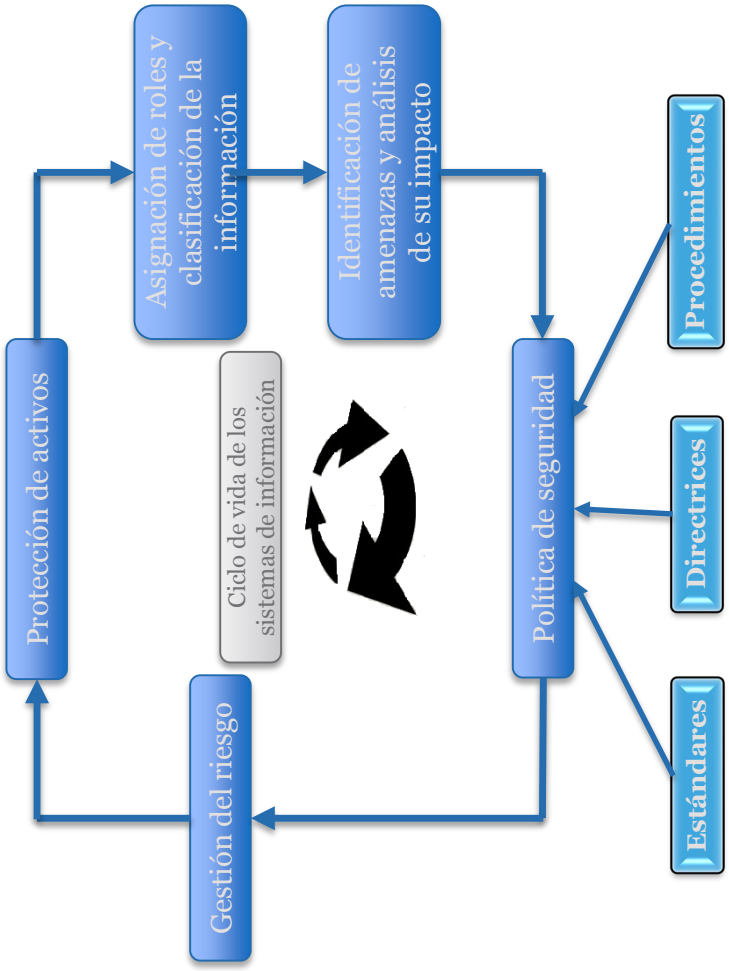
Planificación en la gestión de la seguridad

TEMA 2

Esquema



Ideas clave

2.1. ¿Cómo estudiar este tema?

Para estudiar este tema lee las **Ideas clave** que te presentamos a continuación.

Además tendrás que leer el **capítulo 1 (páginas 1-45)** de siguiente libro disponible en la Biblioteca Virtual de UNIR:

Álvarez, G. y Pérez, P.P. (2004). *Seguridad informática para empresas y particulares*. Madrid: Mc Graw Hill.

El objetivo de este tema es abordar la necesidad de realizar una planificación rigurosa de la seguridad en los sistemas de información que identifique los diferentes activos que son más susceptibles de ser amenazados y que planifique los controles a implementar para mitigar los posibles riesgos. Los elementos claves de tal planificación son:

- Identificar todas las etapas involucradas en la concreción de una política de seguridad y establecer sus consecuencias en la gestión de activos de información.
- Subrayar la necesidad de establecer roles y asignar tareas en base al principio de mínimo privilegio.
- Destacar la importancia del equilibrio entre seguridad y usabilidad.
- Definir el concepto de amenaza e impacto de una amenaza.
- Definir el concepto de riesgo en el ámbito de los SGSI.
- Concretar la necesidad de llevar a cabo políticas de seguridad mediante la creación de adecuados estándares, directrices y procedimientos de seguridad.

2.2. Conceptos relativos a la gestión de la información: ciclo de vida de los sistemas de información y análisis de compromisos

La ISO 27001 determina cómo se gestiona la seguridad de la información mediante un sistema de gestión de seguridad de la información. Este SGSI se compone de distintas fases que se deben implementar secuencialmente para minimizar los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

La primera de las fases es la planificación, que sirve para planificar la empresa y establecer los objetivos de seguridad de la información y elegir los controles correctos de seguridad. La etapa se compone de los siguientes pasos que pueden ampliarse en la web de **ISO 27001**: https://normaiso27001.es/fase-4-planificacion-del-sgsi/

- Inventario de activos.
- Catálogo de amenazas.
- Valoración de las amenazas para la seguridad de la información.
- Identificar activos, vulnerabilidades y amenazas.
- Análisis de riesgos.
- Evaluación de riesgos.
- Plan de tratamiento de riesgos.
- Selección de controles: declaración de aplicabilidad que detalle todos los controles aplicables.

Si no se planifica con atención las actividades de seguridad de la información, es posible que se pase por alto algo importante, lo que se traduce en gastos económicos. Por estos motivos, ISO 27001 trae una fase de planificación bastante compleja y necesita de la redacción de diferentes documentos y la ejecución de varias actividades, siendo la evaluación y tratamiento de riesgos el eje central de esta fase debido a que pone las bases para la etapa de implementación, mediante la definición de controles de seguridad aplicables.

El despliegue de un SGSI requiere en primer lugar determinar su alcance, es decir, proceder a la identificación de los activos del sistema. El siguiente paso engloba la concreción de políticas, estándares, directrices y procedimientos de seguridad. Tal proceso demanda la cuantificación de la importancia de los activos mediante la identificación de las amenazas a la tríada CID y la tasa de ocurrencia de dichas amenazas.

Los SGSI son de carácter procesual, es decir, no se puede asumir sin más que los mecanismos y procedimientos implantados satisfacen todas nuestras expectativas. En este sentido hay que hablar del **ciclo de vida de los sistemas de información** (*System Development Life Cycle –SDLC-*)

Figura 1. SDLC o ciclo de la vida de los sistemas de información.

El desarrollo de un sistema de información consta de una serie de fases:

- **Fase de iniciación** en la que se definen el conjunto de expectativas y los requisitos a satisfacer.
- **Fase de desarrollo y de adquisición,** cuyo objetivo es diseñar el sistema que cubre las expectativas anteriormente destacadas, lo cual requiere llevar a cabo una recolección de información de cara a seleccionar y configurar las tecnologías adecuadas.
- **Fase de implementación:** se produce una vez que se cuenta con un diseño.
- **Fase de operación y mantenimiento**.

Una vez implementado el sistema hay que verificar que el sistema se adecúa a nuestros objetivos y en caso contrario, habrá que llevar a cabo las modificaciones y actualizaciones oportunas.

Asimismo hay que tener en debida consideración el hecho de que nuestro SGSI deje de ser operativo por motivos de actividad de negocio o consideraciones tecnológicas. De esta forma, dentro del ciclo de vida debe tenerse en cuenta la **eliminación** de *software, hardware* e información que no se desea que sea reutilizada por terceros.

En cada una de las anteriores **etapas la identificación de activos de información y la definición de los procedimientos correspondientes** están orientadas a **preservar** las propiedades de **confidencialidad, integridad y disponibilidad**.

Dependiendo del tipo de actividad de nuestro negocio y de la naturaleza de cada activo, se hará énfasis en una o varias propiedades frente al resto. Por ejemplo, en un sistema

de control de tráfico aéreo ha de existir un alto nivel de integridad y disponibilidad de datos.

En el caso de una compañía de automóviles, por el contrario, prima la confidencialidad de los datos de clientes. En cualquier caso, la combinación de confidencialidad, disponibilidad e integridad permite a la empresa conseguir de forma eficiente sus objetivos, al mismo tiempo que se transmite al cliente la sensación de sistema confiable.

Desde el punto de vista de un auditor de seguridad se ha de verificar que se cumplen tal tipo de premisas, así como las consecuencias y resultados esperados de la implantación de un SGSI basadas en tales premisas. Dicho de otro modo**, el auditor ha de constatar que la filosofía de seguridad (ver el gráfico) de una empresa está alineada con su plan de negocio**.

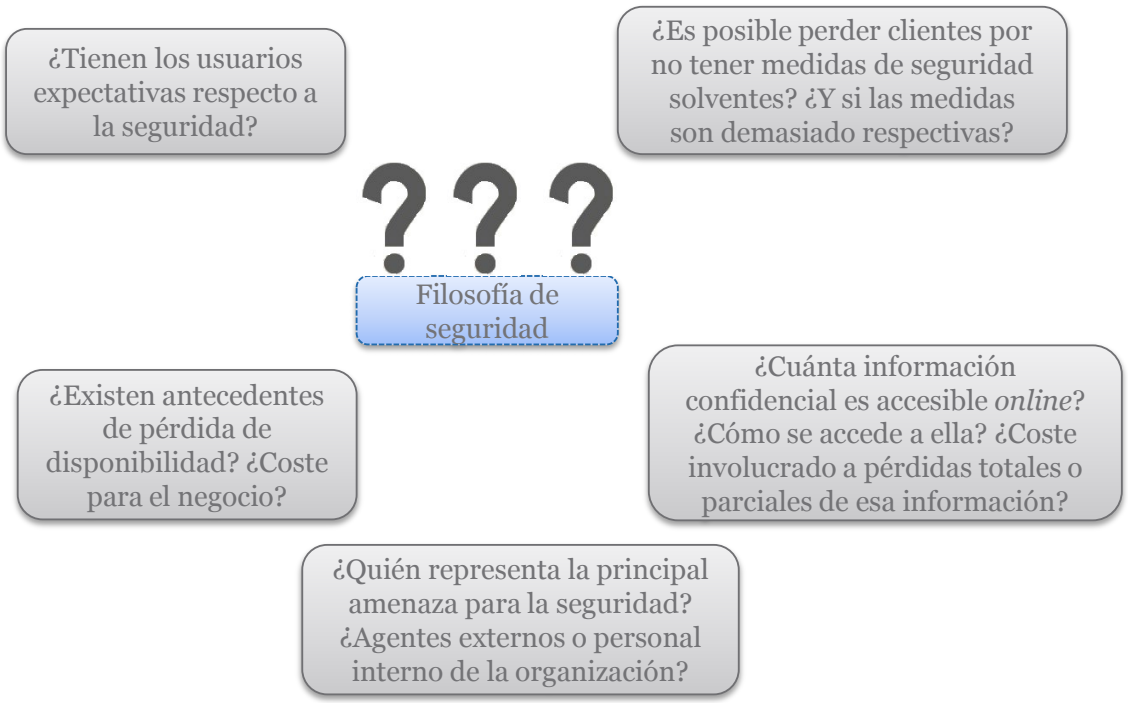


Figura 2. Filosofía de seguridad.

A modo ilustrativo, consideramos los principios de diseño de SGSI que propone el organismo nacional de estándares norteamericano, el NIST (*National institute of standards and technology*). Tales principios deben tenerse en cuenta en el diseño del sistema y además debe llevarse un control exhaustivo de la satisfacción de los mismos durante todo el ciclo de vida del sistema. El papel de la verificación de la calidad y auditoría es por tanto de suma importancia para concluir la solvencia de nuestro sistema.

En junio de 2004 el NIST publicó una guía técnica de recomendación con la numeración NITS SP 800-27 y titulada *Engineering principles for information technology Security (A baseline for achieving security)* de Stoneburner, Haydem y Feringa, (2004). Este documento fue revisado y mejorado por Ross, McEvilley y Oren (2016), dando lugar a la guía NIST 800-160 titulada *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the engineering of Trustworthy secure systems*.

Del conjunto total de **principios de diseño** incluidos por el NIST cabe destacar los siguientes:

- **Principio 1**: establecer una política sólida como base del diseño del sistema.
- **Principio 2:** tratar la seguridad como parte constituyente del sistema en global.
- **Principio 6:** asumir todo sistema externo como inseguro.
- **Principio 7:** identificar posibles compromisos entre reducir riesgos e incrementar costes, así como cualquier decisión de seguridad que implique un empeoramiento del rendimiento en otras actividades.
- **Principio 16:** implementar una seguridad por capas para impedir la existencia de un punto aislado de vulnerabilidad.
- **Principio 20:** aislar puntos de acceso al exterior desde elementos críticos.
- **Principio 21:** separar claramente los dispositivos del resto de equipos.
- **Principio 25:** minimizar el número de elementos confiables.
- **Principio 26:** implementar el principio del mínimo privilegio.
- **Principio 27:** no implementar mecanismos de seguridad innecesarios.
- **Principio 32:** autenticar usuarios y procesos con el objeto de asegurar decisiones apropiadas de control de acceso, tanto dentro de un dominio como a través de diversos dominios.
- **Principio 33:** emplear identidades únicas con el objeto de posibilitar la trazabilidad (*accountability*).

El **principio de mínimo privilegio** en seguridad es heredero de las bases de diseño de interfaces de programación o, si se prefiere, de los elementos base de la ingeniería del *software*.

En efecto todo componente de un sistema complejo ha de tener acceso solo a aquellos recursos que le hacen falta para poder llevar a cabo su tarea.

En el siguiente enlace se recalca la importancia de este principio en seguridad:
http://blogthinkbig.com/principio-de-minimo-privilegio/

Una de las primeras conclusiones que podemos extraer de la anterior colección de recomendaciones es la no necesidad de sobrecargar nuestro sistema con medidas de seguridad (Principio 27).

El uso de las facilidades de un sistema de información no debe verse degradado por la implantación de medidas de seguridad y si hay un impacto, este ha de ser mínimo. En definitiva, es preciso buscar un equilibrio entre protección de activos y el uso de las TIC de nuestro negocio (Principio 7).

El **despliegue de las medidas de seguridad** de un SGSI ha de **evitar interferencias** con respecto a la **actividad principal** de nuestro negocio. En efecto, hay que dimensionar sensatamente las medidas de seguridad: **la seguridad no debe ser enemiga de la eficacia**.

La cumplimentación de ese equilibrio entre objetivos de seguridad y la operatividad requiere la ejecución de un **análisis de compromisos** (***trade-off analysis –TOA***), que comprende **tres etapas**:

- **Definición del objetivo**. En este punto nos referimos a objetivos de seguridad y es recomendable llevar a cabo una ponderación de objetivos. Tal ponderación puede efectuarse mediante lo que se denomina como **medidas de eficacia** (*measures of effectiveness* –MOEs).
- **Identificación de posibles alternativas**. De acuerdo con los objetivos se procede a generar un conjunto de alternativas que faciliten su consecución.
- **Comparación de alternativas**. Cada una de las alternativas tiene asociada un conjunto de medidas de eficacia o MOEs. La comparativa se realizará de acuerdo con las MOEs de las distintas posibilidades contempladas.

2.3. Clasificación de la información: objetivos, conceptos y roles

Otro elemento implícito a los principios NIST de diseño de SGSI es el de la **categorización de la información**. Dicha clasificación es crucial en la fase de iniciación de un sistema pero también lo es tanto en la implementación como en la etapa de desarrollo y mantenimiento.

En este punto cabe destacar la importancia de una **correcta clasificación de nuestros activos de información de cara a ulteriores auditorías**, ya que el tipo de control y de operaciones permitidos estará dado por el tipo de activo de información considerado.

Por último, la clasificación de la información es **crucial para diseñar planes de continuidad de negocio** (*business continuity planning* – BCP) y **planes de recuperación ante desastres** (*disaster recovery planning* – DRP).

El **dueño de la información** es el encargado de valorar el grado de importancia y las implicaciones de la misma. No todos los activos de información tienen el mismo valor y lo que es más, su valor generalmente va a depender de quién accede a los mismos. Por ejemplo, la información no tiene el mismo valor para un analista de sistemas que para un ejecutivo. De modo general podemos distinguir los sistemas de clasificación gubernamentales de los sistemas del sector privado:

- **Clasificación gubernamental**. En este caso los activos se diferencian en función del peligro que entraña el carácter público de la información. Se establecen cinco niveles de información (ordenados de menor a mayor protección):

  - Información no clasificada.
  - Información sensible pero no clasificada.
  - Información confidencial.
  - Información secreta.
  - Información de alto secreto.

- **Clasificación en el sector privado**. En este caso se establecen los siguientes niveles ordenados de menor a mayor control de acceso:

  - Información pública.
  - Sensible.
  - Privada.
  - Confidencial.

Una organización establece las distintas categorías en función de sus exigencias respecto a la tríada CID. Para cada una de esas categorías se establece un **nivel bajo, medio o alto de seguridad**. Por ejemplo, en el caso de información sensible un nivel alto de

seguridad implica que la pérdida de información pueda provocar muerte, encarcelamiento, gran pérdida económica o una acción legal contra nuestra organización. Una pérdida de información sensible de nivel medio lleva asociado un coste económico.

En el caso de información sensible de nivel bajo el acceso no autorizado o su filtración involucraría mínimas pérdidas económicas o acciones administrativas en contra de nuestro organismo.

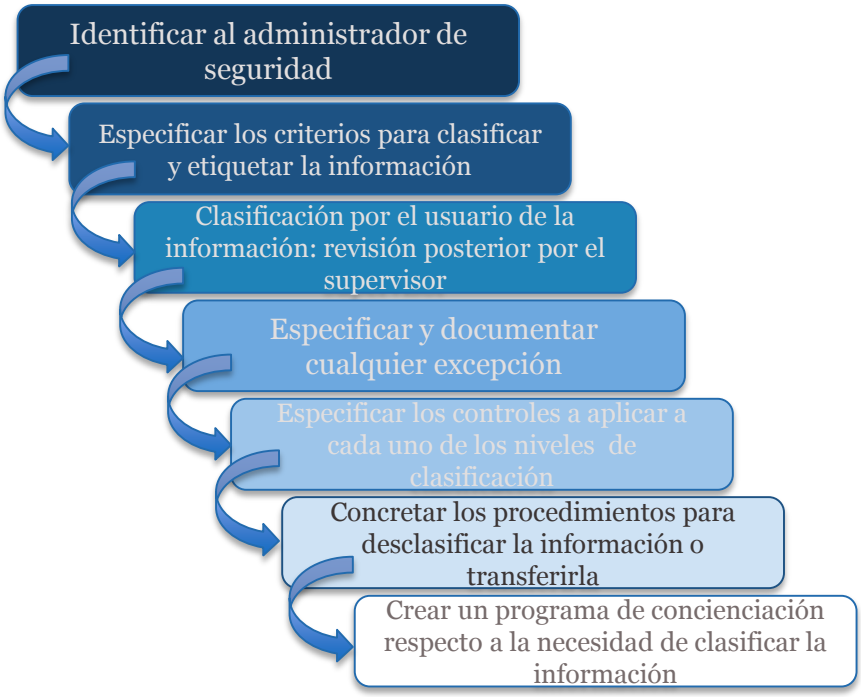


Figura 3. Procedimiento de clasificación de información.

Al margen del tipo de organización (gubernamental versus privada), todo sistema de clasificación ha de partir indefectiblemente de un esquema de distribución de tareas entre los miembros de una organización.

Tal y como queda reflejado en la gráfica de procedimiento de clasificación de información, hay que tomar como **punto de partida** la asignación del **rol de administrador** (o administradores) de seguridad que no serán sino las personas encargadas de implantar los procedimientos de seguridad de acuerdo con el **nivel de clasificación** establecido.

Dicha clasificación **competerá fundamentalmente a los propietarios** de la información que establecerán criterios de acceso a sus activos. Estos criterios han de ser

validados y aceptados por los supervisores de cada una de las áreas en las que están localizados cada uno de los activos. Todo este proceso de clasificación es de carácter transversal y debe hacerse un esfuerzo por incentivar el compromiso del personal de nuestra empresa tanto con el proceso de clasificación como con la política de acceso derivada del mismo (leer el apartado *Funciones y responsabilidades* del libro de Álvarez y Pérez, 2004).

Desde el punto de vista de la revisión de un SGSI, esto es, desde la perspectiva de una auditoría de seguridad es crítico conocer el papel que los distintos miembros de una organización juegan en el nivel de control de acceso a los activos de información.

Desde esta óptica cabe diferenciar entre:

- El **propietario de la información:** ha de ser un ejecutivo o algún directivo de la organización, el cual **es responsable final** (desde el punto de vista de responsabilidad empresarial e incluso jurídico/legal) de los activos de información.
- El **supervisor:** que se encarga de **custodiar los activos bajo mandato del propietario de la información**, que delega en esta figura esta responsabilidad.
- El **usuario** de los mismos: **puede ser un operador, un empleado o un usuario externo** que accede a los activos como parte de su trabajo o para satisfacer algún tipo de necesidad.

2.4. Implementación de las políticas de seguridad: política de seguridad, estándares, directrices y procedimientos

El despliegue de mecanismos de seguridad de modo aislado no garantiza la protección de nuestros activos. Sin duda, la alta complejidad del proceso productivo y de raigambre tecnológica del mismo obliga a llevar a cabo un planteamiento de corte general que debe recorrer todos los elementos que conforman una organización. Dicho de otra forma, **la tecnología no garantiza la seguridad sino que hace falta una política, estándares, directrices y procedimientos de seguridad** (ver la siguiente figura).

La política de seguridad de una empresa es de carácter general y engloba todos los elementos constituyentes de la organización. En el libro *Seguridad informática para empresas y particulares*, sus autores distinguen entre:

- Política de seguridad de la información a nivel empresarial.
- Políticas de seguridad de asuntos específicos.
- Políticas de seguridad de sistemas específicos.

Figura 4. Política de seguridad.

La política de seguridad es de vital importancia para la actividad de una empresa porque determina sus objetivos y los mecanismos para llevarlos a término. Esos mecanismos van a venir dados por las políticas específicas, los estándares, las normas, las directrices y los procedimientos. Si las políticas son documentos estratégicos, los verdaderos detalles de la política quedan recogidos en los estándares, las directrices y los procedimientos. Álvarez y Pérez, (2004, p. 15).

Un estándar es un documento técnico que obliga a **utilizar las tecnologías involucradas de modo uniforme**. Los estándares en el seno de una organización son de carácter obligatorio y constituyen un mecanismo para favorecer la cooperación entre los miembros integrantes de una organización.

Las **directrices** son similares a los estándares pero **no son de carácter obligatorio**. Se suelen utilizar para indicar cómo han de desarrollarse los estándares.

Un **procedimiento** recoge de modo detallado el conjunto de **acciones** que deben efectuarse **para implantar políticas, estándares y directrices**. Suelen venir dados **por *checklists*, guías de instalación, *how-to's***, etc.

Por último, **las normas de seguridad representan el mínimo nivel de seguridad que el sistema ha de satisfacer**. El conjunto de normas es el soporte de la política de seguridad.

2.5. Gestión del riesgo: principios y análisis del riesgo de los activos de información

Una parte muy importante de la planificación de los SGSI es el análisis del riesgo. Álvarez y Pérez, (2004, pp. 29-34). El análisis del riesgo tiene por meta cuantificar el impacto de amenazas potenciales, lo cual se efectúa poniendo un precio a la pérdida de funcionalidad.

Por otro lado, la identificación del riesgo y la valoración del mismo permiten confeccionar una táctica de mitigación de dicho riesgo. Esto a su vez tiene una influencia en elementos tales como la selección de nuevos equipos informáticos, la asignación de recursos, el diseño de las instalaciones que albergan nuestro negocio, etc.

El análisis del riesgo parte de la identificación de los **activos de información**, es decir, aquellos elementos que definimos como necesarios para una empresa y que, consecuentemente, han de protegerse.

Así es, la degradación de alguno de los elementos de la tríada CID de un activo puede cuantificarse económicamente, lo cual permite ponderar el riesgo asociado al citado activo. En el análisis del riesgo además de los activos se toman en consideración las **amenazas** que se ciernen sobre ellos. Se entiende por amenaza **cualquier evento (natural o provocado por el hombre) que desencadena efectos no deseados en la empresa**.

Por último, el análisis de riesgos trabaja con el concepto de **vulnerabilidad**, que es la **debilidad o falta de medidas de seguridad en nuestro sistema frente a una o**

varias amenazas. En este sentido, una pequeña amenaza puede adquirir más peso y peligrosidad fruto de la potencia de una vulnerabilidad en nuestro sistema.

Solo hay riesgo si existe un activo, una vulnerabilidad y una amenaza.

Por otro lado, una vez se concreta una amenaza a través de un incidente de seguridad, este tendrá un impacto. De modo más preciso se define el **impacto de un incidente de seguridad** como la **magnitud de las consecuencias de dicho incidente**. El impacto es función de la criticidad de los activos de información afectados.

Adicionalmente al impacto de un incidente, el análisis de riesgos contempla la probabilidad de ocurrencia del mismo. En esta línea se habla de **probabilidad del riesgo** refiriéndonos a la **probabilidad de vernos afectados por el impacto de un incidente** pero también puede darse como la **probabilidad de incumplir expectativas o la probabilidad de ocurrencia de incidentes**.

La importancia del análisis de riesgo desde el punto de vista de la planificación de la seguridad es incontestable, como también lo es a la hora de evaluar el despliegue de contramedidas y salvaguardas desplegadas para mitigar convenientemente dicho riesgo.

En este sentido el auditor de seguridad debe analizar la existencia de planes de análisis de riesgo y la coherencia entre esos análisis y las políticas, normas, directrices y procedimientos de seguridad.

A tal efecto el auditor de seguridad debe ser conocedor de los dos grandes esquemas de análisis de riesgo existentes: el **análisis cuantitativo y el análisis cualitativo del riesgo.** Álvarez y Pérez, (2004, pp. 31-32).

2.6. Referencias bibliográficas

Álvarez, G. y Pérez, P. P. (2004). *Seguridad informática para empresas y particulares*. Madrid: McGraw Hill.

ISO. (S. f.). ISO 27001: Fase 4 planificación del SGSI. Recuperado de https://normaiso27001.es/fase-4-planificacion-del-sgsi/

Ross, M., McEvilley, S. y Oren, M. (2016). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the engineering of Trustworthy secure systems* (NIST 800-160 vol. 1). Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

Stoneburner, G., Haydem, C. y Feringa, A. (2004). *Engineering principles for information technology Security (A baseline for achieving security)*. (NIST Special publication 800-27 Rev A). [Gaithersburg]: NIST. Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27ra.pdf

Lo + recomendado

No dejes de leer…

Implementación de un SGSI. Etapa 1: planificación

ISO Tools Excellence. (27 de enero de 2014). Implementación de un SGSI. Etapa 1: planificación [Blog post].

En este artículo se comenta la importancia de la planificación en la implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo con la ISO 27001. Desglosa en pasos la secuencia a seguir.

Accede al artículo desde el aula virtual o a través de la siguiente dirección web: https://www.pmg-ssi.com/2014/01/implementacion-de-un-sgsi-etapa-1-planificacion/

Introducción al análisis de riesgos: metodologías (I)

Huerta, A. (30 de marzo de 2012). Introducción al análisis de riesgos: metodologías (I) [Blog post].

En este blog de seguridad *Security art work* se pueden encontrar un par de entradas relativas a las metodologías para el análisis de riesgo. En dichas entradas se muestran de modo sucinto los principios y la importancia del análisis de riesgos, así como las principales metodologías para efectuar tal análisis. Esta es la primera parte.

Accede al artículo desde el aula virtual o a través de las siguientes direcciones web: http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

Introducción al análisis de riesgos: metodologías (II)

Huerta, A. (2 de abril de 2012). Introducción al análisis de riesgos: metodologías (II) [Blog post].

En este blog de seguridad *Security art work* se pueden encontrar un par de entradas relativas a las metodologías para el análisis de riesgo. En dichas entradas se muestran de modo sucinto los principios y la importancia del análisis de riesgos, así como las principales metodologías para efectuar tal análisis. Esta es la segunda parte.

Accede al artículo desde el aula virtual o a través de las siguientes direcciones web: http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

6 consideraciones previas a la implementación de un SGSI

Mendoza, M. A. (6 de noviembre de 2017). 6 consideraciones previas a la implementación de un SGSI [Blog post].

Miguel Ángel Mendoza, de la empresa WeliveSecurity, nos muestra en este artículo algunos aspectos importantes a considerar dentro de una organización durante las fases de **planificación y operación del SGSI** y antes de la implementación de ISO 27001.

Accede al artículo desde el aula virtual o a través de la siguiente dirección web: https://www.welivesecurity.com/la-es/2017/11/06/consideraciones-implementacion-del-sgsi/

Borrado seguro y gestión de soportes

INCIBE. (S. f.). *Borrado seguro y gestión de soportes: políticas de seguridad para la pyme*. León: INCIBE.

Documento del Instituto Nacional de Ciberseguridad de España donde, dentro de las políticas de seguridad para la pyme, ofrecen una *checklist* para el borrado seguro y la gestión de soportes.

Accede al artículo desde el aula virtual o a través de la siguiente dirección web: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/borrado-seguro-y-gestion-soportes.pdf

Google security white paper: Google cloud platform

Google. (2019). *Google security white paper: Google cloud platform*. [S. l.]: Google.

En enero de 2019 la empresa Google publicó un *white paper* sobre seguridad, donde profundiza en los aspectos principales a gestionar dentro de su plataforma Cloud.

Accede al documento desde el aula virtual o a través de la siguiente dirección web: https://services.google.com/fh/files/misc/google_security_wp.pdf

No dejes de ver...

Foundations for planning your ISMS

En febrero de 2019 John Laffey, de la compañía Perry Johnson Registrars especializada en normas ISO, nos facilita los fundamentos para planificar un sistema de gestión de seguridad de la información.

Accede al vídeo desde el aula virtual o a través de la siguiente dirección web:
https://youtu.be/pvvc0C2pecU

Análisis y gestión de riesgos

En la lección 11 de la Intypedia encontramos un buen resumen sobre los principales elementos y conceptos del análisis y gestión de riesgos.

Accede al vídeo desde el aula virtual o a través de la siguiente dirección web:
https://youtu.be/EgiYIIJ8WnU

+ Información

Enlaces relacionados

Risk IT Framework for management of IT Related Business Risks

ISACA nos proporciona una dirección web donde comprender el entorno de trabajo del análisis y gestión de riesgos, dando una visión global de todos los riesgos relacionados con el uso de TI y un tratamiento de la gestión del riesgo.

Accede a la página web desde el aula virtual o a través de la siguiente dirección:
http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx

Security art work

Interesante blog con contenidos y herramientas para la seguridad y auditoría informática.

Accede a la página web desde el aula virtual o a través de la siguiente dirección:
http://www.securityartwork.es/

Cryptex- Seguridad de la información

Blog dedicado a la seguridad de la información, la auditoria informática, la seguridad informática, donde se recopilan las principales noticias, eventos, políticas de seguridad, guías de buenas prácticas, normas, estándares o herramientas.

Accede a la página web desde el aula virtual o a través de la siguiente dirección: http://seguridad-informacion.blogspot.com/

Bibliografía

ISACA. (2017). *Implementation Guideline ISO/IEC 27001:2013 A practical guideline for implementing an ISMS in accordance with the international standard ISO/IEC 27001:2013*. Recuperado de https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf

Test

1. ¿Cuál de los siguientes puntos NO forma parte del desarrollo de una política de seguridad de alto nivel?

A. Identificar los recursos clave de negocio.

B. Identificar el tipo de cortafuegos a emplear en la seguridad perimetral.

C. Definir roles en la organización.

2. Indica la sentencia errónea respecto a los pasos de la fase de planificación de un SGSI:

A. El primer paso consiste en realizar un inventario de activos.

B. La declaración de aplicabilidad contiene todos los controles aplicables.

C. El plan de tratamiento de riesgos se realiza antes del análisis de riesgos.

3. Al establecer nivel de acceso a información sensible, se ha de preservar:

A. Separación de responsabilidades.

B. Una cuenta y un usuario.

C. Mínimo privilegio.

4. ¿Cuál es el principal objetivo perseguido al crear un esquema de clasificación de la información?

A. Controlar el acceso de usuarios autorizados a los recursos.

B. Formalizar y estratificar el proceso de asegurar la información en base a la asignación de etiquetas de importancia y sensibilidad.

C. Establecer una vía para futuras auditorías y depuración de responsabilidades.

5. ¿Qué es una política de seguridad de la información?

A. Las directrices a seguir para definir un programa de seguridad.

B. Procedimientos para configurar cortafuegos.

C. Pronunciamiento de la dirección de empresa al respecto de los objetivos a satisfacer en cuanto a la seguridad.

6. Un programa de seguridad exige un equilibrio entre:

A. Riesgos y contramedidas.

B. Controles de acceso y controles físicos.

C. Roles técnicos y no técnicos.

7. ¿Por qué un análisis del riesgo requiere la intervención de representantes de todos los departamentos de una empresa?

A. Para asegurar que todo el personal está involucrado.

B. Para asegurar que se cubren todos los posibles riesgos en el análisis.

C. Para responsabilizar a cada área respecto al riesgo en ella presente.

8. ¿Quién es el responsable de determinar el nivel de clasificación de la información?

A. Los usuarios.

B. La dirección de empresa.

C. Los propietarios de la información.

9. ¿Cuál de las siguientes opciones no representa un elemento del análisis de riesgos?

A. Analizar el entorno.

B. Crear un informe de coste/beneficio para cada una de las contramedidas.

C. Seleccionar las contramedidas apropiadas e implementarlas.

10. ¿Cuál es el mayor nivel de control de acceso según la clasificación en el sector privado?

A. Confidencial.

B. Privada.

C. Sensible.

