

Guía para la elaboración del marco normativo de un sistema de gestión de la seguridad de la información (SGSI)

Referencia	Guía para la elaboración del marco normativo-Creative common FINAL.doc
Creación	29 de noviembre de 2007
Autor(es)	Firma-e, Javier Cao Avellaneda

ÍNDICE

1. Introducción.....	3
2. Política de seguridad del SGSI	3
3. Normas de seguridad.....	5
4. Procedimientos de seguridad.....	6
5. Instrucción técnica de seguridad.	8
6. Políticas de uso.	8
7. Ejemplos de cada uno de los diferentes documentos.....	9

1. Introducción

El presente documento tiene por objetivo proporcionar unas recomendaciones respecto al contenido de los documentos del marco normativo que pueden aparecer en la construcción de un sistema de gestión de la seguridad de la información (en adelante SGSI), aclarar los diferentes tipos de documentos que pueden conformar el marco normativo y las relaciones entre ellos.

El contenido de cada uno de los documentos comentados no se encuentra definido por norma alguna a excepción de la política de seguridad que se encuentra especificada por la norma ISO 27002:2005 y cada organización podrá elaborarlos según su criterio. Este documento pretende ser simplemente una recomendación basada en la experiencia y conocimiento de Firma, Proyectos y Formación, S.L. en la implantación de sistemas de gestión de la seguridad de la información y en la redacción de los documentos que forman el marco normativo.

2. Política de seguridad del SGSI

Los objetivos (lo que hay que lograr), las estrategias (cómo lograr esos objetivos) y la política de seguridad (las directrices para lograr los objetivos) se pueden definir para cada nivel de la organización y para cada área o departamento.

Al objeto de conseguir una seguridad eficaz es necesario sintonizar los distintos objetivos, estrategias y políticas para poder elaborar un marco normativo en materia de seguridad que satisfaga los requisitos establecidos.

El documento de política de seguridad tiene como misión servir para dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los objetivos establecidos, la legislación y regulaciones existentes.

Este documento viene explícitamente indicado en como primer control de la Norma ISO 27002:2005. La guía de implantación del control indica que el documento debe contener declaraciones relativas a:

- a) una definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información;
- b) el establecimiento del objetivo de la Dirección como soporte de los objetivos y principios de la seguridad de la información en línea con los objetivos y la estrategia del negocio;
- c) un marco para el establecimiento de los controles y objetivos de cada control, incluyendo la estructura de valoración y gestión del riesgo;
- d) una breve explicación de las políticas, principios, normas y requisitos de cumplimiento más importantes para la Organización, por ejemplo:
 - 1) Cumplimiento de los requisitos legales (legislativos), regulatorios y contractuales;
 - 2) Requisitos de formación, aprendizaje y concienciación en seguridad;
 - 3) Gestión de la continuidad del negocio;
 - 4) Consecuencias de las violaciones de la política de seguridad;
- e) una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad de la información;

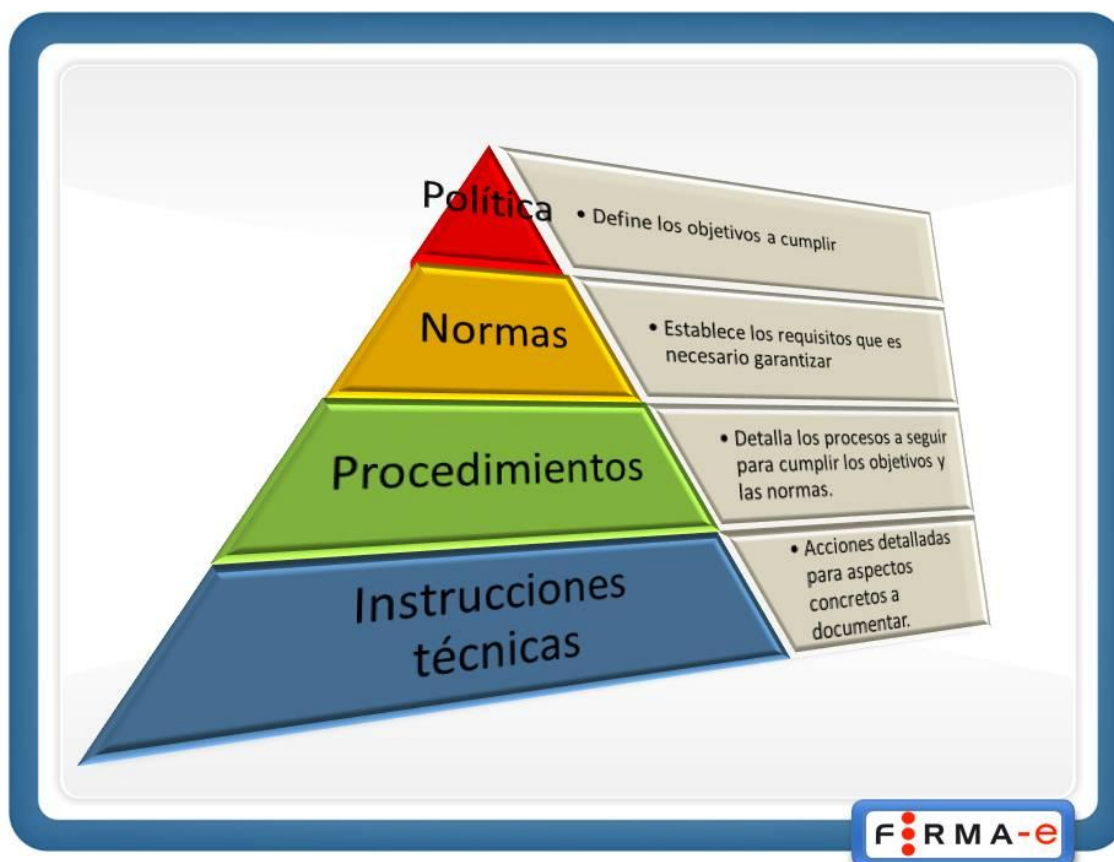
- f) las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deben cumplir.

A su vez, una política de seguridad puede apoyarse en documentos de menor rango que sirven para materializar en hechos tangibles y concretos los principios y objetivos de seguridad establecidos. Hablamos entonces del marco normativo que puede estar constituido por documentos de rango inferior como pueden ser las normas, políticas de uso, procedimientos de seguridad e instrucciones técnicas de trabajo.

A continuación detallamos la relación entre ellos.

- La **Política de Seguridad debe establecer los requisitos y criterios de protección** en el ámbito de la organización y servir de guía para la creación de normas de seguridad. Formalmente describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son sus objetivos de cara a la seguridad.
- Basándose en la Política, **las normas de seguridad definen qué hay que proteger** y los niveles de protección deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.
- Basándose en la política o las normas de seguridad, y dependiendo del ámbito de aplicación, el área responsable de garantizar la seguridad de un activo deberá crear los **procedimientos de seguridad en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables** de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son guías que especifican el cómo, dónde y cuando realizar tareas específicas.
- Basándose en los procedimientos de seguridad, y para entornos o sistemas de información concretos, podrán elaborarse **instrucciones técnicas de seguridad** que documenten de forma explícita y detallada las acciones técnicas a realizar en la ejecución del procedimiento o las tareas a considerar cuando se ejecute un procedimiento. Por ejemplo, el procedimiento de instalación de nuevos equipos podrá a su vez utilizar diferentes instrucciones técnicas adaptadas a cada uno de los diferentes entornos de configuración existentes en la organización.
- También podrán existir, como desarrollo de la propia política de seguridad o de cualquiera de las normas existentes, las **políticas de uso** que establecen las normas de comportamiento que deben cumplir los usuarios en el uso de los sistemas de información. Estos documentos destinados a usuario final resumirán y trasladarán los requisitos de seguridad a contemplar en la utilización o uso de determinadas tecnologías o servicios de manera concisa y fácilmente comprensible.

El siguiente dibujo ilustra a modo de ejemplo estas relaciones:



3. Normas de seguridad

Una norma de seguridad establece unos requisitos que se sustentan en la política y que regulan determinados aspectos de seguridad. Son por tanto, declaraciones a satisfacer. Una norma debe ser clara, concisa y no ambigua en su interpretación. En cuanto a la estructura de un documento normativo, se recomienda estructurarlo en los siguientes apartados:

- **Objetivo:** declaración del propósito o intención de la redacción del documento y de los objetivos de seguridad relacionados con la política que se intentan satisfacer.
- **Definiciones:** Se indican las definiciones de aquellos términos que aparezcan en la norma y que pudieran ofrecer dificultad para su comprensión. Es una forma de eliminar la ambigüedad en la interpretación al establecer el significado en la norma de los términos utilizados.
- **Responsables del cumplimiento:** se define dentro de la Organización qué departamento o responsable velará por el cumplimiento de la norma y revisará su correcta implantación o cumplimiento.
- **Incumplimiento:** se establecen las consecuencias que se derivarán del incumplimiento de la norma cuando éste sea detectado o las acciones disciplinarias que ocasionarán.
- **Normas a aplicar:** debe contener los requisitos de seguridad que se declaran de obligado cumplimiento. Podrán agruparse los requisitos por categorías, estableciendo apartados

donde se agrupen los requisitos relacionados. También los enunciados pueden numerarse para poder posteriormente referenciarlos.

- **Documentos relacionados:** se indican otros documentos del marco normativo que pudieran estar relacionados con el cumplimiento de la norma.

En cuanto a las recomendaciones en la redacción del documento, se debe procurar que:

- El cumplimiento debe ser factible a nivel organizativo y técnico.
- La redacción debe ser clara y resumida.
- Las afirmaciones realizadas dentro del apartado “Normas a aplicar” deben ser taxativas, no ambiguas y deben permitir la revisión o auditoría del cumplimiento del hecho reglado.
- El tiempo verbal de las normas debe ser presente del indicativo.
- La divulgación se realizará entre las áreas afectadas o implicadas en el cumplimiento.
- Su aprobación debe estar formalizada, indicando los plazos de vigencia y de revisión de la norma. Debe estar bajo un control de versiones.

4. Procedimientos de seguridad.

Un procedimiento determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad. Son por tanto, la especificación de una serie de pasos en relación la ejecución de un proceso o actividad. Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. Un procedimiento puede apoyarse en otros documentos para especificar con el nivel de detalle que se desee las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad.

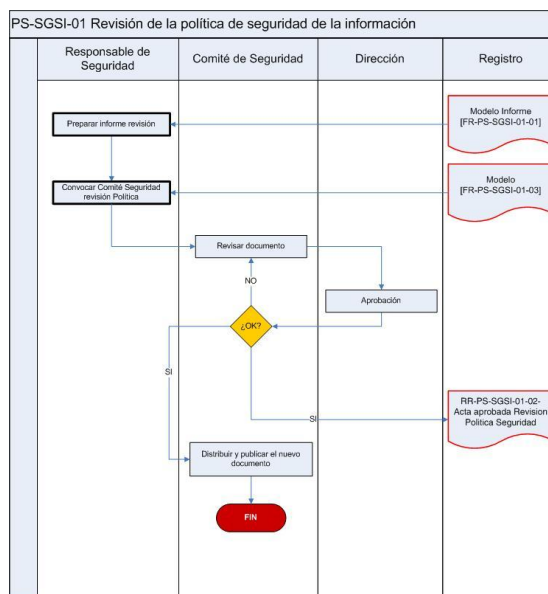
En cuanto a la estructura de un procedimiento, se recomienda estructurarlo en los siguientes apartados:

- **Propósito u Objetivo:** declaración del propósito o intención de la redacción del documento y de los requisitos de seguridad que se intentan satisfacer.
- **Definiciones:** deben especificarse las definiciones de aquellos términos que aparezcan en el procedimiento y que pudieran ofrecer dificultad para su comprensión. Es una forma de eliminar la ambigüedad en la interpretación al establecer el significado en el procedimiento de los términos utilizados.
- **Alcance:** aplicabilidad y límites de la organización donde este procedimiento es vinculante.
- **Desarrollo del proceso:** se debe determinar el conjunto de actividades y tareas a realizar en la ejecución del proceso. Debe responder a las siguientes preguntas:
 - Quién es el responsable de la acción o control.
 - Cuáles son las acciones/controles aplicados y cómo se realizarán, incluyendo la descripción de la información a procesar, los métodos y equipos utilizados, los registros a completar o procesar.
 - Lugar o sistema en dónde se ejecutará el procedimiento.
 - Cuándo, con qué frecuencia y plazo.

La explicación será lo extensa que el autor considere necesario considerando que debe ser claro y debe lograr transmitir qué es lo que hay que hacer.

Deben tener un inicio y un fin y se recomienda establecer un conjunto de registros o evidencias del cumplimiento del procedimiento, con el objetivo de hacerlo revisable o auditable y poder demostrar su correcta implantación.

- **Ejecución:** Suele ser una representación visual de la ejecución del procedimiento en formato de diagrama de flujo, donde en las columnas aparecen los actores que intervienen en la ejecución del proceso, indicando para cada uno de ellos, las actividades de las que son responsables. La última columna debe indicar los registros o evidencias de la ejecución que dejará el procedimiento. El siguiente gráfico ilustra a modo de ejemplo una representación visual de un procedimiento.



- **Registros:** Toda acción que suponga la ejecución de un proceso relacionado con la seguridad debe ser evaluable, para garantizar su correcto funcionamiento y el cumplimiento de los objetivos perseguidos. Por tanto, debe indicarse para cada procedimiento en qué información basaremos el criterio de evaluación del funcionamiento del mismo.
- **Documentos relacionados:** se indicarán otros documentos del marco normativo que pudieran estar relacionados con el cumplimiento del procedimiento.

En cuanto a las recomendaciones en la redacción del documento, debe procurarse:

- El cumplimiento debe ser factible a nivel organizativo y técnico.
- La redacción debe ser clara y resumida.
- El tiempo verbal de los procedimientos debe ser presente del indicativo.
- La divulgación se realizará entre los responsables de la ejecución.
- Su aprobación debe estar formalizada, indicando los plazos de vigencia y de revisión del mismo. Debe estar sometido a control de versiones.

Debe destacarse que un buen procedimiento es aquel que se entiende correctamente y consigue que determinada tarea se realice según lo establecido. En cada momento deberá considerar, de

cara al cumplimiento del objetivo del procedimiento, si debe estar documentado con mayor o menor detalle. Lo importante es que existan registros del funcionamiento del procedimiento para valorar su cumplimiento.

5. Instrucción técnica de seguridad.

Una instrucción técnica de seguridad determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc). Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. Una instrucción técnica debe ser clara y sencilla de interpretar. Deben documentarse los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma.

En cuanto a la estructura de una instrucción técnica, se recomienda estructurarla en los siguientes apartados:

- **Objetivo:** declaración del propósito o intención de ejecución de las tareas especificadas en la instrucción técnica.
- **Definiciones:** deben especificarse las definiciones de aquellos términos que aparezcan en la instrucción técnica y que pudieran ofrecer dificultad para su comprensión. Es una forma de eliminar la ambigüedad en la interpretación al establecer el significado en la instrucción técnica de los términos utilizados.
- **Ejecución:** Debe ser la secuencia ordenada de las actividades a realizar. Es recomendable establecer una numeración de los hitos que componen la instrucción. Puede ser recomendable, cuando la ejecución de la instrucción disponga de opciones o caminos alternativos, la representación visual en forma de diagrama de flujo similar a la utilizada en los procedimientos.
- **Documentos relacionados:** se indicarán otros documentos del marco normativo que pudieran estar relacionados con el cumplimiento del procedimiento. Las referencias pueden ser a documentación técnica necesaria, especificaciones del fabricante, etc.

En cuanto a las recomendaciones en la redacción del documento, se debe procurar que:

- El cumplimiento debe ser factible a nivel organizativo y técnico.
- La redacción debe ser clara y resumida.
- Debe documentar el conjunto de pasos o tareas a realizar, estableciendo la secuencia lógica de acciones para el correcto desempeño de la instrucción.
- El tiempo verbal de las instrucciones técnicas debe ser presente del indicativo.
- La divulgación se realizará entre los responsables de la ejecución.
- Su aprobación debe estar formalizada, indicando los plazos de vigencia y de revisión del mismo. Debe estar sometido a control de versiones.

6. Políticas de uso.

Una política de uso es un documento destinado a usuarios finales con la intención de establecer una regulación específica sobre la utilización de un sistema, tecnología o recurso. En este caso,

deben documentarse las normas de comportamiento que deben cumplir los usuarios en el uso de los sistemas de información o los aspectos generales que se desean regular así como los usos que son considerados autorizados y los usos no aceptables.

En cuanto a la estructura de una política de uso, se recomienda estructurarlo en los siguientes apartados:

- **Introducción:** propósito de la política de uso y justificación de su necesidad.
- **Objetivo:** declaración del propósito o intención de la redacción del documento y de los requisitos de seguridad relacionados con la política que se intentan satisfacer.
- **Definiciones:** deben especificarse las definiciones de aquellos términos que aparezcan en la política de uso y que pudieran ofrecer dificultad para su comprensión.
- **Ámbito de aplicación:** indica el contexto o situación en donde es de aplicación la regulación establecida por la política de uso.
- **Uso aceptable:** establece los términos, finalidades y condiciones en los que se encuentra permitido el uso de un determinado sistema, tecnología o recurso.
- **Uso no aceptable:** establece explícitamente las actividades o finalidades para las que se encuentra prohibido la utilización de un determinado sistema, tecnología o recurso, así como las conductas del personal sancionables.
- **Incumplimiento:** establecer las consecuencias que se derivarán del incumplimiento de la norma cuando este sea detectado o las acciones disciplinarias que ocasionarán.
- **Recomendaciones:** pueden indicarse en esta sección aquellas acciones o conductas que puedan ser consideradas como “buenas prácticas” que sin ser de obligado cumplimiento, al menos, son consideraras deseables por la organización.

En cuanto a las recomendaciones en la redacción del documento, se debe procurar:

- Utilizar términos comunes y comprensibles por cualquier usuario final independientemente de los conocimientos técnicos que posea.
- La redacción debe ser clara y resumida.
- El tiempo verbal de las instrucciones técnicas debe ser futuro.
- Su aprobación debe estar formalizada, indicando los plazos de vigencia y de revisión del mismo. Debe estar sometido a control de versiones.

7. Ejemplos de cada uno de los diferentes documentos.

A continuación y a modo de ejemplo, se van a documentar diferentes aspectos de la seguridad a través del desarrollo de un marco normativo adecuado para un aspecto de la seguridad. Se partirá de un enunciado extraído de una política de seguridad de ejemplo y se ilustrará como pueden ir elaborándose diferentes documentos del marco normativo para garantizar su cumplimiento. Se ha elegido los aspectos relacionados con el control de acceso como ejemplo.



Política de seguridad

Como texto dentro de la política de seguridad podría aparecer el siguiente texto:

“La presente política tiene por objetivo garantizar que el acceso a la información de la Organización se realizará exclusivamente por el personal autorizado.”

Normas de seguridad

Respecto al control de acceso, podrían existir los siguientes documentos:

- Norma general de control de acceso. Este documento debe resolver los aspectos comunes respecto a:
 - Reglas para establecer el identificador de usuario
 - Longitud mínima de contraseñas
 - Tipos de caracteres permitidos en la introducción de contraseñas.
 - Establecer si requiere la limitación en el número de intentos sin éxito.
 - Caducidad de las contraseñas.
 - Determinar si existirán bloqueos por inactividad.

Para ello, pueden formularse sentencias del estilo:

- “Todo identificador asignado por la Organización es único y permite la vinculación biunívoca entre el usuario y la persona física a la que representa.”
- “Las contraseñas en todos los sistemas tienen como mínimo una longitud de ocho caracteres.”
- “Se limitan a cinco el número de reintentos sucesivos sin éxito en la introducción de contraseña para bloquear a un usuario.”

Procedimiento de seguridad

Respecto al control de acceso, deberían documentarse los procedimientos relacionados con:

- Procedimiento de alta, modificación y baja de usuarios.
- Procedimiento de asignación del identificador y contraseña de usuario.

Cada uno de estos procedimientos debe documentar qué tareas deben realizarse, quiénes serán los responsables de su ejecución y qué evidencias de funcionamiento dejará cada procedimiento.

Instrucción técnica para el alta de usuarios en entornos Microsoft Windows

En relación al procedimiento de alta de usuarios, sería interesante documentar qué personas serán las responsables a nivel técnico de realizar el alta dentro de los sistemas Microsoft. Para ello, puede ser necesario documentar cómo se realiza esta tarea y qué perfil dentro del sistema de información está autorizado para su realización. Esta instrucción técnica puede detallar los siguientes aspectos:

- Campos o propiedades del usuario que habrá que rellenar dentro de la ficha de Active Directory cuando un usuario sea dado de alta.
- Criterios para la selección del identificador único dentro de la organización.
- Configuración inicial de la contraseña, indicando que el usuario en el primer inicio deberá forzosamente cambiar la contraseña por defecto para garantizar la confidencialidad de la misma.

Política de uso de contraseñas

Para lograr la participación del usuario final es necesario explicar la importancia que tienen las contraseñas en la seguridad de la organización así como establecer qué usos están autorizados y qué actividades están prohibidas. Por último, es recomendable indicar las buenas prácticas respecto a la custodia y selección de contraseñas, informando al usuario con recomendaciones para que elijan contraseñas robustas y fáciles de recordar.

Por ejemplo:

1. Mantenga su contraseña en secreto: La contraseña es algo muy serio y no debe ser proporcionada a nadie bajo ningún concepto. Cualquier persona que pueda conocerla tiene la posibilidad de suplantarle en cualquier momento, con los problemas que eso le puede ocasionar a usted, y no a él.

2. Utilice contraseñas de calidad: La contraseña debe estar pensada para que sea difícil de reproducir o de adivinar. Como recomendaciones le damos las siguientes:

- Evite palabras del diccionario. Es lo primero que busca cualquier sistema de detección de contraseñas.
- No deben estar basadas en algo que pudieran adivinar u obtener usando información relacionada con usted, como nombre de hijos, fecha de nacimiento, número de teléfono, etc.

Como recomendaciones de contraseñas de calidad le podemos ofrecer las siguientes:

- Reglas nemotécnicas: LleSeupm (La lluvia en Sevilla es una pura maravilla)
- Palabra cambiada de orden: aremlap (palmera al revés)
- Uso de caracteres para recordar frases: esto-es-solo-un-ejemplo, (otro-ejemplo).
- Sustituir números por letras como el 4 por la letra A, el 0 por la o y el 1 por la letra i: Buen4c0ntr4señ4."