Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Objetivos de Seguridad, Indicadores y Métricas

Objetivos de Seguridad, Indicadores y Métricas		
CONTROL DE VERSIONES		
Versión inicial		**Fecha**
V.1.0		**19/03/2019**
Documento elaborado por		
Responsable de actualización		
Versiones Posteriores	**Cambio realizado**	**Fecha**
Estado	**Aprobado por :**	
Etiquetado del documento	**Uso Interno**	

LISTA DE DISTRIBUCIÓN

Este documento ha sido distribuido a los siguientes responsables:

Nombre	Responsabilidad

COPYRIGHT

Tabla de contenido

1. Objeto y campo de aplicación

El presente procedimiento tiene por objeto describir la metodología utilizada para realizar el seguimiento y medición de los objetivos, procesos y de los indicadores empleados para evaluar la eficacia y eficiencia de los procesos, controles y el cumplimiento y seguimiento de los objetivos de calidad y seguridad establecidos por la Organización.

2. Responsabilidades

Las responsabilidades del presente procedimiento quedan definidas en la descripción de cada apartado.

3. Desarrollo

3.1. Recordatorio acerca de los Objetivos

Los objetivos de seguridad deben:

- **Ser coherentes con la política de Seguridad de la Información.**
- **Ser medibles (si es posible).**
- **Tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos.**
- **Ser comunicados.**
- **Ser actualizados, según sea apropiado.**

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar:

- **Lo que se va a hacer.**
- **Qué recursos se requerirán.**
- **Quién será el responsable.**
- **Cuando se finalizará.**
- **Cómo se evaluarán los resultados.**

3.2. Objetivos de seguridad

La organización, en base a estrategia, objetivos de negocio, apetito del riesgo y contexto, ha establecido los siguientes objetivos de seguridad de alto nivel, que son incluidos y aprobados en la política de seguridad de la información:

- **OBJ1.** Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportunos llevar a cabo para mantener un Sistema de Gestión de Seguridad de la Información, que le permita conseguir una mejora continua de su actuación.
- **OBJ2.** Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SGSI, preservando la Disponibilidad, Integridad y Confidencialidad de la información**.**
- **OBJ3.** Demostrar liderazgo por parte de la dirección asegurando que la política de Seguridad de la Información, y los objetivos de seguridad se establecen y son compatibles con la dirección estratégica de la organización.
- **OBJ4.** Asignar las funciones y responsabilidades necesarias en el ámbito de la seguridad y proporcionar el soporte necesario.
- **OBJ5.** Apostar por la "mejora continua", como mecanismo primordial de la evolución y adaptación de la organización.
- **OBJ6.** Implementar medidas de seguridad eficaces y eficientes
- **OBJ7.** Establecer y revisar periódicamente el nivel de seguridad (apetito del riesgo) basándose en análisis de riesgos.
- **OBJ8.** Formar, concienciar y motivar al personal sobre la importancia de cumplir los requisitos del SGSI.
- **OBJ9.** Tener en cuenta la seguridad de la información en proveedores y subcontratistas.

3.3. Mapeo de Objetivos de seguridad y Procesos del SGSI

A continuación, cada objetivo de seguridad a alcanzar, será mapeado con los procesos del SGSI (indicados en (***TFM_PROC_Roles, Responsabilidades y Competencias***), de tal forma que se facilite su planificación, medición y cumplimiento.

	OBJ1	OBJ2	OBJ3	OBJ4	OBJ5	OBJ6	OBJ7	OBJ8	OBJ9
P01		X							
P02	X	X			X				
P03							X		
P04	X	X							
P05		X	X	X					
P06	X	X							
P07					X	X			
P08					X				
P09		X							
P10		X							
P11			X	X	X		X		
P12	X	X							

P13									X
P14				X				X	
P15		X							

3.4. Requisitos en la definición de métricas

La selección o definición apropiada de medidas que aporten información, debe comenzar por tratar de obtener aquellos atributos que son medibles, así como el método para obtenerlos.

Cualquier entidad (procesos, productos, proyectos, recursos, etc.) puede tener atributos, de los que sólo algunos tendrán interés desde el punto de vista cuantificable y medible.

Para cada proceso del SGSI se definen unos indicadores/métricas de medición sobre los que se analiza la eficacia de los procesos y por tanto de los objetivos del SGSI. Dichos indicadores/métricas se encuentran en el registro (***TFM_REG_Medición de Objetivos).***

El primer paso en la definición de un modelo de medidas es seleccionar los atributos más relevantes sobre seguridad de la información. El origen de la información es variado, siendo los más habituales:

- Auditorías internas o externas.
- Análisis de Riesgos.
- Procesos
- Cuestionarios.
- Registro de eventos de seguridad.
- Información y estadísticas de sistemas.

Se deberá definir una adecuada provisión de la información medible y cuantificable, que incluya:

- Disponibilidad y definición de la información y su origen.
- Persona responsable de su captura.
- Ubicación de los datos.
- Periodo de disponibilidad de los datos.

Para poder determinar si los controles implantados cumplen adecuadamente con su cometido de proteger los activos, y servir de apoyo en la consecución de los objetivos de negocio es necesario definir métricas que indiquen el nivel de cumplimiento.

Las métricas suministrarán la información necesaria para conocer el estado y la evolución de dichos controles, la eficacia de los procesos y el grado de cumplimiento de los objetivos de seguridad.

Por tanto, se considerarán métricas que cubran todos los aspectos relacionados con los controles, procesos y objetivos, debiendo determinar si el indicador y la definición de seguridad del indicador especificada está correctamente implementada, comprobando:

- El objetivo de seguridad está identificado.
- El control del que se mide la efectividad y eficiencia está identificado.
- Los procesos evolucionan de forma correcta.

Las métricas dispondrán de valor mínimo y máximo admisible, es decir, un límite a partir del cual (por exceso o por defecto según los casos) se considera que el objetivo no se está alcanzando de forma satisfactoria o que el proceso no evoluciona según lo planificado. Cuando se sobrepase éste límite (por exceso o por defecto) se deberá estudiar.

La especificación técnica (Fórmula, variables que lo componen, periodicidad etc.) del indicador está plenamente identificada en el registro (***TFM_REG_Medición de Objetivos)***.

3.5. Establecimiento de indicadores

Los indicadores deben estar relacionados con los procesos, con los objetivos y con los controles de seguridad establecidos.

El Responsable del SGSI tiene la función de identificar los indicadores de proceso y de seguridad, que se deberán aplicar tanto a los controles implantados para analizar el desempeño de los procesos, el grado de cumplimiento de los objetivos establecidos y para mitigar el riesgo.

Para ello Responsable del SGSI o el Responsable del Departamento afectado documenta el siguiente listado:

- Definición de los indicadores con la siguiente información:
    - Objetivo/s asociado.
    - Indicador : Descripción del indicador.
    - Periodicidad : Cada cuanto tiempo se mide.
    - Responsable : Función del responsable que realizará la toma de datos.
    - Métrica(s): Métrica(s) que intervienen y su fórmula.
    - Mediciones : tomadas según la periodicidad definida.
    - Previsión del año : Resultado esperado.
    - Resultado : valor obtenido para ese año.

3.6. Seguimiento y medición de métricas y objetivos de seguridad

Para el seguimiento del desempeño de los indicadores seleccionados, el Responsable del SGSI o el Responsable del Departamento afectado, realiza el seguimiento y medición.

Una vez recogida toda la información, es función del Responsable del SGSI realizar informe/s de evaluación de la eficacia de controles, de la eficacia de los procesos y del grado cumplimento de objetivos de seguridad, y presentarlos al Comité de

Dirección, para que dichos informes sean estudiados en la revisión del sistema, pudiendo así tomar las decisiones oportunas.

Coincidiendo también con la Revisión del Sistema por la Dirección, se realizará una revisión sobre la idoneidad de los indicadores definidos, con objeto de anular aquellos que no resulten operativos y definir nuevos indicadores cuando sea necesario.

Para llevar a cabo esta tarea, los responsables asistentes a la revisión se deben plantear preguntas tales como:

- ¿Reflejan de forma adecuada los indicadores disponibles la eficacia del sistema?.
- ¿Pueden desarrollarse o utilizarse nuevos o mejorados indicadores para cada uno de los procesos?.
- ¿Puede incrementarse la calidad y la fiabilidad de la recopilación de datos?.
- ¿Se dispone de recursos suficientes para realizar la medición de los indicadores definidos?.
- ¿La frecuencia de medición de los indicadores es adecuada?.

3.7. Impacto de las acciones de mejora en los objetivos

Para el cumplimiento de los objetivos del SGSI se establecerán periódicamente acciones de mejora, de acuerdo con lo establecido en el procedimiento ***TFM_PROC_Gestión de no conformidades - Acciones correctivas y de mejora***. Para cada acción de mejora se establecerá su relación con uno o varios objetivos, así como el proceso o procesos involucrados en el documento ***TFM_REG_Acciones.***

4. Registros y Archivo

Nombre del registro	Responsable del registro	Tipo de archivo	Periodo mínimo
TFM_REG_Medición de objetivos	Responsable de Seguridad	Electrónico	3 años
TFM_REG_Acciones	Responsable de Seguridad	Electrónico	3 años
TFM_PROC_Roles, Responsabilidades y Competencias	Responsable de Seguridad	Electrónico	3 años