derivar de datos históricos, planes, y heurística, o calcular como límites de control estadísticos o intervalos de confianza estadísticos.

7.5.8 Partes interesadas

Por cada medida base y/o derivada, se recomienda que se identifiquen y documenten las partes interesadas apropiadas. Las partes interesadas pueden incluir a los siguientes:

a) cliente de la medición: la alta dirección u otras partes interesadas que solicitan o requieren información sobre la efectividad de un SGSI, controles o grupo de controles;

b) revisor de la medición: la persona o unidad organizacional que valida que las estructuras de medición desarrolladas son apropiadas para evaluar la efectividad de un SGSI, controles o grupo de controles;

c) propietario de la información: la persona o unidad organizacional que es responsable por la información sobre un objeto de medición y sus atributos y es responsable de su medición;

d) recolector de información: la persona o unidad organizacional responsable por la recolección, registro y almacenamiento de los datos; y

e) comunicador de la información: la persona o unidad organizacional responsable por el análisis de los datos y la comunicación de los resultados medidos.

7.6 Estructura de medición

Se recomienda que la especificación de la estructura de medición incluya como mínimo, la información siguiente:

a) el propósito de la medición;

b) el objetivo de control a alcanzar mediante los controles, y controles específicos, grupos de control y procesos del SGSI a ser medidos;

c) el objeto de medición;

d) los datos a recolectar y utilizar;

e) los procesos para la recolección y análisis de los datos;

f) los procesos para informar los resultados de las mediciones, incluyendo los formatos de los informes;

g) los roles y las responsabilidades de las partes interesadas correspondientes; y

h) un ciclo para revisar las mediciones de manera de asegurar su utilidad en relación a la necesidad de información.

El anexo A provee un ejemplo de estructura de medición que incorpora todos los puntos antes mencionados [de a) a h)]. El anexo B provee ejemplos de estructuras de medición aplicadas para medir los procesos y controles de un SGSI.

7.7 Recolección, análisis y reporte de los datos

Se recomienda que se establezcan procedimientos para la recolección y análisis de los datos, y procesos para informar los resultados del desarrollo de las mediciones. Se recomien-

da que también se establezcan, de ser requerido, herramientas de soporte, equipamiento de medición y tecnologías. Dichos procedimientos, herramientas, equipamiento para medición y tecnologías se comprenderán las siguientes actividades:

a) la recolección de los datos, incluyendo el almacenamiento y verificación de ellos (ver 8.3). Se recomienda que los procedimientos identifiquen cómo se colectan los datos a través del método de medición utilizado, la función de medición y el modelo analítico. Se recomienda también indicar cómo y dónde se almacenarán los datos junto con toda la información de contexto necesaria para entender y verificarlos. La verificación se puede realizar contrastando los datos con una lista de control, la cual se construye para verificar que los datos faltantes son mínimos, y que el valor que se asigna a cada medida es válido;

   NOTA. La verificación de los valores a ser asignados a las medidas base se relaciona estrechamente con la verificación del método de medición (ver 7.5.3).

b) el análisis de los datos e informe de los resultados de las mediciones desarrolladas. Se recomienda que el procedimiento especifique las técnicas de análisis de datos (ver 9.2), y la frecuencia, formato y métodos para el reporte de los resultados de las mediciones. Se recomienda que se identifique el conjunto de herramientas necesario para realizar el análisis de datos.

Los ejemplos de formatos de reportes incluyen:

- tablero de control para proveer información estratégica a través de la integración de indicadores de alto nivel;
- tablero de ejecución y operaciones, menos enfocado a objetivos estratégicos y más ligado a la efectividad de controles y procesos específicos;
- reportes, simples y estáticos, por ejemplo una lista de medidas para un período de tiempo dado, como también reportes más sofisticados con agrupamiento anidado, resúmenes rodantes, con hipervínculos dinámicos. Los reportes se utilizan de mejor manera cuando el usuario necesita mirar a datos en crudo en un formato de fácil lectura; y
- indicadores para representar valores dinámicos, incluyendo alertas, elementos gráficos adicionales y etiquetas de los puntos finales.

7.8 Implementación y documentación de la medición

Se recomienda que el enfoque general de la medición se documente en un plan de implementación, y que incluya, como mínimo, la siguiente información:

a) la implementación del Programa de medición de la seguridad de la información para la organización;

b) las especificaciones de medición siguientes:

   1) la estructura de medición genérica de la organización;

   2) la estructura de medición individual de la organización; y

   3) la definición del rango y procedimientos para la recolección y el análisis de los datos;

c) el calendario planificado para desarrollar las actividades de medición;

d) los registros generados a través de la realización de las actividades de medición, incluyendo los datos recolectados y los registros analizados; y

e) los formatos de reporte para los resultados de las mediciones a ser informados a la alta dirección / partes interesadas (ver IRAM-ISO/IEC 27001:2007 capítulo 7 *Revisión por la alta dirección*).

8 OPERACIÓN DE MEDICIÓN

8.1 Visión general

La operación de medición de la seguridad de la información comprende actividades que son esenciales para asegurar que los resultados de las mediciones proporcionan información precisa con respecto a la efectividad de un SGSI, controles o grupos de controles implementados y la necesidad de acciones apropiadas de mejora.

Esta actividad incluye lo siguiente:

a) integrar procedimientos de medición dentro de la operación general del SGSI;

b) recolectar, almacenar y verificar los datos.

8.2 Integración del procedimiento

Se recomienda que el Programa de medición de la seguridad de la información se integre y use por completo dentro del SGSI. Se recomienda que los procedimientos de medición se coordinen con la operación del SGSI, incluyendo:

a) la definición y documentación de roles, autoridades y responsabilidades, con respecto al desarrollo, implementación y mantenimiento de la medición de la seguridad de la información;

b) la recolección de datos, y, cuando sea necesario, la modificación de la operación habitual del SGSI para alinear las actividades de generación y recolección de datos;

c) la comunicación a las partes interesadas pertinentes de los cambios en las actividades de recolección de datos;

d) el mantenimiento de la competencia de los recolectores de información y el entendimiento de los tipos de datos requeridos, herramientas y procedimientos de recolección de datos;

e) el desarrollo de políticas y procedimientos, que defina el uso de mediciones dentro de la organización, la distribución de la información de medición, la auditoría y la revisión del Programa de la medición de la seguridad de la información;

f) la integración del análisis y los reportes de datos dentro de procesos relevantes, para asegurar su rendimiento regular;

g) el seguimiento y control, la revisión y la evaluación de los resultados de la medición;

h) el establecimiento de un proceso que elimine y agregue mediciones, para asegurar que se ajuste a la evolución de la organización; y

i) el establecimiento de un proceso para determinar la vida útil de los datos históricos y los análisis de tendencias.

8.3 Recolección, almacenamiento y verificación de los datos

Las actividades de recolección, almacenamiento y verificación de los datos incluyen lo siguiente:

a) recolección de los datos requeridos dentro de intervalos regulares utilizando un método de medición definido;

b) documentación de la recolección de datos, incluyendo:

   1) fecha, hora y ubicación de la recolección de los datos;

   2) recolector de la información;

   3) propietario de la información;

   4) cualquier asunto que haya ocurrido durante la recolección de los datos que pueda ser útil;

   5) información para la verificación de los datos y validación de la medición.

c) verificar los datos recolectados contra los criterios de selección de las mediciones y

criterios de validación de las estructuras de medición.

Se recomienda que los datos recolectados y cualquier información de contexto necesaria se consolide y almacene en un formato registrable propicio para un análisis de los datos.

9 ANÁLISIS DE DATOS E INFORME DE RESULTADOS DE LAS MEDICIONES

9.1 Visión general

Se recomienda que los datos recolectados se analicen para desarrollar resultados de las mediciones y que estos se comuniquen.

Dicha actividad incluye lo siguiente:

a) análisis de datos y desarrollo de resultados de las mediciones; y

b) comunicación de los resultados de las mediciones a las partes interesadas correspondientes.

9.2 Análisis datos y generación de resultados de las mediciones

Se recomienda que los datos recolectados se analicen e interpreten dentro de los términos de los criterios de decisión. Los datos pueden ser agregados, transformados o codificados nuevamente antes de su análisis. Durante esta tarea, se recomienda que se procesen los datos para producir los indicadores. Se pueden aplicar varias técnicas de análisis. Se recomienda que la profundidad del análisis se determine por la naturaleza de los datos y la necesidad de información.

NOTA. En la ISO/TR 10017 (Guidance on statistical techniques for ISO 9001) se puede encontrar una guía para el desarrollo del análisis estadístico.

Se recomienda que se interpreten los resultados de los análisis. Se recomienda que la persona que analiza los resultados (comunicador), sea capaz de generar conclusiones iniciales basadas en ellos. Sin embargo, debido a que el/los comunicador/es pueden no estar directamente involucrados en los procesos técnicos y de gestión, tales conclusiones necesitan ser revisadas por otras partes interesadas. Se recomienda que todas las interpretaciones tengan en cuenta el contexto de las medidas.

Se recomienda que el análisis de datos identifique brechas entre los resultados esperados de mediciones de un SGSI implementado, controles o grupos de controles, y los resultados reales. Las brechas identificadas indicarán las necesidades de mejora del SGSI implementado, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos.

Se recomienda que se identifiquen aquellos indicadores que demuestran incumplimiento o bajo rendimiento y puedan ser clasificados de la manera siguiente:

a) falla del plan de tratamiento de riesgos para implementar (o implementar satisfactoriamente), operar y gestionar controles o procesos del SGSI (por ejemplo, que una amenaza pase por alto controles y procesos del SGSI);

b) falla en la evaluación de riesgos:

   1) los controles o los procesos del SGSI son inefectivos debido a que son insuficientes para, contrarrestar amenazas estimadas (por ejemplo, debido a la probabilidad de que una amenaza haya sido subestimada) o para contrarrestar nuevas amenazas;

   2) los controles o los procesos del SGSI no se encuentran implementados, debido a haber pasado por alto amenazas.

Se recomienda que los informes que son utilizados para comunicar los resultados de las mediciones a las partes interesadas, se preparen utilizando formatos de informes apropiados (ver 7.7) de acuerdo con el plan de implementación del Programa de medición de la seguridad de la información.

Se recomienda que las conclusiones de los análisis sean revisadas por las partes interesadas relevantes, de manera de asegurar la

interpretación apropiada de los datos. Se recomienda que el resultado del análisis de datos se documente para ser comunicado a las partes interesadas.

9.3 Comunicación de los resultados de las mediciones

Se recomienda que el comunicador de la información determine cómo comunicar los resultados de la medición de la seguridad de la información, tales como:

- cuáles resultados de mediciones se van a informar interna y externamente;
- hacer listados de las mediciones correspondientes a partes interesadas individuales, y otras partes interesadas;
- proveer resultados de mediciones específicos, y el tipo de presentación, adaptada a las necesidades de cada grupo; y
- establecer los medios para obtener respuestas de las partes interesadas, que se van a utilizar para evaluar la utilidad de los resultados de las mediciones y la efectividad del Programa de medición de la seguridad de la información.

Se recomienda que los resultados de las mediciones se comuniquen a una variedad de partes interesadas internas incluyendo, como mínimo, a:

- clientes de la medición (ver 7.5.8);
- propietarios de la información (ver 7.5.8);
- personal a cargo de la gestión del riesgo de la seguridad de la información, especialmente donde se han identificado fallas en la evaluación del riesgo; y
- personal que es responsable por las áreas en las que se ha identificado una necesidad de mejora.

La organización puede requerir en algunos casos distribuir informes de resultados de mediciones a partes externas, incluyendo autoridades reguladoras, accionistas, clientes y proveedores. Se recomienda que los informes de los resultados de las mediciones que se distribuyan externamente, contengan sólo datos que sean apropiados para ser entregados externamente, y que sean aprobados por la alta dirección y por las partes interesadas correspondientes antes de su entrega.

10 EVALUACIÓN Y MEJORA DEL PROGRAMA DE MEDICIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

10.1 Visión general

Se recomienda que la organización evalúe a intervalos planificados lo siguiente:

a) la efectividad del Programa de medición de la seguridad de la información de manera de asegurar que:

   1) produce resultados de mediciones de una manera efectiva;

   2) se ejecuta según lo planificado;

   3) trata los cambios en el SGSI implementado y/o en los controles;

   4) trata los cambios en el ambiente (por ejemplo, requerimientos, legislación o tecnología); y

b) la utilidad de los resultados de mediciones desarrolladas, para asegurar que los mismos satisfacen las necesidades de información relevantes.

Se recomienda que la alta dirección especifique la frecuencia de dicha evaluación, planifique revisiones periódicas y establezca los mecanismos para hacer posibles dichas mediciones (ver capítulo 7.2 de IRAM-ISO/IEC 27001:2007).

Se recomienda que las actividades relevantes sean las siguientes:

1) identificación de los criterios de evaluación del Programa de medición de la seguridad de la información (ver 10.2);

2) seguimiento, control, revisión y evaluación de las mediciones (ver 10.3); e

3) implementación de las mejoras (ver 10.4).

10.2 Identificación del criterio de evaluación del Programa de medición de la seguridad de la información

Se recomienda que la organización defina criterios para evaluar la efectividad del Programa de medición de la seguridad de la información, así como la utilidad de los resultados de las mediciones desarrolladas. Se recomienda que el criterio se defina al inicio de la implementación del PMSI, teniendo en cuenta el contexto de los objetivos técnicos y de negocio de la organización.

Cuando las organizaciones tienen que evaluar y mejorar el Programa de medición de la seguridad de la información, los criterios más probables a utilizar son:

- cambios en los objetivos de negocio de la organización;
- cambios de requerimientos legales o regulatorios y obligaciones contractuales en la seguridad de la información;
- cambios en los requerimientos de la organización sobre la seguridad de la información;
- cambios en los riesgos de la seguridad de la información de la organización;
- aumento en la disponibilidad de datos más refinados o adecuados, y/o métodos para recolectar datos con el propósito de medir; y
- cambios en el objeto de medición y/o sus atributos.

Para evaluar los resultados de medición desarrollados se pueden aplicar los criterios siguientes:

a) los resultados de medición son:

   1) sencillos de entender;

   2) comunicados a tiempo; y

   3) objetivos, comparables y reproducibles.

b) los procesos establecidos para desarrollar resultados de las mediciones son:

   1) bien definidos;

   2) sencillos de operar; y

   3) seguidos apropiadamente.

c) los resultados de las mediciones son útiles para mejorar la seguridad de la información;

d) los resultados de las mediciones tratan las necesidades de información correspondientes.

10.3 Seguimiento, control, revisión y evaluación del Programa de medición de la seguridad de la información

Se recomienda que la organización siga, controle, revise y evalúe su Programa de medición de la seguridad de la información contra los criterios establecidos (ver 10.2).

Se recomienda que la organización identifique potenciales necesidades de mejora del Programa de medición de la seguridad de la información, incluyendo:

a) revisar o remover estructuras de medición adoptadas que ya no son apropiadas; y

b) reasignar recursos para dar soporte al Programa de gestión de la seguridad de la información.

Se recomienda que la organización también identifique necesidades potenciales de mejora del SGSI implementado, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos; y documente las decisiones de la alta dirección para permitir la comparación y el

análisis de tendencias durante las revisiones subsecuentes.

Se recomienda que el resultado de dicha evaluación y las potenciales necesidades de mejora identificadas, se comuniquen a las partes interesadas relevantes de manera de permitir la toma de decisiones con respecto a mejoras necesarias.

Se recomienda que la organización asegure la obtención de respuesta de las partes interesadas sobre los resultados de esta evaluación y sobre las potenciales necesidades de mejora identificadas, así como también, que la organización entienda que dicha respuesta es uno de los datos de entrada con respecto a la efectividad del Programa de medición de la seguridad de la información.

10.4 Implementar mejoras

Se recomienda que la organización asegure que las partes interesadas correspondientes identifiquen las necesidades de mejora del Programa de medición de la seguridad de la información (ver 7.3 e) de la IRAM-ISO/IEC 27001:2007). Se recomienda que las mejoras identificadas sean aprobados por la alta dirección y que los planes aprobados se documenten y comuniquen a las partes interesadas apropiadas.

Se recomienda que la organización asegure que las mejoras aprobadas del Programa de medición de la seguridad de la información se implementen según lo planificado.

La organización puede aplicar técnicas de gestión de proyectos para cumplir con las mejoras.

Anexo A
(Informativo)

Plantilla para estructurar la medición de la seguridad de la información

El anexo A provee una plantilla de ejemplo de una estructura de medición de la seguridad de la información que incluye todos los componentes identificados en 7.5 como los descriptos en 5.4. Las organizaciones pueden modificar la plantilla de acuerdo a sus necesidades.

Identificación de la estructura de medición	
Nombre de la estructura de medición	Nombre de la medición
Identificador numérico	Identificador numérico único específico de la organización
Propósito de la estructura de medición	Describe las razones para introducir la medición
Objetivo del control / proceso	Objetivo del control/proceso bajo medición (planificado o implementado)
Control(1)/proceso(1)	Control/proceso bajo medición
Control(2)/proceso(2)	Opcional: controles/procesos adicionales dentro del agrupamiento, incluidos en la misma medida, de ser aplicable (planificadas o implementadas).
Objeto de medición y atributos	
Objeto de medición	Objeto (entidad) que se caracteriza a través de la medición de sus atributos. Un objeto puede incluir procesos, planes, proyectos, recursos y sistemas o componentes de sistemas.
Atributo	Propiedad o característica de un objeto de medición que puede distinguirse cuantitativa o cualitativamente, por medios manuales o automatizados.
Especificación de medidas base (para cada medida base [1…n])	
Medida base	Una medida base es definida en términos de un atributo y el método de medición especificado para cuantificarlo (por ejemplo la cantidad de personas entrenadas, cantidad de ubicaciones, costo acumulativo a la fecha). A medida de que los datos son recolectados, se asigna un valor a la medida base
Método de medición	Secuencia lógica de operaciones utilizadas para cuantificar un atributo con respecto a la escala especificada.
Tipo de método de medición	Dependiendo de la naturaleza de las operaciones utilizadas para cuantificar un atributo, se pueden identificar dos tipos de métodos: - Subjetivo: cuantificación que involucra el juicio humano - Objetivo: cuantificación basada en reglas numéricas tal como contar.
Escala	Conjunto ordenado de valores o categorías con las cuales se mapean los atributos de las medidas base.
Tipo de escala	Dependiendo de la naturaleza de la relación entre los valores en

	la escala, normalmente se definen cuatro tipos de escalas: nominal, ordinal, intervalo y ratios.
Unidad de medición	Cantidad particular, definida y adoptada por convención, con la cual cualquier otra cantidad del mismo tipo se puede comparar para expresar la proporción de dos cantidades como un número.
Especificación de medida derivada	
Medida derivada	Una medida que se obtiene en función de dos o más medidas base
Función de medición	Algoritmo o cálculo realizado para combinar dos o más medidas base. La escala y unidad de la medida derivada depende de las escalas y unidades de las medidas base que la componen, así como también de cómo se combinan las mismas en la función.
Especificación del indicador	
Indicador	Medida que provee una estimación o evaluación de atributos específicos, derivados de un modelo analítico con respecto a una determinada necesidad de información. Los indicadores son la base para el análisis y la toma de decisiones.
Modelo analítico	Algoritmo o cálculo que combina una o muchas medidas base y/o derivadas con criterios de decisión asociados. Se basa en un entendimiento o suposición sobre las relaciones esperadas entre la medida base y/o la medida derivada y/o su comportamiento en el tiempo. Un modelo analítico produce estimaciones o evaluaciones que corresponde a una necesidad de información definida.
Especificación de los criterios de decisión	
Criterios de decisión	Umbrales, objetivos o patrones utilizados para determinar la necesidad de una acción o investigación adicional, o para describir el nivel de confianza en un resultado dado. Los criterios de decisión son útiles para interpretar los resultados de la medición.
Resultados de medición	
Interpretación de un indicador	Una descripción de cómo se recomienda interpretar el indicador de la muestra (ver la figura de muestra en la descripción del indicador).
Formatos de los informes	Se recomienda que los formatos de los informes se identifiquen y documenten. Describen las observaciones que la organización o el propietario de la información pueden querer en los registros. Los formatos de los informes representarán visualmente las medidas y proveerán una explicación verbal de los indicadores. Se recomienda que los formatos de los informes se adapten al cliente de la información.
Partes interesadas	
Cliente de la medición	La alta dirección u otra parte interesada que requiera o solicite información sobre la efectividad del SGSI, controles o grupos de control.
Revisor de la medición	Persona o unidad organizacional que valida que las estructuras de medición desarrolladas son apropiadas para evaluar la efectividad del SGSI, controles o grupo de controles.

Propietario de la información	Persona o unidad organizacional que posee la información sobre un objeto de medición y los atributos, y es responsable por la medición.
Recolector de la información	Persona o unidad organizacional responsable de recolectar, registrar y almacenar los datos.
Comunicador de la información	Persona o unidad organizacional responsable de analizar los datos y comunicar los resultados de la medición
Frecuencia / Periodicidad	
Frecuencia de la recolección de datos	Periodicidad con la cual se recolectarán los datos
Frecuencia del análisis de datos	Periodicidad con la cual se analizarán los datos
Frecuencia del informe de los resultados de la medición	Periodicidad con la cual se van a informar los resultados de la medición (esto podría ser menos frecuente que la recolección de datos)
Revisión de la medición	Fecha de la revisión de la medición (expiración o renovación de la validez de la medición)
Período de medición	Define el período que se va a medir.

Anexo B
(Informativo)

Ejemplos de estructuras de medición

Los siguientes capítulos proveen ejemplos de estructuras de medición. Éstos ejemplos tienen la intención de demostrar como aplicar esta Norma Internacional utilizando la plantilla provista en el anexo A.

Tabla de contenidos

Procesos y controles relacionados (capítulo en IRAM-ISO/ IEC 27001:2007 o número de control en el anexo A)	**Ejemplos de estructuras de medición relacionadas** (referencia en este anexo)	**Nombres de los ejemplos de estructuras de medición**
Capítulo 4.2.2 h)	B.4.1	Efectividad de la gestión de incidentes de la seguridad de la información
Capítulo 5.2.2 d)	B.1.1	Personal entrenado en el SGSI
Capítulo 8.2	B.4.2	Implementación de una acción correctiva
Control A.6.1.8	B.3	Proceso de revisión del SGSI
Control A.6.1.1 y A.6.1.2	B.5	Compromiso de la alta dirección
Control A.6.2.3	B.10	Seguridad en acuerdos con

		terceras partes
Control A.8.2 y A.8.2.2	B.1.2	Entrenamiento en seguridad de la información
Control A.8.2 y A.8.2.2	B.1.3	Concientización en el cumplimiento de la seguridad de la información
Control A.9.1.2	B.7	Controles físicos de entrada
Control A.9.2.4	B.9	Gestión del mantenimiento periódico
Control A.10.4.1	B.6	Protección contra código malicioso
Control A.10.10.1 y A.10.10.2	B.8	Revisión de los archivos de registro de actividades
Control A.11.3.1	B.2.1	Calidad de las contraseñas – manual
Control A.11.3.1	B.2.2	Calidad de las contraseñas – automática

B.1 Entrenamiento en el SGSI

B.1.1 Personal entrenado en el SGSI

Identificación de la estructura de la medición	
Nombre de la estructura de medición	Personal entrenado en el SGSI
Identificación numérica	Específica de la organización
Propósito de la construcción de medición	Establecer el cumplimiento del control con las políticas de seguridad de la información de la organización
Objetivo de control/proceso	Capítulo 5.2.2 [27001:2007]. Formación, toma de conciencia y competencia
Control (1)/proceso (1)	Capítulo 5.2.2.d [27001:2007]. Formación, toma de conciencia y competencia. La organización debe asegurar que todo el personal al que se asigne responsabilidades definidas en el SGSI sea competente para realizar las tareas exigidas, mediante: d) el mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones.
Control (2)/proceso (2)	Opcional: controles adicionales dentro del agrupamiento incluidos en la misma medida, si son aplicable (planeada o implementada)
Objeto de medición y atributos	
Objeto de medición	Base de datos de empleados
Atributo	Registros de entrenamiento

Especificación de la medida base (1)	
Medida base	Número de empleados que recibieron entrenamiento en el SGSI de acuerdo al plan anual de entrenamiento. Número de empleados que deben recibir entrenamiento en el SGSI.
Método de medición	Cantidad de registros con columnas/filas de formación en SGSI rellenas como “Recibidas”
Tipo de método de medición	Objetivo
Escala	Numérica
Tipo de escala	Proporción
Unidad de medición	Empleados
Especificación de la medida derivada	
Medida derivada	Porcentaje del personal entrenado en el SGSSI
Función de medición	La cantidad de empleados que recibieron formación en el SGSI / la cantidad de empleados que tienen que recibir formación en el SGSI * 100
Especificación del indicador	
Indicador	Uso de identificadores de color. Gráfico de barras que representa cumplimiento en varios períodos de reporte con respecto a los umbrales (rojo, amarillo, verde) definidos por el Modelo analítico. Se recomienda que el número de períodos informados a usar en la tabla los defina la organización.
Modelo analítico	0-60% - Rojo; 60-90% - Amarillo; 90-100% Verde. Para Amarillo, si el progreso es menor a 10% por trimestre, la calificación pasa automáticamente a ser roja.
Especificación de los criterios de decisión	
Criterios de decisión	Rojo - se requiere intervención, es necesario efectuar un análisis de las causas para determinar las razones del no cumplimiento o rendimiento pobre Amarillo – se recomienda que se siga de cerca este indicador por la posibilidad de que se deslice a Rojo Verde - no se requiere acción.
Medición del resultado	
Interpretación del indicador	Especifico de la organización.
Formatos de reporte	Gráfico de barras con codificación de colores en función a los criterios de decisión. Se recomienda adjuntar al gráfico de barras una breve descripción del significado de la medida y las posibles acciones de la alta dirección.
Partes Interesadas	
Cliente de la medición	Gerentes responsables del SGSI
Revisor de la medición	Gerentes responsables del SGSI

Propietario de la Información	Responsable de entrenamiento - Recursos humanos.
Recolector de la información	Departamento de gestión de entrenamiento - Recursos humanos
Comunicador de la información	Gerentes responsables del SGSI
Frecuencia/Período	
Frecuencia de la recolección de datos	Mensualmente, primer día hábil de cada mes.
Frecuencia del análisis de datos	Trimestral
Frecuencia de informe de los resultados de la medición	Trimestral
Revisión de la medición	Revisar anualmente
Periodo de medición	Anual

B.1.2 Entrenamiento en seguridad de la información

Identificación de la estructura de medición	
Nombre de la estructura de medición	Entrenamiento en seguridad de la información
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Evaluar el cumplimiento de los requerimientos sobre entrenamiento anual en concientización sobre Seguridad de la información
Objetivo del control/proceso	A.8.2 Durante el empleo Objetivo: asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de las amenazas y preocupaciones de la seguridad de la información, sus responsabilidades y obligaciones, y estén preparados para respaldar las políticas de seguridad organizacional en el curso de su trabajo normal, y para reducir el riesgo de error humano.
Control(1)/proceso(1)	A.8.2.2 [27001:2007] Concientización, educación y entrenamiento en seguridad de la información. Todos los empleados de la organización y, cuando sea pertinente, los contratistas y usuarios de terceras partes deben recibir una apropiada concientización y actualizaciones regulares en las políticas y procedimientos organizacionales, que sean importantes para su tarea.
Objeto de medición y atributos	
Objeto de medición	Base de datos de empleados
Atributo	Registros de entrenamientos

Especificación de medida base(1)	
Medida base	Cantidad de empleados que recibieron entrenamiento anual sobre concientización en seguridad de la información. Número de empleados que necesitan recibir entrenamiento anual sobre concientización en seguridad de la información.
Método de medición	Cantidad de registros / registros con campo sobre el entrenamiento anual en concientización sobre seguridad de la información / registros marcados como “Recibidos”.
Tipo de método de medición	Objetivo
Escala	Numérica
Tipo de escala	Proporción
Unidad de medición	Empleado
Especificación de medida derivada	
Medida derivada	Porcentaje del personal que ha recibido el entrenamiento anual sobre concientización en seguridad de la información
Función de medición	Número de empleados que han recibido entrenamiento anual en concientización sobre seguridad de la información / número de empleados que necesitan recibir entrenamiento anual en concientización sobre seguridad de la información * 100
Especificación del indicador	
Indicador	Gráfico de barras mostrando cumplimiento sobre varios períodos de reporte, en relación con los umbrales (rojo, verde, amarillo, con identificadores de colores) definidos por el Modelo analítico. Se recomienda que la organización defina el número de períodos de reporte a utilizar en el gráfico.
Modelo analítico	0-60% - Rojo; 60-90% - Amarillo; 90-100% - Verde. Para Amarillo, si no se alcanza un progreso de al menos 10% por trimestre, la calificación pasa a ser automáticamente roja.
Especificación de los criterios de decisión	
Criterios de decisión	Rojo – se requiere intervención, se debe conducir un análisis de las causas para determinar las razones del no-cumplimiento o del rendimiento pobre. Amarillo – se recomienda que el indicador se observe de cerca por posible movimiento a rojo Verde – no se requiere ninguna acción.
Resultados de la medición	
Interpretación del indicador	Específico de la organización

Formatos de reporte	Gráfico de barras con los colores de las barras codificados en base a los criterios de decisión. Se recomienda que se adjunte al gráfico de barras un resumen de lo que significa la medición y las posibles acciones de la alta dirección.
Partes interesadas	
Cliente de la medición	Gerentes responsables por el SGSI. Gerencia de seguridad. Gerencia de capacitación
Revisor de la medición	Gerente de seguridad
Propietario de la información	Oficial de la Seguridad de la información y el Gerente de capacitación
Recolector de la información	Gerencia de capacitación – Departamento de recursos humanos
Comunicador de la información	Gerentes responsables por el SGSI
Frecuencia/Período	
Frecuencia de la recolección de datos	Mensualmente, primer día hábil de cada mes
Frecuencia del análisis de datos	Trimestral
Frecuencia de informe de los resultados de la medición	Trimestral
Revisión de la medición	Revisar anualmente
Período de medición	Anual

B.1.3 Cumplimiento con la concientización sobre seguridad de la información

Identificación de la estructura de medición	
Nombre de la estructura de medición	Cumplimiento con la política sobre concientización en Seguridad de la información.
Identificador numérico	Específico de la organización.
Propósito de la estructura de medición	Evaluar el estado del cumplimiento con la política organizacional sobre concientización en seguridad entre el personal correspondiente.
Objetivos de control/procesos	A.8.2 Durante el empleo Objetivo: asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de las amenazas y preocupaciones de la seguridad de la información, sus responsabilidades y obligaciones, y estén preparados para respaldar las políticas de seguridad organizacional en el curso de su trabajo normal, y para reducir el riesgo de error humano.

Control(1)/proceso(1)	A.8.2.2 Todos los empleados de la organización y, cuando sea pertinente, los contratistas y usuarios de terceras partes deben recibir una apropiada concientización y actualizaciones regulares en las políticas y procedimientos organizacionales, que sean importantes para su tarea. (Implementación) Todo el personal concerniente al SGSI debe recibir entrenamiento en concientización sobre seguridad de la información antes de que se le conceda acceso a un sistema de información. El entrenamiento incluye...
Control(2)/proceso(2)	A.8.2.1 La dirección debe requerir a los empleados, contratistas y usuarios de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización. (Implementación) Todo el personal relevante al SGSI debe firmar acuerdos de usuario antes de que se le conceda acceso a un sistema de información
Objeto de medición y atributos	
Objeto de medición	1.1 Plan / programa de entrenamiento en concientización sobre seguridad de la información 1.2 Personal que ha completado o que se encuentra en progreso de entrenamiento 2.1 Plan / programa para firmar los acuerdos de usuario / cronograma 2.2 Personal que ha firmado los acuerdos
Atributo	1.1 Personal identificado en el plan 1.2 Estado del personal con respecto al entrenamiento 2.1 Personal identificado en el plan para firmar los acuerdos/ cronograma 2.2 Estado del personal con respecto a la firma de los acuerdos / cronograma
Especificación de la medida base	
Medida base	1.1 Cantidad de personas planificado hasta la fecha 1.2 Cantidad de personas que ha firmado 2.1 Cantidad de personas planificado para firmar hasta la fecha 2.2 Cantidad de personas que ha firmado hasta la fecha
Método de medición	1.1 Contar la cantidad de personas planificadas para firmar y completar el entrenamiento a la fecha 1.2 Preguntar al responsable por el porcentaje del personal que ha completado el entrenamiento y ha firmado. 2.1 Contar la cantidad de personas planificadas para firmar a la fecha.

	2.2 Contar cantidad de personas que ya han firmado los acuerdos de usuario
Tipo de método de medición	1.1 Objetivo 1.2 Subjetivo 2.1 Objetivo 2.2 Objetivo
Escala	1.1 Enteros, desde cero hasta infinito 1.2 Enteros, desde cero hasta cien 2.1 Enteros, desde cero hasta infinito 2.2 Enteros, desde cero hasta infinito
Tipo de escala	1.1 Ordinal 1.2 Proporcional 2.1 Ordinal 2.2 Ordinal
Unidad de medición	1.1 Personas 1.2 Porcentual 2.1 Personas 2.2 Personas
Especificación de medida derivada	
Medida derivada	1. Progreso a la fecha 2. Progreso a la fecha con las firmas
Función de medición	1. Contar aquellas personas que firmaron y estaban planificadas para completar a la fecha 2. Dividir el personal que haya firmado a la fecha, sobre el personal planificado de haber firmado a la fecha
Especificación del indicador	
Indicador	a) Estado expresado como la combinación de proporciones, y; b) tendencia
Modelo analítico	a) [Dividir el Progreso a la fecha por (Personal planificado a la fecha por 100)] y Progreso a la fecha con firma b) Comparar estado con estados previos.
Especificación de los criterios de decisión	
Criterios de decisión	a) Se recomienda que las proporciones resultantes se encuentren respectivamente entre 0,9 y 1,1 y entre 0,99 y 1,01 para concluir el cumplimiento del objetivo de control y de no acción, y; b) Se recomienda que la tendencia sea alcista o estable.

Resultados de la medición	
Interpretación del indicador	Se recomienda que la interpretación del indicador a) sea la siguiente: – el criterio de la organización para el cumplimiento con la política de concientización de seguridad se ha cumplido satisfactoriamente entre 0,9 ≤ 1er proporción ≤ 1,1 y 0,99 ≤ 2da proporción ≤ 1,01; se muestra con fuente regular. – el criterio de la organización no se ha cumplido satisfactoriamente en [1er proporción < 0,9 o 1er proporción >1,1] y 0,99 ≤ 2do proporción ≤ 1,01; se muestra con fuente itálica; – el criterio de la organización no se ha cumplido en [2do proporción <0,99 o 2do proporción >1,01]; se muestra con fuente negrita. Se recomienda que la interpretación del indicador b) sea la siguiente: – una tendencia alcista indica cumplimiento mejorado, una tendencia a la baja indica un deterioro en el cumplimiento. El grado del cambio de la tendencia puede proveer una idea de la efectividad de la implementación del control. Un cambio fuerte en cualquier dirección indica que la implementación del control requiere un análisis detallado para determinar su causa. Las tendencias negativas pueden requerir intervención de la alta dirección. Se recomienda que las tendencias positivas se analicen para identificar “mejores prácticas” potenciales.
Formatos de reporte	Fuente normal = el criterio ha sido cumplido satisfactoriamente Fuente itálica = el criterio no se ha cumplido satisfactoriamente Fuente negrita = el criterio no ha sido cumplido
Partes interesadas	
Cliente de la medición	Gerentes responsables del SGSI. Gerencia de seguridad. Gerencia de capacitación
Revisor de la medición	Gerente de seguridad
Propietario de la información	Oficial de la seguridad de la información y el Gerente de capacitación
Recolector de la información	Gerencia de capacitación – Departamento de recursos humanos
Comunicador de la información	Gerentes responsables del SGSI
Frecuencia / Período	
Frecuencia de la recolección de datos	Mensualmente, primer día hábil del mes
Frecuencia del análisis de	Trimestral

datos	
Frecuencia del informe del resultado de las mediciones	Trimestral
Revisión de la medición	Revisar anualmente
Período de medición	Anual

B.2 Políticas de contraseñas

B.2.1 Calidad de las contraseñas – manual

Identificación de la estructura de medición	
Nombre de la estructura de medición	Calidad de la contraseña
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Evaluar la calidad de las contraseñas utilizadas por los usuarios para acceder a los sistemas de información de la organización
Objetivos de control/procesos	Prevenir a los usuarios de la utilización de contraseñas inseguras
Control(1)/proceso(1)	A.11.3.1 Se debe solicitar a los usuarios que sigan las buenas prácticas de seguridad en la selección y uso de contraseñas. Implementación. Todos los usuarios deben seleccionar contraseñas robustas para todos los sistemas, las cuales deben: 1) tener un tamaño mayor que 8; 2) no basarse en nada en lo cual otra persona pueda adivinar fácilmente u obtener utilizando información relacionada a la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, etc; 3) no consistir en palabras que existan en los diccionarios; 4) no tener caracteres consecutivos idénticos, sean de solo caracteres numéricos o de sólo caracteres alfabéticos. Todas las cuentas de usuario y contraseñas para los sistemas de información de la organización deben ser controladas por el sistema de empleados.
Objeto de medición y atributos	
Objeto de medición	La base de datos de contraseñas
Atributo	Contraseñas individuales
Especificación de la medida base	
Medida base	1 – Número de contraseñas registradas

	2 – Número de contraseñas que satisfacen la política organizacional de calidad de contraseñas para cada usuario
Método de medición	1 – Contar el número de contraseñas en la base de datos de contraseñas de los usuarios 2 – Preguntar a cada usuario sobre el número de contraseñas que satisfacen la política de contraseñas de la organización
Tipo de método de medición	1 - Objetivo 2 - Subjetivo
Escala	1 - Enteros, desde cero hasta infinito 2 - Enteros, desde cero hasta infinito
Tipo de escala	1 – Ordinal 2 - Ordinal
Unidad de medición	1 - Contraseñas 2 - Contraseñas
Especificación de medida derivada	
Medida derivada	Número total de contraseñas que cumplen con la política de calidad de contraseñas de la organización
Función de medición	Sumatoria del Número total de contraseñas que cumplen con la política de calidad de contraseñas de la organización por cada usuario
Especificación del indicador	
Indicador	a) Proporción de contraseñas que cumplen con la política de calidad de contraseñas de la organización. b) Tendencias de estado de cumplimiento con respecto a la política de calidad de contraseñas
Modelo analítico	a) Dividir [Número total de contraseñas que cumplen con la política de calidad de contraseñas de la organización] por [Número de contraseñas registradas] b) Comparar la proporción con la proporción previa.
Especificación de los criterios de decisión	
Criterios de decisión	El objetivo de control se alcanza y no se requiere ninguna acción si la proporción resultante es sobre 0,9. Si la proporción resultante es entre 0,8 y 0,9 el objetivo de control no se ha cumplido, pero una tendencia positiva indica mejora. Si la proporción resultante es menor que 0,8 se recomienda que se tomen acciones inmediatas
Resultados de la medición	
Interpretación del indicador	Se recomienda que la interpretación del indicador a) con respecto al cumplimiento del criterio de la organización para la política de contraseñas sea la siguiente: – se cumplió satisfactoriamente si la proporción es mayor que 0,9;

Interpretación del indicador	– no se cumplió satisfactoriamente si la proporción es [0,8 ≤ proporción ≤ 0,9]; – no se cumplió si la proporción es menor que 0,8. Se recomienda que la interpretación del indicador b) sea la siguiente: – una tendencia alcista indica un cumplimiento mejorado, una tendencia a la baja indica deterioro en el cumplimiento; – el grado del cambio de la tendencia puede proveer una idea de la efectividad de los controles implementados; – una tendencia negativa puede requerir mayores controles tal como concientización, o a través de medios técnicos para forzar a la selección de contraseñas robustas o el cambio periódico de las mismas – se recomienda que se examine una tendencia positiva para estimar términos necesarios para cumplir con la política de contraseñas desde la proporción actual. El efecto / impacto de que no se cumpla con el criterio es un incremento en el riesgo de brechas de confidencialidad. Las causas potenciales de desviación incluyen una falta de concientización en seguridad, deficiencias en la implementación técnica y falta de tiempo para implementarlo en todos los sistemas de información.
Formatos de reporte	Una línea de tendencia que muestre el número de contraseñas que cumplen con la política de calidad de contraseñas de la organización, superpuesta con las líneas de tendencias producidas durante períodos de reportes previos.
Partes interesadas	
Cliente de la medición	Gerentes responsables del SGSI. Gerencia de seguridad.
Revisor de la medición	Gerencia de seguridad
Propietario de la información	Administrador de sistemas
Recolector de la información	Personal de seguridad
Comunicador de la información	Personal de seguridad
Frecuencia / Período	
Frecuencia de la recolección de datos	Anual
Frecuencia del análisis de datos	Anual
Frecuencia del informe del resultado de las mediciones	Anual
Revisión de la medición	Revisado y actualizado todos los años
Período de medición	Anual

B.2.2 Calidad de las Contraseñas – automático

Identificación de la estructura de medición	
Nombre de la estructura de medición	Calidad de la contraseña
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Evaluar la calidad de las contraseñas utilizadas por los usuarios para acceder a los sistemas de información de la organización
Objetivos de control/procesos	Prevenir a los usuarios de utilizar contraseñas inseguras
Control(1)/proceso(1)	A.11.3.1 Se debe solicitar a los usuarios que sigan las buenas prácticas de seguridad en la selección y uso de contraseñas. Implementación: Todos los usuarios deben seleccionar contraseñas robustas para todos los sistemas, las cuales deben: 1) tener un tamaño mayor que 8; 2) no basarse en nada en lo cual otra persona pueda adivinar fácilmente u obtener utilizando información relacionada a la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, etc; 3) no consistir en palabras que existan en los diccionarios; 4) no tener caracteres consecutivos idénticos, sean de solo caracteres numéricos o de sólo caracteres alfabéticos. Todas las cuentas de usuario y contraseñas para los sistemas de información de la organización deben ser controladas por el sistema de gestión de empleados. La fortaleza de la contraseña debe ser examinada utilizando un sistema para craquear contraseñas.
Objeto de medición y atributos	
Objeto de medición	La base de datos de cuentas del sistema de gestión de empleados
Atributo	Contraseñas individuales almacenadas en los registros de las cuentas del sistema de empleados
Especificación de la medida base	
Medida base	1 – Número total de contraseñas 2 – Número total de contraseñas que no se han podido craquear

Método de medición	1 – Generar una consulta sobre los registros de las cuentas de empleados 2 – Ejecutar el sistema para craquear contraseñas en los registros de cuentas del sistema de empleados utilizando un ataque híbrido
Tipo de método de medición	1 - Objetivo 2 – Objetivo
Escala	1 - enteros, desde cero hasta infinito 2 - enteros, desde cero hasta infinito
Tipo de escala	1 - Ordinal 2 - Ordinal
Unidad de medición	1 - Contraseñas 2 - Contraseñas
Especificación de medida derivada	
Medida derivada	Ninguna
Función de medición	Ninguna
Especificación del indicador	
Indicador	1 - Proporción de contraseñas descifrables en menos de 4 horas 2 - Tendencia de proporción 1
Modelo analítico	a) Dividir [Número total de contraseñas no craqueadas] por [Número total de contraseñas] b) Comparar la proporción con la proporción previa.
Especificación de los criterios de decisión	
Criterios de decisión	El objetivo de control se alcanza y no se requiere ninguna acción si la proporción resultante es sobre 0,9. Si la proporción resultante es entre 0,8 y 0,9 el objetivo de control no se ha cumplido, pero una tendencia positiva indica mejora. Si la proporción resultante es por debajo de 0,8 se recomienda que se tomen acciones inmediatas
Resultados de la medición	
Interpretación del indicador	Se recomienda que la interpretación del indicador 1 con respecto al cumplimiento del criterio de la organización para la política de contraseñas sea la siguiente: – se cumplió satisfactoriamente si la proporción es mayor que 0,9; – no se cumplió satisfactoriamente si la proporción es [0,8 ≤ proporción ≤ 0,9]; – no se cumplió si la proporción es menor que 0,8; – una tendencia alcista indica un cumplimiento mejorado, una tendencia a la baja indica deterioro en el cumplimiento;

Interpretación del indicador	– el grado del cambio de la tendencia puede proveer una idea de la efectividad de los controles implementados; – una tendencia negativa puede requerir mayores controles tal como concientización, o a través de medios técnicos para forzar a la selección de contraseñas robustas o el cambio periódico de las mismas; – se recomienda que se examine una tendencia positiva para estimar términos necesarios para cumplir con la política de contraseñas desde la proporción actual. El efecto / impacto de que no se cumpla con el criterio es un incremento en el riesgo de contraseñas comprometidas que puede derivar en acceso no autorizado a sistemas. Las causas potenciales de desviación incluyen una falta de concientización en seguridad, deficiencias en la implementación técnica y falta de tiempo para implementarlo en todos los sistemas de información.
Formatos de reporte	Una línea de tendencia que muestre la vulnerabilidad de las contraseñas para todos los registros probados superpuestos con líneas producidas en pruebas previas
Partes interesadas	
Cliente de la medición	Gerentes responsables del SGSI. Gerencia de seguridad.
Revisor de la medición	Gerencia de seguridad
Propietario de la información	Administrador de sistemas
Recolector de la información	Personal de seguridad
Comunicador de la información	Personal de seguridad
Frecuencia / período	
Frecuencia de la recolección de datos	Semanal
Frecuencia del análisis de datos	Semanal
Frecuencia del reporte del resultado de las mediciones	Semanal
Revisión de la medición	Revisado y actualizado todos los años
Período de medición	Aplicable por 3 años

B.3 Proceso de revisión del SGSI

Identificación de la estructura de medición	
Nombre de la estructura de medición	Proceso de revisión del SGSI
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Evaluar el grado de cumplimiento de la revisión independiente de la seguridad de la información
Objetivos de control/procesos	Gestionar la seguridad de la información dentro de la organización
Control(1)/proceso(1)	A.6.1.8 El enfoque de la organización para la gestión de la seguridad de la información y su implementación (por ejemplo: objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado en forma independiente a intervalos planificados o cuando ocurran cambios significativos en la implementación de la seguridad. Implementación: El enfoque de la organización para gestionar la seguridad de la información y su implementación es revisada por un consultor de seguridad externo cada 3 meses.
Objeto de medición y atributos	
Objeto de medición	1 – Reportes de las revisiones de tercera parte 2 – Planes de revisiones de tercera parte
Atributo	1 – Revisiones de tercera parte reportadas 2 – Revisiones de tercera parte planificadas
Especificación de la medida base	
Medida base	1 – Número de revisiones conducidas por tercera parte 2 – Número total de revisiones de tercera parte planificadas
Método de medición	1 – Contar el número de reportes de revisiones regulares conducidas por tercera parte 2 – Contar el número total de revisiones de tercera parte planificadas
Tipo de método de medición	1 - Objetivo 2 - Objetivo
Escala	1 - enteros, desde cero hasta infinito 2 - enteros, desde cero hasta infinito
Tipo de escala	1 - Ordinal 2 - Ordinal

Unidad de medición	1 - Revisión 2 – Revisión
Especificación de medida derivada	
Medida derivada	Ninguna
Función de medición	Ninguna
Especificación del indicador	
Indicador	Proporción de progreso de revisiones independientes alcanzadas
Modelo analítico	Dividir [Número de revisiones conducidas por tercera parte] por [Número total de revisiones de tercera parte planificadas]
Especificación de los criterios de decisión	
Criterios de decisión	Se recomienda que la proporción resultante del indicador se encuentre primariamente entre 0,8 y 1,1 para concluir el cumplimiento de los objetivos de control y no tomar ninguna acción. Se recomienda que entre 0,6 y 0,8 se realice un seguimiento. Si la proporción resultante está por debajo de 0,6 se recomienda que se tomen acciones inmediatas.
Resultados de la medición	
Interpretación del indicador	Se recomienda que la interpretación del indicador sea la siguiente: El criterio organizacional para gestionar la seguridad de la información dentro de la organización a través de revisiones externas se ha cumplido satisfactoriamente en 0,8 ≤ proporción ≤ 1,1. El criterio organizacional no se ha cumplido de manera satisfactoria en [0,6 ≤ proporción ≤ 0,8 o en proporción > 1,1]. Se requiere seguimiento y control para asegurar que se ha realizado un progreso apropiado. Si al finalizar el segundo trimestre el indicador a) no es satisfactorio, se necesita una acción correctiva y se recomienda que se lo comunique a la alta dirección responsable por el SGSI. Si al finalizar el año el indicador a) no es satisfactorio, se debe informar a la alta dirección y es le debe solicitar su apoyo. El efecto/impacto de que no se cumpla con el criterio es un proceso de revisión por la dirección inefectivo. Las causas potenciales de desviación incluyen un bajo presupuesto, planificación incorrecta y falta de personal crítico o compromiso de la alta dirección
Formatos de reporte	Gráfico de barras representando cumplimiento en base a varios reportes de períodos, en relación a los umbrales definidos por el criterio de decisión.

Partes interesadas	
Cliente de la medición	Gerentes responsables del SGSI. Gerente del sistema de calidad.
Revisor de la medición	Gerentes responsables del SGSI
Propietario de la información	Gerentes responsables del SGSI
Recolector de la información	Auditoría interna. Gerente de calidad
Comunicador de la información	Auditoría interna. Gerente de calidad responsable por un SGSI
Frecuencia / Período	
Frecuencia de la recolección de datos	Cada 3 meses
Frecuencia del análisis de datos	Cada 3 meses
Frecuencia del reporte del resultado de las mediciones	Cada 3 meses
Revisión de la medición	Revisar y actualizar cada 2 años
Período de medición	Aplicable por 2 años

B.4 Mejora continua del SGSI

B.4.1 Efectividad de la gestión de incidentes de la seguridad de la información

Identificación de la estructura de medición	
Nombre de la estructura de medición	Efectividad de la gestión de incidentes de la seguridad de la información
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Evaluar la efectividad de la gestión de incidentes de la seguridad de la información
Objetivos de control/procesos	Permitir la detección temprana de eventos de seguridad y responder a incidentes de seguridad
Control(1)/proceso(1)	Capítulo 4.2.2 h) [27001:2007]
Objeto de medición y atributos	
Objeto de medición	SGSI
Atributo	Incidente individual
Especificación de la medida base	
Medida base	Número de umbral predeterminado
Método de medición	Contar las ocurrencias de incidentes de seguridad de la información informados a la fecha
Tipo de método de medición	Objetivo
Escala	Numérico

Tipo de escala	Ordinal
Unidad de medición	Incidente
Especificación de medida derivada	
Medida derivada	Incidentes que exceden el umbral
Función de medición	Comparación del número incidentes totales con el umbral
Especificación del indicador	
Indicador	Gráfico lineal que representa la línea horizontal constante ilustrando el número umbral contra el número total de incidentes durante varios períodos de reporte.
Modelo analítico	Rojo cuando el número total de incidentes excede el umbral (va por sobre la línea); amarillo cuando el número total de incidentes se encuentra dentro del 10% del umbral; verde cuando el número total de incidentes se encuentra por debajo del umbral en un 10% o más.
Especificación de los criterios de decisión	
Criterios de decisión	Rojo – se requiere investigación inmediata de las causas del aumento en el número de incidentes. Amarillo – los números necesitan ser seguidos y controlados de cerca y se recomienda que se inicie una investigación si los números no mejoran. Verde – no se requiere ninguna acción
Resultados de la medición	
Interpretación del indicador	Si se observa rojo en dos ciclos de reporte, se requiere una revisión de los procedimientos de gestión para corregir procedimientos existentes o para identificar procedimientos adicionales. Si la tendencia no se revierte durante los próximos dos períodos de informe, se requiere una acción correctiva, como proponer una extensión al alcance del SGSI
Formatos de reporte	Gráfico de líneas
Partes interesadas	
Cliente de la medición	Comité de gestión del SGSI Gerentes responsables del SGSI Gestión de seguridad Gestión de incidentes
Revisor de la medición	Gerentes responsables del SGSI
Propietario de la información	Gerentes responsables del SGSI
Recolector de la información	Gerente de la gestión de incidentes
Comunicador de la información	Comité de gestión del SGSI

Frecuencia / Período	
Frecuencia de la recolección de datos	Mensual
Frecuencia del análisis de datos	Mensual
Frecuencia del reporte del resultado de las mediciones	Mensual
Revisión de la medición	Semestral
Período de medición	Mensual

B.4.2 Implementación de Acción Correctiva

Identificación de la estructura de medición	
Nombre de la estructura de Medición	Implementación de acción correctiva
Identificador numérico	Identificador específico de la organización
Propósito de la estructura de medición	Evaluar el desempeño de la implementación de la acción correctiva
Objetivos de control/procesos	Capítulo 8.2 [27001:2007] acción correctiva La organización debe emprender acciones para eliminar la causa de no conformidades asociadas con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente.
Control(1)/proceso(1)	El procedimiento documentado de acciones correctivas debe definir los requerimientos para: a) identificar no-conformidades; b) determinar las causas de no-conformidades; c) evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir; d) determinar e implementar la acción correctiva necesaria; e) registrar los resultados de las acciones tomadas (ver 4.3.3); y f) revisar las acciones correctivas tomadas. Implementación: ……. La organización determina las acciones correctivas requeridas, y genera el informe de acción correctiva documentando: la información concerniente a las no-conformidades, su causa, y la fecha de vencimiento para que se realicen las acciones correctivas. Luego de recibir el informe, se requiere que el gerente responsable por el área donde se ha detectado la no-conformidad asegure que las acciones se realicen sin

Control(1)/proceso(1)	demasiada demora, para eliminar las no-conformidades detectadas y sus causas. Si la acción correctiva no se ha implementado como se requiere, se debe identificar la causa de la no-implementación, así como las alternativas a la acción correctiva original que será determinada como apropiada. Se recomienda que se documenten las acciones tomadas junto a las fechas correspondientes y los resultados. Si la acción correctiva no esta implementada según lo planeado, se debe documentar la razón y la acción alternativa. Se recomienda que se provea del informe al Gerente de seguridad de la información.
Objeto de medición y atributos	
Objeto de medición	Informes de acciones correctivas
Atributo	Fecha de vencimiento de la acción correctiva en el informe Fecha de las acciones correctivas tomadas en el registro del informe Razón por demorar y no tomar la acción
Especificación de la medida base	
Medida base	1. Cantidad de acciones correctivas planeadas a la fecha 2. Cantidad de acciones correctivas implementadas tal como se planificaron a la fecha 3. Cantidad de acciones correctivas no implementadas a la fecha, con la causa
Método de medición	1. Contar las acciones correctivas planeadas a ser implementadas hasta la fecha 2. Contar las acciones correctivas registradas como implementadas a la fecha de vencimiento 3. Contar las acciones correctivas registradas como acciones planificadas no tomadas, con la causa
Tipo de método de medición	1 – 3 Objetivo
Escala	1 – 3 Enteros desde cero hasta infinito
Tipo de escala	1 – 3 Ordinal
Unidad de medición	1 – 3 Acción correctiva
Especificación de medida derivada	
Medida derivada	a) Acción correctiva no implementada a la fecha b) Acción correctiva no implementada sin una acción legítima
Función de medición	a) Restar [acciones correctivas tomadas según lo planificado a la fecha] de [acciones correctivas planificadas a la fecha] b) Restar [acciones correctivas no implementadas a la

	fecha] de [acciones correctivas no tomadas según lo planeado, con causa, a la fecha]
Especificación del Indicador	
Indicador	a) Estatus expresado como una proporción, de acción correctiva no implementada b) Estatus expresado como una proporción, de acción correctiva no implementada sin razón c) Tendencia de los estatus
Modelo analítico	a) Dividir [acción correctiva no implementada a la fecha] por [acciones correctivas planificadas a la fecha] b) Dividir [acción correctiva no implementada sin razón] por [acciones correctivas planificadas a la fecha] c) Comparar estados con estados previos
Especificación de los criterios de decisión	
Criterios de decisión	De manera de concluir el cumplimiento de los objetivos y de no tomar ninguna acción, se recomienda que las proporciones del indicador a) y b) caigan respectivamente entre 0,4 y 0,0 y entre 0,2 y 0,0, y la tendencia del indicador c) se encuentre decayendo durante los últimos 2 períodos de informe. Se recomienda que el indicador c) se presente en comparación con indicadores previos de manera que se pueda examinar la tendencia de las acciones correctivas implementadas.
Resultados de la medición	
Interpretación del indicador	Se recomienda que la interpretación del indicador a) y b) sea la siguiente: Se deben implementar las acciones correctivas planificadas salvo que las prioridades de la organización hayan cambiado, dando como resultado la necesidad de implementar acciones correctivas diferentes o la redirección de recursos asignados a la implementación de dichas acciones. Si las acciones correctivas no implementadas son mayores que el 40%, independientemente de la razón, se requiere acción de la alta dirección. Si las acciones correctivas no implementadas son mayores que el 20%, sin una buena razón, se requiere acción de la alta dirección. Se recomienda que las acciones correctivas que no se implementaron se examinen para identificar las razones de su no-implementación. Dependiendo del porcentaje general de las acciones correctivas no implementadas y las razones de la no-implementación, pueden requerir más acciones Se recomienda que la interpretación del indicador c) sea la siguiente: Que se examine una tendencia en la implementación de acciones correctivas por cualquier deterioro general en el

Interpretación del indicador	rendimiento o por cualquier mejora significativa en el mismo. Si el porcentaje de las acciones correctivas implementadas ha ido decayendo sostenidamente durante los últimos 2 períodos de informe, se requiere una acción de la alta dirección sin importar el detalle de las razones de la no-conformidad. El efecto/impacto de que los criterios no sean alcanzados es una falta potencial de la mejora continua del SGSI. Las causas potenciales pueden incluir falta de recursos, planificación incorrecta, y falta de personal crítico, así como también falta en el compromiso de la alta dirección.
Formatos de reporte	Gráfico de barras con la definición de resultados medidos, incluyendo un resumen ejecutivo de los hallazgos y las posibles acciones de la alta dirección, que represente el número total de acciones correctivas, separados en implementados, no implementados sin una razón legítima, y no implementados con una razón legítima.
Partes interesadas	
Cliente de la medición	Gerentes responsables por el SGSI. Gerente de la seguridad de la información
Revisor de la medición	Gerentes responsables por el SGSI
Propietario de la información	Gerentes responsables por el SGSI
Recolector de la información	Gerentes responsables por el SGSI
Comunicador de la información	Gerentes responsables por el SGSI
Frecuencia / Período	
Frecuencia de la recolección de datos	Trimestral
Frecuencia del análisis de datos	Trimestral
Frecuencia del reporte del Resultado de las mediciones	Trimestral
Revisión de la medición	Revisado anualmente
Período de medición	Aplicable por 1 año

B.5 Compromiso de la alta dirección

Identificación de la estructura de medición	
Nombre de la estructura de medición	Frecuencia de la revisión de la alta dirección
Identificador numérico	Específico de la organización

Propósito de la estructura de medición	Evaluar el compromiso de la alta dirección y de las actividades de revisión de la seguridad de la información concernientes a las actividades de revisión de la alta dirección
Objetivos de control/procesos	A.6.1 Gestionar la seguridad de la información dentro de la organización (planificada). Para gestionar la seguridad de la información dentro de la organización a través de la realización regular de revisiones de la alta dirección
Control(1)/proceso(1)	A.6.1.1 La dirección debe dar soporte activo a la seguridad dentro de la organización a través de una directiva clara, compromiso demostrado, asignación explícita, y conocimientos de responsabilidades de seguridad de la información (implementado). La organización debe tener reuniones de revisión mensuales de la alta dirección para dar soporte a la seguridad dentro de la organización a través de una clara dirección, demostrado compromiso, asignaciones explícitas, y aprobación de la seguridad de la información. Se recomienda que la revisión por la alta dirección del SGSI se combine con la revisión por la alta dirección del SGC (Sistema de gestión de calidad).
Control(2)/proceso(2)	A.6.1.2 Coordinación de la seguridad de la información Las actividades de seguridad de la información deben estar coordinadas por representantes de diferentes partes de la organización con los roles y funciones de trabajo correspondientes. (implementado). Se recomienda que representantes de diferentes departamentos que tengan roles y responsabilidades relevantes, coordinen y participen de la revisión por la alta dirección
Objeto de medición y atributos	
Objeto de medición	1. Plan/programa de la revisión por la alta dirección sobre la seguridad de la información 2. Registros de minutas de la revisión por la alta dirección
Atributo	1.1 Las fechas de reuniones de la revisión por la alta dirección programadas en el plan 1.2 Los gerentes convocados a las reuniones de revisión por la alta dirección 2.1 Las fechas registradas en las minutas de las reuniones de revisión por la alta dirección

	2.2 Los gerentes registrados que hayan asistido a las reuniones de revisión por la alta dirección
Especificación de la medida base	
Medida base	1.1 Cantidad de reuniones de revisión por la alta dirección planificadas a la fecha 1.2 Cantidad de gerentes convocados a las reuniones de revisión de por alta dirección 2.1.1 Cantidad de reuniones de revisión por la alta dirección planificadas, que se hayan llevado a cabo a la fecha 2.1.2 Cantidad de reuniones de revisión por la alta dirección no planificadas, que se hayan llevado a cabo a la fecha 2.1.3 Cantidad de reuniones de revisión por la alta dirección reprogramadas, llevadas a cabo a la fecha 2.2 Cantidad de gerentes que hayan asistido a las reuniones de revisión por la alta dirección a la fecha
Método de medición	1.1 Contar las reuniones de revisión por la alta dirección programadas a la fecha 1.2 Para las reuniones de revisión por la alta dirección a la fecha, contar los gerentes convocados y agregar una nueva entrada con un valor por defecto para reuniones no planificadas realizadas de una manera ad hoc 2.1.1 Contar las reuniones de revisión por la alta dirección planificadas, llevadas a cabo a la fecha. 2.1.2 Contar las reuniones de revisión por la alta dirección no planificadas, llevadas a cabo a la fecha 2.1.3 Contar las reuniones de revisión por la alta dirección reprogramadas, llevadas a cabo a la fecha 2.2 Para todas las reuniones de revisión por la alta dirección llevadas a cabo, contar el número de gerentes que han asistido.
Tipo de método de medición	1.1 Objetivo 1.2 Objetivo o subjetivo 2.1.1 Objetivo 2.1.2 Objetivo 2.1.3 Objetivo 2.2 Objetivo
Escala	1.1 enteros, desde cero hasta infinito 1.2 enteros, desde cero hasta infinito 2.1.1 enteros, desde cero hasta infinito 2.1.2 enteros, desde cero hasta infinito

	2.1.3 enteros, desde cero hasta infinito 2.2 enteros, desde cero hasta infinito
Tipo de escala	1.1 Ordinal 1.2 Ordinal 2.1.1 Ordinal 2.1.2 Ordinal 2.1.3 Ordinal 2.2 Ordinal
Unidad de medición	1.1 Reunión 1.2 Personal 2.1.1 Reunión 2.1.2 Reunión 2.1.3 Reunión 2.2 Personal
Especificación de medida derivada	
Medida derivada	a) Cantidad de reuniones de revisión por la alta dirección llevadas a cabo hasta la fecha b) Índices de participación en las reuniones de revisión por la alta dirección llevadas a cabo hasta la fecha
Función de medición	a) Sumar [cantidad de reuniones de revisión por la alta dirección planificadas a la fecha] más [cantidad de reuniones de revisión por la alta dirección no planificadas a la fecha] más [cantidad de reuniones de revisión de la alta dirección reprogramadas a la fecha] b) Por cada reunión de revisión por la alta dirección dividir [cantidad de gerentes que asistieron a la reunión] por [cantidad de gerentes convocados a la reunión]
Especificación del indicador	
Indicador	a) Reuniones de revisión por la alta dirección llevadas a cabo a la fecha b) Promedio de índices de participación en las reuniones de revisión por la alta dirección a la fecha
Modelo analítico	a) Dividir [reuniones de revisión por la alta dirección llevadas a cabo] por [reuniones de revisión por la alta dirección programadas] b) Calcular desviación media y estándar de todos los índices de participación a las reuniones de revisión por la alta dirección
Especificación de los criterios de decisión	
Criterios de decisión	Se recomienda que la proporción resultante del indicador a) se encuentre entre 0,7 y 1,1 para establecer que se ha

Criterios de decisión	cumplido con el objetivo de control y que no se requiere ninguna acción. Aunque falle, se recomienda que igualmente sea mayor que 0,5 para establecer que se ha cumplido con lo mínimo establecido por el control. Con respecto al indicador b), los intervalos de confianza calculados basados en la desviación estándar indican la probabilidad de que se alcance un resultado cercano a los índices de participación promedio. Intervalos de confianza muy amplios indican una potencial dispersión y la necesidad de una planificación de contingencia para hacer frente a este resultado.
Resultados de la medición	
Interpretación del indicador	Se recomienda que la interpretación del indicador a) sea la siguiente: Los criterios de la organización para gestionar la seguridad de la información dentro de la revisión de todos los niveles de gestión, se ha cumplido satisfactoriamente si la proporción se encuentra entre 0,7 y 1,1; Los criterios de la organización no se han cumplido satisfactoriamente si la proporción se encuentra entre [0,5 ≤ proporción < 0,7 o la proporción >1,1]. Este resultado puede indicar una posible falta de compromiso de la alta dirección y puede requerir una acción correctiva. Se recomienda que se sigan y controlen los resultados de medición subsecuentes y que se los evalúe para mejorarlos. Los criterios de la organización no se han cumplido si la proporción se encuentra en [0 ≤ proporción < 0,5]. Este resultado indica falta de compromiso de la alta dirección y requiere intervención inmediata para implementar una acción correctiva apropiada. Se recomienda que se informe a la alta dirección de éste resultado. Una proporción cercana a 0 puede indicar falta de compromiso de la alta dirección. Si los gerentes del SGSI no entienden a la revisión de la gerencia del SGSI como una prioridad, entonces ellos pueden ser influenciados por los máximos responsables de la organización. El efecto/impacto de que no se cumpla con los criterios es la potencial falta de un proceso de revisión por la alta dirección, continuo y efectivo. Las causas potenciales de la desviación en el indicador b) pueden incluir planificación incorrecta, compromiso insuficiente de los gerentes responsables del SGSI, prioridades en conflicto y/o un trabajo excesivo que afec-

	te a los gerentes del SGSI.
Formatos de reporte	Gráfico de líneas representando el indicador con los criterios en varios períodos de recolección de datos y de reporte con la declaración de los resultados de las mediciones. Se recomienda que la organización defina la cantidad de datos recolectados y los períodos de reporte.
Partes interesadas	
Cliente de la medición	Gerentes responsables por el SGSI. Gerente del sistema de calidad
Revisor de la medición	Autoridad del programa de auditoria del SGSI interno
Propietario de la información	Gerente del sistema de calidad Asumiendo sistemas de gestión combinados de sistema de gestión de calidad y del SGSI
Recolector de la información	Gerente de calidad. Gerente de seguridad de la información
Comunicador de la información	Gerente de seguridad de la información. Gerente de calidad
Frecuencia / Período	
Frecuencia de la recolección de datos	Mensual
Frecuencia del análisis de datos	Trimestral
Frecuencia del reporte del resultado de las mediciones	Trimestral
Revisión de la medición	Revisada y actualizada cada 2 años
Período de medición	Aplicable por 2 años

B.6 Protección contra código malicioso

Identificación de la estructura de medición	
Nombre de la estructura de medición	Protección contra software malicioso
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Para evaluar la efectividad del sistema de protección contra ataques de software maliciosos
Objetivos de control/procesos	Objetivo de control A.10.4 [27001:2007] Proteger la integridad del software y la información. (Planificado) Proteger la integridad del software y de la información de software malicioso
Control(1)/proceso(1)	Control A.10.4.1 [27001:2007] Controles contra código malicioso

	Se deben implementar los controles de detección y prevención para la protección contra software malicioso, y procedimientos adecuados de concientización de los usuarios
Objeto de medición y atributos	
Objeto de medición	1 Reportes de incidentes 2 Registro de contramedidas de software contra el software malicioso
Atributo	Incidentes causados por software malicioso
Especificación de la medida base	
Medida base	1. Cantidad de incidentes de seguridad causados por software malicioso 2. Total de ataques bloqueados originados por software malicioso
Método de medición	1. Contar el número de incidentes de seguridad causados por software malicioso en los reportes de incidentes 2. Contar el número de registros de ataques bloqueados
Tipo de método de medición	1. Objetivo 2. Objetivo
Escala	1. enteros, desde cero hasta infinito 2. enteros, desde cero hasta infinito
Tipo de escala	1. Ordinal 2. Ordinal
Unidad de medición	1. Incidentes de seguridad 2. Registros
Especificación de medida derivada	
Medida derivada	Capacidad de protección contra el software malicioso
Función de medición	Cantidad de incidentes de seguridad causados por software malicioso / cantidad de ataques detectados y bloqueados originados por software malicioso.
Especificación del Indicador	
Indicador	Tendencia de ataques detectados que no fueron bloqueados en múltiples períodos de reporte
Modelo analítico	Comparar la proporción con porcentajes previos
Especificación de los criterios de decisión	
Criterios de decisión	Se recomienda que las líneas de tendencia se mantengan por debajo del número especificado. Se recomienda que la tendencia resultante se mantenga a la baja o constante.

Resultados de la medición	
Interpretación del indicador	Una tendencia alcista indica que el cumplimiento se deteriora, una tendencia a la baja indica una mejora en el cumplimiento; y Cuando la tendencia se eleva demasiado, se recomienda que se realice una investigación de la causa y se haga lugar a una contramedida.
Formatos de reporte	Una línea de tendencia que represente una proporción de detección y prevención de software malicioso con las líneas producidas durante períodos de reporte previos.
Partes interesadas	
Cliente de la medición	Gerencia de seguridad
Revisor de la medición	Gerencia de seguridad
Propietario de la información	Administrador del sistema
Recolector de la información	Gerencia de seguridad, administrador del sistema, administrador de la red
Comunicador de la información	Coordinador del servicio
Frecuencia / Período	
Frecuencia de la recolección de datos	Diario
Frecuencia del análisis de datos	Mensual
Frecuencia del reporte del resultado de las mediciones	Mensual
Revisión de la medición	Revisado anualmente
Período de medición	Aplicable por 1 año

B.7 Controles de acceso físico

Identificación de la estructura de medición	
Nombre de la estructura de medición	Control de acceso físico con tarjetas de acceso
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Para mostrar la existencia, alcance y calidad del sistema utilizado para el control de acceso.
Objetivos de control/procesos	Objetivo de control A.9.1 [27001:2007] Impedir accesos físicos no autorizados, daños e interferencia a las instalaciones e información de la organización

Control(1)/proceso(1)	Control A.9.1.2 [27001:2007] Controles de acceso físico. Las áreas seguras deben ser resguardadas por controles de acceso adecuados que garanticen que sólo se permite el acceso a personal autorizado.
Objeto de medición y atributos	
Objeto de medición	Áreas seguras
Atributo	Registros de la gestión de identidad
Especificación de la medida base	
Medida base	Control de ingreso físico con tarjetas de acceso
Método de medición	Método de medición relativo donde cada subconjunto de categorías es parte de una categoría superior. Control del tipo de sistema de control de ingreso e inspección de los siguientes aspectos: – la existencia de un sistema de tarjetas de control de acceso; – utilización de un código de identificación personal; – funcionalidad de registro de actividades; – autenticación biométrica.
Tipo de método de medición	Subjetivo
Escala	0-5 **0 No existe un sistema de control de acceso** **1** Existe un sistema de acceso donde se utiliza un código de identificación personal (sistema de un factor) para el control de acceso **2** Existe un sistema de tarjetas de control de acceso donde la tarjeta de contraseña (sistema de un factor) se usa para el control de acceso. **3** Existe un sistema de control de ingreso por tarjetas donde se utiliza la tarjeta de contraseña y un código de identificación personal para el control de acceso. **4** Lo anterior + un registro funcional activado **5** Lo anterior + el código de identificación personal reemplazado por autenticación biométrica (huellas digitales, reconocimiento de voz, escáner de retina, etc)
Tipo de escala	Ordinal
Unidad de medición	No está disponible
Especificación de medida derivada	
Medida derivada	Ninguna
Función de medición	Ninguna

Especificación del indicador	
Indicador	Barras de progreso. Rojo hasta 0,8, Verde entre 0,8 y 1
Modelo analítico	Análisis de medidas
Especificación de los criterios de decisión	
Criterios de decisión	Valor 3 = satisfactorio
Resultados de la medición	
Interpretación del indicador	Por debajo de 3 no satisfactorio, donde (3 – grado actual = gap de seguridad), es el esfuerzo de la acción a ser realizada basado en el alcance del gap de seguridad. Por arriba de 3 es satisfactorio con excelencia, donde el grado puede indicar una sobre inversión con respecto al tema bajo medición
Formatos de reporte	Gráficos
Partes interesadas	
Cliente de la medición	Comité de la alta dirección
Revisor de la medición	Auditor interno / auditor externo
Propietario de la información	Administrador del control de acceso físico
Recolector de la información	Auditor interno / auditor externo
Comunicador de la información	Auditoría interna y gerencia de seguridad
Frecuencia / Período	
Frecuencia de la recolección de datos	Anual
Frecuencia del análisis de datos	Anual
Frecuencia del reporte del resultado de las mediciones	Anual
Revisión de la medición	12 meses
Período de medición	Aplicable por 12 meses

B.8 Revisión de los archivos de registro de actividades

Identificación de la estructura de medición	
Nombre de la estructura de medición	Revisión de los archivos de registro de actividades
Identificador numérico	Identificador numérico único específico de la organización

Propósito de la estructura de medición	Evaluar el estado de cumplimiento de la revisión regular de los archivos críticos de registro de actividades del sistema
Objetivos de control	Objetivo de control A.10.10 [27001:2007] Detectar las actividades no autorizadas de procesamiento de información. (planificado) Para detectar actividades de procesamiento de la información no autorizadas de los sistemas críticos a partir del registro de actividades del sistema
Control(1)	Control A.10.10.2 [27001:2007] Se deben establecer procedimientos para el uso de las instalaciones de procesamiento de la información y se deben revisar de forma regular los resultados de las actividades de seguimiento.
Objeto de medición y atributos	
Objeto de medición	Sistema
Atributo	Archivos individuales de registro de actividades
Especificación de la medida base	
Medida base	Cantidad de archivos de registro de actividades
Método de medición	Sumar el número total de archivos de registro de actividades listados en la lista de revisión del registro de actividades
Tipo de método de medición	Objetivo
Escala	Enteros, desde cero a infinito
Tipo de escala	Ordinal
Unidad de medición	Archivo de registro de actividades
Especificación de la medida base (2)	
Medida base	Cantidad de archivos de registro de actividades revisados
Método de medición	Sumar la cantidad total de archivos de registro de actividades en todos los sistemas dentro del alcance del SGSI
Tipo de método de medición	Objetivo
Escala	Numérica
Tipo de escala	Proporción
Unidad de medición	Archivo de registro de actividades
Especificación de la medida base (3)	
Medida base	Cantidad de sistemas dentro del alcance del SGSI
Método de medición	Identificar la cantidad de archivos de registro de actividades revisados
Tipo de método de medición	Objetivo
Escala	Numérica

Tipo de escala	Proporción
Unidad de medición	Archivo de registro de actividades
Especificación de medida derivada	
Medida derivada	Porcentaje de archivos de registro de actividades derivados a auditoría de acuerdo al período de tiempo establecido
Función de medición	(cantidad de archivos de registro revisados dentro del período de tiempo especificado) / (cantidad total de archivos de registro de actividades) • 100
Especificación del indicador	
Indicador	Gráfico de línea de una tendencia a través del período de tiempo en la tasa de la revisión del registro de actividades por parte de auditoría
Modelo analítico	Es deseable una tendencia alcista hacia el 100%
Especificación de los criterios de decisión	
Criterios de decisión	Se recomienda que los resultados por debajo del 20% se examinen en búsqueda de las causas por el bajo desempeño.
Resultados de la medición	
Interpretación del indicador	Valores por debajo del valor definido por la organización son insatisfactorios, donde (valor definido por la organización – valor real = gap de seguridad). Se requiere una acción de la alta dirección basada en la extensión del gap de seguridad. Valores por encima del valor definido por la organización pueden indicar sobre inversión salvo que dichos mecanismos de control de acceso sean requeridos por la evaluación de riesgos.
Formatos de reporte	Gráfico de líneas que representa la tendencia con una síntesis de los hallazgos y cualquier acción sugerida por la alta dirección
Partes interesadas	
Cliente de la medición	Gerentes responsables por un SGSI, gerente de seguridad
Revisor de la medición	Gerente de seguridad
Propietario de la información	Gerente de seguridad
Recolector de la información	Personal de seguridad
Comunicador de la información	Personal de seguridad
Frecuencia / Período	
Frecuencia de la recolección de datos	Mensual

Frecuencia del análisis de datos	Mensual
Frecuencia del reporte del resultado de las mediciones	Trimestral
Revisión de la medición	Revisado y actualizado cada 2 años
Período de medición	Aplicable por 2 años

B.9 Gestión del mantenimiento periódico

Identificación de la estructura de medición	
Nombre de la estructura de medición	Gestión del mantenimiento periódico
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Evaluar líneas de tiempo de actividades de mantenimiento en relación con lo programado
Objetivos de control/procesos	Objetivo de control A.9.2 [27001:2007]. Impedir pérdidas, daños, robos o exposiciones al riesgo de los activos así como impedir la interrupción de las actividades de la empresa. (planificado) Para impedir pérdidas, daños, robos o exposiciones al riesgo de los activos así como impedir la interrupción de las actividades de la empresa a través de mantenimiento periódico del sistema
Control(1)	Control A.9.2.4 [27001:2007] El equipo debe recibir el correcto mantenimiento para asegurar su disponibilidad e integridad continuas.
Objeto de medición y atributos	
Objeto de medición	1 Plan / programa de los mantenimientos del sistema 2 Registros de los mantenimientos del sistema
Atributo	1 Fechas del mantenimiento del sistema planificado / programado 2 Fechas del mantenimiento completo del sistema
Especificación de la medida base (1-4)	
Medida base	1 Fechas de mantenimiento programado 2 Fechas de mantenimiento completado 3 Cantidad total de eventos de mantenimiento planificados 4 Cantidad total de eventos de mantenimiento completados

Método de medición	1 Extraer fechas programadas del plan de mantenimiento del sistema 2 Extraer fechas de completado de los registros de mantenimiento del sistema 3 Contar la cantidad de eventos de mantenimiento planificados en el plan de mantenimiento del sistema 4 Contar los registros de mantenimiento
Tipo de método de medición	Objetivo
Escala	1 Tiempo 2 Tiempo 3 Enteros, desde cero hasta infinito 4 Enteros, desde cero hasta infinito
Tipo de escala	1 Lista 2 Lista 3 Ordinal 4 Ordinal
Unidad de medición	1 Intervalo 2 Intervalo 3 Eventos de mantenimiento 4 Eventos de mantenimiento
Especificación de medida derivada	
Medida derivada	Retraso en el mantenimiento por evento de mantenimiento completado
Función de medición	Por cada evento completado, sustraer [Fecha real del mantenimiento] de [Fecha programada para el mantenimiento]
Especificación del indicador	
Indicador	1 Retraso promedio de mantenimiento 2 Proporción de los eventos de mantenimiento completados 3 Tendencia del promedio de retraso en los mantenimientos completados 4 Tendencia de la proporción de eventos de mantenimiento completados
Modelo analítico	1 Dividir (suma de [Retraso del mantenimiento por evento de mantenimiento completado]) por [Cantidad de eventos de mantenimiento completados] 2 Dividir [Cantidad de eventos de mantenimiento completados] por [Cantidad de eventos de mantenimiento planificados] 3 Comparar el indicador 1 sobre múltiples períodos de tiempo

	4 Comparar el indicador 2 sobre múltiples períodos de tiempo
Especificación de los criterios de decisión	
Criterios de decisión	1 Específico de la organización, por ejemplo, si el retraso promedio es consistente y muestra más de 3 días, es necesario que se examinen las causas 2 Se recomienda que las proporciones de eventos de mantenimientos completados sea mayor a 0,9 3 Se recomienda que la tendencia sea estable o cercana a 0 4 Se recomienda que la tendencia sea estable o que vaya en aumento
Resultados de la medición	
Interpretación del indicador	El indicador ayuda a medir la calidad del proceso de mantenimiento del equipamiento
Formatos de reporte	Gráfico de línea que representa la desviación estándar del retraso del mantenimiento, superpuesto con líneas producidas durante períodos de reporte previos y el número de sistemas dentro del alcance Una explicación de los hallazgos y recomendaciones para una acción potencial de la alta dirección
Partes interesadas	
Cliente de la medición	Gerentes responsables por el SGSI, Gerente de seguridad
Revisor de la medición	Gerente de seguridad
Propietario de la información	Administrador del sistema
Recolector de la información	Personal de seguridad
Comunicador de la información	Personal de seguridad
Frecuencia / Período	
Frecuencia de la recolección de datos	Anual
Frecuencia del análisis de datos	Anual
Frecuencia del reporte del resultado de las mediciones	Anual
Revisión de la medición	Anual
Período de medición	Anual

B.10 Seguridad en acuerdos con terceras partes

Identificación de la estructura de medición	
Nombre de la estructura de medición	Seguridad en acuerdos con terceras partes
Identificador numérico	Específico de la organización
Propósito de la estructura de medición	Para evaluar el grado con el cual se trata la seguridad en acuerdos con terceras partes sobre procesamiento de información personal
Objetivos de control/procesos	Objetivo de control A.6.2 [27001:2007] : Mantener la seguridad de la información de la organización y las instalaciones de procesamiento de información que son accedidas, procesadas, comunicadas o gestionadas por terceras partes.
Control(1)/proceso(1)	Control A.6.2.3 [27001:2007] Los acuerdos con terceras partes que involucren el acceso, procesamiento, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de la información, o el agregado de productos o servicios a las instalaciones de procesamiento de información, deben cubrir todos los requerimientos de seguridad importantes.
Objeto de medición y atributos	
Objeto de medición	Acuerdos con terceras partes
Atributo	Cláusulas de seguridad o requerimientos dentro de cada acuerdo con terceras partes
Especificación de la medida base	
Medida base	Cantidad de acuerdos con terceras partes
Método de medición	Revisar los acuerdos con terceras partes, contar la cantidad de acuerdos
Tipo de método de medición	Objetivo
Escala	Enteros, desde cero hasta infinito
Tipo de escala	Ordinal
Unidad de medición	Acuerdo con terceras partes
Especificación de la medida base (2)	
Medida base	Cantidad de requerimientos de seguridad estándares requeridos por los acuerdos con terceras partes
Método de medición	Identificar la cantidad de requerimientos de seguridad por política que tienen que ser tratados en cada acuerdo.
Tipo de método de medición	Objetivo
Escala	Enteros, desde cero hasta infinito
Tipo de escala	Ordinal

Unidad de medición	Requerimiento
Especificación de la medida base (3)	
Medida base	Cantidad de requerimientos de seguridad tratados en cada acuerdo con terceras partes
Método de medición	Revisar los acuerdos con terceras partes, contar la cantidad de requerimientos de seguridad tratados en cada acuerdo
Tipo de método de medición	Objetivo
Escala	Enteros, desde el cero hasta el infinito
Tipo de escala	Ordinal
Unidad de medición	Requerimiento
Especificación de medida derivada	
Medida derivada	Porcentaje promedio de requerimientos de seguridad relevantes tratados en acuerdos con terceras partes
Función de medición	Sumar (por cada acuerdo (cantidad de requerimientos requeridos – cantidad de requerimientos tratados)) / cantidad de acuerdos
Especificación del indicador	
Indicador	1 Proporción promedio de la diferencia de los requerimientos estándar para tratar los requerimientos 2 Tendencia de la proporción
Modelo analítico	1 Sumar (por cada acuerdo ([Total de los requerimientos de seguridad tratados] – [Total de los requerimientos de seguridad estándar])) / [Cantidad de acuerdos con terceras partes 2 Comparar con el indicador 1 del período previo
Especificación de los criterios de decisión	
Criterios de decisión	1 Se recomienda que el indicador 1 sea mayor a 0.9 2 Se recomienda que el indicador 2 sea estable o vaya en aumento
Resultados de la medición	
Interpretación del indicador	Este indicador provee puntos de vista sobre la habilidad de la función de tercerización para tratar los requerimientos de seguridad
Formatos de reporte	Gráfico de líneas que representa la tendencia sobre múltiples períodos de reporte. Un resumen de los hallazgos y las posibles acciones de la alta dirección
Partes interesadas	
Cliente de la medición	Gerentes responsables por un SGSI, Gerente de seguridad
Revisor de la medición	Gerente de seguridad

Propietario de la información	Oficina contratante
Recolector de la información	Personal de seguridad
Comunicador de la información	Personal de seguridad
Frecuencia / Período	
Frecuencia de la recolección de datos	Mensual
Frecuencia del análisis de datos	Trimestral
Frecuencia del reporte del resultado de las mediciones	Trimestral
Revisión de la medición	2 años
Período de medición	Aplicable por 2 años

Bibliografía de la ISO/IEC 27004:2009

[1] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary.*

[2] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management.*

[3] ISO/IEC 15504-3:2004, *Information technology — Process assessment — Part 3: Guidance on performing an assessment.*

[4] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process.*

[5] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management.*

[6] ISO/TR 10017:2003, *Guidance on statistical techniques for ISO 9001:2000.*

[7] ISO Guide 99:2007, *International vocabulary of metrology — Basic and general concepts and associated terms (VIM).*

[8] NIST Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, July 2008.

[9] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management.*

Anexo C - IRAM
(Informativo)

Bibliografía

En el estudio de esta norma se ha tenido en cuenta la bibliografía siguiente:

ISO – INTERNATIONAL ORGANIZATION FOR STANDARIZATION
IEC – INTERNATIONAL ELECTROTECHNICAL COMMISION
ISO/IEC 27004:2009 – Information technology – Security techniques - Information security management — Measurement

Anexo D - IRAM

(Informativo)

Integrantes de los organismos de estudio

El estudio de este esquema estuvo a cargo del organismo respectivo, integrado en la forma siguiente:

Subcomité de Seguridad en Tecnología de la Información

Integrante:		Representa a:
Sr.	Darío Mateo BRUNEL	RED LINK S.A.
Sr.	Raúl Eduardo CABRERA	CONSULTOR INDEPENDIENTE/ SADAIC
Lic.	Adriana DE ROSE	CONSULTOR INDEPENDIENTE
Sr.	Guillermo DESCALZO	RED LINK S.A.
Lic.	Ma. Virginia´DELL´ ÁRCIPRETE	BDO BECHER
Ing.	Norberto ESARTE	GATECH S. R. L.
Sr.	Ariel FERNÁNDEZ	HARDINEROS
Sra.	Laura FIORELLI	RED LINK S.A.,
Ing.	Graciela FRIGERI	INVITADA ESPECIAL
Ing.	Gustavo GARFINKIEL	MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL
Lic.	Jorge GUERRA	GRUPO DE INF. BIOMÉDICA DE BS. AS.
Dr.	Ricardo HERRERO	AMA – ASOCIACIÓN MÉDICA ARGENTINA
Cont.	Silvia IGLESIAS	IGLESIAS, RUBIO & ASOC./IT FOR SECURE BUSSINESS
Sr.	Humberto MANDIROLA	GRUPO DE INFORMÁTICA BIOMÉDICA DE BS.AS.
Lic.	Claudio MENAL	DIVERSIS
Ing.	Liliana Rosa MIRA	SAYQA SOLUTION PARTNER
Sra.	Patricia MUÑOZ	INVITADA ESPECIAL
Lic.	Ricardo OTERO	INVITADO ESPECIAL
Sr.	Marcos PASSARELLO	INVITADO ESPECIAL
Lic.	Osvaldo PERÉZ	IEEE INST. DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS DE ARGENTINA
Dr.	Fernando PLAZZOTTA	HOSPITAL ITALIANO DE BS AS
Dra.	Sandra PRIETO	ARBA - AGENCIA DE RECAUDACIÓN DE LA PCIA DE BS. AS.
Sr.	Fernando RADICCHI	BNA – BANCO DE LA NACION ARGENTINA
Sr.	Leonardo RAMOS	ARBA - AGENCIA DE RECAUDACIÓN DE LA PCIA DE BS. AS.
Ing.	Marcelo RÉ	UNIVERSIDAD NACIONAL DEL LITORAL
Sra.	Susana ROMANIZ	FACULTAD REGIONAL STA. FE - UTN
Ing.	Pablo Miguel ROMANOS	MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Integrante:		Representa a:
Ing.	Rubén Fernando ROMERO	BCRA- BANCO CENTRAL DE LA REPÚBLICA ARGENTINA
Ing.	Juan Pablo SKOCZDOPOLE	INSSJP - PAMI
Ing.	Jorge Luis CEBALLOS	IRAM
Lic.	Pedro Claudio COSTA	IRAM
Lic.	Domingo DONADELLO	IRAM
Ing.	Sergio Fabián ROJAS	IRAM

TRÁMITE

El estudio de este esquema ocupó la atención del Subcomité de Seguridad en Tecnología de la Información en las reuniones del 2009-06-04 (Acta 4-2009), 2009-07-02 (Acta 5-2009), 2009-08-06 (Acta 6-2009),2009 -09-03 (Acta 7-2009), 2009-10-01 (Acta 8-2009), 2009-11-05 (Acta 9-2009), 2009-12-03 (Acta 10-2009), 2010-03-04 (Acta 1-2010), 2010-04-08 (Acta 2-2010), 2010-05-06 (Acta 3-2010), 2010-06-03 (Acta 4-2010), 2010-07-01 (Acta 5-2010), 2010-08-05 (Acta 6-2010) y 2010-09-02 (Acta 7-2010). En esta última se aprobó como Esquema 1 y se envió a Discusión Pública por 45 días.

Asimismo, en el estudio de este Esquema se han considerado los aspectos siguientes:

Aspectos	¿SE HAN INCORPORADO? Sí / No / No corresponde	Comentarios
Ambientales	No	
Salud	No	
Seguridad	No	

****

APROBADO SU ENVÍO A DISCUSIÓN PÚBLICA POR EL SUBCOMITÉ DE TECNOLOGÍA DE LA INFORMACIÓN Y SEGURIDAD DE LA INFORMACIÓN EN SU SESIÓN DEL 2 DE SEPTIEMBRE DE 2010 (Acta 7-2010).

FIRMADO
Ing. Fabián Rojas
Coordinador del Subcomité

FIRMADO
Dra. Silvia Iglesias
Secretario del Subcomité

FIRMADO
Lic. Marta R. de Barbieri
Vº Bº Gerente de Tecnología Química