Universidad de Valladolid

ESCUELA DE INGENIERÍAS INDUSTRIALES

Estudio de las normas españolas y estadounidenses de seguridad de la información

Rodrigo Marcos Carvajal

Universidad de Valladolid

ESCUELA DE INGENIERÍAS INDUSTRIALES

UNIVERSIDAD DE VALLADOLID

ESCUELA DE INGENIERIAS INDUSTRIALES

Grado en Ingeniería en Organización Industrial

Estudio de las normas españolas y estadounidenses de seguridad de la información

Autor:

Marcos Carvajal, Rodrigo

Tutor:

Gonzalo Tasis, Margarita

Departamento de Informática

Valladolid, Julio de 2015.

Resumen

Las normativas con las que cuenta EE.UU son mucho más extensas y detalladas que la normativa que se utiliza en España, lo que evidencia la diferencia histórica a nivel tecnológico que siempre existió entre ambos países. Este hecho, en realidad no se ve reflejado en el número de certificaciones que estos países tienen en la norma de carácter internacional ISO/IEC 27001.

Los dos marcos normativos se basan en principios muy diferentes y tienen enfoques dispares; aunque estemos tratando con normativas en materia de seguridad de la información.

Palabras clave: Seguridad, Información, ISO/IEC 27001, NIST, Comparativa.

The American standards are more extensive and far more detailed than the standard which is used in Spain, which proves that historic technological differences that have always existed between both countries, even though it isn't specifically reflected in the number of certifications that these countries have in an international standard as ISO/IEC 27001.

Both frameworks are based on very different principles and have unlike approaches, although we are dealing with security information standards.

Key words: Security, Information, ISO/IEC 27001, NIST, Contrast.

ÍNDICE

CAPÍTULO 1.

INTRODUCCIÓN

1. INTRODUCCIÓN

1.1. Justificación del estudio

Existen una serie de impulsores que han originado la existencia de una potenciación de la seguridad de la información, tales como: el extenso rango de conectividad que existe hoy en día y el cual en gran parte es debido a internet, el aumento creciente de concienciación ante problemas de privacidad y seguridad, el rápido desarrollo de los ordenadores y toda la tecnología con la que están relacionados, así como la llegada de nuevas normas y legislación.

En la última década han surgido muchas normativas y guías de buenas prácticas con la idea de poder abordar la dirección de todas, están las tecnologías que mencionaba anteriormente.

Un sistema de gestión de seguridad de la información[1] (SGSI) es un sistema que nos permite mantener una confidencialidad, integridad y disponibilidad de toda la información. El objetivo de este sistema es identificar las vulnerabilidades y amenazas que puedan afectar a los diferentes activos que están relacionados con este ámbito, así como el de identificar controles que reduzcan riesgos que puedan afectar a la misión de la organización.

Es importante destacar que cuando nos referimos al termino garantía de seguridad, "security assurance", tenemos que tener presente que lo que tendremos será un nivel de confianza o de garantía en nuestro sistema, no hay una seguridad absoluta, no existe una seguridad total o perfecta. A veces, todo lo que podemos hacer es calcular la probabilidad de que las cosas vayan mal, normalmente con dinero nos podemos asegurar de que esto no suceda, pero esto no es siempre así.

1.2. Objetivos

El objetivo principal de este Trabajo Fin de Grado consiste en realizar un estudio de las normas más relevantes estadounidense y española de seguridad de la información (normas desarrolladas por NIST y ISO/IEC respectivamente), así como compararlas de la forma más detallada posible mediante una comparación, considerando diferentes puntos de vista.

[1] Un sistema de gestión de seguridad de la información también es conocido por sus siglas en inglés ISMS (Information Security Management System).

El estudio de tales normas nos plantea que la finalidad global del trabajo es comprobar cómo se establece un sistema de gestión de seguridad de la información dentro de una organización dada la transcendencia que ha adquirido esta materia según hemos visto en la justificación del estudio.

Esta finalidad global es compatible con fines más concretos, relacionados con los planteamientos normativos usados tanto a nivel español como a nivel estadounidense en las distintas fases que comportan el establecimiento de la seguridad de la información. Cuando hablamos de estas finalidades más concretas estamos descendiendo a aspectos que tocan de lleno la implantación de un SGSI. En este sentido dentro de tales fines más concretos necesitaremos conocer, según el tipo de organización de la que se trate, las necesidades especificas de dicha organización que delimitarán dichos fines para la implementación del sistema.

Se trata en definitiva de evaluar riesgos y decidir como eliminarlos, minimizarlos, o simplemente aceptarlos.

Lo dicho afecta a objetivos o finalidades perseguidas. Toda finalidad necesita de un planteamiento instrumental para que dichos objetivos puedan cumplirse.

Cuando hablamos de planteamiento instrumental estamos refiriéndonos a los criterios que nos aportan tanto las normativas españolas como las normativas estadounidense. Por ello resulta imprescindible el análisis de tales instrumentos y su desarrollo, comenzando por un análisis independiente y concluyendo con una comparación entre los dos tipos de normativas.

Precisamente la estructura que se plantea a continuación está pensada para llevar a cabo el tratamiento al que nos estamos refiriendo.

1.3. Estructura del proyecto

Si quisiéramos tener una visión global de este Trabajo Fin de Grado y de su estructura, podríamos identificar tres partes principales y que están claramente diferencias:

En una primera parte española, hablaremos de la ISO 27001, una norma de carácter internacional que es utilizada por organizaciones y empresas que trabajan en un ámbito comercial. Esta norma es adoptada por AENOR y aplicada por las empresas en España.

En una segunda parte estadounidense, hablaremos de los estándares desarrollados por NIST en materia de seguridad de la información que se utilizan en Estados Unidos. Cabe decir que la ISO 27001 al ser una norma de carácter internacional también es aplicada en Estados Unidos, pero al haber trabajado ya con ella en la parte española, nos centraremos en los aspectos peculiares del NIST y en presentar sus publicaciones.

Una tercera y última parte donde realizamos una comparación entre estos dos marcos normativos.

El trabajo desarrollado se encuentra dividido en diferentes capítulos, cuyo contenido se estructura del siguiente modo:

Comenzaremos con el presente capítulo en el que estamos realizando una introducción, partiendo del estudio de los antecedentes que generan la realización del proyecto, planteando el por qué de su elaboración y describiendo las causas o motivos de su formalización documental.

En el segundo capítulo explicaremos el origen de esta serie, para entender cómo hemos llegado a disponer de las normas principales que componen la serie y cuál fue su punto de partida. También enumeraremos las normas que componen esta serie, así como los objetivos y aspectos principales de las mismas. La norma ISO/IEC 27001 es la norma principal de la serie y las otras normas que la componen, que o bien añaden información o ayuda en torno al SGSI, o bien son especificas para un entorno o sector.

El tercer capítulo lo usaremos para detallar con mucha más amplitud que en el capitulo anterior, los aspectos y requisitos que posee la normal principal de la serie ISO 27000, la ISO/IEC 27001. Al final de éste hemos planteado un modelo de implementación del SGSI que cumple los requisitos de la ISO/IEC 27001 aplicando el ciclo PDCA.

En el cuarto capítulo responderemos a qué es NIST y a qué es FISMA, las dos piezas claves que conforman la parte estadounidense y veremos cómo y en qué fases una de estas piezas implementa a la otra.

En el quinto capítulo desarrollaremos de forma detallada el marco de gestión del riesgo que expone FISMA y gracias al cual obtendremos varios puntos de comparación respecto a ISO/IEC 27001.

En el último capítulo trataremos la última parte que compone este TFG, discutiremos las diferencias y semejanzas que poseen ambos marcos.

CAPÍTULO 2.

SERIE ISO 27000

2. SERIE ISO 27000

2.1. Introducción

Una organización puede contar con una amplia variedad de activos, que pueden ser tanto tangibles como intangibles, así como vitales para su éxito y no vitales para la consecución del mismo. En el caso de la información, podríamos decir que es un activo vital para la consecución del éxito de la organización y para que ésta pueda tener una unión con el mercado.

Estableceremos un sistema de gestión de la seguridad de la información que trabaje de una forma sistemática, precisa y documentada. Podemos decir que este sistema, tiene un origen en unos objetivos claros de seguridad, así como en una evaluación de los diversos riesgos a los que la información de una organización puede estar expuesta.

La serie 27000 nos proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Hablaremos sobre una serie de normativas que han sido desarrolladas o aún se encuentran en desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), estos estándares o normativas nos ofrecen un marco de gestión de seguridad de la información que puede ser usado por cualquier tipo de organización, como hemos dicho antes, pero además de una forma eficiente.

Podemos considerar la ISO 27001 como la norma más importante de la serie, esto se debe a que detalla todos los requisitos necesarios con los que debe contar nuestro sistema de gestión de seguridad de la información. Se puede ver la historia de la misma como un simple ciclo de normas (Figura 2.1.1). En este ciclo observamos que la primera norma que da origen a la serie y que inicia el ciclo es la norma BS 7799 de BSI. BSI (British Standards Institution) es la primera entidad de normalización que existió a nivel mundial, data de 1901, es británica y su equivalente en España es AENOR.

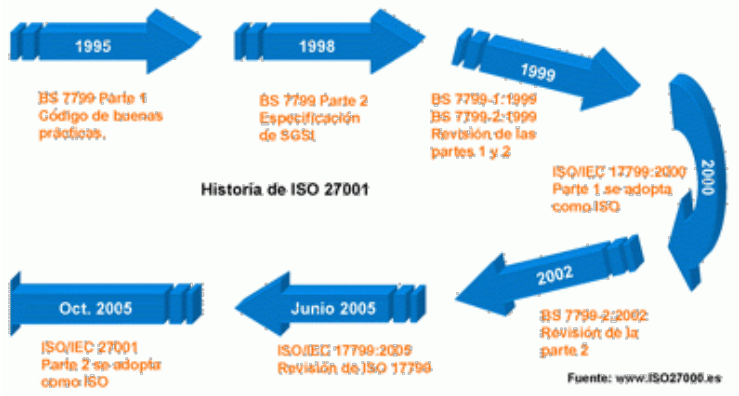

Figura 2.1.1 Ciclo normativo historia ISO 27001

La principal diferencia entre las dos partes de BS7799 es que la primera solo prestaba un guía de buenas prácticas para la organización, sin prestar un esquema de certificación. En la segunda parte, que se publicó en 1998, se mostraron por primera vez unos requisitos de certificación en materia de seguridad de información.

Después de una revisión de ambas partes de la norma BS7799 en 1999, la primera parte de ellas se convierte en el origen de la primera norma ISO en esta materia, bajo el nombre de ISO 17799 en el año 2000, y sin cambios sustanciales.

Hicieron falta algunos cambios y una revisión en el año 2002, para que la parte dos se adoptara como ISO, bajo el nombre de ISO 27001 en el año 2005. En este mismo año se revisa la ISO 17799 y más tarde en el año 2007 se renombró como ISO 27002.

Cabe destacar que se han desarrollado y que se están desarrollando en este momento, otras normas en la serie que permiten entender y poder llegar a implantar la norma principal de la serie, la ISO 27001, ya que como destaca ISO, es la norma principal y única certificable dentro de la serie. Podemos decir que las otras normas de la serie son un soporte de la norma principal.

No debemos olvidar las últimas publicaciones de las revisiones de las normas ISO/IEC 27001, ISO/IEC 27002 ambas aprobadas en la misma fecha: 25 de Septiembre de 2013.

2.2. Publicaciones

En este apartado vamos a discutir las diferentes normas que componen la serie ISO 27000. Trataremos la ISO/IEC 27000 que es una síntesis de todas las normas que forman la serie, la ISO/IEC 27001 que es la pieza fundamental de la serie y la cual desarrollaremos más ampliamente en el capítulo tres, y trataremos de realizar una síntesis de cada una de las otras normas que componen la serie 27000.

- ISO/IEC 27000 (Publicada)

Fue publicada por primera vez el 1 de Mayo de 2009 y revisada con una segunda edición el 1 de Diciembre del 2012 y una tercera edición el 14 de Enero de 2014. La misión de esta norma es la de detallar los límites de cada una de las normas que componen la serie 27000, así como especificar la finalidad de ellas. Es decir, es un resumen de todas ellas, un resumen que será útil a la hora de tener una idea general de las normas que componen la serie. También nos habla de la importancia de los sistemas de gestión de seguridad de la información, y un resumen de las etapas que hay que seguir para su establecimiento, seguimiento, mantenimiento y mejora de los mismos.

- ISO/IEC 27001 (Publicada)

Como hemos dicho ya la ISO 27001 es la norma principal y única certificable dentro de la serie. Podemos decir que las otras normas de la serie son un soporte de la norma principal. Es la norma de la serie ISO en la que nos centraremos. Nosotros trabajaremos con la UNE-ISO/IEC 27001:2014, una norma idéntica a la ISO/IEC 27001:2013 pero traducida al español por AENOR. Cabe decir que esta publicación cuenta con un anexo en el que, en un formato tipo resumen, define los diferentes objetivos de control y controles que más tarde la ISO 27002 desarrolla. Como más tarde especificaremos en el apartado 3.5, no es obligatorio que se utilicen todos estos controles, pero es necesario argumentar por qué hay controles que no han sido implementados.

Esta norma contará con dos objetivos básicos, que consisten en establecer dos tipos de requisitos: requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información, y requisitos para la apreciación y el tratamiento de los riesgos de seguridad de la información a la medida de las necesidades de la organización.

- **ISO/IEC 27002** (Publicada)

Describe los objetivos de control [2] y los controles de seguridad de la información [3]. Son 39 objetivos de control y 133 controles, que se encuentran agrupados en 11 dominios. Un ejemplo de uno de los dominios con sus objetivos de control y controles sería el siguiente:

> 13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. (Dominio)
>
> 13.1 Notificación de eventos y puntos débiles de seguridad de la información. (Objetivo de control)
> 13.1.1 Notificación de los eventos de seguridad de la información. (Control)
> 13.1.2 Notificación de puntos débiles de seguridad. (Control)
>
> 13.2 Gestión de incidentes y mejoras de seguridad de la información. (Objetivo de control)
> 13.2.1 Responsabilidades y procedimientos. (Control)
> 13.2.2 Aprendizaje de los incidentes de seguridad de la información. (Control)
> 13.2.3 Recopilación de incidencias. (Control)

- **ISO/IEC 27003** (Publicada)

Se centra en los aspectos más críticos necesarios para diseñar e implementar un sistema de gestión de seguridad de la información, tomando como base la ISO/IEC 27001. Habla de la especificación, diseño, implementación y aprobación de los mismos. Esta norma podría utilizarse tanto para implementar un SGSI desde cero, como en el caso de que una persona en una organización necesitara resolver dudas relativas a cómo se realizó la implementación del mismo, como para poder trabajar con él de forma diaria.

Es decir, presta toda su atención a un diseño exitoso y una implementación correcta del SGSI, aunque siempre partiendo de la base que ofrece la ISO/IEC 27001. Si una organización quisiera especificar los límites y delimitar el

[2] Un objetivo de control puede definirse como la descripción de lo que se quiere lograr como resultado de la utilización de un control.
[3] Un control de seguridad de información es un método para gestionar un riesgo relativo a la seguridad de la información.

proyecto de implementación del SGSI, sería la norma en la que debería fijarse para cumplir con tal objetivo.

- ISO/IEC 27004 (Publicada)

Nos ayuda a la hora de comprobar la eficacia de nuestros sistema de gestión de la seguridad de información, nos enseña a desarrollar y a hacer uso de unas métricas y técnicas de medida, así como de los controles que hablábamos anteriormente.

En las organizaciones se necesita contar con herramientas que tengan carácter práctico en la mayoría de la ocasiones, largas normativas que expresan conceptos de teoría que son difíciles de interpretar o llevar a cabo no son útiles. Esta norma se puede considerar beneficiosa dado que establece una serie de prácticas que permiten medir el resultado de un SGSI.

Siempre que queremos realizar la medición de algún elemento en la vida real como puede ser una longitud, tenemos una medida asociada al mismo, es decir no todos los tipos de medida son aplicables a un objeto de medición. ISO/IEC 27004 especifica que parámetros debemos medir con un tipo concreto de métrica, cómo y cuándo debemos hacerlo, y establece un programa de medición.

Esta norma también desarrolla cómo se deben interpretar los datos obtenidos en la medición así cómo deben ser comunicados dentro de la organización.

- ISO/IEC 27005 (Publicada)

Utilizando como norma de apoyo la norma principal de la serie (ISO/IEC 27001), y basándose en sus conceptos, nos aporta una guía para la gestión de riesgos relacionados con la seguridad de la información.

A la hora de llevar a cabo cualquier tipo de proyecto siempre el primer paso a realizar consiste en definir el alcance[4] del mismo. En este caso, estamos hablando del proyecto de implementación de una norma de seguridad de la información, por lo que el alcance vendrá delimitado por los límites del SGSI.

[4] El alcance es el trabajo que debe realizarse para lograr los objetivos del proyecto. Su definición consiste en asegurar que el proyecto incluya todo el trabajo requerido y sólo el trabajo requerido para completar satisfactoriamente el proyecto.

Esta norma no recomienda una metodología concreta para llevar a cabo la gestión de los riesgos que puedan complicar la seguridad de la información de la organización, sino que especifica diferentes metodologías que son función del alcance del SGSI y del sector de la propia industria.

- ISO/IEC 27006 (Publicada)

Esta norma trata los requisitos para los organismos que llevan a cabo las auditorias y certificaciones[5] de los SGSI. Es decir, está enfocada no a las organizaciones que utilizarán los SGSI, sino a los organismos que están encargados de certificar que esos SGSI funcionan conforme a lo que marca ISO/IEC 27001.

Si reflexionamos sobre ello podemos darnos cuenta de que la existencia de una norma que contemple estas características es algo más que necesario. Simplemente tenemos que preguntarnos cómo podemos fiarnos de que un organismo esté certificando de forma correcta SGSI si ese mismo organismo no ha sido acreditado para ello. Para entenderlo con claridad pensemos en un cirujano que debe operar y no ha sido acreditado para ello, es decir, no ha conseguido un titulo universitario que le acredita y le permite operar. En ese caso no podríamos fiarnos de que operara de forma correcta, luego no le permitiríamos ejercer.

- ISO/IEC 27007 (Publicada)

Proporciona unas directrices útiles para las organizaciones acreditadas de certificaciones a la hora de auditar los SGSI.

Esta norma toma como base ISO 9001[6] y lo orienta a los SGSI. También hace uso de ISO 17021[7], del cual recoge ideas que dirige a:

- La gestión del programa de auditoría del SGSI.
- Ejecución de la auditoria del SGSI.
- Gestión de los auditores. Es decir, gestionar sus competencias, habilidades y atributos.

[5] El proceso de certificación consiste en auditar el SGSI para el cumplimiento de ISO 27001, esto es realizado por organizaciones como AENOR.
[6] La ISO 19001 Requisitos para los sistemas de gestión de la calidad. Está dirigida a la certificación de sistemas de gestión de la calidad.
[7] ISO/IEC 17021 Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.

Especifica los requisitos y suministra una guía para la auditoría y la certificación del sistema.

Para entender mejor la situación ponemos como ejemplo el caso en el que AENOR audita un SGSI, el cual ha sido desarrollado conforme a los requisitos que establece la ISO/IEC 27001, para llegar a su certificación tiene que seguir los procedimientos que establece está norma ISO/IEC 27007.

- ISO/IEC 27008 (Publicada)

Llegado a este punto podríamos plantearnos si existe una norma que esté dirigida a la comprobación de los controles de seguridad, que se desarrollan en el anexo de la ISO/IEC 27001 y que se detallan más extensamente en la ISO/IEC 27002, bien, esta norma es la ISO/IEC 27008.

Es decir, una vez que esos controles de seguridad de la ISO/IEC 27001 han sido ya implementados, existe una norma que detalla cómo realizar una auditoria a estos controles.

Podríamos pensar que no se necesita una norma que se dedique exclusivamente a dirigirnos en la comprobación y auditoria de los controles de seguridad de la información, pero lo cierto es que una organización no solo tiene que ser capaz de realizar auditorias, sino que también es importante que lo haga de una forma en la que optimice los recursos de los que dispone para realizarla, ya que no puede haber perdidas innecesarias. Si no tuviéramos una norma de este tipo no seríamos capaces de realizar estas auditorias de los controles de una forma en la que optimizáramos los recursos disponibles para ello.

- ISO/IEC 27009 (Baja desarrollo)

Cuando tratamos con aspectos relacionados con la seguridad de la información, es necesario que tengamos en cuenta el sector en el que la organización se encuentra inmersa, ya que de esta forma podremos conocer los límites en los que nos movemos, y llegar a obtener una seguridad de la información mucho más precisa que si simplemente aplicáramos conceptos y procedimientos más abstractos.

Especifica cómo debe ser el uso y la puesta en marcha de ISO/27001 en cualquier sector especifico, se explica como adaptar los requisitos ISO/IEC 27001.

Cuando consideremos un sector específico, esta es la norma que deberíamos comenzar a aplicar antes de buscar una norma de esta serie que sea específica para el sector con el que tratamos, ya que nos da una idea de cómo incluir requisitos adicionales a los de la ISO/IEC 27001, cómo redefinirlos y cómo incluir controles de seguridad en adicción a los de el anexo de la ISO/IEC 27001.

- ISO/IEC 27010 (Publicada)

Es una norma que difiere de las anteriores, ya que está destinada al intercambio de información. Se refiere a la información cuyo origen son los riesgos de seguridad de la información, controles y los problemas relativos a la seguridad de la información que puedan surgir en las organizaciones.

Si reflexionamos sobre los diferentes elementos entre los cuales puede existir este intercambio de información, nos daremos cuenta que son los mismos elementos que trata esta norma, considerando el intercambio de información relativo a la seguridad de la información dentro del propio sector de la organización, diferentes sectores, con los gobiernos y a nivel interno en la organización.

ISO 27010 proporciona los métodos, modelos, procesos y controles para llegar a un intercambio de información de una manera segura.

En este ejemplo podemos ver como no seguir un procedimiento adecuado de intercambio de información en materia de seguridad de la información, puede llevar a un filtrado de información entre empresas privadas que puede perjudicar a terceras personas.

En 2011 salió una noticia que declaraba el posible filtrado de fotos, datos personales y conversaciones que la compañía Facebook podría haber filtrado de forma accidental a empresas privadas, como por ejemplo anunciantes. La fuente del fallo serían las más de 100000 aplicaciones de Facebook que filtraron información de los perfiles a empresas desde 2007 hasta el 2011.

Podemos darnos cuenta como una filtración de estos datos puede ser algo muy jugoso para los anunciantes, que con estos datos de perfiles pueden

conocer sus gustos, localización, edad… y de esta forma saber como satisfacer sus necesidades para ofrecer sus productos o servicios.

- ISO/IEC 27011 (Publicada)

Se utiliza para la gestión de la seguridad de la información en organizaciones que se encuentran relacionadas con el sector de las telecomunicaciones.
Debemos tener presente que el sector de las telecomunicaciones es un sector propenso a filtraciones de datos y fallos de seguridad dado la cantidad de información que fluye en el mismo. Además debemos tener en cuenta que la información es un activo esencial para este sector, las telecomunicaciones se basan en la transmisión y recepción de señales con el objetivo de comunicar información.

Es decir, busca seguridad de información mediante directrices prácticas para organizaciones del sector de telecomunicaciones y que dan una confianza a la hora de realizar actividades a estas organizaciones.

- ISO/IEC 27012 (Cancelada)

ISO/IEC 27012 fue una norma que su realización fue propuesta, pero finalmente fue cancelada y no se llevo a cabo por falta de interés. El sector financiero volvió a proponer su realización, pero hasta el momento no tenemos noticias al respecto.

- ISO/IEC 27013 (Publicada)

Las tecnologías de la información y la comunicación se puede definir como un conjunto heterogéneo de herramientas, métodos y recursos tecnológicos empleados para crear, recabar, almacenar, gestionar y distribuir información.

Cuando nos referimos a los servicios de tecnologías de la información podemos estar hablando de que una empresa facilita recursos humanos que están especializados en informática a otra empresa, esto puede ser de forma temporal o definitiva. También hablamos de servicios como correo electrónico, la búsqueda de información, la banca online, el audio y música, la televisión…

Esta serie 27000 también incluye normas que detallan cómo realizar la integración de otras dos normas ISO, este es el caso de ISO/IEC 27013, la

cual se utiliza a la hora de integrar ISO/IEC 27001 e ISO 20000[8]. Esto es algo que sucede en muchas series ISO y que permite trabajar con los conceptos o directrices que exponen varias normas ISO, es decir existe una compatibilidad entre normas ISO.

Básicamente lo que haremos será integrar los dos sistemas de los que habla cada una de las series, la ISO/IEC 27001 un SGSI e ISO 20000 un SGSTI[9].

Imaginemos una situación para poner un ejemplo sobre lo que propone esta normativa:

Una pequeña empresa que se dedica a la fabricación de chocolate cuenta con servicios de las tecnologías de la información, como por ejemplo firma con certificación digital, diferentes sitios web y correo electrónico. Esta empresa cuenta con una gran cantidad de competidores interesados en su información y vulnerabilidades que la hacen susceptible a ataques informáticos.

Dadas las consideraciones anteriores podría estar interesada tanto en la utilización de un SGSI como en la de un SGSTI. Para trabajar de forma conjunta con ambos sistemas necesitaría hacer uso de ISO/IEC 27013.

Para estas situaciones ISO/IEC 27013 considera tres situaciones posibles:

a) Implementar la ISO 27001 cuando la ISO 20000 está ya implementada o viceversa.

b) Implementar la ISO 27001 y la ISO 20000 juntas a la vez.

c) Que ambos sistemas se encuentren ya implementados y simplemente haya que integrarlos.

De esta manera, esta empresa de chocolate sería capaz de utilizar conjuntamente un SGSTI y un SGSI, y lo que es más importante optimizando recursos y de forma eficaz.

[8] ISO 20000 Guía completa de aplicación para la gestión de los servicios de tecnologías de la información.
[9] Un sistema de gestión de servicios de las tecnologías la información (SGSTI) es un sistema que mediante la utilización de procesos y métodos trata de alinear los servicios de tecnologías de la información proporcionados con el entorno y necesidades de la organización.

- ISO/IEC 27014 (Publicada)

Es importante que una organización sepa valorar, gestionar, realizar supervisiones y comunicar información de las tareas de seguridad de la información, pero intentado que las estrategias de la empresa queden orientadas y alineadas con la seguridad de la información.

La norma se centra en la alineación entre la estrategia de seguridad de la información que trata la ISO/IEC 27001 y la propia estrategia que tenga la empresa. En una organización todo tiene que estar pensado en conjunto, es decir las diferentes estrategias con las que cuente deben mantenerse alineadas, no podemos tener una estrategia en seguridad de la información que no persiga los objetivos que quiere conseguir la organización, por lo tanto la estrategia de seguridad de la información debe estar trazada en la misma línea que la estrategia de la organización para conseguir sus objetivos.

También al leer esta norma podemos darnos cuenta de la importancia de la formación, educación y prestación de seguridad por parte del factor humano en las actividades de seguridad de la información, ya que a la hora de coordinar las dos estrategias de las que venimos hablando es necesario que las personas de la organización estén implicadas.

- ISO/IEC TR 27015 (Publicada)

Como en el caso de ISO/IEC 27011 esta norma es una norma que se encuentra enfocada a un sector especifico, en esta situación no es el sector de las telecomunicaciones, sino que se encuentra destinado a organizaciones que trabajen en el sector financiero y seguros. Las empresas que trabajen en el sector financiero siempre contarán con una serie de activos que son atractivos ante ataques cibernéticos, como por ejemplo: información del balance disponible en cuentas corrientes, movimientos de saldo, datos personales…

Además muchos bancos se centran hoy en día en dar un tipo de servicio al cliente que le facilite realizar operaciones con comodidad desde su casa, mediante servicios de banca electrónica, esto hace mucho más susceptible a las empresas del sector financiero a ataques cibernéticos y phishing[10].

[10] El phishing se basa en el envío de correos electrónicos que intentan conseguir datos confidenciales del usuario, intentando hacer creer que provienen de fuentes fiables (como por ejemplo una entidad bancaria), estos datos confidenciales del usuario son utilizados para llevar a cabo algún tipo de fraude.

El siguiente ejemplo o suceso puede ser útil para darnos cuenta de la importancia que tiene la seguridad de la información en este sector, o bien para entender lo vulnerable que puede llegar a ser. Según un informe que fue llevado a cabo por Kapersky Lab, el 28,8% de los ataques phising en todo el año 2014 fueran destinados conseguir datos financieros de usuarios, es decir estaban dirigidos al sector financiero.

- ISO/IEC TR 27016 (Publicada)

Hemos estado hablando de normas que aportan una seguridad de la información a la empresa, pero el objetivo principal de la mayoría de las organizaciones que trabajen con estas normas de la serie ISO 27000 será el de hacer dinero, generar dividendos, y lo que es aún más importante no perderlo con decisiones que pueden ocasionar perdidas monetarias.

Siempre que una organización considera la adquisición de un activo o la toma de una decisión se pregunta cuál es el coste que lleva asociado. Esta norma se encarga no solo de la toma de decisiones relativas a la seguridad de la información, sino también nos ayuda a entender las consecuencias económicas de esas decisiones.

- ISO/IEC TS 2017 (Bajo desarrollo)

La computación en la nube o “cloud computing” es un concepto que se aplica de forma amplia en la actualidad. La idea es que nuestra información se encuentra en una nube y nosotros podemos acceder a ella, es decir, esta información no se encuentra con nosotros, sino que está en unos servidores de internet que atienden a nuestras peticiones en cualquier momento. Este concepto reduce riesgos informáticos y costes.

Esta norma proporciona una serie de controles de seguridad orientados a la seguridad en la nube, recomendando cuales se deben utilizar, así como unas directrices a seguir en esta materia.

- ISO/IEC 27018 (Publicada)

Cuando hablamos de la información que nos permite identificar, contactar o localizar a una persona concreta, o que junto a otras fuentes de información nos permite hacerlo, nos referimos al concepto de información personal,

también denominado "Personally Identifiable Information" o PII según sus siglas en inglés.

Lo que en esta norma vamos a encontrar son directrices que tratan de proteger este tipo de información. Es aplicable a todo tipo de organizaciones, incluyendo empresas privadas y públicas, y entidades que se encuentren relacionadas con el gobierno. Esta norma también presenta unos controles de seguridad que son específicos para proteger la información personal.

- ISO/IEC TR 27019 (Publicada)

Nos encontramos con otro caso en el que una norma de la serie 27000 está enfocada a un sector especifico, en este caso está relacionada con los procesos de sistemas de control del sector de la industria energética.

De esta forma permite a las empresas y organizaciones que se encuentran o están relacionados con la industria energética, crear y utilizar un SGSI según los requisitos de ISO/IEC 27001. Es decir, nos indica de forma más detallada como este tipo de organizaciones deben abordar la implementación de un SGSI.

Detallando de forma más exacta el ámbito de esta normativa, podemos decir que se centra en los sistemas de control que son usados en la industria energética para realizar un seguimiento de la generación, transmisión, almacenaje y distribución de energía, en combinación con los controles que se implementen en base a la ISO/IEC 27001.

- ISO/IEC 27031 (Publicada)

Se centra en la continuidad del negocio tomando como base las TIC[11]. Es decir, es la norma que usaríamos si quisiéramos conocer los conceptos relacionados con las TIC, así como lo que podríamos considerar como métodos o procedimientos que nos ayuden a mejorar las TIC para poder sumar a la continuidad del negocio.

Podríamos preguntarnos cómo estas TIC pueden llegar a influir en la continuidad del negocio, pero solo tenemos que darnos cuenta de que hoy en día las TIC son algo que podemos encontrar en casi todas las empresas y que permiten aumentar el valor de sus activos y crear beneficios. En ciertos

[11] Las tecnologías de la información y la comunicación (TIC) se puede definir como un conjunto heterogéneo de herramientas, métodos y recursos tecnológicos empleados para crear, recabar, almacenar, gestionar y distribuir información.

momentos la continuidad de un negocio puede estar totalmente incompleta si no se considera una continuidad de las TIC.

- ISO/IEC 27032 (Publicada)

Enfoca sus directrices en la colaboración que debe existir en la organización, entre los miembros de la organización para poder llegar a reducir los diferentes riesgos en seguridad de la información. Básicamente nos dice que la existencia de una colaboración y coordinación dentro de la organización es algo vital para la existencia de una seguridad de la información.

Tomando como base estos conceptos, intenta mejorar la información de seguridad, seguridad en las redes, seguridad en Internet y en la información. De esta forma podremos estar preparados, monitorizar y responder ante ataques cibernéticos.

- ISO/IEC 27033 (Publicada)

Esta norma esta destinada a la seguridad en las redes, se centra en proteger toda la información que puede fluir a través de la red, como puede ser por ejemplo información que se encuentre en aplicaciones que trabajan no solo en nuestro dispositivo, sino que también trabajan en la red.

Pero no solo debemos fijarnos en las directrices o pasos a seguir para tener esta seguridad en las redes, sino que también es importante que prestemos atención a las personas que podríamos calificar como propietarios de estas redes. Es decir todas las personas que las utilizan, ya que estas personas son las más propensas a generar fallos de seguridad, muchas veces por imprudencias, como por ejemplo usar contraseñas simples o fáciles de adivinar que permiten a otros usuarios acceder a nuestra cuenta a través de la red.

- ISO/IEC 27034 (Publicada)

Esta norma trata otro de los aspectos particulares que demandan protección en una organización. Está destinada a la seguridad en aplicaciones informáticas que son utilizadas por las organizaciones, tanto las que son creadas por ellas como las que han sido creadas por terceros.

Está destinada al diseño, selección, especificación y aplicación de los controles de seguridad que utilizaremos para estas aplicaciones.

También trata los aspectos económicos que están relacionados con la utilización de controles de seguridad. Algo que tenemos que tener presente es que en una empresa pueden existir muchos tipos de aplicaciones que tienen que encontrarse definidos y diferenciados. Esta norma también trata la seguridad en estas aplicaciones dependiendo de su contexto.

- ISO/IEC 27035 (Publicada)

Cuando nos referimos al concepto de amenaza estamos hablando de cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema de información. En cambio, cuando nos referimos al concepto de incidente de seguridad nos referimos a la materialización de esa amenaza que tendrá un correspondiente impacto sobre la organización, el impacto sería la medición o valoración del daño que provoca en la organización.

Teniendo claro estos conceptos, que a menudo son confundidos, tenemos la norma ISO/IEC 27035 que se centra en la gestión de los incidentes de seguridad, en la gestión de la materialización de las amenazas.

Debemos tener claro que los controles de seguridad que implantemos con el SGSI siempre pueden fallar, no son algo perfecto. Esta norma habla de una serie de controles que podríamos destacar como muy específicos, son unos controles que aplicaban acciones correctivas que actúan ante impactos desfavorables y que nos proporcionan lecciones aprendidas.

Esto último es algo muy importante a la hora de llevar a cabo planes de seguridad de la información, aprender de los errores pasados y nunca cometer los mismos errores. De esta forma empezaremos teniendo un amplio margen de errores que con el tiempo iremos haciendo más pequeño, cerrando sus limites y trabajando cada vez mejor.

- ISO/IEC 27036 (Publicada)

Podríamos considerar una organización como una cadena que siguiera el esquema de la figura 2.2.1. En el comienzo de la cadena tenemos los proveedores, en el centro la empresa y al final de la cadena los clientes. ISO/IEC 27036 se centra en el inicio de esta cadena, en el proceso de suministro.

Las relaciones con los proveedores es una parte de la cadena en la que se comparte mucha información. La seguridad en este punto es algo importante,

no solo por razones de seguridad propias de la empresa, sino porque estamos utilizando información que puede contener datos de otras empresas, de nuestros proveedores. Además si no tuviéramos una protección sobre los datos relativos a nuestro suministro, otras empresas o terceros podrían hacerse con ellos y deducir qué es lo que vamos a hacer en el resto de la cadena organizativa.

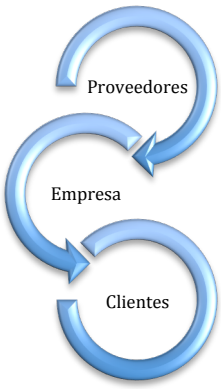

Figura 2.2.1 Cadena básica de una organización

Esta norma se centra en las relaciones con los diferentes proveedores de la organización.

- ISO/IEC 27037 (Publicada)

Esta norma se centra en las actividades que son necesarias para identificar, recopilar, consolidar y preservar la integridad de evidencias digitales[12]. Se intenta explotar el valor probatorio de las mismas , esta norma se destina a investigaciones forenses en las que participa un recurso electrónico o digital. Es decir, relaciona la seguridad de la información con las evidencias digitales. En este caso podríamos considerar que la información con la que trabajamos es esa evidencia digital.

La norma habla de evidencias digitales distinguiendo entre diferentes casos de procedencia de las mismas, como pueden ser dispositivos de almacenamiento, teléfonos móviles, tarjetas de memoria…

- ISO/IEC 27038 (Publicada)

Toda organización tiene en posesión información que no es conveniente que sea revelada a otras organizaciones. Uno de los puntos fuertes de esta norma es un proceso el cual denomina “redaction of the document” y que en

[12] El concepto de evidencia digital cubre cualquier tipo de información que se encuentre en formato digital y que pueda definir una relación entre el autor y un delito.

español sería la redacción del documento. Este proceso se centra en una modificación de ciertos documentos para proteger su información y dotarles de una seguridad de la información. Hablamos de eliminación de ciertas secciones, párrafos o frases. De esta forma podemos enviar documentos a otras organizaciones que se encuentren modificados y de esta forma no correr riesgos.

Algo que la propia norma destaca como importante es que aquella parte de la información que sea eliminada, sea eliminada de forma completa, es decir que no exista ninguna forma de recuperarla.

Una posible situación que nos permite concienciarnos de la situación de la que estamos hablando, de información que pensamos que ha sido eliminada de forma completa o que no hemos llegado a eliminar totalmente por error, podría darse en aquellos casos en los que una empresa simplemente oculte cierta parte de la información dejando ocultos iconos o elementos sin llegar a eliminarlos. Esto puede ser una vía para otras empresas o individuos para hacerse con la información.

- ISO/IEC 27039 (Publicada)

Algo que toda organización debe hacer es aprender de incidentes de seguridad que hayan causado un impacto en la organización para prevenir futuros errores de carácter similar. No deben preocuparse únicamente de cómo y cuándo ha ocurrido una intrusión, sino que deben conocer que vulnerabilidad del sistema fue usada para facilitar la intrusión y que medidas del tratamiento de riesgo se deberían usar para prevenir el mismo tipo de intrusión.

Esta norma nos ayuda a seleccionar, establecer y operar con IDPS[13] (es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos).

La norma define que para que se pueda obtener los máximos beneficios de este sistema, se necesita ser cuidadoso con la planificación e implantación de las operaciones, utilizando siempre la experiencia personal y una adecuada formación para la utilización de estos sistemas.

[13] IDPS son las siglas de “Intrusion Detection and Prevention Systems”, en español quiere decir sistemas de prevención y detección de intrusiones.

- ISO/IEC 27040 (Publicada)

Venimos hablando de muchas normas que tratan de proteger los datos de la información, esta norma se centra de nuevo en estos datos que pertenecen a la organización, solo que considerando esta vez el almacenamiento de los mimos.

Para muchas organizaciones, sus datos es el activo que más valora, ya que son la puerta de acceso a todos los campos en los que trabaja. Por esta razón es importante que se mantengan y almacenen de una forma eficaz y segura. Todo esto que estamos diciendo puede parecer muy sencillo, pero hay que tener algo en cuenta, el proceso se puede complicar si pensamos que el almacenamiento de datos debe estar coordinado con un acceso de forma sencilla y con una posibilidad de comunicar esta información entre dispositivos.

Nos da una orientación sobre cómo debemos gestionar el almacenamiento de datos, especificando la planificación, el diseño, implementación y documentación del proceso para llevarlo a cabo.

- ISO/IEC 27041 (Bajo desarrollo)

Una norma que vuelve a lidiar con aspectos relacionados con los incidentes de seguridad. En este caso nos referimos a la investigación de los propios incidentes de seguridad, pero debemos tener presente que siempre que queramos realizar una investigación sobre algún asunto, necesitamos seguir unos métodos, procesos o procedimientos que nos permitan hacerlo.

Nos ayuda a garantizar la competencia y adecuación de los métodos de investigación. Buscamos asegurar que los métodos y procesos que utilizamos para investigar incidentes de seguridad sean aptos.

Define la importancia de que el alcance, es decir los limites de la investigación de incidentes, quede bien definido y que se establezcan los requisitos, lo que queremos investigar.

- ISO/IEC 27042 (Bajo desarrollo)

Puede ser confundida fácilmente con la ISO/IEC 27037. Pero si recordamos, la norma ISO/IEC 27027 se encargaba de identificar, recopilar, consolidar y preservar la integridad de evidencias digitales, lo cual podríamos considerar como un proceso incompleto, ya que cuando trabajamos con evidencias

digitales en investigaciones forenses necesitamos llegar a algo más que almacenarlas de forma segura y eficiente.

Lo que esta norma nos proporciona son directrices para el análisis e interpretación de las evidencias digitales. Cuando trabajemos con una evidencia digital de una investigación se necesitará analizar y necesitaremos unos pasos o procedimientos que nos permitan hacerlo.

- ISO/IEC 27043 (Publicada)

Utilizar normas que definan pautas para investigaciones de incidentes permite que sea más fácil comparar, combinar y contrastar los resultados de tales investigaciones, incluso cuando es realizada por diferentes personas u organizaciones.

Es otra norma que se utiliza para la investigación de los incidentes de seguridad, trata los procesos forenses que están involucrados con las investigaciones de incidentes. Proporciona una serie de modelos para diferentes procesos de investigación aplicables a diferentes escenarios de investigación, en los cuales existe de por medio una evidencia digital. En resumen, esta norma internacional proporciona una visión general de todos los principios y procesos de investigación de incidentes sin describir detalles particulares.

- ISO/IEC 27044 (Bajo desarrollo)

Se basa en la combinación de la gestión de eventos de seguridad con la seguridad de la información, esto se traduce en SIEM[14]. A veces es necesario hacer revisiones durante un largo periodo de tiempo para poder llegar encontrar incidentes, los sistemas SIEM nos proporcionan ayuda recopilando datos, analizándolos e informando.

Es decir, nos ofrece alertas de seguridad en tiempo real. La parte que podríamos considerar como SEM se encarga de realizar una supervisión en tiempo real, realizar una correlación de eventos de seguridad y notificaciones.

La parte SIM se encarga de almacenar, analizar y comunicar de forma segura los datos.

[14] SIEM son las siglas de “Security Information and Event Management” .

- ISO/IEC 27799 (Publicada)

Esta es otra norma de la serie ISO 27000 que se encuentra destinada a un sector en concreto, el sector sanitario.

Los controles y directrices que ofrece se encuentran ajustados a las necesidades de una organización que trabaje en el ámbito de la salud. Como otras normas intenta dar una seguridad de la información en todos los aspectos: cualquier sea la forma en la que venga representada (palabras, números…), todos los medios que se usen para almacenarla y las formas que se usen para enviarla.

Una aplicación práctica de esta norma podría ser su utilización en un hospital a la hora de proteger los datos personales de los pacientes con los que cuente.

CAPITULO 3.

ISO/IEC 27001

3. ISO 27001

3.1. Introducción

Los organismos nacionales miembros de ISO o IEC disponen de un comité técnico conjunto en tecnologías de la información (ISO/IEC JTC 1), las reglas o normas son elaboradas conforme al procedimiento establecido en la parte de las directivas ISO/IEC. De esta manera el comité técnico elabora un proyecto de normas que se somete a votación de los organismos miembros. Si se obtiene una mayoría del 75% la norma pasa a ser publicada.

Podemos decir que la base de esta normativa es la de establecer, implementar, mantener y mejorar de una forma continua un sistema de gestión de seguridad de la información que haya sido implementado en la empresa, todo esto lo hace a través de la exposición de una serie de requisitos. Un sistema de gestión de seguridad de la información es un sistema que nos permite mantener una confidencialidad, integridad y disponibilidad de toda la información, para lograrlo necesitamos implementar un proceso de gestión de riesgos y de esta forma conseguiremos otorgar una confianza a las partes interesadas del proceso.

Llegado a este punto, nos damos cuenta que en el momento que una empresa u organización decide adoptar un sistema de gestión de seguridad de la información, dentro de los diferentes procesos que la componen, lo que realmente esta haciendo no es más que tomar un decisión estratégica como cualquier otra que podría tomar para otro tipo de materia. Este apartado es importante, ya que puede condicionar la forma en la que la empresa actúa, al igual que cualquier otro sistema de gestión, un sistema de gestión de seguridad de la información debe estar orientado a las necesidades que la organización presente.

Por todas estas razones la normativa ISO 27001 que presentaré en los siguientes puntos, recalca que un sistema de gestión de seguridad de la información debe estar integrado con los procesos de la organización, así como con la estructura global, y que el concepto de seguridad de la información se debe considerar durante el diseño de los procesos, de los sistemas de información y de los controles.

Un sistema de información se encarga de entregar la información oportuna y precisa con la presentación y formato adecuados, a la persona que lo necesita dentro de la organización para tomar la decisión o realizar alguna

operación y justo en el momento en que esta persona necesita disponer de dicha información.

Cuando se pretende comprobar o poner a prueba la capacidad de una organización para cumplir con sus requisitos de seguridad, se puede utilizar esta norma, de una forma tanto externa como interna.

Las consideraciones que trataremos en los puntos se ajustan al esquema planteado por la ISO/IEC 27001, sin perjuicio de realizar no un simple análisis de normativa, sino también comentar y considerar el valor que la misma tiene para un sistema de gestión de seguridad de la información en el ámbito de una organización, por lo cual se introducirán ejemplos y situaciones posibles.

3.2. Objeto y campo de aplicación

Partiendo de los objetivos básicos de la ISO (sistema de gestión de seguridad de la información en el contexto de la organización y tratamiento de riesgos de seguridad de información a la medida de las necesidades de la organización) se matiza que los requisitos de la norma son aplicables a todas las organizaciones, pero no se acepta la declaración de conformidad con la norma si se excluye alguno de los requisitos de los capítulos 4 y 10 de la norma.

Con todo esto podríamos decir que esta norma tiene dos objetivos básicos en materia de seguridad[15] de la información, que consisten en establecer dos tipos de requisitos:

- Requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información.

- Requisitos para la apreciación y el tratamiento de los riesgos de seguridad de la información a las medidas de las necesidades de la organización.

[15] Entendemos por seguridad la reducción de riesgo o la confianza en algo o alguien, el termino se puede aplicar a muchos campos, entre ellos el de la información.

3.3. Contexto de la organización

La organización tiene activos (cualquier bien con valor para ella). Uno de esos activos son los datos significativos (información) que aseguran el correcto funcionamiento del negocio al que se dedica la organización, por ello, ésta debe proteger frente a riesgos y amenazas a ese activo de información.

La organización debe tener claro los aspectos internos y externos de la organización, los cuales pueden afectar a la capacidad de lograr resultados de un sistema de gestión de seguridad de la información. De esta forma será capaz de lograr los propósitos pertinentes en relación a un sistema de gestión de seguridad de la información. A tal efecto, debe:

- Como en todo proyecto debe determinar las partes interesadas [16] relevantes y recopilar los requisitos de esas partes interesadas también relevantes. Un compromiso con las partes interesadas constituye la oportunidad para que una organización pueda conocer sus problemas e inquietudes y además puede llevar a que el conocimiento sea adquirido por ambos lados afectos de poder influir en las opiniones y percepciones. Algunos ejemplos de partes interesadas pueden ser: clientes, proveedores, empleados, instituciones, medios de comunicación, inversores...

- Recopilar los requisitos de las partes interesadas tiene por objeto llegar a un acuerdo en el proyecto de implementación del SGSI para satisfacer las necesidades de todas las partes interesadas en materia de seguridad de la información. Es necesario llegar a un acuerdo para satisfacer las necesidades de todas las partes interesadas ya que de no ser así conllevaría implicaciones negativas.

Por ejemplo, un ingeniero del área de producción puede presentar la necesidad de cifrar todos los datos que se tomen en los procesos de configuración del taller, esos procesos que permiten establecer el orden en el que los pedidos se procesan en el taller, ya que son datos que suele exportar fuera de la organización. Los trabajadores que operan en las máquinas o equipos informáticos del taller pueden considerar que cifrar todos estos datos puede llevar demasiado tiempo, dado que con la pequeña

[16] Las partes interesadas (también llamados partes involucradas, interesados, stakeholders) son las personas, grupos, equipos u organizaciones que están interesados en la realización del proyecto, o que podrían afectar o ser afectados por una decisión, actividad o resultado del proyecto de implementación del SGSI.

cantidad de pedidos que llegan al taller es algo innecesario, y que con los equipos que disponen no se puede realizar con facilidad este tipo de control.

Teniendo en cuenta las necesidades que tienen ambas partes en cuanto a este control de cifrado de datos se llegará a un acuerdo, que podría ser por ejemplo no cifrar todo el conjunto de datos o simplemente cifrar los datos con una frecuencia elevada (mensualmente).

Es decir, escuchamos las necesidades que presentan cada una de las partes interesadas en el proyecto de implementación del SGSI y combinándolas intentamos conseguir unos requisitos, que son esas mismas necesidades no siempre satisfechas totalmente, ya que muchas de ellas son opuestas.

- Determinar límites y aplicabilidad del sistema para constituir su alcance.

Cuando hablamos de constituir el alcance nos referimos a determinar el trabajo necesario para cumplir con los objetivos del proyecto de implementación del SGSI, en esta tarea deben considerarse los requisitos antes referidos, así como las relaciones y dependencias entre las actividades realizadas por la organización y las que se realizan por otras organizaciones. De esta forma nos aseguramos que el alcance contenga todo el trabajo requerido y solo el trabajo requerido.

El alcance debe estar disponible como información documentada para tenerlo siempre presente y poder recurrir a él.

Partiendo de este alcance, esta norma ISO determina los requisitos para establecer, implementar , mantener y mejorar el sistema de gestión de seguridad de la información, incluyendo el tratamiento de riesgos.

Debemos mencionar las clases de activos de información que hay que tener en cuenta a la hora de trabajar con un SGSI:

- Servicios o procesos de negocio de la organización.
- Datos que son manejados dentro de la organización como núcleo del sistema y los demás activos se encargan de darles soporte.
- Aplicaciones (software).
- Equipo informático (hardware).

- Personal.
- Redes de comunicación.
- Soporte de información.
- Instalaciones.
- Activos intangibles.

También debemos tener en cuenta una diferencia que puede dar lugar a confusión en el contexto de la organización, estamos hablando de la diferencia entre documento y registro. El documento recoge la información y su medio de soporte, y el registro es el documento que indica los resultados obtenidos o que proporciona evidencia de las actividades desempeñadas.

Un ejemplo muy común y que se escapa del ámbito de la seguridad de la información, pero que nos permite entender la diferencia entre documento y registro es el de la compraventa de un inmueble, donde el documento consta de una escritura de compraventa y el registro de la propiedad proporciona evidencia de que dicha propiedad pertenece a quien lo ha comprado.

Según lo expuesto, en el contexto organizativo, la seguridad de la información es el conjunto de medidas preventivas y correctivas que permiten proteger la información en todas sus variedades.

Para entender de una forma más clara las variedades de tipos información con las que puede contar una organización, podemos poner el siguiente ejemplo: imaginemos la situación de una organización que tenga que trabajar con información que provenga de diferentes fuentes, variedades o tipos. Una organización podría estar trabajando con información escrita a mano, impresa, enviada vía correo electrónico, mostrada en videos corporativos para presentaciones, incluida en su página web, etc…

La protección de la información exige confidencialidad[17], disponibilidad[18] e integridad[19].

3.4. Liderazgo

En este apartado la norma explica la importancia de que exista un compromiso de la dirección, como en todo proyecto, y que esta dirección sea capaz de demostrar su liderazgo. Desarrolla una serie de requisitos, en los que expone las diferentes tareas o matices a tener en cuenta.

Desde el punto de vista de la Organización industrial parecen importantes los siguientes requisitos:

- La alta dirección debe asegurar que se establezcan la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización. Este punto es importante dado que todo debe ir en consonancia con la estrategia de la organización.

- Como ya hemos dicho antes, una organización posee diferentes procesos que están interrelacionados unos con otros y que interactúan entre si, por lo tanto, los requisitos con los que cuente el sistema de gestión de seguridad de la información debe estar integrado con esos procesos.

- Asegurarse de que existen recursos para poder llevar a cabo este sistema de gestión de seguridad de la información.

La política de seguridad de la información debe estar siempre disponible y comunicarse.

Basándonos en la política de seguridad de la información, que debe ser establecida por la alta dirección, la norma determina una serie de puntos en los que especifica los requisitos con los que debe contar un sistema de gestión de seguridad de la información.

Otra tarea importante con la que se va a encontrar la alta dirección además de mostrar un liderazgo y compromiso, es la de tener la seguridad de que las

[17] La confidencialidad consiste en dar acceso a la información solamente a aquellas personas o sistemas autorizados.
[18] La disponibilidad consiste en prestar acceso a la información y a los sistemas a las personas autorizadas en el momento en el que lo requieran.
[19] La confidencialidad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

responsabilidades, así como las autoridades para los diferentes roles pertinentes a la seguridad de la información están asignados y se comunican dentro de la organización.

Encuentro oportuno explicar la diferencia que existe entre los términos anteriormente nombrados, ya que en un ámbito coloquial son normalmente confundidos y tergiversados.

- Rol. Es la parte de este sistema de gestión de seguridad de la información de la que una persona es responsable.

- Responsabilidad. El trabajo que se espera que realice un miembro del equipo a fin de completar las actividades.

- Autoridad. Derecho a aplicar los recursos disponibles, tomar decisiones y firmar aprobaciones.

Si no existiese esta responsabilidad y autoridad, no se podría tener la seguridad de que nuestro sistema de gestión de seguridad de la información se ajusta a los requisitos que esta norma dicta, ni se podría informar a la alta dirección sobre el comportamiento del sistema.

3.5. Planificación

Es importante que a la hora de planificar todo el sistema de gestión de seguridad de la información en su conjunto tengamos en cuenta dos aspectos:

- Por un lado debemos tener en cuenta el alcance que hemos definido anteriormente, es decir ese trabajo necesario para cumplir con los objetivos del proyecto de implementación del SGSI.

- Y por otro lado, la determinación de riesgos y oportunidades que son necesarios tratar. En general se maximizarán las oportunidades y se minimizarán los riesgos.

Podemos establecer dos partes claramente diferenciadas, una primera parte en la que realizamos la apreciación de los riesgos y una segunda parte en la que realizamos el tratamiento de los mismos.

Con respecto a la apreciación:

- Debemos definir unos criterios sobre riesgos de seguridad de la información, tanto criterios para aceptar el riesgo, como criterios para poder realizar las apreciaciones de los riesgos[20]. Cuando el equipo no consigue encontrar ningún tipo de estrategia, el riesgo se debe aceptar, estos riesgos se denominan aceptados o residuales. A su vez, se puede trabajar con ellos de forma pasiva o activa, pasiva si son riesgos poco importantes sobre los cuales no se requiere ninguna acción, y activa si se consideran importantes. Trabajar de forma activa sería actuar con planes de contingencias y reservas para contingencias.

- Identificar tanto los riesgos que actúan sobre el alcance del sistema de gestión de seguridad de la información, como los ''dueños de estos riesgos''[21]. En muchos casos hablamos también de "dueños de la acción del riesgo"[22]. Para realizar esta identificación de riesgos podemos usar técnicas como por ejemplo: tormenta de ideas, análisis DAFO y listas de chequeo.

- Partiendo de todos estos riesgos identificados tenemos que analizarlos, valorando de forma realista su probabilidad y los niveles de impacto de esos riesgos si llegan a materializarse en un incidente de seguridad.

- Por último solo queda evaluarlos utilizando los criterios establecidos. De esta manera podremos conocer la importancia de los mismos y priorizar su tratamiento, o determinarlos como residuales.

Conviene plantearse situaciones posibles que puedan producirse en cuenta a la vulnerabilidad, las amenazas y la relación entre ambas. Ya que a la hora de identificar riesgos puede ser muy importante conocer de que vulnerabilidad proceden ciertas amenazas. En los siguientes cuadros se exponen ejemplos relativos a posibles vulnerabilidades, amenazas y relaciones entre ellas.

[20] Los criterios que permiten realizar las apreciaciones de los riesgos son aquellos propios de la organización que delimitan los valores limite de probabilidad e impacto que definen la importancia de un riesgo.
[21] El dueño del riesgo es el responsable del riesgo y de planificar las respuestas a los riesgos.
[22] El dueño de la acción del riesgo es el responsable de implementar con éxito los planes de respuesta a los riesgos identificados y de hacerlo en el momento apropiado.

Con respecto a la vulnerabilidad la debilidad de una activo puede ser explotada por una o más amenazas y estas vulnerabilidades pueden ser intrínsecas o extrínsecas a la organización. Por ejemplo si el tipo de vulnerabilidad proviene del hardware puede haber un problema de mantenimiento insuficiente o que sea fácilmente portable, de esta forma nuestra información puede ser robada más fácilmente. Si proviene del software puede que el defecto surja de falta de documentación para un correcto uso o de interfaces que lo compliquen, se podrían cometer errores a la hora de usarlo que deriven en una publicación de información privada. Por último, si la vulnerabilidad fuese de tipo personal podemos encontrarnos ante una formación insuficiente o ante una falta de capacidad.

En cuanto a las amenazas, entendidas como cualquier situación que pueda producir daño a los elementos de la información. Si la amenaza es un daño físico podemos pensar en posibles daños por fuego o por agua, si es un desastre natural podemos hablar de terremotos e inundaciones, y si el tipo de amenaza es una perdida de servicios esenciales podría ser un corte de luz y falta de aire acondicionado en un área tropical o falta de calefacción en un área extremadamente castigada por el frio.

Pongamos ahora en contacto posibles vulnerabilidades que permitirían a algunas amenazas materializarse en un incidente de seguridad. Por ejemplo, de un procedimiento de backup mal realizado puede surgir una perdida de información. Del hecho de no revisar los derechos de acceso puede producirse un acceso no autorizado, por ejemplo de personas que ya no están en la organización. Si los datos no están cifrados puede surgir una apropiación indebida de información, si se usa un software pirata pueden aparecer algún tipo de malware (gusanos, troyanos y virus). Si no se han segregado convenientemente las tareas entre las personas de la organización puede haber usos no correspondientes a la responsabilidad de una persona, y dar lugar a algo tan evidente como que una oficina esté desprotegida. Por último podemos considerar que sin tener vigilancia en la organización, nuestra información puede ser objeto de robo.

También es importante relacionar las amenazas con faltas de integridad, confidencialidad y disponibilidad.

Podemos poner algunos ejemplos de amenazas que si se materializaran en incidentes de seguridad podrían afectar a la confidencialidad, integridad o disponibilidad. Sobre la confidencialidad puede darse una invasión de la privacidad de usuarios, clientes o empleados o una fuga de información confidencial. Sobre la integridad podrían ocurrir alteraciones en los datos de información accidentales o intencionados. En el caso de la disponibilidad podemos considerar una degradación del rendimiento de los equipos que lleguen incluso a interrupciones o faltas del servicio que nos brindan estos equipos.

Con respecto al tratamiento:

Debe desarrollar un plan de tratamiento de riesgos de seguridad de la información y que por parte de los dueños de esos riesgos dicho plan sea aprobado, así como aceptados todos esos riesgos que tienen carácter residual. Antes de esto, la normativa marca como importante que se hayan seleccionado todas las opciones adecuadas teniendo en cuenta los resultados del paso anterior (la apreciación de los riesgos), determinar controles sin omitir controles necesarios, para ello se deben observar los controles que dispone esta norma en el anexo A, y que se haya elaborado una ''Declaración de Aplicabilidad'' en la que se recojan los controles necesarios, justificación de inclusiones (implementadas o no) y la justificación de las exclusiones.

Los objetivos de seguridad de la información se establecen en las funciones y niveles pertinentes y conservándolos en información documentada.

Los objetivos de control[23] y los controles[24] vienen determinados en el Anexo A de la ISO/IEC 27001. Tales controles no son exhaustivos, es decir pueden establecerse objetivos de control y controles adicionales.

Los controles pueden ser preventivos, de investigación o correctivos.

- Un control preventivo trata de evitar la aparición de problemas.

[23] Un objetivo de control puede definirse como la descripción de lo que se quiere lograr como resultado de la utilización de un control.
[24] Un control de seguridad de información es un método para gestionar un riesgo relativo a la seguridad de la información.

- El control de investigación sirve para buscar e identificar anomalías en el sistema de seguridad de la información.

- Los controles correctivos actúan una vez que ha ocurrido el hecho e intentan corregir las consecuencias.

Por ejemplo algunos controles preventivos podrían ser: publicar la política de seguridad de la información de la organización para que sea conocida por los miembros de esta, hacer que socios y empleados firmen acuerdos de confidencialidad, mantener contactos apropiados y frecuentes con los grupos de especialistas en seguridad de la información o contratar solo personal cualificado.

Algunos controles de investigación son los siguientes: controles de ecos en las telecomunicaciones, utilización de cámaras de video, sistemas de detección de intrusiones (IDPS), alarmas de calor, humo, fuego o riesgos relacionados con el agua.

Para controles correctivos podríamos pensar en: los procedimientos de emergencia (copias de seguridad de datos en caso de apagón eléctrico), implementar planes de formación para saber cómo actuar en casos de emergencia, y establecer líneas o redes en la organización que faciliten la comunicación entre personas de la misma para reportar fallos.

3.6. Soporte

La organización tiene dos tareas asignadas en cuanto a los recursos y en base al establecimiento, implementación, mantenimiento y mejora del sistema de gestión de seguridad de la información, debe determinar los recursos y como poder proporcionarlos.

La organización debe determinar la competencia necesaria de las personas que realizan un trabajo que afecta a su desempeño en seguridad de la información.

Al igual que hicimos en apartados anteriores es conveniente dar una definición, lo más clara posible de qué es competencia. Competencia es la habilidad y capacidad para completar las actividades.

Se tiene que tener una seguridad de que las personas con las que trabajamos son competentes (tienen educación, formación y experiencia) y que puede ser necesario tener que llevar acciones para obtener esa competencia que necesitamos.

La parte de soporte la cerramos hablando de la importancia de la Información documentada. A la hora de hablar de información documentada tenemos que tener en cuenta los dos tipos de información que vamos a almacenar:

- La requerida por la norma ISO.

- La que haya determinado la organización, que es necesaria para poder obtener una eficacia en el sistema de gestión de seguridad de la información.

En su creación debe determinarse la identificación, descripción, el formato, su revisión y su aprobación. En su control debe asegurarse que está disponible y protegida adecuadamente.

3.7. Operación

Se refiere a la implementación del sistema de gestión de seguridad de la información que ya ha sido creado y al plan de tratamiento de riesgos.

Se deben efectuar apreciaciones de riesgos a intervalos planificados.

Al final del presente capítulo veremos como puede implementarse un SGSI haciendo uso del ciclo PDCA[25].

[25] PDCA son las siglas de Plan Do Check Act que en español quiere decir Planificar Hacer Verificar Actuar.

3.8. Evaluación del desempeño

Sin perjuicio de las determinaciones que debe realizar la organización para el seguimiento, medición y análisis para obtener la evaluación, se prevén auditorias internas a intervalos planificados para comprobar no solo si se cumplen los requisitos de la norma y los establecidos por la organización, sino también para controlar si el sistema está implementado y mantenido de forma eficaz.

También a intervalos planificados la revisión del sistema debe ser efectuado por la alta dirección cerrando un circulo que comienza con la determinación del sistema de gestión apropiado a la empresa y que no excluye posibles mejoras. Las salidas de revisión por la dirección se enmarcan en la figura 3.8.1.

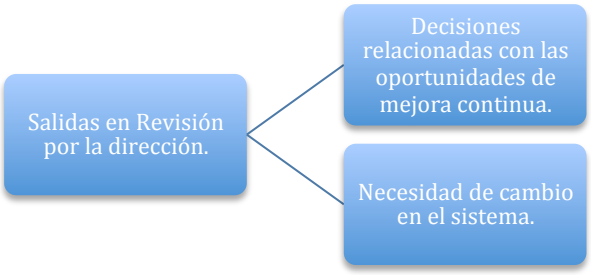

Figura 3.8.1 Salidas de revisión por la dirección

3.9. Mejora

Ante una no conformidad debe reaccionarse con acciones para controlarla y corregirla y hacer frente a las consecuencias que esto conlleva.

Como mejor se pueden eliminar y prever futuros fallos es actuando sobre la propia causa del fallo, con esto quiero decir, eliminar la raíz del problema para asegurar que no volverá a ocurrir.

Además de establecer estas causas de la no conformidad es necesario la determinación de no conformidades similares, o que potencialmente pueden ocurrir. Con esto logramos eliminar la no conformidad así como estar seguros de que no suceda en otra parte.

La organización debe aplicar una mejora continua al sistema de gestión de seguridad de la información.

3.10. Implementación un SGSI haciendo uso del ciclo PDCA

El ciclo Deming, también conocido como ciclo PDCA, se constituye como una de las principales herramientas para lograr la mejora continua en las organizaciones o empresas que desean aplicar medios eficientes en los sistemas de gestión.

La figura 3.10.1 describe el funcionamiento del ciclo PDCA y un resumen de los aspectos más representativos en cada una de las fases del ciclo.

Figura 3.10.1 Ciclo PDCA con aspectos más representativos del ciclo

Como es lógico antes de plantearnos las cuatro partes del ciclo PDCA debe tenerse en cuenta la organización sobre la que actuamos, esto es, deberemos definir en función de las características de dicha organización, y de su negocio, localización, activos y tecnología el alcance y los límites del SGSI. Debemos tener en cuenta que la ISO/IEC 27001 es suficientemente flexible en esta materia a la hora de ser aplicable a distintas organizaciones, ya que

es una norma dirigida a cualquier organización independientemente de su tamaño y tipo.

Lo dicho anteriormente nos servirá para determinar el alcance del SGSI según los límites de la organización, los límites de los sistemas de información, su ámbito y límites físicos, la extensión del ámbito de aplicación y sus posibilidades de cambio.

El ciclo PDCA puede aplicarse a cualquier sistema de gestión con el que trabaje nuestra organización, esto no excluye la aplicación que tendría en un SGSI. Lo que quiere decir que se puede aplicar a la hora de desarrollar el proyecto de implementación de un SGSI según la norma ISO/IEC 27001. En los siguientes fases se relaciona las diferentes fases del ciclo PDCA con los conceptos que hemos definido en los apartados anteriores y que son los requisitos que detalla la norma ISO/IEC 27001.

- **Primera fase. Planificar**

Entendemos por planificar el desarrollo de las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del sistema de gestión dentro del alcance fijado para el mismo.

Dentro de esta fase del ciclo del PDCA destacamos los conceptos de la norma ISO/IEC 27001 que se realizan en esta fase del ciclo:

- Definir el alcance del SGSI.
- Definir la política de seguridad.
- Establecer metodología de la evaluación de riesgos. Algunas metodologías de evaluación de riesgos son las siguientes:
  - Magerit usada en España.
  - Octave usada en Estados Unidos.
  - Cramm usada en Reino Unido.
  - Ebios usada en Francia.
  - Tra usada en Canada.

- Inventariar activos.
- Identificar vulnerabilidades y amenazas sobre los activos.
- Identificar impactos.
- Analizar y evaluar riesgos.
- Seleccionar controles.

- **Segunda fase. Hacer**

Se trata de desplegar las actividades concretas de implementación del sistema. Las actividades o conceptos de la norma ISO/IEC 27001 relativos a esta fase del ciclo PDCA son lo siguientes:

- Definición del plan de tratamiento de riesgos.
- Implementación de dicho plan.
- Implementación de controles.
- Operar con el SGSI.

- **Tercera fase. Verificar**

Se persigue la revisión del SGSI para evidenciar el cumplimiento de los requisitos de la norma. Para ello deben determinarse objetivos de medición, porque demasiadas medidas pueden distorsionar el enfoque de una organización y olvidarse de lo que es verdaderamente importante.

Dentro de esta fase del ciclo del PDCA destacamos las actividades o conceptos de la norma ISO/IEC 27001 que se realizan en esta fase del ciclo:

- Revisar el SGSI.
- Medición de la eficacia de los controles de seguridad de la información.
- Revisar riesgos residuales.
- Realización de auditorias internas del sistema.

- Asegurarse de que los eventos de seguridad son detectados e identificados.

- **Cuarta fase. Actuar**

Consiste en auditar e implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la norma.

Las actividades de la norma que se refieren a esta fase del ciclo PDCA son los siguientes:

- Implementar mejoras.

- Adopción de acciones correctoras.

- Llevar a cabo acciones preventivas.

- Comprobar la eficacia de las acciones.

Lógicamente el objetivo y finalidad de todas estas fases es obtener la certificación a través de la cual un tercero garantiza por escrito que el sistema cumple los requisitos establecidos por la normativa vigente.

CAPITULO 4.

FISMA

4. FISMA

4.1. Introducción

Como podemos considerar que en Estados Unidos existen dos marcos normativos o fuerzas más relevantes en materia de seguridad de la información, que han surgido de forma más destacada en ese país.

- Por una parte tenemos la normativa sobre la que hemos estado hablando en los apartados anteriores, las normas relativas a la serie ISO 27000. Esta normativa es utilizada por organizaciones y empresas que trabajan en un ámbito comercial.

- El segundo marco importante que cabe diferenciar y sobre el cual desarrollaremos los siguientes puntos, es la normativa que usan las agencias federales en los Estados Unidos, para cumplir con todos los requisitos que se establecen en FISMA y que ha sido desarrollada por NIST.

En Estados Unidos existen algunas otras normativas que se centran en una serie de activos de información muy particulares y específicos, por lo que podemos decir que cuando una organización quiere proteger todos sus activos, estas normativas deben estar integradas en un marco mucho más general para cumplir con los requisitos de las necesidades de la organización. Nos centraremos en una normativa que conforma este marco general de gestión de la seguridad de la información.

Por ejemplo alguna de las normativas que son usadas en Estados Unidos y que buscan un propósito muy particular es PCI DSS[26]. Respecto a esta última normativa, se ha formado un comité denominado PCI SSC (Payment Card Industry Security Standards Council) y que esta compuesto por el conjunto de compañías de tarjetas tanto de crédito como de debito, más importantes. Este comité lo que ha hecho ha sido desarrollar una guía que permite asegurar los datos de las tarjetas de crédito y débito, con el objetivo principal de evitar estos famosos fraudes.

[26] "Payment Card Industry Data Security Standard", que en español quiere decir Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago.

4.2. ¿Qué es NIST?

"NIST (Instituto Nacional de Estándares y Tecnología) una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida."

Desde 1901 hasta 1908 este instituto fue denominado Oficina Nacional de Normas (NBS por sus siglas del inglés National Bureau of Standards).

4.3. ¿Qué es FISMA?

La Ley Federal de Gestión de Seguridad de la Información de 2002 ("FISMA", Federal Information Security Management Act) es una ley federal de los Estados Unidos y fue promulgada en 2002. En esta ley se habla de la importancia que tiene la seguridad de la información para los intereses tanto económicos como de seguridad nacional de los Estados Unidos. Esta ley nos habla de desarrollar, documentar e implementar un programa que nos aporta una seguridad en la información y en los sistemas de información que están apoyando las diversas operaciones de la empresa, así como en sus activos, bien los que son gestionados por otra agencia, contratista o bien los que proceden de otra fuente.

Tal como se establece en FISMA, NIST, el instituto que hemos nombrado en el apartado anterior, será el encargado o responsable de desarrollar las normas, diferentes directrices, métodos y técnicas para poder así prestar una seguridad de la información en los dos aspectos fundamentales que marca FISMA respecto a una agencia federal, que son los activos y las operaciones de la misma.

Teniendo en cuenta qué es FISMA y qué es NIST podemos decir que el ISMS (Information Security Management System) descrito por NIST surgió como respuesta a esta Ley Federal de Gestión de Seguridad de la Información de 2002.

NIST tiene asociada la tarea de realizar el denominado "Federal Information Security Management Act (FISMA) Implementation Project", es decir, el proyecto de implementación de FISMA, el cual desarrollaremos en los siguientes apartados.

Cabe destacar que los estándares y normativa desarrollada por NIST son utilizados por agencias federales en Estados Unidos, empresas contratistas y todos aquellos que formen parte de la denominada ''Critical infrastructure''[27], que incluye empresas de servicio público (eléctricas, nucleares…), salud pública y servicios de emergencia, información y telecomunicaciones, defensa nacional, banca y finanzas, correo, transporte, agricultura, agua y comida, y la industria química para cumplir con los requisitos dispuestos en la ley.

Todo esto quiere decir que si quieres trabajar para el gobierno de Estados Unidos debes cumplir con los requisitos que han sido desarrollados por NIST.

4.4. Proyecto de Implementación de FISMA

Haremos una breve introducción para conocer en qué consiste este proyecto de implementación de FISMA desarrollado por NIST, hablaremos de su visión y de a qué está dirigido.

- Respecto a la visión: Se intenta apoyar tanto la implementación como el cumplimiento de la Federal Information Security Management act mediante el desarrollo de una serie de normas y directrices de seguridad.

Es decir, NIST va a ser el encargado de implementar esa ley usando una serie de normas y directrices que el mismo desarrolla.

Hablando de estas normas y directrices encontramos:

- Normas cuyo uso está destinado a poder clasificar tanto los sistemas de información como la propia información en si misma.

- Normas que establecen los requisitos mínimos de seguridad para los sistemas de información, así como para la propia información.

- Una guía para poder seleccionar los diferentes controles de seguridad de la información más apropiados para los sistemas de información.

- Guía para evaluar los controles de seguridad en los sistemas de información y para determinar la efectividad de estos controles.

- Guía para autorizar la seguridad de los sistemas de información.

[27] "Critical infrastructure" quiere decir infraestructura crítica, y son todos los activos que son esenciales para el funcionamiento de una economía y una sociedad.

- Guía para monitorizar los controles de seguridad definidos y la autorización de seguridad de los sistemas de información.

Respecto a qué está dirigido:

- Establecer un nivel de seguridad para las agencias federales y contratistas que apoyan al gobierno federal.

- Proporcionar una aplicación de los controles de seguridad más coherente y rentable a través de la infraestructura tecnológica de la información federal.

- Evaluaciones de los controles de seguridad mucho más coherentes comparables y repetitivas.

- Sistemas de información que son más seguros dentro del gobierno federal, incluyendo la denominada “critical infrastructure”.

El proyecto de implementación de FISMA se estableció en Enero del año 2003, con el fin de definir varias normas clave de seguridad y directrices demandadas por la legislación.

CAPITULO 5.

MARCO DE GESTIÓN DEL RIESGO PERTENECIENTE A NIST

5. Marco de Gestión del Riesgo perteneciente a NIST

La gestión de los riesgos es un pieza clave en un programa de seguridad de la información, nos proporciona un marco que nos permite seleccionar los controles de seguridad que venimos hablando y que son adecuados para nuestro sistema de información. Unos controles que nos permiten proteger los activos y operaciones de la organización como ya hemos dicho antes.

Existen una serie de actividades en este marco de gestión que se desarrollan en forma de ciclo, establecidas en diferentes pasos, como podemos ver en la figura 5.1 (en la figura 5.2 podemos ver el mismo ciclo con sus correspondientes publicaciones). Son actividades que se encuentran relacionadas con la gestión del riesgo de la organización, es decir forman el marco de gestión del riesgo, todas estas actividades tienen una vital importancia dentro de un programa de seguridad de la información y pueden ser aplicadas a sistemas de información que se consideren nuevos como a otros que no lo son.

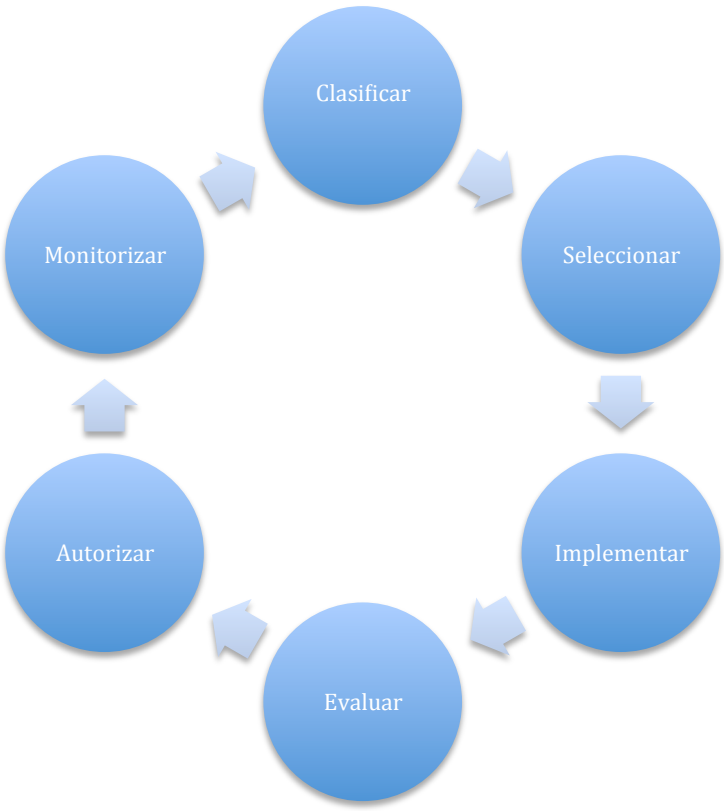

Figura 5.1 Ciclo de actividades del marco de gestión del riesgo

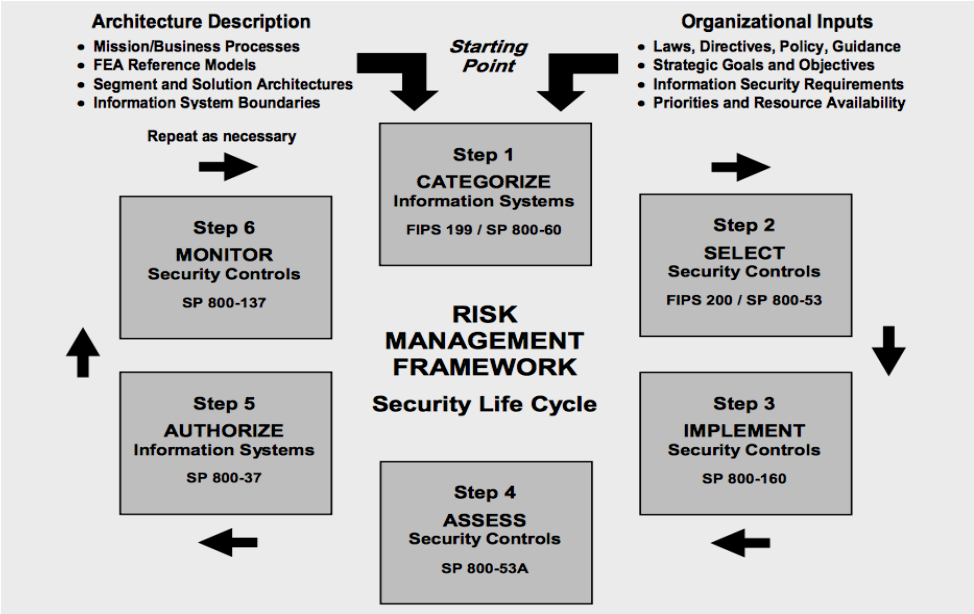

Figura 5.2 Ciclo de actividades y publicaciones del marco de gestión del riesgo

5.1. Primer paso: Clasificar los sistemas de información

En este primer paso nos dedicaremos a clasificar o categorizar tanto nuestro sistema de información como la información que este sistema se encarga de procesar o tratar, almacenar y transmitir, todo esto lo haremos mediante un análisis de impacto.

FISMA encomienda a NIST diferentes tareas en este aspecto:

- Debe desarrollar una serie de normas que permitan categorizar tanto sistemas de información, como información para poder llevar a cabo este primer paso. Todo esto esta dirigido a proporcionar unos niveles adecuados de seguridad de la información de acuerdo a un rango de niveles de riesgo.

- Debe desarrollar unas directrices que sean capaces de relacionar los diferentes tipos de sistemas de información o información con una categoría.

- Debe establecer unos requisitos de seguridad mínimos para los sistemas de información como para la información.

La primera de estas tareas viene expuesta en **FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems** (Normas para la categorización de información federal y sistemas de información). Toda esta categorización se basa en el impacto potencial que habría en una organización, si ocurriesen unos eventos o sucesos que pusieran en peligro a los sistemas de información y a la información, que se necesitan por la organización correspondiente para llevar a cabo su misión, cumplir con sus diferentes responsabilidades legales y mantener su funciones diarias. A la hora de realizar la evaluación del riesgo de la organización se usará la categorización junto con las vulnerabilidades y amenazas.

Durante los siguientes párrafos explicaremos como se realiza esta categorización de los sistemas de información e información según FIPS Publication 199.

Se definen una serie de **objetivos de seguridad** (la parte que nos interesa es en qué consiste una perdida de cada una de ellos):

- Confidencialidad. Una perdida de confidencialidad es la divulgación no autorizada de información.

- Integridad. Una perdida de integridad es la modificación o destrucción no autorizada de información.

- Disponibilidad. Una perdida de disponibilidad es la interrupción al acceso o uso de un sistema de información o información.

Se definen tres **niveles de impacto potencial**, todo basado en las perdidas de integridad, disponibilidad y confidencialidad:

- Impacto Potencial bajo. Una perdida de integridad, disponibilidad y confidencialidad debería tener un efecto adverso limitado sobre las operaciones, activos de la organización e individuos.

- Impacto Potencial moderado. Una perdida de integridad, disponibilidad y confidencialidad debería tener un efecto adverso grave sobre las operaciones, activos de la organización e individuos.

- Impacto Potencial alto. Una perdida de integridad, disponibilidad y confidencialidad debería tener un efecto adverso severo o catastrófico sobre las operaciones, activos de la organización e individuos.

Como hemos explicado hasta ahora vamos a categorizar dos cosas, por un lado la información y por otro los sistemas información. Para la información nos basaremos en los tipos de información que maneja la organización, y para categorizar este tipo de información simplemente necesitamos conocer el impacto potencial sobre cada uno de los objetivos de seguridad anteriormente mencionados, para ese tipo de información.

Para expresar la categoría de seguridad de un determinado tipo de información utilizaremos el siguiente formato:

SC tipo de información = {(**confidencialidad**, impacto), (**integridad**, impacto), (**disponibilidad**, impacto)}

Cabe destacar que en el caso de la confidencialidad el impacto potencial puede ser "no aplicable", y solo en este caso.

Para entender mejor el proceso de categorización de información establecemos el siguiente ejemplo. Una organización o empresa trabaja con una información que hace pública (información publica) a través de su servidor de internet, esta organización determina que no hay impacto potencial por una perdida de confidencialidad, un impacto potencial moderado por una perdida de integridad y un impacto moderado por una perdida de disponibilidad. Se definiría la categoría de seguridad del correspondiente tipo de información (información pública) a través del formato explicado anteriormente.

SC información publica = {(**confidencialidad**, NA), (**integridad**, MODERATE), (**disponibilidad**, MODERATE)}

A la hora de categorizar los diferentes sistemas de información, se sigue un proceso diferente y que requiere un análisis mayor. Tenemos que considerar la categorización realizada para los tipos de información que residen en ese sistema de información. Los valores asignados de impacto potencial por perdida de cada uno de los objetivos de seguridad, será el más alto de los valores en ese objetivo de seguridad de entre todos los tipos de información que residen en ese sistema.

Cabe decir que el valor de no aplicable no puede ser utilizado para ningún objetivo de seguridad en el caso de los sistemas de información. Siempre existe un impacto potencial mínimo debido a la perdida de alguno de los objetivos de seguridad en el ámbito de los sistemas de información, esto se

lleva a cabo para proteger las funciones de procesamiento a nivel de sistema y la información crítica del mismo. Para establecer la categoría de seguridad de un sistema de información se usa el siguiente formato:

SC sistema de información = {(confidencialidad, impacto), (integridad, impacto), (disponibilidad, impacto)}.

Como ejemplo de una categorización de un sistema de información presentamos el siguiente. En una planta de energía existe un SCADA[28] es un software con el que podemos controlar procesos industriales a distancia, nos aporta una retroalimentación de los diferentes sensores y actuadores con los que contemos y va a controlar el proceso de forma automática. Nos aporta toda la información que necesitemos que haya sido creada durante el proceso productivo y nos permitirá su gestión e intervención. En este sistema SCADA consideramos información de los sensores e información administrativa rutinaria. Si para los dos tipos de información del sistema se tiene lo siguiente:

SC datos de sensor = {(**confidencialidad**, NA), (**integridad**, HIGH), (**disponibilidad**, HIGH)}

y

SC información administrativa = {(**confidencialidad**, LOW), (**integridad**, LOW), (**disponibilidad**, LOW)}

La categorización para SCADA será:

SC SCADA = {(**confidencialidad**, LOW), (**integridad**, HIGH), (**disponibilidad**, HIGH)}

Aún así, si la organización considerase que un impacto de una perdida de confidencialidad, por ejemplo no fuera bajo, sino moderado, para hacerlo más realista también podría modificar esa categorización a:

SC SCADA = {(**confidencialidad**, MODERATE), (**integridad**, HIGH), (**disponibilidad**, HIGH)}

[28] SCADA son las siglas en inglés de “Supervisory Control and Data Acquisition”, que en español quiere decir control de supervisión y adquisición de datos.

Normas y directrices posteriores abordarán las tareas segunda y tercera de FISMA a la hora de categorizar los sistemas de información.

Special Publication 800-60 Rev. 1 (Volume 1, Volume 2), Guide for Mapping Types of Information and Information Systems to Security Categories (Guía para la Asignación de tipos de información y sistemas de información para las Categorías Seguridad), es la otra publicación que compone esta fase. En ella se ayudará a identificar los sistemas de información y la información que contienen los mismos, así como a establecer unos niveles de impacto por esa perdida de confidencialidad, integridad y disponibilidad.

Esta publicación contiene dos volúmenes, empezaremos hablando del **volumen 1.**

En este volumen se explica un proceso en el que se alinea las dos ideas principales sobre las que venimos hablando, niveles de impacto potencial con la categorización de los sistemas de información e información (en la figura 5.1.1 se muestra esquematizado el proceso).

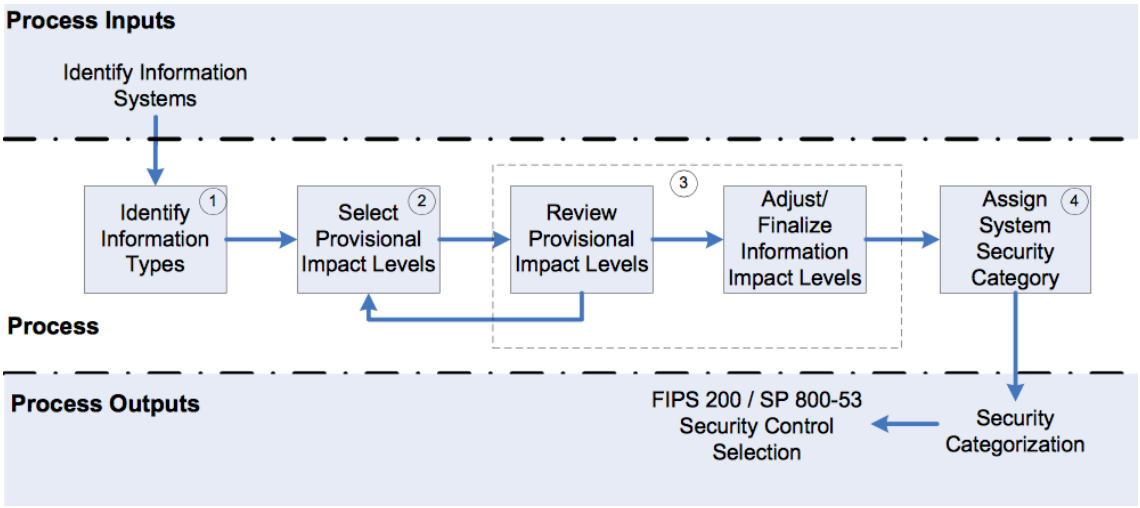

Figura 5.1.1 Proceso de categorización de sistemas de información

Es un proceso que cuenta con una entrada: Identificación de sistemas de información; y una salida: categorización de la seguridad. A partir de esa identificación de los sistemas de información que se tiene como entrada, se identifican los tipos de información, se seleccionan unos niveles de impacto provisional, los cuales son revisados y ajustados, y por último se asigna la categoría de seguridad del sistema.

Se desarrolla los diferentes pasos del proceso de categorización de sistemas de información:

5.1.1. Identificar tipos de información

Debemos realizar la documentación de la misión de las diferentes áreas de negocio de la compañía. La base para identificar los tipos de información está en cuatro áreas fundamentales, que separan las operaciones del gobierno en categorías relacionadas:

- El propósito del gobierno (servicios para los ciudadanos).
- Los mecanismos que el gobierno usa para lograr su propósito (modo de entrega de ese servicio).
- Las funciones de apoyo necesarias para llevar a cabo las operaciones del gobierno (ayuda para entregar esos servicios).
- Las funciones de gestión de recursos que ayudan a todas las áreas de negocio del gobierno (gestión de los recursos del gobierno).

Puede ocurrir que un tipo de información no encaje perfectamente en alguno de los tipos de información de la lista y que sea necesario añadirlo. Una vez que a partir de estas listas se extraigan los diferentes tipos de información, se recomienda que se realicen revisiones de la información que procesan los diferentes sistemas de información con los que cuenta la organización, para poder encontrar tipos de información adicionales que se necesiten identificar para cumplir con los propósitos de la evaluación de impacto.

En la siguiente figuras (figura 5.1.2 y figura 5.1.3) se establecen veintiséis servicios y modos de entrega de estos servicios, estos a su vez contienen noventa y ocho tipos de información en total, esto responde a las dos primeras operaciones de las que hablábamos antes, podemos caracterizar a esta información como un tipo de información que esta relacionado con la misión de la organización.

D.1 Defense & National Security	**D.7 Energy**	**D.14 Health**
Strategic National & Theater Defense	Energy Supply	Access to Care
Operational Defense	Energy Conservation and Preparedness	Population Health Mgmt & Consumer Safety
Tactical Defense	Energy Resource Management	Health Care Administration
D.2 Homeland Security	Energy Production	Health Care Delivery Services
Border and Transportation Security	**D.8 Environmental Management**	Health Care Research and Practitioner Education
Key Asset and Critical Infrastructure Protection	Environmental Monitoring and Forecasting	**D.15 Income Security**
Catastrophic Defense	Environmental Remediation	General Retirement and Disability
Executive Functions of the Executive Office of the President (EOP)	Pollution Prevention and Control	Unemployment Compensation
D.3 Intelligence Operations	**D.9 Economic Development**	Housing Assistance
Intelligence Planning	Business and Industry Development	Food and Nutrition Assistance
Intelligence Collection	Intellectual Property Protection	Survivor Compensation
Intelligence Analysis & Production	Financial Sector Oversight	**D.16 Law Enforcement**
Intelligence Dissemination	Industry Sector Income Stabilization	Criminal Apprehension
Intelligence Processing	**D.10 Community & Social Services**	Criminal Investigation and Surveillance
D.4 Disaster Management	Homeownership Promotion	Citizen Protection
Disaster Monitoring and Prediction	Community and Regional Development	Leadership Protection
Disaster Preparedness and Planning	Social Services	Property Protection
Disaster Repair and Restoration	Postal Services	Substance Control
Emergency Response	**D.11 Transportation**	Crime Prevention
D.5 International Affairs & Commerce	Ground Transportation	*Trade Law Enforcement*
Foreign Affairs	Water Transportation	**D.17 Litigation & Judicial Activities**
International Development and Humanitarian Aid	Air Transportation	Judicial Hearings
Global Trade	Space Operations	Legal Defense
D.6 Natural Resources	**D.12 Education**	Legal Investigation
Water Resource Management	Elementary, Secondary, and Vocational Education	Legal Prosecution and Litigation
Conservation, Marine and Land Management	Higher Education	Resolution Facilitation
Recreational Resource Management and Tourism	Cultural and Historic Preservation	**D.18 Federal Correctional Activities**
Agricultural Innovation and Services	Cultural and Historic Exhibition	Criminal Incarceration
	D.13 Workforce Management	Criminal Rehabilitation
	Training and Employment	**D.19 General Sciences & Innovation**
	Labor Rights Management	Scientific and Technological Research and Innovation
	Worker Safety	Space Exploration and Innovation

Figura 5.1.2 Tipos de información relacionados con la misión (1)

D.20 Knowledge Creation & Management	**D.22 Public Goods Creation & Management**	**D.24 Credit and Insurance**
Research and Development	Manufacturing	Direct Loans
General Purpose Data and Statistics	Construction	Loan Guarantees
Advising and Consulting	Public Resources, Facility and Infrastructure Management	General Insurance
Knowledge Dissemination	Information Infrastructure Management	**D.25 Transfers to State/ Local Governments**
D.21 Regulatory Compliance & Enforcement	**D.23 Federal Financial Assistance**	Formula Grants
Inspections and Auditing	Federal Grants (Non-State)	Project/Competitive Grants
Standards Setting/Reporting Guideline Development	Direct Transfers to Individuals	Earmarked Grants
Permits and Licensing	Subsidies	State Loans
	Tax Credits	**D.26 Direct Services for Citizens**
		Military Operations
		Civilian Operations

Figura 5.1.3 Tipos de información relacionados con la misión (2)

Debe haber un representante para cada sistema de información que sea claramente responsable de identificar aquellos tipos de información que son procesados, almacenados y generados por el sistema de información correspondiente.

El siguiente paso es identificar la información relacionada con la prestación de un servicio o con la administración de una serie de recursos. Para ello, se encuentran divididas estas dos operaciones principales en trece líneas de

negocio que a su vez contienen un total de setenta y dos sub-funciones. Todo esto se puede apreciar en las figuras 5.1.4 y 5.1.5.

C.2.1 Controls and Oversight	**C.2.4 Internal Risk Management & Mitigation**	**C.2.8 General Government**
Corrective Action (Policy/Regulation)	Contingency Planning	Central Fiscal Operations
Program Evaluation	Continuity of Operations	Legislative Functions
Program Monitoring	Service Recovery	Executive Functions
C.2.2 Regulatory Development	**C.2.5 Revenue Collection**	Central Property Management
Policy & Guidance Development	Debt Collection	Central Personnel Management
Public Comment Tracking	User Fee Collection	Taxation Management
Regulatory Creation	Federal Asset Sales	Central Records & Statistics Management
Rule Publication	**C.2.6 Public Affairs**	*Income Information*
C.2.3 Planning & Budgeting	Customer Services	*Personal Identity and Authentication*
Budget Formulation	Official Information Dissemination	*Entitlement Event Information*
Capital Planning	Product Outreach	*Representative Payee Information*
Enterprise Architecture	Public Relations	*General Information*
Strategic Planning	**C.2.7 Legislative Relations**	
Budget Execution	Legislation Tracking	
Workforce Planning	Legislation Testimony	
Management Improvement	Proposal Development	
Budgeting & Performance Integration	Congressional Liaison Operations	
Tax & Fiscal Policy		

Figura 5.1.4 Tipos de información relacionados con la prestación de un servicio

C.3.1 Administrative Management	**C.3.3 Human Resource Management**	**C.3.5 Information & Technology Management**
Facilities, Fleet, and Equipment Management	HR Strategy	System Development
Help Desk Services	Staff Acquisition	Lifecycle/Change Management
Security Management	Organization & Position Mgmt	System Maintenance
Travel	Compensation Management	IT Infrastructure Maintenance
Workplace Policy Development & Management	Benefits Management	Information Security
C.3.2 Financial Management	Employee Performance Mgmt	Record Retention
Accounting	Employee Relations	Information Management
Funds Control	Labor Relations	System and Network Monitoring
Payments	Separation Management	Information Sharing
Collections and Receivables	Human Resources Development	
Asset and Liability Management	**C.3.4 Supply Chain Management**	
Reporting and Information	Goods Acquisition	
Cost Accounting/ Performance Measurement	Inventory Control	
	Logistics Management	
	Services Acquisition	

Figura 5.1.5 Tipos de información relacionados con la administración de recursos

5.1.2. Seleccionar los niveles de impacto provisionales

En el otro volumen de esta publicación, **Special Publication 800-60 volumen 2,** se dan unos niveles de impacto provisionales ante una perdida de confidencialidad, integridad y disponibilidad para esa información relacionada con el apoyo a la prestación de un servicio, con la administración de una serie de recursos o con la misión de la organización.

Hay que tener en cuenta que en muchos casos un mismo tipo de información puede contener varios elementos de información en su interior, es decir que es posible que unos elementos de ese tipo de información tengan unos niveles de impacto diferentes a otros elementos dentro del mismo tipo de información.

Por ejemplo, información considerada del tipo *integración de rendimiento y presupuesto (ver figura 5.1.4)*, puede llevar asociada elementos como la identificación del empleado, información de costos, información de política de rembolso, procedimientos de reclamación. Esto quiere decir que normalmente no tendrá el mismo impacto en la organización una pérdida en confidencialidad para la información de costos, que si hablamos de identificación del empleado. Es decir a la hora de establecer niveles de impacto para este tipo de información en concreto, debemos estudiar todos los elementos que contiene ese tipo de información, ya que si en este caso solamente tuviéramos en cuenta la información del empleado que hay dentro de este tipo de información, sin considerar otros elementos como información de costos, podríamos asignar unos niveles de impacto potencial más bajos a este tipo de información.

Para ello, este volumen 2 incorpora unos apéndices o puntos en los que identifica estos elementos que pueden causar variaciones en la evaluación del impacto.

Las recomendaciones de los niveles de impacto provisionales para información relacionada con el apoyo a la prestación de un servicio, o con la administración de una serie de recursos, se dan en las siguientes figuras, figura 5.1.6, figura 5.1.7 y figura 5.1.8.

	Confidentiality	Integrity	Availability
Service Recovery	Low	**Low**	Low
Revenue Collection			
Debt Collection	Moderate	Low	**Low**
User Fee Collection	**Low**	Low	**Moderate**
Federal Asset Sales	Low	**Moderate**	**Low**
Public Affairs			
Customer Services	Low	Low	Low
Official Information Dissemination	**Low**	Low	Low
Product Outreach	**Low**	Low	**Low**
Public Relations	Low	Low	**Low**
Legislative Relations			
Legislation Tracking	Low	**Low**	**Low**
Legislation Testimony	Low	**Low**	Low
Proposal Development	Moderate	**Low**	Low
Congressional Liason Operations	Moderate	**Low**	Low
General Government			
Central Fiscal Operations[4]	Moderate	**Low**	**Low**
Legislative Functions	**Low**	**Low**	Low
Executive Functions[5]	**Low**	**Low**	**Low**
Central Property Management	Low[6]	**Low**	Low[7]
Central Personnel Management	Low	Low	Low
Taxation Management	Moderate	Low	Low
Central Records and Statistics Management	Moderate	**Low**	**Low**
Income Information[8]	**Moderate**	Moderate	Moderate
Personal Identity and Authentication[8]	Moderate	Moderate	Moderate
Entitlement Event Information[8]	**Moderate**	Moderate	Moderate
Representative Payee Information[8]	**Moderate**	Moderate	Moderate
General Information[9]	Low	Low	Low

Figura 5.1.6 Niveles de impacto provisionales para información relacionada con el apoyo a la prestación de un servicio, o con la administración de una serie de recursos (1)

	Confidentiality	Integrity	Availability
Administrative Management			
Facilities, Fleet, and Equipment Mgmt	Low[6]	Low[7]	Low[7]
Help Desk Services	Low	Low	Low
Security Management	Moderate	**Moderate**	Low
Travel	Low	**Low**	**Low**
Workplace Policy Development and Management	**Low**	**Low**	**Low**
Financial Management			
Asset and Liability Management	Low	Low	**Low**
Reporting and Information	Low	**Moderate**	**Low**
Funds Control	Moderate	**Moderate**	**Low**
Accounting	Low	Moderate	**Low**
Payments	Low	Moderate	Low
Collections and Receivables	**Low**	**Moderate**	**Low**
Cost Accounting/ Performance Measurement	**Low**	**Moderate**	**Low**
Human Resource Management			
HR Strategy	Low	**Low**	**Low**
Staff Acquisition	Low	**Low**	**Low**
Organization and Position Management	Low	**Low**	**Low**
Compensation Management	Low	Low	**Low**
Benefits Management	Low	**Low**	**Low**
Employee Performance Management	Low	**Low**	**Low**
Employee Relations	Low	Low	**Low**
Labor Relations	Low	Low	Low
Separation Management	Low	**Low**	**Low**
Human Resources Development	Low	**Low**	**Low**
Supply Chain Management			
Goods Acquisition	Low	Low	Low
Inventory Control	Low	**Low**	Low
Logistics Management	Low	**Low**	Low
Services Acquisition	Low	Low	**Low**
Information & Technology Management			
System Development	**Low**	Moderate	**Low**
Lifecycle/Change Management	Low	Moderate	**Low**
System Maintenance	**Low**	Moderate	**Low**
IT Infrastructure Maintenance[10]	Low	Low	Low
Information System Security	**Low**	**Moderate**	**Low**

Figura 5.1.7 Niveles de impacto provisionales para información relacionada con el apoyo a la prestación de un servicio, o con la administración de una serie de recursos (2)

	Confidentiality	Integrity	Availability
Record Retention	Low	Low	**Low**
Information Management[11]	Low	Moderate	**Low**
System and Network Monitoring	Moderate	Moderate	**Low**
Information Sharing	N/A	N/A	N/A

Figura 5.1.8 Niveles de impacto provisionales para información relacionada con el apoyo a la prestación de un servicio, o con la administración de una serie de recursos (3)

Las recomendaciones de los niveles de impacto provisionales para información relacionada con la misión, se dan en las siguientes figuras, figura 5.1.9, figura 5.1.10, figura 5.1.11 y figura 5.1.12.

	Confidentiality	Integrity	Availability
Defense & National Security	**Nat'l Security**	**Nat'l Security**	**Nat'l Security**
Homeland Security			
Border Control and Transportation Security	**Moderate**	**Moderate**	**Moderate**
Key Asset and Critical Infrastructure Protection	**High**	**High**	**High**
Catastrophic Defense	**High**	**High**	**High**
Executive Functions of the EOP[23]	**High**	**Moderate**	**High**
Intelligence Operations[24]	**High**	**High**	**High**
Disaster Management			
Disaster Monitoring and Prediction	**Low**	**High**	**High**
Disaster Preparedness and Planning	**Low**	**Low**	**Low**
Disaster Repair and Restoration	**Low**	**Low**	**Low**
Emergency Response	**Low**	**High**	**High**

Figura 5.1.9 Niveles de impacto provisionales para información relacionada con la misión (1)

	Confidentiality	Integrity	Availability
International Affairs and Commerce			
Foreign Affairs	**High**	**High**	Moderate
International Development and Humanitarian Aid	Moderate	Low	Low
Global Trade	**High**	**High**	**High**
Natural Resources			
Water Resource Management	Low	**Low**	**Low**
Conservation, Marine, and Land Management	Low	Low	Low
Recreational Resource Management and Tourism	Low	Low	Low
Agricultural Innovation and Services	Low	**Low**	**Low**
Energy			
Energy Supply	Low[25]	Moderate[26]	Moderate[26]
Energy Conservation and Preparedness	Low	Low	Low
Energy Resource Management	Moderate	Low	**Low**
Energy Production	Low	Low	**Low**
Environmental Management			
Environmental Monitoring/ Forecasting	Low	Moderate	**Low**
Environmental Remediation	**Moderate**	**Low**	**Low**
Pollution Prevention And Control	**Low**	**Low**	**Low**
Economic Development			
Business and Industry Development	Low	**Low**	**Low**
Intellectual Property Protection	Low	**Low**	**Low**
Financial Sector Oversight	Moderate	Low	**Low**
Industry Sector Income Stabilization	**Moderate**	**Low**	**Low**
Community and Social Services			
Homeownership Promotion	Low	**Low**	**Low**
Community and Regional Development	Low	**Low**	**Low**
Social Services	Low	**Low**	**Low**
Postal Services	Low	Moderate	**Moderate**
Transportation			
Ground Transportation	Low	Low	Low
Water Transportation	Low	Low	Low
Air Transportation	Low	Low	Low
Space Operations	Low	**High**	**High**
Education			
Elementary, Secondary, and Vocational Education	**Low**	**Low**	**Low**
Higher Education	Low	Low	**Low**
Cultural & Historic Preservation	Low	Low	**Low**
Cultural & Historic Exhibition	Low	Low	**Low**
Workforce Management			

Figura 5.1.10 Niveles de impacto provisionales para información relacionada con la misión (2)

	Confidentiality	Integrity	Availability
Training and Employment	Low	Low	**Low**
Labor Rights Management	**Low**	**Low**	**Low**
Worker Safety	**Low**	**Low**	**Low**
Health			
Access to Care	Low	**Moderate**	Low
Population Health Management and Consumer Safety	Low	Moderate	Low
Health Care Administration	Low	Moderate	**Low**
Health Care Delivery Services	Low	**High**	Low
Health Care Research and Practitioner Education	**Low**	**Moderate**	**Low**
Income Security			
General Retirement and Disability	**Moderate**	Moderate	Moderate
Unemployment Compensation	Low	**Low**	**Low**
Housing Assistance	Low	**Low**	**Low**
Food and Nutrition Assistance	Low	**Low**	**Low**
Survivor Compensation	Low	**Low**	**Low**
Law Enforcement			
Criminal Apprehension	Low	Low	**Moderate**
Criminal Investigation and Surveillance	Moderate	Moderate	Moderate
Citizen Protection	Moderate	Moderate	Moderate
Leadership Protection	Moderate	Low	Low
Property Protection	Low	Low	Low
Substance Control	Moderate	Moderate	Moderate
Crime Prevention	Low	**Low**	Low
Trade Law Enforcement[27]	**Moderate**	Moderate	**Moderate**
Litigation and Judicial Activities			
Judicial Hearings	Moderate	**Low**	Low
Legal Defense	Moderate	High	Low
Legal Investigation	Moderate	Moderate	Moderate
Legal Prosecution and Litigation	Low	Moderate	Low
Resolution Facilitation	Moderate	**Low**	**Low**
Federal Correctional Activities			
Criminal Incarceration	**Low**	Moderate	Low
Criminal Rehabilitation	Low	**Low**	**Low**
General Science and Innovation			
Scientific and Technological Research and Innovation	Low	**Moderate**	**Low**
Space Exploration and Innovation	Low	**Moderate**	**Low**
Knowledge Creation and Management			
Research and Development	Low	**Moderate**	**Low**
General Purpose Data and Statistics	Low	**Low**	**Low**
Advising and Consulting	Low	**Low**	**Low**
Knowledge Dissemination	Low	Low	Low

Figura 5.1.11 Niveles de impacto provisionales para información relacionada con la misión (3)

	Confidentiality	Integrity	Availability
Regulatory Compliance and Enforcement			
Inspections and Auditing	Moderate	**Moderate**	**Low**
Standards Setting/ Reporting Guideline Development	**Low**	**Low**	**Low**
Permits and Licensing	Low	**Low**	**Low**
Public Goods Creation and Management			
Manufacturing	**Low**	**Low**	**Low**
Construction	Low	**Low**	**Low**
Public Resources, Facility, and Infrastructure Management	Low	**Low**	Low
Information Infrastructure Management	Low	Low	Low
Federal Financial Assistance			
Federal Grants (Non-State)	Low	Low	**Low**
Direct Transfers to Individuals	Low	Low	Low
Subsidies	Low	**Low**	**Low**
Tax Credits	**Moderate**	**Low**	**Low**
Credits and Insurance			
Direct Loans	Low	Low	**Low**
Loan Guarantees	Low	**Low**	**Low**
General Insurance	Low	**Low**	Low
Transfers to State/Local Governments			
Formula Grants	Low	**Low**	**Low**
Project/Competitive Grants	Low	**Low**	**Low**
Earmarked Grants	Low	**Low**	**Low**
State Loans	**Low**	**Low**	**Low**
Direct Services for Citizens			
Military Operations[28]	**N/A**	**N/A**	**N/A**
Civilian Operations[28]	**N/A**	**N/A**	**N/A**

Figura 5.1.12 Niveles de impacto provisionales para información relacionada con la misión (4)

Puede ocurrir que no toda la información que procese un sistema de información se encuentre en las tablas, lo que quiere decir que se puede identificar información que no se encuentre asociada a ningún tipo de las figuras 5.1.2, 5.1.3, 5.1.4, 5.1.5, o puede que no elija los niveles provisionales de impacto que se recojan en las figuras 5.1.6, 5.1.7, 5.1.8, 5.1.8, 5.1.9, 5.1.10, 5.1.11, 5.1.12. Para ello se muestra la tabla 5.1.1 que es un resumen de algo que se expuso anteriormente, las definiciones de confidencialidad, integridad y disponibilidad, y además incorporamos una, lo que supone un impacto potencial alto, moderado y bajo por perdida de confidencialidad, integridad y disponibilidad, pero aplicado a cada objetivo de seguridad exclusivamente. Se aplicaría esta tabla a los tipos de información identificados sin categorización.

	Impacto Potencial		
Objetivo de seguridad	Bajo	Moderado	Elevado
Confidencialidad: Mantener unas restricciones para autorizar el acceso a la información y divulgación de la misma, y que se incluyan medios para la protección de la intimidad personal y la propiedad de la información.	Una divulgación de información debería tener un efecto adverso **limitado** sobre las operaciones, activos de la organización e individuos.	Una divulgación de información debería tener un efecto adverso **grave** sobre las operaciones, activos de la organización e individuos.	Una divulgación de información debería tener un efecto adverso **severo o catastrófico** sobre las operaciones, activos de la organización e individuos.
Integridad: Protección contra la modificación de información de forma incorrecta o destrucción de la misma, e incluye asegurar la ‘’information non-repundiation” y su autenticidad.	Una modificación o destrucción no autorizada de información debería tener un efecto adverso **limitado** sobre las operaciones, activos de la organización e individuos.	Una modificación o destrucción no autorizada de información debería tener un efecto adverso **grave** sobre las operaciones, activos de la organización e individuos.	Una modificación o destrucción no autorizada de información debería tener un efecto adverso **severo o catastrófico** sobre las operaciones, activos de la organización e individuos.

Disponibilidad: Garantizar el acceso a la información cuando sea necesario, así como el uso de la misma.	Una interrupción al acceso o uso de un sistema de información o información debería tener un efecto adverso **limitado** sobre las operaciones, activos de la organización e individuos.	Una interrupción al acceso o uso de un sistema de información o información debería tener un efecto adverso **grave** sobre las operaciones, activos de la organización e individuos.	Una interrupción al acceso o uso de un sistema de información o información debería tener un efecto adverso **severo o catastrófico** sobre las operaciones, activos de la organización e individuos.

Tabla 5.1.1 Relación objetivos de seguridad con impacto potencial

5.1.3. *Revisar niveles de impacto provisionales y ajustar/finalizar los niveles de impacto para el tipo de información*

En este paso la organización debería realizar una revisión de esos niveles de impacto potencial que han sido fijados en el paso anterior. Al realizar esta revisión la organización debería tener en cuenta que debe realizarlo bajo el contexto de la organización, entorno, misión que defiende la propia organización y teniendo presente como es el uso y compartición de datos de ese sistema de información. Para revisar los niveles de impacto provisionales, se debe usar como base los objetivos de seguridad hemos hablado y tener en cuenta que es muy probable que se necesite revisar estos niveles más de una vez, es posible que con un solo ajuste no sea necesario.

5.1.4. *Asignar la categoría de seguridad del sistema de información*

En este último paso se debe realizar un proceso el cual en su mayoría ya ha sido explicado anteriormente. Después de haber realizado el paso anterior y revisado la categorización aplicada a los diferentes tipos de información también identificados, se debe realizar la categorización para los sistemas de

información. Se realiza lo explicado en **FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems** (Normas para la categorización de información federal y sistemas de información), es decir por agregación de tipos de información se extraen los valores de impacto potencial para confidencialidad, integridad y disponibilidad del sistema de información. Más tarde si es necesario se debe ajustar el valor de cada objetivo de seguridad del sistema de información, si se considera necesario, para ello se debe tener en cuenta la tabla 5.1.1 de nuevo.

Por último solo hay que realizar dos últimas etapas. Para tener una idea global de los niveles de impacto para un sistema de información, hay que hacer algo más, no es suficiente tener una idea de los diferentes niveles de impacto para cada objetivo de seguridad dentro de un mismo sistemas de información. Esto puede ser útil para comparar dos sistemas de información diferentes con los que cuente la organización. Generalmente el valor que se tome de referencia para un sistema de información, será el valor más alto de entre sus objetivos de seguridad. Es decir, por ejemplo si el valor de referencia que se da a un sistema de información es un impacto potencial bajo (LOW), quiere decir que en todos sus objetivos de seguridad aparece un nivel bajo.

Continuando y aplicando estas ideas al ejemplo que tratábamos en la página 61, sobre una planta eléctrica que cuenta con un sistema SCADA en el que la categorización del sistema se puede expresar de la siguiente manera:

SC SCADA = {(**confidencialidad**, MODERATE), (**integridad**, HIGH), (**disponibilidad**, HIGH)}

Obtendríamos un valor de referencia para este sistema de información que sería el más alto de entre los niveles de impacto asignados a una perdida de cada objetivo de seguridad. Es decir, entre moderado, elevado y elevado elegiríamos elevado. El nivel de impacto que se toma de referencia para este sistema SCADA es elevado.

Solo quedaría documentar todo el proceso, las investigaciones y decisiones que se hayan tomado que consideren clave.

5.2. Segundo paso: Seleccionar los controles de seguridad

En este segundo paso del ciclo de vida de la seguridad, en el marco del gestión del riesgo, encontramos dos publicaciones que NIST nos ofrece, estas son:

- **NIST Special Publication 800-53 Revision 4 , Security and Privacy Controls for Federal Information Systems and Organizations** (Controles de Seguridad y Privacidad para los Sistemas de información Federales y Organizaciones).

- **FIPS 200, Minimum Security Requirements for Federal Information and Information Systems** (Requisitos Mínimos de Seguridad para la Información Federal y Sistemas de Información).

Empezaremos hablando sobre **NIST Special Publication 800-53 Revision 4 , Security and Privacy Controls for Federal Information Systems and Organizations** .

El objetivo que tiene esta publicación es el de darnos una serie de directrices para poder llegar a seleccionar todos los controles de seguridad, que sean necesarios para los diferentes sistemas de información, y que sirven como apoyo a las agencias del gobierno federal de los Estados Unidos.

Se estructura los controles de seguridad en algo denominado ‘’Familia de controles de seguridad’’, en estas familias podemos encontrar controles de seguridad que están relacionados con el tema de esa familia, que viene determinado en el nombre de la familia. Para denotar a esta familia se utiliza un conjunto de dos caracteres que la definirá de forma única. La figura 5.2.1 muestra las familias de controles de seguridad con sus correspondientes identificadores.

Por ejemplo, Risk Assessment viene determinado con los caracteres “RA” y contiene controles de seguridad que están relacionados con la evaluación del riesgo.

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Figura 5.2.1 Familias de controles de seguridad con sus correspondientes identificadores

Se define un proceso de selección de controles de seguridad para los sistemas de información que posee la organización, este proceso se compone de los siguientes pasos:

5.2.1. Seleccionar las líneas base de los controles de seguridad

Antes de realizar este paso la organización debe haber realizado todo lo anterior. Los resultados de esa categorización son los que ayudarán a una elección correcta y adecuada de los diferentes controles de seguridad, tenemos que tener en cuenta que estos controles de seguridad van en consonancia con el impacto potencial sobre la organización, es decir que si el impacto potencial de nuestro sistema de información es muy elevado los controles de seguridad a aplicar deberán ser elevados también.

En resumen, una vez hecho todo el proceso de categorización anterior, teniendo una referencia del impacto potencial sobre cada sistema de información del que disponemos, la organización debe comenzar con el proceso de selección de los controles de seguridad.

Existen tres líneas base para las controles de seguridad que corresponden a los niveles de impacto potencial con los que venimos trabajando, es decir bajo-impacto, moderado-impacto y elevado-impacto, cada una de estas líneas bases se compone de una serie de controles. La organización debe seleccionar una línea base de las tres para cada sistema de información, a la hora de seleccionar una de las tres nos basaremos en la categorización del sistema.

Un control puede ser asignado a varias líneas base, a una o a ninguna, cuando no es asignado a alguna de las líneas bases es designado en las tablas con “not selected”, y cuando un control es seleccionado para una de las líneas base, se escribe el identificador de la familia con los caracteres que

hemos presentado en la figura 5.2.1 seguido del número que identifica a ese control de seguridad. También hablamos de las mejoras que ha habido para estos diferentes controles de seguridad, es decir, mejoras que los complementan con algún aspecto particular, utilizamos números entre paréntesis para detonar el número de la mejora. En las figuras 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7 y 5.2.8 podemos ver los controles de seguridad que son asignados a cada línea base.

Para entender todo lo explicado hasta ahora en este segundo paso: seleccionar los controles de seguridad, se plantea el siguiente ejemplo:

- Podemos considerar el control ‘’grabaciones del contenido de auditorias”.
- Este control de seguridad corresponde a la familia de controles audit and accountability (auditoria y contabilidad), esta familia se denomina mediante los caracteres AU como podemos ver en la figura 5.2.1.
- Es el tercer control de esta familia como podemos ver en la figura 5.2.3. Por lo tanto la denominación a dar a este control será AU-3.
- Existe la posibilidad de que este control se aplique con de forma simple o aplicando dos mejoras diferentes. Por lo tanto tendremos AU-3 (1), AU-3 (2). La primera de ellas incorpora información adicional a estas grabaciones como por ejemplo una grabación con las identidades de los intervinientes en la auditoria. La segunda mejora, especifica que todas las grabaciones de las auditorias se controlen de forma centralizada (para esta mejora, se requiere una automatización)
- Y finalmente como podemos ver en la figura 5.2.3, este control con sus correspondientes mejoras se ha establecido de forma simple en la línea base de bajo impacto, con su primera mejora en la de moderado y con su primera y segunda mejora en la de elevado.

Además de que no todos los controles de seguridad son asignados a las líneas base como ya hemos dicho antes, no todas las mejoras son asignadas a la líneas base. Estos controles y mejoras que no son asignados a ninguna línea base, están disponibles para la organización si los necesitase.

En todas estas figuras 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7 y 5.2.8 , puede observarse que algún control de seguridad esta expuesto con el calificativo de

"withdrawn". Los controles con el calificativo de "withdrawn", que quiere decir excluido, han sido rechazados por estar incluidos en otros controles. Por ejemplo el AC-13 ha sido excluido por estar incorporado en el AC-2 y AU-6.

En las figuras 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7 y 5.2.8 también podemos ver que existen números de prioridad en los controles, lo que quiere decir que hay controles de seguridad que tiene una prioridad de implementación mayor que otros. Esto es debido a que hay controles de seguridad que dependen de otros controles de seguridad a su vez, de esta forma aseguramos que se implantan en primer lugar los controles de seguridad de los que otros controles dependen, así podemos conseguir una estructuración en la implementación de los mismos. Cabe decir que estos códigos de prioridad se utilizan para establecer la secuencia de implementación y en ningún caso para seleccionar controles. Esto viene explicado en la siguiente tabla 5.2.1.

Código de prioridad	Secuenciación	Acción
Código de prioridad 1 (P1)	PRIMERO	Implementa los controles de seguridad P1 primero.
Código de prioridad 2 (P2)	SIGUIENTE	Implementa los controles de seguridad P2 después de implementar los controles P1.
Código de prioridad 3 (P3)	ÚLTIMO	Implementa los controles de seguridad P3 después de implementar los controles P1 y P2.
Código de prioridad sin especificar (P0)	NINGUNO	Control de seguridad no seleccionado en ninguna línea base.

Tabla 5.2.1 Códigos de prioridad en controles de seguridad

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

Figura 5.2.2 Relación controles de seguridad y líneas base (1)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

Figura 5.2.3 Relación controles de seguridad y líneas base (2)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**Withdrawn**	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)

Figura 5.2.4 Relación controles de seguridad y líneas base (3)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P2	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	Not Selected
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected	Not Selected
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	P3	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	P2	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Maintenance Personnel	P2	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P2	Not Selected	MA-6	MA-6
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2	MP-2
MP-3	Media Marking	P2	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected	Not Selected
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P2	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-7	**Withdrawn**	---	---	---	---
PE-8	Visitor Access Records	P3	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P2	PE-16	PE-16	PE-16

Figura 5.2.5 Relación controles de seguridad y líneas base (4)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected
Planning					
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2 (3)	PL-2 (3)
PL-3	**Withdrawn**	---	---	---	---
PL-4	Rules of Behavior	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	**Withdrawn**	---	---	---	---
PL-6	**Withdrawn**	---	---	---	---
PL-7	Security Concept of Operations	P0	Not Selected	Not Selected	Not Selected
PL-8	Information Security Architecture	P1	Not Selected	PL-8	PL-8
PL-9	Central Management	P0	Not Selected	Not Selected	Not Selected
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P1	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected
System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	P1	SA-3	SA-3	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	Information System Documentation	P2	SA-5	SA-5	SA-5
SA-6	**Withdrawn**	---	---	---	---
SA-7	**Withdrawn**	---	---	---	---
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9 (2)	SA-9 (2)

Figura 5.2.6 Relación controles de seguridad y líneas base (5)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected
SA-14	Criticality Analysis	P0	Not Selected	Not Selected	Not Selected
SA-15	Development Process, Standards, and Tools	P2	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	P2	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	P1	Not Selected	Not Selected	SA-17
SA-18	Tamper Resistance and Detection	P0	Not Selected	Not Selected	Not Selected
SA-19	Component Authenticity	P0	Not Selected	Not Selected	Not Selected
SA-20	Customized Development of Critical Components	P0	Not Selected	Not Selected	Not Selected
SA-21	Developer Screening	P0	Not Selected	Not Selected	Not Selected
SA-22	Unsupported System Components	P0	Not Selected	Not Selected	Not Selected
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24

Figura 5.2.7 Relación controles de seguridad y líneas base (6)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	**Withdrawn**	---	---	---	---
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	---	---	---	---
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

Figura 5.2.8 Relación controles de seguridad y líneas base (7)

5.2.2. *Adaptar líneas base o de referencia*

Este proceso consiste simplemente en realizar una alineación de los controles de la línea base, es decir lo que haremos será modificar esos controles y alinearlos con las condiciones que se den en la organización.

El problema se puede abordar desde dos puntos de vista: la aplicación del proceso sistemas de información de nuevo desarrollo o a sistemas de información antiguos. En el primer caso estamos ante una nueva situación de construcción, es decir lo enfocamos desde una perspectiva en la que estamos incluyendo las categorizaciones por primera vez. En el segundo caso, lo basamos en una perspectiva de análisis sobre lo categorización y controles de seguridad que ya hay en el sistema.

Este proceso de adaptación esta formado por los siguientes pasos:

5.2.2.1. *Identificar y designar controles comunes en las líneas base de controles de seguridad*

Los controles de seguridad denominados “comunes”, son aquellos controles de seguridad que son heredados por un sistema de información que no es un sistema de información de nuevo desarrollo, es decir ya existía. Si un sistema de información hereda un control de seguridad, ese control de seguridad no tiene por qué ser implementado lógicamente. Es decir, si uno de los controles perteneciente a la línea base que hemos seleccionado para el sistema de información, se encuentra ya implementado, no hace falta implementarlo.

Por lo tanto considerando el párrafo anterior podemos decir que no hace falta implementar todos los controles. Que existan una serie controles comunes influye a los gastos de la organización, ya que si ya están implantados muchos controles comunes con la línea base, esto deriva en un ahorro mayor.

5.2.2.2. *Aplicación de consideraciones de alcance*

Aplicar estas consideraciones es útil para poder llegar a eliminar controles de la línea base seleccionada para el sistema de información que consideremos innecesarios. De esta forma solo nos quedaremos con los controles de seguridad que den el nivel de protección adecuado al sistema de información.

Se utilizan diferentes tipos de consideraciones que se pueden esquematizar de la siguiente manera:

- Consideraciones de disposición y distribución de los controles. Por ejemplo, los controles de las líneas base son un conjunto muy amplio, puede que alguno no sea aplicable a ningún elemento del sistema.

- Consideraciones de factores medioambientales y operacionales.

- Consideraciones de objetivos de seguridad. Esta relacionado con el número de objetivos de seguridad a los que presta apoyo ese control. Es decir, puede darse el caso en el que consideremos que un control solo presta apoyo a un objetivo de seguridad y que no es útil su aplicación.

- Consideraciones de tecnología. Existen controles de seguridad que se refieren a tecnologías muy especificas, como puede ser wireless, estos controles no son necesarios si no se encuentran esas tecnologías en los sistemas de información.

- Consideraciones relacionadas con los requisitos que exige la misión.

5.2.2.3. Seleccionar los controles de seguridad de compensación

Estos controles de compensación son una serie de controles que permiten una protección equivalente o comparable a los controles específicos de las líneas base. Es decir, estos controles de compensación son una alternativa a esos controles específicos de la líneas base. Es decir un control que compensa a otro por su protección equivalente y comparable.

Podrían necesitarse controles de compensación cuando las organizaciones no son capaces de implantar de forma correcta los controles de línea base o cuando por la naturaleza de los sistemas de información, esos controles de la línea base no consiguen la reducción del riesgo necesaria.

Estos controles pueden ser cualquiera de los controles de las figuras 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7 y 5.2.8 o simplemente controles que determine la organización cuando no considera que haya controles comunes en estas figuras.

5.2.2.4. Alineación de los valores de los parámetros de los controles de seguridad

Aquellos controles que contengan una serie de parámetros dotan a la organización de libertad a la hora de ajustar esos parámetros a los requisitos de la organización.

Cabe decir que la organización puede realizar este paso (alineación de los valores de los parámetros de los controles de seguridad), antes de seleccionar esos controles de compensación del paso anterior.

Existen situaciones en la que esto último no es útil, por ejemplo imaginemos una organización que se encuentra trabajando con un sistema de información en concreto. Si decidiese ajustar los parámetros de los controles de seguridad pertenecientes a este sistema de información antes de sustituir alguno de estos controles por controles de seguridad de compensación, podría ocurrir que una vez que se hubieran sustituido por controles de compensación hubiera que volver a ajustar parámetros.

5.2.2.5. *Complementación de las líneas base*

Se basa en la determinación final de la colección de controles de seguridad que vamos a usar para nuestro sistema de información. En muchas situaciones, se van a requerir controles de seguridad adicionales para poder hacer frente a amenazas especificas o vulnerabilidades. Estos controles pueden ser cualquiera de los contenidos en NIST Special Publication 800-53 en su apéndice F.

Debemos tener en cuenta que esas líneas base simplemente nos proporcionan una orientación inicial, más tarde tenemos que realizar modificaciones a sus controles. Podríamos considerar que esas líneas base son un bloque de piedra maciza que debemos tallar para conseguir una figura.

5.2.2.6. *Proporcionar información adicional para la implementación de los controles*

Consiste en dar una información adicional que pueda ser necesaria en caso de falta de detalles para la implementación de los controles o de una amplia abstracción de dicho control.

5.2.3. *Documentar el proceso de selección de controles de seguridad*

Como en la mayoría de las publicaciones del NIST, es importante que se realice una documentación del proceso. Para establecer una base fuerte en el proceso de toma decisiones, las organizaciones deben documentar las

decisiones que se hayan tomado en el proceso de selección de los controles de seguridad.

Esto puede ser fundamental cuando se quieran comprobar las condiciones de seguridad que poseen los diferentes sistemas de información.

- La otra de las publicaciones de las que consta el Segundo paso : Seleccionar los controles de seguridad es la siguiente: **FIPS 200, Minimum Security Requirements for Federal Information and Information Systems** (Requisitos Mínimos de Seguridad para la Información Federal y Sistemas de Información).

En esta publicación se especifican los requisitos mínimos de seguridad con los que debe contar la información y los sistemas de la información. Estos requisitos vienen expuestos a través de diecisiete áreas que corresponden a diecisiete de las dieciocho familias de controles de seguridad y que debe cumplir el sistema de información, la única familia que se excluye es la familia "PM", que esta orientada a proporcionar controles de seguridad a nivel organizativo. Todo ello se encuentra orientado a otorgar a los mismos una confidencialidad, integridad y disponibilidad de la información. Las organizaciones deben desarrollar políticas y procedimientos documentados que se basen en estos requisitos mínimos de seguridad de la información.

5.3. Tercer paso: Implementación de los controles de seguridad

Esta paso consiste en implementar los diversos controles de seguridad especificados en el Paso dos, y además poder documentar como implementan dentro del sistema de información y en el ambiente de las operaciones de la organización.

Actualmente no existen publicaciones para este paso que se puedan considerar como norma desarrollada por NIST, lo único que existe hasta la fecha es un borrador incompleto el cual se espera que se convierta en futura norma pronto, estoy hablando de **SP 800-160 DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient System,** que salió el 12 de Mayo de 2014 y no ha tenido ninguna revisión hasta la fecha.

Gracias a este borrador podemos saber que la futura norma se estructurará en tres capítulos, estos capítulos desarrollan aspectos de los sistemas de información útiles para su implementación:

- Un primer capítulo que será una introducción de los diferentes aspectos con los que cuenta este borrador.

- Un segundo capítulo que desarrolla el funcionamiento de los sistemas de información y los principios fundamentales de seguridad. En este capítulo se definen los conceptos y la terminología relacionados con todos los procesos de los sistemas de información.

- Un tercer capítulo en el que vuelve a hablar de los procesos relacionados con los sistemas de información, pero esta de vez de una forma más detallada. Extiende estos procesos de los sistemas de información en el ámbito de sus resultado, actividades y tareas que se realizan con ellos.

5.4. Cuarto paso: Evaluación de los controles de seguridad

Para este paso la publicación que ha desarrollado NIST es **NIST Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations** (Guía para la Evaluación de ontroles de Seguridad en Sistemas de Información Federales y Organizaciones).

El objetivo principal es lograr que se realicen evaluaciones más rentables y constantes de los diferentes sistemas de información con los que cuente la empresa, para ello se promueve que las empresas realicen evaluaciones de seguridad en la organización.

La publicación define en sucesivos pasos el proceso de evaluación de los diferentes controles de seguridad:

5.4.1. Preparación para la evaluación de controles de seguridad

Es necesario que exista una colaboración entre todas las figuras de la organización que tienen interés en la seguridad de la información de toda organización. Si queremos obtener unos resultados adecuados es necesario que se determinen unas expectativas, estas deben estar fijadas antes, durante y después de la evaluación que se está llevando a cabo en este paso cuatro: Evaluación de los controles de seguridad.

A la hora de elegir a los evaluadores de los controles de seguridad hay que tener en cuenta que deben haber tenido una preparación adecuada. Las organizaciones consideran que es importante que los evaluadores de los controles de seguridad tengan una experiencia técnica y las habilidades requeridas para poder llevar a cabo todas las evaluaciones. Nos referimos a que exista un conocimiento y experiencia sobre hardware, software y los componentes del firmware que utiliza la organización.

5.4.2. Desarrollo de planes de evaluación de seguridad

Un plan de evaluación de seguridad[29] es la pieza fundamental del engranaje que conforma el proceso. Es decir, cuando hablamos de realizar una evaluación de la seguridad necesitamos algo que nos sirva como guía para realizar la tarea. Los siguientes pasos son los que se deben considerar para el desarrollo de planes de evaluación de los controles de seguridad. Existen planes de seguridad[30], que no se deben confundir con los planes de evaluación de seguridad o de los controles seguridad. A la hora de desarrollar estos planes de evaluación debemos seguir los siguientes puntos:

5.4.2.1. Determinar los controles de seguridad y mejoras que van a ser evaluados. Es decir, determinar cuales van estar incluidos en la evaluación

Los contenidos del plan de seguridad y en el propósito de la evaluación son la base para determinar los controles de seguridad que están incluidos en la evaluación. Esta evaluación que se realiza sobre los controles de seguridad puede ser completa, es decir se realiza sobre todos los controles del sistema de información, o puede ser parcial, se realiza sobre solo algunos. Por ejemplo, el primer supuesto sería el caso de un proceso de evaluación inicial.

5.4.2.2. Seleccionar los procedimientos apropiados para evaluar los controles de seguridad

En el apéndice F de NIST Special Publication 800-53A se dan unos procedimientos de evaluación para cada control de seguridad y mejora, los evaluadores deben seleccionar el procedimiento adecuado para esa mejora o control. Este último detalle quiere decir que puede existir para un mismo control o mejora dos procedimientos o más, de los cuales los evaluadores

[29] Un plan de evaluación de seguridad es el plan que nos proporciona los objetivos de la evaluación de los controles de seguridad y como llevar a cabo esa evaluación.
[30] Los planes de seguridad muestran los diferentes controles de seguridad, así como un resumen de los requisitos de seguridad para los sistemas de información de la organización.

deberán escoger uno, por ejemplo, PL6.1 se refiere al primer procedimiento de evaluación del control PL-6.

Un procedimiento de evaluación se compone de dos partes:

Un objetivo de evaluación, es decir, qué se quiere comprobar.

Métodos de evaluación: examinar, entrevistar… Objetos de la evaluación: políticas, planes, softwares, individuos…

La mejor forma de comprender como se llega a un procedimiento de evaluación es con un ejemplo de un control de seguridad determinado.

Pensemos en el control AT-2 SECURITY AWARENESS TRAINING. En este control la organización proporcionará la instrucción de concienciación de seguridad a los usuarios del sistema de información (incluyendo managers, ejecutivos sénior y contratistas):

a) Como parte de la instrucción inicial a nuevos usuarios.

b) Cuando se requiera por cambios en los sistemas de información.

c) Con la frecuencia definida por la organización.

Una mejora de este control de seguridad (AT-2(1)), habla de incluir en este entrenamiento ejercicios prácticos que simulan ataques cibernéticos. El procedimiento de evaluación para esta mejora sería el siguiente:

AT-2(1)	SECURITY AWARENESS TRAINING
AT-2(1).1	OBJETIVO DE LA EVALUACIÓN: Determinar si la organización incluye ejercicios prácticos en la instrucción de concienciación de seguridad que simulan ataques cibernéticos. MÉTODOS Y OBJETOS DE EVALUACIÓN: EXAMINAR: Concienciación de seguridad y política de entrenamiento; procedimientos que abordan la implementación de la instrucción en concienciación de la seguridad; currículo de instrucción en concienciación de

	seguridad; materiales de instrucción en concienciación de seguridad; otras grabaciones o documentos relevantes. ENTREVISTAR: Realizarla al personal de la organización que participa en la instrucción en concienciación de seguridad.

5.4.2.3. Adaptación de los procedimientos de evaluación

En esta parte adaptaremos a la misión, negocios, funciones y características de la organización los procedimientos de evaluación de los que venimos hablando.

Esta adaptación la conseguiremos a través de:

- Seleccionar los métodos de evaluación y objetos necesarios para poder satisfacer los diferentes objetivos de la evaluación.

Estamos hablando de unos métodos y objetos que son potenciales, estos actúan como un recurso para ayudar en la selección de los métodos y objetos, y nunca con la idea de limitar esta selección.

Las organizaciones usan su juicio propio para seleccionar los métodos de evaluación potencial y la lista de objetos de evaluación asociada con los mismos. De esta forma buscamos que las organizaciones encuentren la opción que más ayude a cumplir con el objetivo de la evaluación.

No va a ser siempre necesario aplicar cada método de evaluación a cada objeto de evaluación para obtener los resultados de la evaluación que se quieran. A veces puede ser bueno aplicar un método que no se encuentre en la lista de métodos potenciales.

- Selección de los valores de profundidad y cobertura para definir el rigor y ámbito de la evaluación.

Los métodos de evaluación se caracterizan por dos atributos: profundidad y cobertura.

La profundidad del método de evaluación define el rigor y el nivel de detalle con el que se realiza la evaluación. La cobertura del método de evaluación define el alcance y la amplitud de la evaluación. Como podemos ver, esto está relacionado con los requisitos de evaluación que especifique la organización.

- Identificación de los controles que han sido evaluados por un plan de evaluación de seguridad por separado, y por lo tanto no es necesario repetir la evaluación.

Suele ocurrir que la mayoría de los controles de seguridad son controles comunes, según la definición que ya dimos de controles comunes en el segundo paso : selección de los controles de seguridad, esos controles que ya estaban implantados en el sistema de información y no era necesario volverlos a implantar.

Este paso es importante porque por ejemplo puede ocurrir que estos controles comunes hayan ya sido evaluados como parte del plan de seguridad de la organización, o incluso puede ocurrir que exista un plan de evaluación específico para estos controles.

- Desarrollar sistemas de información específicos y planes de evaluación específicos. Esta situación se da con frecuencia cuando estamos trabajando con controles de seguridad con cualidades o que provienen de familias de controles de seguridad más técnicas.

- Tener en cuenta los resultados de evaluaciones previas donde los resultados se consideran aplicables. En este caso tienen importancia el uso de los resultados de evaluaciones anteriores, estos ayudaran a determinar la eficacia del control de seguridad.

- Hacer los ajustes apropiados en los procedimientos de evaluación para los sistemas de información externos[31] (Proveedores).

5.4.2.4. Desarrollar los procedimientos de evaluación para los controles de seguridad específicos de la organización

Como dijimos en el segundo paso: Selección de los controles de seguridad y como definía su publicación más importante, NIST Special Publication 800-53, la organización puede desarrollar e implementar controles de seguridad adicionales y mejoras que salgan del alcance de esta publicación. Todo esto lo realiza basándose en sus políticas, misión y requisitos.

[31] Un sistema de información externo es un sistema de información o un componente de un sistema de información que se encuentra fuera de los limites de autorización establecidos por la organización, en él la organización no posee un control directo sobre los controles de seguridad.

Para evaluar estos controles los evaluadores deben usar unas directrices que marca esta norma y que se encuentran en el capitulo 2 de la publicación NIST Special Publication 800-53, ya que es un caso especial a tener en cuenta.

5.4.2.5. *Optimizar los procedimientos de evaluación seleccionados para asegurar la máxima eficiencia*

Para reducir los costes de la evaluación, maximizar la utilidad que tendrán los resultados de la evaluación y ahorrar tiempo se deben usar técnicas que lo permitan. Nos basaremos en la revisión de los procedimientos de evaluación seleccionados y en la combinación de los mismos.

Por ejemplo, se puede tratar de ahorrar tiempo consolidando entrevistas o mediante el análisis de parámetros de software o hardware similares dentro del sistema de información. Si vamos a entrevistar a una persona del personal que conforma la organización en relación a un control de seguridad, podemos aprovechar para preguntarle acerca de otro y no esperar a organizar otra entrevista, al igual con las examinaciones de software o hardware.

5.4.2.6. *Finalizar el plan de evaluación de seguridad y obtener aprobación para ejecutar el plan*

Por último el plan de evaluación de seguridad debe ser revisado y aprobado, para estar seguros de que está completado y cumple con los objetivos de seguridad de la organización.

5.4.3. *Llevar a cabo las evaluaciones de los controles de seguridad*

Se debe haber elaborado un calendario en el que se marque la ejecución del plan de evaluación de seguridad elaborado en pasos anteriores.

Realizar la evaluación de los controles de seguridad no es más que un proceso, por lo tanto tiene un resultado, este resultado se denomina informe de evaluación de seguridad. Es un informe cuyo objetivo es ser el documento que garantiza la seguridad de la información del sistema de información, y es uno de los documentos determinados como clave en el paquete de autorización de seguridad.

A la hora de realizar la evaluación de los controles de seguridad podríamos decir que los evaluadores y su actuación es una pieza clave. A la hora de informar de los resultados estos evaluadores deben ser lo más imparciales posibles, y no deben dar un informe subjetivo de los resultados. El procedimiento a seguir es el siguiente: cuando los evaluadores encuentran algo en el control de seguridad que no funciona como debería, deben especificar que parte exacta del control de seguridad no funciona como es debido, también deben detallar en que difiere este funcionamiento del ideal. Si los niveles de impacto potencial en confidencialidad, integridad y disponibilidad no son los adecuados, también el evaluador debe declarar este hecho a fin de obtener una adecuada protección de seguridad de la información, ya que existe una falta de protección.

5.4.4. Analizar los resultados de los informes de evaluación de seguridad

Este último paso se puede considerar uno de los más importantes del proceso, ya que su resultado influirá en plan de seguridad de la organización.

Lo que tenemos que realizar es una revisión de los informes de evaluación de seguridad y actualizar la evaluación de riesgos. Con actualizar la evaluación de riesgos nos referimos a definir los niveles de impacto potencial de confidencialidad, disponibilidad e integridad una vez que tenemos esos controles de seguridad. Si se han encontrado debilidades se deben marcar los pasos necesarios para poder corregirlo y llevar a cabo algunas acciones como remedio de los problemas que podemos considerar iniciales.

5.5. Quinto paso: Autorización de los sistemas de información

Para poder realizar la autorización de los sistemas de información, haremos uso de una de las publicaciones más importantes que NIST ha desarrollado, el nombre de esta publicación es: **NIST Special Publication 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach** (Guía para la Aplicación del Marco de Gestión del Riesgo para los Sistemas de Información Federales).

Esta guía tiene el objetivo de dar unas directrices para aplicar todos los pasos del marco de gestión del riesgo que NIST presenta, y poder llevar acabo las actividades de categorización, selección de los controles de seguridad, implementación de los controles de seguridad, evaluación de los controles de

seguridad, autorización de los sistemas de información y monitorización de los controles de seguridad.

Como podemos deducir por su nombre, es una guía que nos proporciona algo más que unas directrices para poder realizar ese proceso de autorización de los sistemas de información, nos basaremos en un apartado de ella para poder estudiar como NIST marca los pasos a seguir para poder llegar a la autorización de un sistema de información.

Resumiendo, lo que esta guía nos aporta es un resumen de todo lo que venimos viendo ahora y los dos pasos restantes, la autorización de los sistemas de información y la monitorización de los controles de seguridad. Es decir, que para cada uno de los pasos del marco de gestión del riesgo, realiza un esquema estructurado para cada paso, donde resume el mismo.

Si tuviera un sistema de información que contuviera diversos tipos de información, sobre el cual quisiera gestionar los riesgos relativos a la seguridad de la información, para el cual necesitara categorizar sus tipos de información para poder obtener una categorización del sistema, para el cual quisiera seleccionar unos controles de seguridad que después tuviera que evaluar e implementar, y para finalizar necesitará autorizarlo y monitorizar sus controles, está sería la guía en la que debería fijarme para resumir los pasos o el proceso que tengo que realizar.

En el caso de realizar la autorización, se podría ver desde el siguiente punto de vista. En el paso anterior evaluación de controles de seguridad, el fin que perseguíamos era ver si esos controles de seguridad funcionaban de forma correcta. El fin que perseguimos al autorizar el sistema de información es determinar si el riesgo para las operaciones, activos, individuos, otras organizaciones o para la nación es aceptable.

Para entender mejor la diferencia entre los objetivos de evaluación y acreditación se presenta el siguiente ejemplo.

Imaginemos que para proteger nuestra empresa decidimos contratar un guardia de seguridad de cualquier compañía de seguridad privada. Estableceremos que esta persona se mantenga junto a la puerta de nuestra empresa durante un periodo de 8 horas. Considerando a esta persona como un control de seguridad veremos la diferencia entre evaluarlo y autorizarlo.

Cuando se evalúa este control de seguridad, estamos comprobando si este

agente de seguridad realiza las tareas que tiene acometidas de forma correcta. Es decir, si se encuentra el periodo marcado de 8 horas junto a la puerta, si presta la atención necesaria al exterior de la empresa o si se asegura de que solamente entren personas con identificación. De esta forma estamos evaluando este control de seguridad, y suponiendo que este control de seguridad fuese el único control que posee el sistema de información, si los datos procedentes de la evaluación fueran aceptables pasaríamos a desarrollar la certificación del sistema.

Una vez evaluado este control de seguridad nos plantearíamos la siguiente duda, el control de seguridad establecido (agente de seguridad) funciona de forma correcta, realiza todo lo que le habíamos pedido, pero con este control de seguridad el riesgo que aún tenemos para las operaciones, activos, individuos es aceptable o necesitamos más controles de seguridad (más guardias de seguridad u otros sistemas de protección). Esto último, comprobar si el riesgo que existe para la organización es aceptable sería comprobar si se puede autorizar el sistema de información. Obtener la autorización del sistema cuando ya teníamos esa certificación se denomina acreditación del sistema de información.

En la autorización del sistema de información esta guía nos aporta tres tareas:

5.5.1. Preparar un plan de acción e hitos

Basándonos en el informe de evaluación de seguridad, en sus recomendaciones y detalles encontrados (con exclusión de las acciones tomadas para remediar problemas, consideradas como acciones iniciales al analizar los resultados de los informes de evaluación de seguridad), vamos a preparar un plan de acción e hitos.

Para esta tarea la responsabilidad recae sobre el propietario del sistema de información y el proveedor del control común[32].

En esta tarea preparamos el denominado plan de acción e hitos, este uno de los tres documentos que podemos considerar como claves en el paquete de autorización de seguridad.

[32] El proveedor del control común es la persona que implemento ese control común en el sistema de información que no es de nuevo desarrollo.

Creo que es importante destacar cuál es cada uno de los tres documentos claves que conforman el paquete necesario para la autorización de seguridad:

- Informe de evaluación de seguridad. Realizar la evaluación de los controles de seguridad no es más que un proceso, por lo tanto tiene un resultado y este informe es el resultado que garantiza la seguridad de la información del sistema de información.

- Plan de seguridad. Un documento de carácter formal que proporciona un resumen de los requisitos de seguridad para un sistema de información o un programa de seguridad de la información, y describe los controles de seguridad existentes o planeados para cumplir con esos requisitos.

- Plan de acción e hitos. Un documento que identifica las tareas necesarias que deben realizarse. Detalla que recursos son necesarios para realizar los elementos del plan, algunos hitos importantes en el cumplimiento de las tareas y las fechas previstas de finalización de esos hitos.

Hablando un poco más de este plan de acción e hitos podemos decir que describe una serie de tareas especificas:

- Corregir cualquier debilidad o deficiencia en los controles de seguridad que se haya percibido durante la evaluación.

- Para abordar vulnerabilidades de carácter residual en el sistema de información.

Es decir, el plan de acción e hitos es usado para monitorizar el proceso de corregir esas debilidades y deficiencias de los controles que se identificaron en la evaluación.

5.5.2. Conformar el paquete de autorización de seguridad y entregar este paquete al oficial autorizado para su adjudicación

Como hemos dicho ya, este paquete contiene el plan de seguridad, el informe de evaluación de seguridad y el plan de acción e hitos. Estos documentos son utilizados para tomar las decisiones de autorización. Cuando estamos hablando de esos controles comunes que son heredados en el sistema de información, en este paquete de autorización de seguridad se incluye un paquete de autorización de seguridad para ellos o una referencia. En el caso de que los controles sean proporcionados por proveedores externos, la

organización debe asegurar que la información necesaria para tomar las decisiones basadas en el riesgo, es facilitada por el proveedor.

Algo que está siendo cada vez mas desarrollado y empleado son las herramientas de soporte automatizados para la preparación y gestión del paquete de autorización de seguridad. Esto permite un mantenimiento y actualización de la información, teniendo en cuenta el uso de sistemas de información de seguridad continua que hay dentro de la organización.

5.5.3. *Determinar el riesgo para las operaciones de la organización, sus activos, para los diferentes individuos, otras organizaciones o la nación*

Se emplean evaluaciones del riesgo para dar información acerca de amenazas, vulnerabilidades e impactos potenciales, también se emplean las recomendaciones para la mitigación del riesgo.

Se da información relacionada con el riesgo para las operaciones de la organización, sus activos, para los diferentes individuos, otras organizaciones o la nación que surge del uso de ese sistema de información.

En la información relacionada con los riesgos se incluye el riesgo que aporta ese sistema de información a la misión de la organización, como hemos dicho en el párrafo anterior, y la estrategia de gestión de los riesgos de la organización.

Esta estrategia de gestión de los riesgos expone:

- Como los riesgos deben ser evaluados en esa organización.
- Como los riesgos son evaluados respecto a su probabilidad e impacto.
- Riesgos agregados, conocidos y existentes procedentes de sistemas de información y otras fuentes.
- Estrategias para dar respuesta a los riesgos.
- La tolerancia que se le da al riesgo.
- Cómo el riesgo es monitorizado en el tiempo.

5.5.4. *Determinar si el riesgo para las operaciones, activos, individuos, otras organizaciones o para la nación es aceptable*

Se deben considerar muchos factores a la hora de determinar si el riesgo para las operaciones, activos, individuos, otras organizaciones o para la nación es aceptable. Que exista un equilibrio entre las consideraciones de seguridad que sean pertinentes y la misión-operaciones de la organización es algo primordial para conseguir una autorización aceptable.

Podemos decir que las decisiones que tomemos respecto a la autorización, son la base para conformar el paquete de autorización de seguridad y en cualquier aporte que se haya recibido de personas clave en la organización. Esto se debe a que el paquete de autorización de seguridad, nos da gran información de cómo es el estado en materia de seguridad de ese sistema de información.

El oficial autorizado por la organización para el cargo expresa a través del documento de decisión de autorización que autoriza al propietario de ese sistema de información. Este documento contiene la siguiente información:

- La decisión de autorización.
- Términos y condiciones para la autorización
- Fecha de la autorización.

5.6. Sexto paso: Monitorizar los controles de seguridad

Para este paso, **NIST Special Publication 800-37 Revison 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach**, resume los pasos que se deben seguir para monitorizar los controles de seguridad:

1. Determinar el impacto de los cambios sobre los sistemas de información y su ambiente de operación. Los sistemas de información están en un estado de cambio continuo con actualizaciones del hardware, software o firmware y modificaciones del ambiente donde estos sistemas de información residen y operan.

2. Evaluación de los controles de seguridad de los sistemas de información en consonancia con la estrategia de monitorización definida por la organización.

3. Llevar a cabo las acciones recomendadas basadas en los resultados de las actividades de monitorización en curso, evaluación del riesgo y elementos pendientes del plan de acción e hitos.

4. Actualizar el plan de seguridad, informe de evaluación de seguridad y el plan de acción e hitos basándonos en el resultado del proceso de monitorización continua.

5. Informar del estado de seguridad del sistema de información (incluyendo la efectividad de los controles de seguridad empleados).

6. Revisar el estado de seguridad del sistema de información en concordancia con la estrategia de monitorización para determinar si el riesgo sobre las operaciones de la organización, sus activos, individuos, otras organizaciones o para la Nación continua siendo aceptable.

Existe otra publicación que NIST ha desarrollado, donde detalla esta monitorización, es la siguiente: **SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations** (Monitorización Continua de la Seguridad de la Información[33] para Sistemas de Información Federales y Organizaciones).

Esto surge como respuesta a las siguientes necesidades:

- Mantener un conocimiento acerca de lo que ocurre en los sistemas de información de la organización.

- Mantener un conocimiento de las amenazas y actividades que se pueden convertir en amenaza.

- Evaluar controles de seguridad.

- Recoger, correlacionar y analizar la información en materia de seguridad.

[33] Monitorización Continua de la Seguridad de la Información viene definido bajo las siglas ISCM, se considera como un mantenimiento continuo del conocimiento en seguridad de la información, vulnerabilidades y amenazas para apoyar las decisiones de la gestión de riesgos.

- Dotar de una comunicación del estado de seguridad de la información a lo largo de los diferente niveles de la organización.

- Para que se active la gestión del riesgo.

También existe una necesidad creciente a la hora de tener que hacer frente a unos desafíos de seguridad mucho mayores y diseños que deben ser desarrollados mediante métodos. ISCM es capaz de abordar estas necesidades de la forma más eficiente posible, monitoriza y evalúa los controles de seguridad para supervisar el estado de seguridad y la eficacia del proceso. Incorpora un proceso que también permite asegurarnos de que las acciones de respuesta apropiadas se han tomado ante un problema y que han tenido los efectos esperados.

Para implantar ISCM se debe:

- Definir la estrategia de ISCM.

- Establecer un programa ISCM.

- Implementar el programa ISCM.

- Analizar e informar de algún hallazgo.

- Responder a esos hallazgos.

- Revisar y actualizar la estrategia y programa de ISCM.

Este proceso ISCM viene esquematizado en la figura 5.6.1.

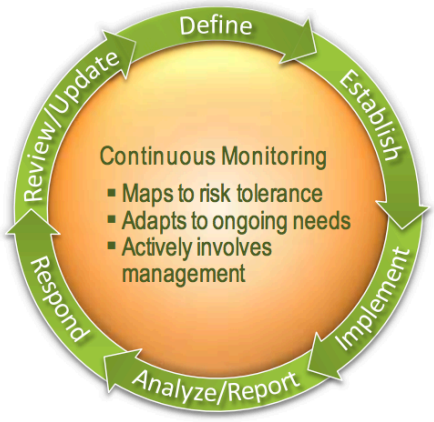

Figura 5.6.1 Proceso ISCM

En este proceso se requiere que toda la organización este implicada, desde los altos directivos que proporcionan una visión estratégica, a las personas que desarrollan, implementan y operan sistemas de información en apoyo a las misiones centrales de la organización y funciones de negocio. Todo esto se ilustra en la figura 5.6.2.

Figura 5.6.2 Pirámide organizativa

- Nivel 1

Las Actividades de gestión de los riesgos en el nivel uno están orientadas a abordar políticas de seguridad de la información de alto nivel, ya que es capaz de relacionar al riesgo de la organización si la consideramos como un todo, a sus misiones base y sus funciones de negocio.

Los diferentes criterios para ISCM van a quedar definidos por la estrategia de gestión de riesgos de esa organización, todo esto incluye la forma en la que la organización va a planear esas evaluaciones, la manera en la que responde al riesgo y en la que les monitoriza y una supervisión sobre la efectividad de la estrategia en gestión de riesgos.

Se desarrollan métricas[34] que permiten apoyar las decisiones de gobierno que la organización considere, también apoyan a las misiones centrales de la organización y a las funciones de negocio. Si pensamos en la frecuencia con

[34] Las métricas son herramientas que facilitan el proceso de toma de decisiones, sirven como ayuda para la toma de las mismas, mejoran el desempeño a través de la recogida, análisis y el informe del datos sobre el rendimiento.

la que se deben usar, nos podemos dar cuenta de que esta frecuencia debe ser tal que permita cumplir los requisitos para mantener todas las operaciones dentro de las tolerancias de riesgo.

- Nivel 2

Los miembros de la organización a los que se les puede considerar responsables de una misión o proceso de negocio dentro de la organización también están obligados a supervisar y controlar las actividades de riesgo para esos procesos de los que son responsables.

Para comprender a qué nos referimos cuando hablamos de las misiones o proceso de negocio que existen dentro de la organización podemos pensar en diferentes ejemplos:

- En el área de mercadotecnia y ventas podemos encontrar funciones como: Planeación y desarrollo de producto, y promoción de ventas.
- En el área de finanzas podemos encontrar funciones como: Tesorería, Obtención de recursos, Inversiones y Gestión de las relaciones con inversionistas.

SI en el nivel anterior decíamos que los criterios de ISCM estaban definidos por la estrategia de gestión de riesgos de la organización, en este nivel están definidos por cómo los procesos de las misiones centrales de la organización son priorizados con respecto a los propósitos u objetivos generales, los tipos de información necesarios para poder realizar con éxito los procesos de las misiones y en la estrategia del programa de seguridad de información de toda la organización.

- Nivel 3

Este nivel lo abordaremos desde una perspectiva del sistema de información. Estamos hablando de asegurarnos que todos los controles de seguridad a nivel de sistema de información han sido implementados de una forma correcta, funcionan correctamente , nos dan los resultados adecuados y se puede apreciar que con el tiempo seguirá así.

Se busca que los resultados de las evaluaciones en este nivel sirvan para apoyar a las decisiones en los otros niveles, tanto de organización como en los procesos de las misiones.

El proceso para desarrollar ISCM se explica en los siguientes puntos:

5.6.1. *Definir la estrategia ISCM basada en la tolerancia del riesgo que mantiene una vigilancia en los activos, el conocimiento de vulnerabilidades, en la información sobre amenazas y en los impactos sobre la misión de la organización*

Lo primero que debemos realizar para conseguir un ISCM efectivo es realizar una estrategia que abordará los requisitos ISCM y las actividades para cada nivel organizacional (organización, procesos misión/negocio y sistema de información). Esta estrategia debe estar basada en la tolerancia del riesgo[35].

Primero vamos a definir qué es el director del riesgo. Un director de riesgo puede ser un individuo o incluso un grupo que fue formado en una organización y que aborda diferentes tareas para asegurar que:

- Gestión de los riesgos de los diferentes sistemas de información es coherente en toda la organización, refleja esa tolerancia al riesgo y es considerada junto con los riesgos que afectan al éxito de la misión.

- Las consideraciones de los riesgos oportunas de los sistemas de información, para que las decisiones de autorización sean vistas desde una perspectiva de la organización completa en relación a los objetivos estratégicos más generales y los objetivos de esa organización, para llevar a cabo su misiones y diferentes funciones de negocio.

Cada nivel monitoriza o supervisa las diferentes métricas de seguridad así como realiza una valoración de los controles de seguridad, las frecuencias con las que esto se realiza deben quedar establecidos y usando informes de estado que permitirán ayudar al proceso de toma de decisiones de ese nivel. En los niveles más bajos es muy probable que se requiera información adicional a la requerida en esos niveles más altos, por consiguiente, esto se ve enmarcado en el desarrollo de unas estrategias más especificas para ese

[35] La tolerancia al riesgo es el nivel de riesgo que una entidad está dispuesta a asumir par lograr el resultado potencial deseado.

nivel, que deben tener coherencia con las de los niveles más altos y ser suficientes para plantar cara a los requisitos del nivel correspondiente.

Hablando de estas estrategias para cada nivel tenemos:

- **Estrategia ISCM en los niveles uno y dos**

La función de director de riesgo - Risk Executive (Function) - tiene la obligación de determinar la tolerancia el riesgo y la estrategia de mitigación del mismo en el nivel de la organización. La estrategia ISCM se desarrolla para poder apoyar a la gestión del riesgo en conformidad con la tolerancia del riesgo. Mientras que la estrategia ISCM más especifica, su política y los procedimientos se pueden desarrollar en cualquier nivel, la estrategia ISCM de la organización completa y las políticas que lleva asociadas normalmente se desarrollan en el nivel de la organización con procedimientos más generales.

Si la estrategia ISCM de la organización completa se desarrolla en el nivel de los procesos de misión o negocio, las personas responsables se encargan de revisar esta estrategia para tener completa seguridad de que se ajusta con la tolerancia del riesgo a lo largo de todos los procesos de misión o negocio. Todo esta información creada se comunica a un equipo en los niveles dos y tres , y queda reflejada en los procesos de misión/negocios, en las políticas, estrategia y procedimientos de los sistemas de información.

- **Estrategia en el nivel 3**

En este nivel hablamos de una estrategia ISCM que se desarrolla a nivel de sistema (del sistema de información). Esta estrategia se apoya en la gestión del riesgo, no solo a nivel de sistema (nivel 3), sino también en los tres niveles en consonancia con la tolerancia del riesgo. Aunque como ya hemos visto, la estrategia más general es definida en los niveles uno y dos, las políticas y procedimientos más específicos pueden ser desarrollados en el nivel tres (sistemas de información). Incluiremos evaluaciones de controles de seguridad a niveles de sistema y también datos de evaluaciones de métricas muy especificas.

Es decir, obtenemos una estrategia ISCM a nivel de sistema que sirve de complemento a las estrategias de nivel uno y dos y al programa de seguridad de toda la organización.

En definitiva, podemos ver como hay dos tipos de estrategias de ISCM podríamos decir, una que es a nivel global de toda la organización y una más especifica que se aplica a nivel de sistema complementaria de la global.

5.6.2. *Establecer un programa ISCM determinando métricas, frecuencias de la monitorización del estado de seguridad, frecuencias de la evaluación de los controles y la arquitectura técnica ISCM*

Los objetivos que queremos conseguir con la implementación son los siguientes:

- Detección de anomalías y cambios en los ambientes operacional y de los diferentes sistemas información con los que cuenta la empresa.
- Seguimiento de los activos.
- Consciencia de las amenazas.
- Efectividad del control de seguridad.
- Seguimiento del control de seguridad.

Las diferentes sub-etapas a la hora de establecer el programa ISCM son:

5.6.2.1. *Determinación de métricas*

Las métricas nos dan información de las evaluaciones y de la monitorización. Estas métricas se calculan y derivan de una combinación de la monitorización del estado de seguridad, los datos que resultan de la evaluación de los controles de seguridad.

Las métricas pueden ser halladas en cualquiera de los tres niveles. Algunos ejemplos para entender mejor qué es una métrica son el número de vulnerabilidades así como su gravedad, número de intentos de acceso no autorizado que ha habido, umbrales o niveles de tolerancia del riesgo, la puntación del riesgo asociado a una configuración del sistema …

Es importante destacar la fuerte relación que mantienen las métricas con los controles de seguridad, las métricas en parte derivan de los resultados obtenidos con los controles. Es decir que si estos controles de seguridad no son evaluados, esto no tiene ningún sentido, porque la información que contienen las métricas no es fiable. Esto se debe a que cuando hacemos una interpretación de las métricas, suponemos que los controles que se han usado directa e indirectamente para el cálculo de esa métrica han sido implementados y se encuentran trabajando perfectamente.

5.6.2.2. Establecer frecuencias de evaluación y monitorización

Realizar un estudio y determinar las frecuencias con las que se monitorizará el estado de la seguridad y con la que se realizaran las evaluaciones de los controles pertinentes, es algo que podríamos definir como crítico en el proceso.

Podemos poner como ejemplo una serie de situaciones posibles, que pueden darse en la organización y que podrían ayudarnos a la hora de establecer esa frecuencia de monitorización de las métricas y para evaluar los controles de seguridad de los que disponemos:

- Volatilidad de los controles de seguridad. Si los controles varían de forma muy volátil deben ser evaluados mucho más frecuentemente.
- Niveles de impacto del sistema. Si son controles implantados en sistemas con niveles de impacto potencial elevados deben ser evaluados más frecuentemente.
- Controles de seguridad con debilidades identificadas. Cuanto más débiles mayor número de evaluaciones en un menor periodo de tiempo.
- Tolerancia del riesgo de toda la organización. En organizaciones con baja tolerancia al riesgo las monitorizaciones son más frecuentes.
- Informes de amenazas. Si se tienen se deben realizar evaluaciones más frecuentes.
- Informes de vulnerabilidades. Si somos conscientes de que existen vulnerabilidades del sistema realizamos monitorizaciones más frecuentemente.

- Resultados de la evaluación de riesgos. Si no son buenos, es decir, identificamos un alto número de los mismos, aumentará el número de evaluaciones.

5.6.2.3. *Desarrollar arquitectura ISCM*

Las organizaciones establecen como la información debe ser recogida y entregada entre los diferentes niveles, también con el exterior, los requerimientos básicos con los que debe contar esta arquitectura son la recopilación de datos, su almacenamiento, análisis y recuperación, así como una presentación de informes.

5.6.3. *Implementar un programa ISCM y recoger la información relacionada con la seguridad que se necesita para métricas, evaluaciones e informes*

Al implantar el programa ISCM:

La información de seguridad se recoge para que las métricas que hemos determinado antes puedan funcionar, se llevan a cabo evaluaciones de los controles, y toda la información que se genere relacionada con la seguridad se presenta en consonancia con la política y los procedimientos, ambos de toda la organización.

En el ISCM se incluyen todos los tipos de controles que ya hemos visto (operacionales, técnicos y de dirección), las fuentes de información para el estado de la seguridad son las personas, procesos, tecnologías y informes que proceden de la evaluación de los controles.

Para conseguir una efectividad mayor a largo plazo con la automatización de los procesos, debemos intentar usar recogidas, análisis e informe de datos de una forma automatizada donde sea posible.

5.6.4. *Analizar los datos recogidos e informar de los hallazgos hechos y determinar la respuesta más apropiada*

Debemos tener presente que puede ser necesario recoger información adicional para clarificar los datos que ya tenemos de la monitorización.

Después de haber desarrollado la implementación del ISCM, vamos a hablar de una serie de procedimientos clave que son desarrollados por las

organizaciones y que son útiles a la hora de analizar e informar de los resultados de evaluación y monitorización.

Hablaremos de tres puntos:

5.6.4.1. Análisis de datos

Toda la información resultante de ISCM debe ser analizada por las organizaciones en este paso, como ya hemos dicho es probable que esto no sea suficiente y que necesitemos una información adicional que complemente a la anterior. Toda esta información que va a ser analizada puede proceder de diferentes orígenes como de informes que se realizan de forma periódica, informes mucho más automatizados…

5.6.4.2. Informe de las evaluaciones de los controles de seguridad

Para ello se pueden usar plantillas, hojas de calculo o si tenemos un proceso más moderno usaremos una forma mucho más automatizada.

5.6.4.3. Informe de la monitorización del estado de seguridad

Existen procedimientos que permiten informar sobre esta monitorización. Es importante recalcar que los datos relativos al estado de seguridad derivan de la monitorización que se realiza a las métricas determinadas.

5.6.5. Responder a los diferentes hallazgos con actividades de mitigación (que puede ser técnica, de gestión u operacional), con la aceptación del riesgo, con transferencia/compartición o con la anulación/rechazo

Tras ese análisis anterior llega el momento de dar respuestas. Estas respuestas (mitigación del riesgo[36], aceptar el riesgo[37], rechazar/anular[38] el riesgo, transferir/ compartir[39] el riesgo) deben ser hechas teniendo en cuenta la tolerancia del riesgo que estamos considerando.

Las estrategias de respuesta pueden ser implementadas durante un periodo de tiempo, documentando los planes de implementación necesarios en el plan de acción e hitos.

[36] Mitigar el riesgo consiste en disminuir la probabilidad o el impacto del riesgo hasta un umbral aceptable.
[37] Se acepta el riesgo cuando no se ha encontrado ninguna estrategia adecuada.
[38] Eliminar el riesgo, es decir reducir su probabilidad al 0%.
[39] No eliminamos el riesgo, simplemente trasladamos a un tercero la propiedad de su gestión.

5.6.6. *Revisar y actualizar el programa de monitorización, ajustar la estrategia ISCM y las capacidades de medición para mejorar el seguimiento de los activos y el conocimiento de vulnerabilidades*

Todos los programas y estrategias de ISCM no son algo estático, están en continuo movimiento, es decir son dinámicos. Esto quiere decir que los controles de seguridad con los que contemos, las métricas, las frecuencias de evaluación y monitorización cambian con el tiempo según las necesidades de la organización. Es decir, la estrategia ISCM es dinámica, es revisada y actualizada de forma constante para que se adapte a las necesidades de la organización.

CAPÍTULO 6.

COMPARACIÓN ENTRE FISMA Y ISO/IEC 27001

6. Comparación entre FISMA y ISO/IEC 27001

En esta parte cuatro del desarrollo nos dedicaremos a realizar una comparación entre las dos publicaciones o grandes grupos de publicaciones en materia de seguridad de la información que hemos presentado en el trabajo. Estoy hablando de realizar una comparación entre los estándares o normativas que el NIST presenta y la norma principal de la serie 27000, la ISO/IEC 27001.

Haremos el contraste desde el punto de vista de diferentes aspectos:

6.1. Aplicabilidad

La aplicabilidad se encuentra en el primer punto porque es el aspecto en el que podemos ver una diferencia más apreciable entre las dos.

La aplicabilidad de ambas es muy diferente. Por un lado tenemos los estándares de NIST que son utilizados por agencias federales en Estados Unidos, empresas contratistas y todos aquellos que formen parte de la denominada ''Critical infrastructure'' (recordando la definición que dimos en la página 53) , que incluye empresas de servicio público (eléctricas, nucleares…), salud pública y servicios de emergencia, información y telecomunicaciones, defensa nacional, banca y finanzas, correo, transporte, agricultura, agua y comida, y la industria química. Por otro lado la ISO/IEC 27001 es aplicada por organizaciones y empresas que trabajan en un ámbito comercial.

Tenemos que darnos cuenta que las publicaciones de NIST son una respuesta a la tarea que tiene este instituto de realizar el proyecto de implementación de FISMA, es decir, de desarrollar normas, directrices, métodos y técnicas para aportar seguridad de información a los activos y operaciones. En FISMA se establece que el encargado de desarrollar estas normas, directrices, métodos y técnicas debe ser NIST, lo que nos hace ver que esas publicaciones derivan de una ley. Todo esto quiere decir que no son formalmente reconocidas fuera de los sistemas de seguridad nacionales de los Estados Unidos, es decir su aplicación esta limitada a los Estados Unidos de América.

Por otra parte tenemos la ISO/IEC 27001, que es una norma de carácter internacional, que AENOR ha adoptado como UNE-ISO/IEC y que hemos

presentado en la primera parte del proyecto. Al ser una norma de carácter internacional puede ser aplicada en muchos países, no solo en uno, lo que hace la aplicabilidad de esta noma mucho mayor. Es una norma que busca asegurar evaluaciones de seguridad de la información precisas y conformes por todo el mundo. En el caso de Estados Unidos, si nos fijamos en el ámbito de la misma, podemos darnos cuenta de que esta norma está orientada a aquellas empresas u organizaciones que trabajen en un ámbito comercial, no para empresas u organizaciones que tienen una relación de algún tipo con el gobierno, como ocurre en el caso de NIST.

Estos dos marcos (NIST e ISO) son los marcos que más han crecido y más importantes se han hecho en Estados Unidos. Una posible forma de entender la diferencia de aplicabilidad entre ambas, sería plantearse por qué dos tipos de normas en una misma materia (seguridad de la información) pueden llegar a ser tan relevantes en un mismo país al mismo tiempo, ya que sería mas razonable que si estuvieran dirigidas a un mismo propósito, se hubiera optado por una de los dos. La razón es clara, uno de ellos (NIST) tiene una orientación principal a las Agencias Federales del gobierno de Estados Unidos, mientras que la ISO/IEC tiene una orientación a empresas comerciales.

6.2. Limitaciones en el alcance

Hemos hablado de los diferentes objetivos de aplicación que tiene cada uno de los dos marcos, en este apartado 6.2 nos centraremos en algo más preciso, vamos a definir los limites del alcance de cada uno de los marcos normativos.

Los dos marcos enfocan sus principios y sus ideas en dos objetivos diferentes. Por un lado la ISO/IEC 27001 se centra en la organización, mientras que los estándares desarrollados por NIST se centran en los sistemas de información de una organización.

La ISO/IEC especifica mucho más cómo la organización tiene que apoyar la seguridad de la información, es decir, sus límites se centran en la propia organización y en los sistemas de información que se encuentran bajo el control, supervisión y responsabilidad de la organización. El enfoque que ISO/IEC 27001 presenta es muy general, es un punto de vista mucho más alejado del que NIST expone, debe ser un enfoque mucho más general y útil para cualquier organización, ya que como la norma dice, los requisitos que establece la misma son aplicables a todas las organizaciones independiente de su tipo, naturaleza o tamaño.

Por otro lado las publicaciones del NIST desarrollan continuamente aspectos orientados a los sistemas de información, los tipos de información que estos incluyen y los controles de seguridad necesarios para protegerlos. Aunque esto no quiere decir que las publicaciones del NIST estén solo enfocadas a los sistemas de información, también cubre un amplio margen de tipo organizativo.

Sin embargo, aunque cada tipo de estándar se centre o preste más atención a alguno de los dos aspectos (la organización o sistemas de información), no quiere decir que descuide o no preste atención al otro.

6.3. Gestión del Riesgo

La mejor forma para realizar una comparación más clara entre las dos normativas es utilizar como referencia el proceso general de gestión del riesgo. Tenemos que tener en cuenta que realizar un proceso de gestión del riesgo es algo vital y un proceso central a la hora de alcanzar el objetivo de la seguridad de información, independientemente de las necesidades más particulares que pueda tener esa organización en materia de seguridad de la información.

Partiendo de este proceso general de gestión del riesgo intentaremos especificar como establecen el contexto, realizan la evaluación de riesgos, el tratamiento de los riesgos y la comunicación de los mismos, cada una de ellas. En la figura 6.3.1 podemos ver un esquema del proceso más generalizado del que estamos hablando.

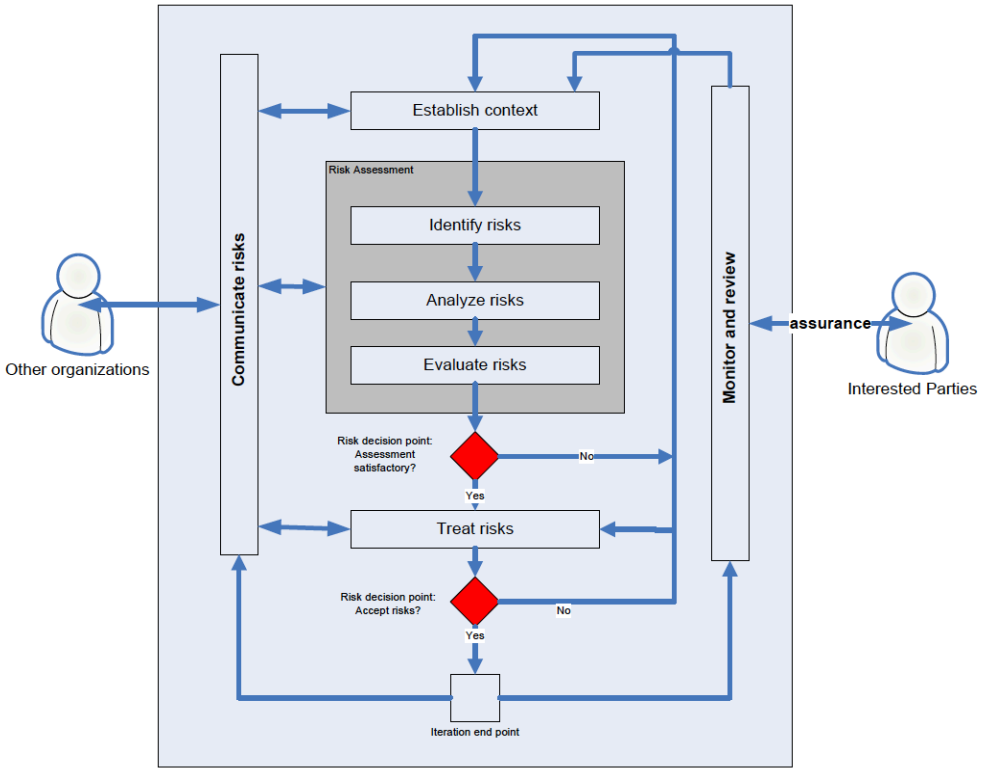

Figura 6.3.1 Proceso general de gestión del riesgo

- Establecer el contexto.

Establecer el contexto consiste en determinar la aplicabilidad y los límites de la organización (lo que hemos explicado anteriormente para cada normativa en los apartados 6.1 y 6.2), los recursos disponibles o con los que podemos contar para realizar la gestión de los riesgos de la organización, las necesidades que tiene la organización y las relaciones que existen con otras empresas. La comunicación de riesgos con otras empresas también es algo bastante importante y por eso es una parte del proceso general del riesgo como podemos ver en la figura 6.3.1.

En el caso de los estándares que han sido desarrollados por NIST podemos decir que el contexto está en gran parte definido, dado que los límites y la aplicabilidad quedó claramente especificado cuando dijimos que básicamente está orientado a sistemas de información y principalmente a agencias federales. En las necesidades además de las particulares que pueda tener esa organización, también encontramos la de cumplir con los requisitos que marca FISMA (la ley de seguridad de la información federal). Las relaciones que este tipo de organizaciones tienen serán principalmente con el gobierno y los recursos con los que puede contar para realizar la gestión de los riesgos, también estarán relacionados con el gobierno.

Para la ISO/IEC 27001 establecer el contexto es algo mucho más particular para cada organización, dado que las organizaciones o empresas que trabajan en un ámbito comercial pueden llegar a ser muy diferentes y estar muy distanciadas unas de otras. De ello podemos darnos cuenta en el momento en que esta norma dice que los requisitos que establece la misma son aplicables a todas las organizaciones independiente de su tipo, naturaleza o tamaño. Esta norma intenta conseguir que se implementen sistemas de gestión de seguridad de la información que se ajusten a las necesidades que presenta la organización, lo cual es algo que tenemos en cuenta a la hora de determinar el contexto, pero siempre estableciendo, implementando, manteniendo y mejorando estos sistemas de gestión de seguridad de la información según los requisitos que marca la norma.

La ISO/IEC 27001 centra la base del proceso de establecer el contexto en la organización, determina que para que se establezca un contexto y este quede bien definido, la dirección de la correspondiente organización debe participar en ello y verse involucrada. Es decir, esta norma plantea los requisitos desde un punto de vista mucho más alejado y general que los estándares que NIST desarrolla, prefiere verlo desde un enfoque de una organización en general, para que sea útil para cualquier organización independientemente del tipo, tamaño o naturaleza.

La idea es que la ISO/IEC te da los requisitos que debes cumplir para tu sistema de gestión de seguridad de la información y después tú debes trabajar con un SGSI que cumpla esos requisitos y que se adecue al contexto de tu organización.

- Evaluación del riesgo

Debemos darnos cuenta que debido a las diferencias en las limitaciones y aplicabilidad que ya hemos mencionado anteriormente tienen que existir algunas diferencias o diferentes formas a la hora de aplicar métodos para la evaluación de riesgos.

Por un lado ISO/IEC 27001, nos habla de un proceso de evaluación del riesgo, que debido al enfoque organizativo que antes presentábamos y que esta normativa hace en relación a la gestión de riesgos, es un proceso de evaluación del riesgo desarrollado a alto nivel. Es decir en la ISO/IEC 27001 no podemos encontrar un proceso que se pueda considerar especifico a la hora de realizar la evaluación de los riesgos, encontramos un apartado denominado apreciación de riesgos en el que nos dice que debemos identificarlos, analizarlos (analizar consecuencias si se materializan, analizar

su probabilidad) y evaluarlos (comparar los resultados del análisis de riesgos con unos criterios de apreciación de riesgos[40] ya establecidos).

Entonces para llevar a cabo esta evaluación, la cual ya viene descrita de una forma muy generalizada en la apreciación de riesgos de seguridad de la información de la norma ISO/IEC 27001, debemos tener en cuenta que:

- A la hora de considerar una organización de forma global, como un todo, se pueden observar varias formas de evaluar los riesgos dentro de esa misma organización. Todo esto se debe a que dentro de una organización podemos clasificar los riesgos entre las diferentes áreas de actuación de la organización. Por ejemplo, los riesgos que existen para los negocios de la compañía (fluctuaciones monetarias, vulnerabilidades del sector que atraigan riesgos) son muy diferentes a los riesgos que puede tener un proyecto o a los pertenecientes a los propios sistemas de información.

- Existen muchas metodologías establecidas a la hora de desarrollar la evaluación de los riesgos, pero eso no quita que una organización pueda desarrollar la suya propia y que se ajuste mucho más a sus necesidades.

Por otra parte, las normativas desarrolladas por NIST son mucho más precisas en este aspecto como hemos podido ver en la presentación de estas publicaciones. Realiza el proceso de identificar, analizar y evaluar en un solo paso que denomina categorización de los tipos de información y sistemas de información.

No solo nos indican como debemos realizar la evaluación de los riesgos en el proceso de categorización establecido en FIPS Publication 199, mediante la explicación de cómo determinar el impacto potencial que tendría una perdida de confidencialidad, disponibilidad o aplicabilidad en un sistema de información a partir de los tipos de información que lo componen, sino que también nos da ya calculados unos valores de impacto potencial que denomina provisionales para cada tipo de información, que se recogen en uno de los volúmenes de Special Publication 800-60, y que después tendremos que revisar y ajustar/finalizar para cada tipo de información.

[40] Teniendo en cuenta la definición de criterios de apreciación de riesgos que dimos en la página 38

- Tratamiento del riesgo

Por otra parte NIST desarrolla SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations (Monitorización Continua de la Seguridad de la Información para Sistemas de Información Federales y Organizaciones), que se centra en la monitorización de los controles de seguridad, habla de una monitorización continua de la seguridad de la información, en esta publicación es donde podemos ver los controles de seguridad que seleccionamos funcionando. En esta publicación se habla de dar una respuesta a los riesgos hallados, y presenta con más detalle este proceso que la ISO/IEC 27001.

Lo especifica en función de los diferentes niveles organizativos que vimos en la página 105. Para el nivel uno la respuesta pueden ser cambios en las políticas de seguridad de toda la organización, aunque estas respuestas pueden estar limitadas por las diferentes funciones de negocio y por limitaciones que tengan que ver con la estructura empresarial (incluyendo los componentes humanos), políticas que no se pueden alterar, o por razones externas. Para el nivel dos estas respuestas pueden ser información relacionada con seguridad adicional, nuevas o modificación de métricas, cambios en los propios procesos de las misiones/negocios de la organización o en los requisitos de información que se piden al nivel tres, y/o modificaciones o adicciones de controles de seguridad. Las limitaciones que se pueden encontrar en el nivel dos pueden ser debidas a las políticas de seguridad de toda la organización y sus estrategias, objetivos de los propios negocios/misiones de la organización y las limitaciones que nos den los recursos de la organización y su estructura. Para el nivel tres recordamos que las estrategias están orientados a un nivel de sistema, las respuestas pueden ser incluir controles adicionales, modificar controles ya implementados, quitar la autorización a sistemas de información que estén ya operando, cambios en la frecuencia de monitorización/evaluación, o análisis más detallados de la seguridad de la información. Para este nivel, las limitaciones a las respuestas son dadas por las políticas de los niveles uno y dos, sus requisitos y estrategias.

Por una parte la ISO/IEC nos dice que se deben seleccionar los controles de seguridad necesarios para implementar las opciones que se hayan elegido en el tratamiento de riesgos.

Ambas tipos de normas prestan mucha atención a la selección de los controles de seguridad. En el caso de la ISO/IEC 27001 existe una lista de controles en el anexo y que se desarrolla en la ISO/IEC 27002, que pueden ser seleccionados por la organización además de los controles que puede

identificar de otras fuentes o realice ella misma. En el caso de NIST, como ya vimos en la página 76 existe una publicación (NIST Special Publication 800-53 Revision 4 , Security and Privacy Controls for Federal Information Systems and Organizations) que trata esta materia.

En NIST Special Publication 800-53 Revision 4 se dan unas tablas (tablas de líneas base) en las que dependiendo del valor del impacto potencial que tenga un sistema de información se le asignan unos controles de seguridad que más tarde serán ajustados a las necesidades de la organización.

En resumen, podemos ver que en el tratamiento de riesgos la publicación del NIST habla de más formas para tratar los riesgos que simplemente los controles de seguridad necesarios para implementar las opciones que se hayan elegido en el tratamiento de riesgos (como cambios en las políticas de seguridad), que es lo único que dice ISO/IEC 27001. Pero a la hora de seleccionar los controles de seguridad, podemos ver como en este aspecto la ISO/IEC 27001 no se queda tan atrás en detalle o especificación respecto a los estándares del NIST, dado que la lista de controles de seguridad que dispone es bastante detallada y precisa.

- Comunicación de riesgos

En el caso de las publicaciones del NIST se define claramente gracias a la figura del "accreditor"[41] y a través del proceso de comunicación con la dirección, a través del informe de certificación los riesgos se comunican al "accreditor". También presenta que se debe informar del estado de seguridad cuando se este realizando el proceso de monitorización continua.

ISO/IEC 27001 habla de la necesidad de comunicar los riesgos residuales a la dirección y la importancia de las comunicaciones tanto internas como externas respectivas al sistema de gestión de seguridad de la información.

- Monitorización

La ISO/IEC 27001 nos marca como requisito las evaluaciones del desempeño, en las que se deben realizar seguimiento, análisis y evaluación, auditorias internas (donde podemos ver como destaca la importancia de la organización, relativa a su enfoque organizativo).

[41] El "accreditor" es la persona dentro de la organización cuya responsabilidad reside en conocer los riesgos y recibir los informes de riesgos para llegar a realizar la acreditación del sistema de información.

Por otra parte NIST tiene una publicación de la que ya hemos hablado en la página 103, SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations (Monitorización Continua de la Seguridad de la Información para Sistemas de Información Federales y Organizaciones), que nos habla de ISCM (Monitorización Continua de la Seguridad de la Información).

6.4. Líneas base

Este concepto es algo que diferencia claramente a los dos tipos de normativas. Es un concepto que aparece en una de las publicaciones del NIST, concretamente en NIST Special Publication 800-53 Revision 4 , Security and Privacy Controls for Federal Information Systems and Organizations (Controles de Seguridad y Privacidad para los Sistemas de información Federales y Organizaciones).

Esta es una publicación que utilizábamos en el segundo paso: selección de los controles de seguridad (página 76). Como dijimos en capítulos anteriores existen tres líneas base para los controles de seguridad que corresponden a los niveles de impacto potencial con los que venimos trabajando, es decir bajo-impacto, moderado-impacto y elevado-impacto, cada una de estas líneas bases se compone de una serie de controles. La organización debe seleccionar una línea base de las tres para cada sistema de información para así tomar esos controles como referencia, nos basaremos en la categorización del sistema que hemos hecho anteriormente para elegir una de las tres líneas bases. Después de haber seleccionado una de estas líneas bases para el sistema, realizamos un proceso de alineación de estos controles que conforman la línea base, modificamos esos controles y los intentamos alinear con las necesidades o condiciones que presente la organización en la que se encuentra el sistema.

También existe otra publicación que NIST ha desarrollado, y de la cual también hemos hablado en la página 90, donde se especifican los requisitos mínimos de seguridad con los que debe contar la información y los sistemas de la información, estamos hablando de FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (Requisitos Mínimos de Seguridad para la Información Federal y Sistemas de Información). Como ya explicamos, estos requisitos vienen expuestos a través de diecisiete áreas que corresponden a diecisiete de las dieciocho familias de controles de seguridad y que debe cumplir el sistema de información, la única familia que se excluye es la familia “PM”, que esta orientada a proporcionar controles de seguridad a nivel organizativo.

Es decir, además de existir un concepto en las publicaciones de NIST que en ISO/IEC ni si quiera aparece, y el cual puede llegar a ser bastante útil a la hora de realizar la gestión de la seguridad de la información, NIST ha desarrollado una publicación exclusiva en el que habla de unos requisitos mínimos para el sistema de información.

ISO/IEC 27001 no hace uso de este concepto y el set de controles que se use queda dirigido a través del proceso de gestión del riesgo. Es decir, como dice la norma se deben elegir los controles que se consideren necesarios para el tratamiento de los riesgos, y comprobando que no se omiten controles que puedan ser necesarios utilizando los que vienen en su anexo o en la ISO/IEC 27002. Es decir, no marca un mínimo preciso, el mínimo es el que satisfaga las necesidades de seguridad de la información.

6.5. Certificación y acreditación

En este apartado hablaremos de una serie de términos que pueden inducir a cierta confusión a la hora de abordar los dos marcos normativos de los que nos estamos ocupando. Esto se debe a que en múltiples ocasiones ambos tipos de normativas utilizan mismos términos o palabras para referirse a ideas muy diferentes, esto a la hora de realizar una comparación o contraste entre ambas puede llegar a confundirnos.

En este punto del trabajo, encuentro oportuno comentar lo siguiente. A la hora de realizar este trabajo fin de grado, no solo se ha intentado llevar a cabo una comparación entre marcos normativos españoles y estadounidenses en materia de seguridad de la información, sino que se ha procurado que este trabajo fin de grado tenga una utilidad y que pueda ser útil si se pretende estudiar cualquiera de los dos marcos normativos de los que venimos hablando todo el trabajo. Respecto a esto último, este apartado 6.5 se considera como uno de los puntos fuertes de este trabajo, ya que aunque no es tan amplio como alguno de los diferentes apartados que hemos desarrollado, nos da una información bastante relevante.

Esta información relevante consiste en una serie de diferencias que existen entre ambos marcos normativos, en base a conceptos clave que trata cada uno de ellos. Es decir, este apartado podría ser útil, si un usuario quisiera estudiar los dos marcos normativos en seguridad de la información y antes de comenzar quisiera estar seguro de que no va a tergiversar ninguno de los términos que se presentan. Ya que debemos tener en cuenta que a la hora de estudiar una norma es importante conocer la jerga que utiliza la misma, este

apartado nos permite un acercamiento a esa jerga sin necesidad de leer toda la norma para llegar a conocerla.

- Sistema.

Debido a las diferentes ideas que describe esta palabra, podemos suponer de partida que existirán diferencias en cada marco normativo.

Cuando en algunas de las publicaciones del NIST se hace mención a la palabra sistema, se refiere a un sistema de información que se quiere proteger frente a posibles riesgos y para el cual se seleccionan unos controles después de haberlo categorizado. Esto se debe a que este tipo de normativa está más orientado a los sistemas de información como hablábamos antes.

Cuando ISO/IEC 27001 habla de un sistema, la gran mayoría de los casos se esta refiriendo al sistema de gestión de la seguridad de la información que nos ayuda a implementar cumpliendo unos requisitos que expone la norma. Esto no quita que algunas veces, en las que bien podemos identificar por el contexto o porque viene detallado explícitamente, hable de sistema como un sistema de información que necesita esa protección de su información.

- Certificación.

En el caso de NIST es una evaluación exhaustiva de los controles de seguridad tanto operacionales, de dirección y técnicos que se encuentran en un sistema de información, para determinar la medida en la que los controles están implementados correctamente y funcionan como es debido. Unos evaluadores auditan, evalúan y comprueban que los controles se hayan implementado de forma correcta. Es decir, simplemente nos fijamos si esos controles han sido implementados de forma correcta, todo esto se realiza durante la evaluación de dichos controles. Voy a evaluar esos controles ya que quiero saber si funcionan, la comprobación de si producen el efecto deseado lo dejaré para la acreditación.

En el caso de ISO/IEC 27001 entra en juego la conformidad del sistema de gestión con la norma. Cuando un cuerpo de certificación independiente a la organización asegura que el sistema de gestión es conforme con la ISO/IEC 27001.

- Acreditación.

En el caso de las publicaciones de NIST, el termino acreditación es usado para referirse a que el sistema de información se encuentra certificado y

autorizado para que funcione. Es decir, autorizamos el funcionamiento del sistema de información y aceptamos de forma explicita el riesgo que ocasiona para los activos y las operaciones. Por lo tanto esta acreditación incluye la certificación de la que hablábamos antes, pero la acreditación va más allá de realizar esa evaluación de los controles de seguridad, que es básicamente lo que realiza el evaluador en la certificación, esta acreditación también considera autorizar el funcionamiento del sistema de información dada una tolerancia de los riesgos (según la definición de tolerancia de los riesgos que dimos en la página 107). No solo he mirado si los controles funcionan como es debido, sino que ahora voy a ver si lo riesgos que hay mientras ellos funcionan son de una cantidad relevante para la tolerancia de riesgo que tengo definida en mi organización.

En ISO/IEC 27001 cuando aparece el termino acreditación se refiere a que un cuerpo de certificación ha cumplido con las normas de un organismo de acreditación, por ejemplo ENAC con AENOR. El papel de las agencias de acreditación es acreditar a la organizaciones que realizan las auditorías de conformidad, es decir a los "organismos de certificación".

6.6. Casos en los que una integración FISMA y ISO/IEC 27001 sería adecuada

Podemos considerar dos casos en los que una integración de ambas normas podría ser adecuada:

- Puede ser que una organización no relacionada con el gobierno, que hace uso de ISO/IEC 27001, pueda encontrar beneficios a la hora de aplicar, simplemente fijarse o tomar ideas de alguna de las publicaciones que ha desarrollado NIST.

- También puede darse el caso de que alguna organización que actué como contratista del gobierno de Estados Unidos, encuentre en el marco que desarrolla la ISO/IEC 27001 beneficios o una integración completa con la aplicación de FISMA.

6.7. Legibilidad

La legibilidad es la capacidad o posibilidad que tiene un texto de ser leído, por su claridad. Es decir cómo de fácil es leer y entender la documentación.

En este aspecto podemos decir que es el único aspecto en el que la ISO/IEC 27001 supera claramente a las normas del NIST. Podemos darnos cuenta

claramente que cuando estás leyendo la ISO/IEC 27001 es mucho más fácil de comprender y de entender, además gracias a AENOR disponemos de esta norma en español. Lo único que se puede hacer un poco más detallado y técnico son los controles que aparecen en el anexo, que son los mismos que aparecen en la ISO/IEC 27002 pero sin estar explicados de una forma tan detallada.

Las normas que NIST ha desarrollado son mucho más complejas y difíciles de leer, sobre todo porque debemos tener presente que estamos hablando de un conjunto amplio de publicaciones que están muy detalladas y son muy especificas a la hora de gestionar los riesgos, además están dirigidas a un lector que tenga una habilidad elevada de lectura en inglés, el estudio de estas publicaciones puede comportar mucho tiempo. Uno de los problemas principales que nos podemos encontrar cuando estamos leyendo una de las publicaciones para alguno de los pasos del marco de gestión del riesgo, como puede ser para la categorización FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, es que continuamente esta citando apartados, puntos, anexos y definiciones que se encuentran en otras publicaciones, lo que hace que para poder seguir entendiendo esa misma norma tengas que cambiar de norma por un instante, de esta forma la lectura nunca puede ser continua.

En resumen, la ISO/IEC 27001 utiliza una jerga empresarial, clara, simple y mucha más cercana al lector, mientras que las publicaciones del NIST están escritas en una jerga mucho más cercana al gobierno, mucho más formal. En NIST tenemos la SP800-39 que ayuda a dar una visión general al proceso, pero siempre hay que profundizar y por consecuencia nos encontramos con la gran cantidad de publicaciones que tiene. En este aspecto ISO/IEC 27001 da una visión mucho más general al proceso, pero sin estar tan detallado.

6.8. Disponibilidad

En este aspecto NIST brilla mucho más que ISO/IEC 27001. En la página web de NIST podemos encontrar todas las normas de las que hemos estado hablando y lo que es más importante, de forma totalmente gratuita, solo necesitamos descargarlo a través de internet.

Por otra parte las publicaciones que ISO desarrolla se pueden descargar a través de Internet y todas tienen un precio. Descargar la ISO/IEC 27001 en español a través de AENOR, es decir como norma UNE, tiene un precio que ronda los cuarenta euros. No es la más cara, es de las más baratas, ya que por ejemplo, si queremos conseguir la ISO/IEC 27005 en español en internet,

lo podemos hacer a través del UNIT (Instituto Uruguayo de Normas Técnicas) ya que no se encuentra en español a través de AENOR, pero nos encontramos con el problema de que su precio es de 315 dólares.

6.9. Dominios de seguridad cubiertos

En este apartado lo enfocaremos a una visión completa de las normas de la serie 27000, no solo prestaremos atención a la ISO/IEC 27001, sino a toda la serie.

En la tabla 6.9.1 podemos ver los diferentes campos o dominios que cubren cada uno de los marcos normativos, los estándares del NIST y la serie ISO 27000.

Característica técnica de Seguridad	FISMA	ISO 27000
Categorización del sistema	Sí	No
Identificación de Riesgos del Sistema	Sí	Sí
Establecer políticas de seguridad	Sí	Sí
Identificación de controles de seguridad	Sí	Sí
Referencia a la seguridad en las redes	Sí	Sí
Especificaciones de configuración	Sí	Sí
Disposiciones para la privacidad de los datos del usuario	Sí	Sí
Consideraciones de seguridad para el ciclo de vida del sistema	Sí	Sí
Seguridad para PDA y teléfonos móviles	Sí	No
Seguridad de los servidores	Sí	Sí
Protección de la confidencialidad de la información de identificación personal	Sí	Sí
Seguridad bluetooth	Sí	No
Métodos usados en autentificación de acceso para redes wireless	Sí	Sí
Uso de credenciales PIV en sistemas de control de acceso físico	Sí	Sí
Comprobación y evaluación de la seguridad de información	Sí	Sí
Dispositivos externos de seguridad para teletrabajo y acceso remoto	Sí	No
SSL in VPNs	Sí	Sí

Tecnologías de encriptación de almacenamiento para los dispositivos del usuario	Sí	Sí
Key derivation que usa funciones pseudoaleatorias	Sí	No
Aplicaciones que usan algoritmos Hash	Sí	Sí
Seguridad de sistemas de identificación por radiofrecuencia	Sí	No
Wireless Robust Security Networks IEEE 802.11i	Sí	Sí
PIV Card to Reader Interoperability	Sí	No
Servicios de seguridad web	Sí	Sí
Detección de intrusiones y sistemas de prevención (IDPS)	Sí	Sí
Gestión de registros de seguridad computacionales	Sí	Sí
Generación de números aleatorios que usan Deterministic Random Bit Generator	Sí	No
Seguridad para las aplicaciones de firma electrónica	Sí	No
Introducción de técnicas forenses en la respuesta a incidentes	Sí	No
Guías para comprobar modelos de datos de PIV	Sí	No
Guías para comprobar interfaces Middleware y aplicaciones de tarjetas PIV	Sí	No
Comprobación, entrenamiento y programas de prácticas para planes de tecnología de la información	Sí	Sí
Prevención de incidentes malware	Sí	Sí
Seguridad de DNS	Sí	No
Guía para la acreditación de distribuidores de tarjetas PIV	Sí	No
Algoritmos de cifrado y tamaños de clave para PIV	Sí	No
Especificación de datos de biometría para PIV	Sí	Sí
PDA Forense	Sí	No
Programa checklist para productos IT- Guías para usuarios del checklist y desarrolladores	Sí	No
Seguridad de Microsoft Windows XP	Sí	No

Seguridad de los sistemas Microsoft Windows XP para profesiones de la tecnología de la información	Sí	No
Triple Data Encryption Algorithm (TDEA) Block Cipher	Sí	No
Seguridad de las tecnologías de la información en el planeamiento financiero y el proceso de control de inversiones	Sí	No
Consideraciones de seguridad en el ciclo de vida del sistema	Sí	Sí
Guía de autentificación electrónica	Sí	Sí
Gestión de incidentes de seguridad en los ordenadores	SÍ	Sí
Asignación de tipos de información y sistemas de información a categorías de seguridad	Sí	Sí
Consideraciones de seguridad para Voice Over IP Systems	Sí	No
Gestión de claves	Sí	Sí
Guía para las medidas de rendimiento para la seguridad de la información	Sí	Sí
Controles de seguridad para sistemas de información federales	Sí	No
Selección y uso de implementaciones de Transport Layer Security (TLS)	Sí	Sí
Construcción de un programa de entrenamiento y concienciación de seguridad para las tecnologías de seguridad	Sí	No
Seguridad en sistemas de la tecnología de la información interconectados	Sí	Sí
Seguridad para teletrabajo y acceso remoto de las empresas	Sí	Sí
Guías para la seguridad del correo electrónico	Sí	No
Asegurar servidores web públicos	Sí	Sí
Política de firewall	Sí	Sí
Programa de gestión de vulnerabilidades y parches	Sí	Sí
Selección de productos de seguridad de información	Sí	Sí

Servicios de seguridad de información	Sí	Sí
Sistemas de tecnología de la información para planes de contingencia	Sí	Sí
Principios de ingeniería para la seguridad de la información	Sí	Sí
Análisis de vulnerabilidades	Sí	No

Tabla 6.9.1 Dominios de seguridad cubiertos por estándares NIST y serie ISO 27000

Después de ver los diferentes campos o dominios que cubren cada uno de los marcos normativos, los estándares del NIST y la serie ISO 27000, nos damos cuenta que en la mayoría de estos dominios los estándares del NIST sobrepasan a los de ISO. Esto viene representado en la figura 6.9.1 donde podemos ver como el alcance que tiene NIST es mucho mayor que el que tiene ISO.

Figura 6.9.1 Alcance estándares NIST y serie ISO 27000

6.10. Estadísticas en España y Estados Unidos en certificaciones de ISO/IEC27001

En las figuras 6.10.1 y 6.10.2 podemos ver unos gráficos que muestran la cantidad de certificaciones desde 2009 para España y Estados Unidos. Estos gráficos vienen acompañados de las tablas 6.10.1 y 6.10.2 respectivamente que contienen los datos.

Figura 6.10.1
Certificaciones ISO 27001 España

Año	Certificaciones
2006	23
2007	93
2008	203
2009	483
2010	711
2011	642
2012	805
2013	799

Tabla 6.10.1 Certificaciones ISO
ISO 27001 España

Figura 6.10.2
ISO 27001 Estados Unidos

Año	Certificaciones
2006	69
2007	94
2008	168
2009	252
2010	247
2011	315
2012	415
2013	566

Tabla 6.10.2 Certificaciones
ISO 27001 Estados Unidos

Podemos ver como España estuvo por detrás en número de certificaciones hasta el año 2008, llegando a superar en más de doscientas certificaciones en el año 2013.

El TOP 10: Norma ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información en todo el mundo, es el siguiente:

Puesto 10: Estados Unidos con 566 certificados.
Puesto 9: Alemania con 581 certificados.
Puesto 8: España con 799 certificados.
Puesto 7: Rumania con 840 certificados.
Puesto 6: Taiwán con 861 certificados.
Puesto 5: Italia con 901 certificados.
Puesto 4: China con 1710 certificados.
Puesto 3: Reino Unido con 1.923 certificados.
Puesto 2: India con 1.931 certificados.
Puesto 1: Japón con 7.084 certificados.

Como podemos ver en la clasificación España posee la octava posición a nivel mundial, algo que puede ser beneficioso para nuestro país. Dos posiciones por detrás queda Estados Unidos, que teniendo en cuenta la diferencia de tamaño y avances tecnológicos entre España y Estados Unidos es algo remarcable.

En la figura 6.10.3 podemos ver un mapa de la densidad de certificaciones a nivel mundial ISO 27001.

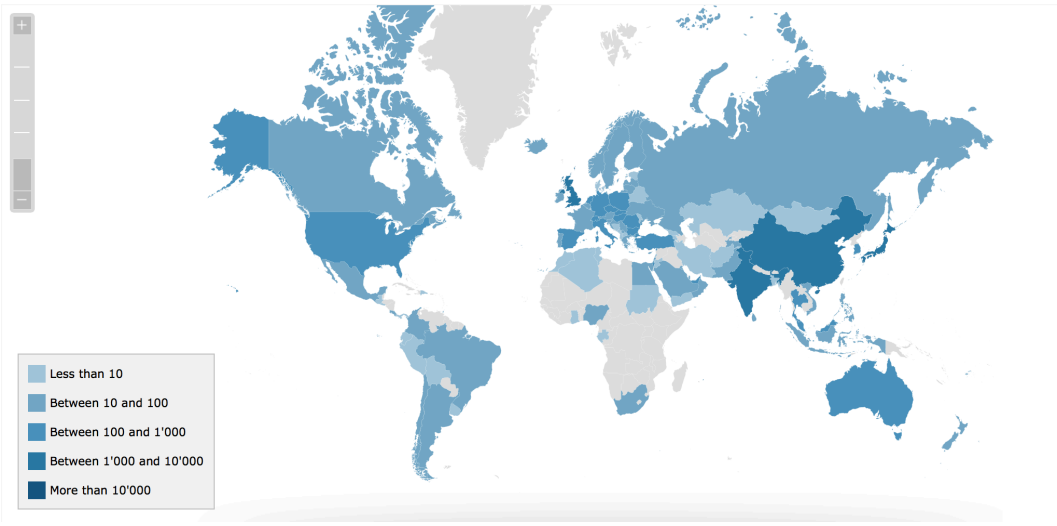

Figura 6.10.3 Mapa de la densidad de certificaciones a nivel mundial ISO 27001

CAPÍTULO 7.

CONCLUSIÓN

7. Conclusión

Hemos discutido y hablado sobre los estándares de NIST e ISO/IEC 27001, presentando lo que expone cada uno, a lo que se refieren y hablando de sus similitudes y diferencias.

El marco que FISMA propone es poco probable que adquiera una relevancia fuera de Estados Unidos, mientras que la norma ISO/IEC 27001 es una norma internacional que puede ser relevante a nivel mundial, y que se utiliza a menudo por organizaciones con una presencia global o internacional, como en las empresas y organizaciones españolas.

También debemos tener en cuenta que las normativas de seguridad de la información deben estar en continuo desarrollo y actualización, de no ser así no podrían cumplir con los nuevos requisitos que presentan las organizaciones, por la utilización de nuevos dispositivos o por los avances tecnológicos a los que la sociedad está sometida de forma continua. Si las normativas en materia de seguridad de la información no se renovasen, modificasen o añadieran nuevos aspectos podrían perder su eficiencia y efectividad.

No hay que olvidar que no solo es importante la aplicación de los requisitos que una norma expone, sino que igual de importante es estudiar y conocer cómo una implementación influirá en los procesos de la organización, de esta forma podremos actuar con antelación ante problemas derivados de la implementación.

Ambos marcos normativos aún continúan mejorándose y madurando, la serie ISO 2700 está pendiente de recibir nuevas normativas de la serie de las que solo han sido titulados o definidos sus contenidos por el momento. Igualmente sucede con las publicaciones del NIST, en las que por el momento existen una gran cantidad de publicaciones que se encuentran en estado de borradores y que llegarán a ser normas en breve.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Se han seguido las normas APA para realizar las referencias bibliográficas.

NIST. (2004). FIPS Publication 199 , Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, USA: NIST

NIST. (2008). Special Publication 800-60 Rev 1 (Volume 1, Volumen 2), Guide for Mapping Types of Information and Information Systems to Security Categories. Gaithersburg, USA: NIST

NIST. (2013). NIST Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg, USA: NIST

NIST. (2006). FIPS 200 Minimum Security Requirements for Federal Information and Information Systems. Gaithersburg, USA: NIST

NIST. (2010). NIST Special Plublication 800-53A Rev 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Gaithersburg, USA: NIST

NIST. (2010). NIST Special Publication 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Gaithersburg, USA: NIST

NIST. (2011). NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations. Gaithersburg, USA: NIST

ISO/IEC (2014). ISO/IEC 27001. Madrid, España: AENOR

Universidad de Burgos.(2011). ¿Qué recursos debo utilizar para buscar normas ISO, UNE y EN?. Consultado el 21 de Mayo de 2015 desde: http://www.ubu.es/bubu/es/inforgeneralbubu/preguntas-frecuentes-faq/busqueda-informacion-faq/informacion-bibliografica-faq/recursos-debo-utilizar-buscar-normas-iso-une

Constantine Gikas, Program Manager.(2010). Information Systems Security: A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Consultado el 21 de Mayo de 2015 desde: https://www.catapulttechnology.com/pdf/Insights_Files/white_papers/Information_Security_White_Paper.pdf

HITRUST.(2013). Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53. Consultado el 21 de Mayo de 2015 desde: https://www.atsec.com/downloads/documents/FISMA_27001.pdf

Christine Kuligowski.(2009). COMPARISON OF IT SECURITY STANDARDS. Consultado el 21 de Mayo de 2015 desde: http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf

Sbqconsultores.(2010). Consultora de Sistemas de Gestión y Normas ISO. Consultado el 21 de Mayo de 2015 desde: http://www.sbqconsultores.es/el-top-10-de-la-norma-iso/

Priteshgupta.(2005). ISO 27000. Consultado el 21 de Mayo de 2015 desde: http://www.iso27000.es

NIST.(2014). Federal Information Security Management Act (FISMA) Implementation Project. Consultado el 21 de Mayo de 2015 desde: http://csrc.nist.gov/groups/SMA/fisma/

Maurice Frayssinet Delgado.(2011): Taller de Implementación ISO 27001. Consultado el 21 de Mayo de 2015 desde: http://www.ongei.gob.pe/docs/ISO_27001_v011.pdf