SEGURIDAD EN REDES Y SISTEMAS INFORMÁTICOS

Ana González (Kao)

ÍNDICE GENERAL DEL CURSO

UNIDAD 8. SEGURIDAD EN REDES.

1. Conceptos de red.
2. Amenazas.
3. Red Privada Virtual.
4. Redes inalámbricas.
5. Cortafuegos.
6. Sistemas de detección de intrusiones.
7. Ataques específicos.

UNIDAD 9. SEGURIDAD EN SERVICIOS DE INTERNET.

1. Comercio electrónico y sistemas de pago por Internet.
2. PEM, PGP, S-MIME, SSL.
3. Ataques específicos.
4. Etiquetas inteligentes RFID.
3. Inferencia.
4. Bases de datos multinivel.
5. Ataques específicos: inyección de código SQL.

Contenidos prácticos:

Ejercicios prácticos on-line de cada unidad de contenido del módulo formativo. Las actividades son de diversa naturaleza: actividades de opción múltiple, de verdadero/falso, de completar... Además de glosario de términos, recursos y bibliografía...

UNIDAD 2. La ley y otros aspectos de la seguridad informática.

Ana González (Kao)

ÍNDICE UNIDAD 2

Empecemos con las definiciones:

Se puede definir la Ética como la ciencia que estudia la bondad o maldad de los actos humanos.

Definir y justificar la ética también es una cuestión de debate, pero en este caso citaremos a John Ladd (Professor Emeritus of Philosophy at Brown University):

Para comenzar, la ética es, básicamente, una actividad intelectual abierta, reflexiva y crítica. También es esencialmente problemática y controversia tanto respecto de los principios a los cuales se refiere como a su aplicación.

La ética consiste en cuestiones que deben ser examinadas, explotadas discutidas, deliberadas y argumentadas.

Los principios éticos solo pueden establecerse como resultado de una liberación y argumentación, no son del tipo de objetos o de hechos que pueden ser resueltos por decreto o por autoridad.

Pensar que esto es posible es confundir la ética con la creación de leyes, reglamentos o políticas y otras formas de toma de decisión.

Como todos sabemos internet es la red de redes que fluye a nivel global mientras que las legislaciones son nacionales o locales, entonces, ¿Cómo se crea una ley que aborde estas cuestiones?, y ¿cual es la ética que deben seguir los profesionales que manejan la información y cuales son los problemas existentes para necesitar definir estos principios?.

No existe una regulación de internet a nivel global, ya que es un sistema libre y compuesto de otros micro sistemas, intentar crear una legislación mundial sobre internet es como intentar ponerle puertas al campo, podemos vallar nuestra parcela, pero no el campo entero.

La seguridad informática, es uno de los temas que mayor auge comienza a tener en la actualidad, visto ya sea desde las necesidades de promoverla así como de implementarla.

De donde es importante entender que esta, no implica sólo a la red de redes, sino a todo lo que hace referencia a la preservación, respeto y buen manejo de la información.

Para ello, es de vital importancia aclarar que el valor protegido, tanto tangible como intangible, será siempre la información y debemos entender que hablar de seguridad en sistemas de la información debe de ser hablar de políticas globales en todo el entorno empresarial, no sólo en los puntos relevantes del mismo.

Para clarificar este punto con un ejemplo, pensemos en el centro de salud de nuestro barrio, imaginemos que ocurriría sí sólo se implantasen políticas de backup en los servidores principales del centro pero no en los equipos de administración y admisión.

¿Qué ocurrirá con nuestros datos si el equipo de la administradora de admisión fuese infectado? No queremos ni pensarlo, ¿verdad?, por esto es importante remarcar que cualquier equipo de dentro de la red ha de ser protegido y securizado aplicando las políticas de forma individual a cada uno de ellos pero como parte de una unidad global que es la entidad en la que se encuentran.

Debido a lo anterior hemos de ser consientes de que por nuestras manos van a pasar una serie de datos y sistemas sensibles por lo que hemos de tener muy clara nuestra ética para su tratamiento.

Las asociaciones de profesionales de informática y algunas empresas relacionadas con la informática han desarrollado códigos de conducta profesional.

Estos códigos tienen distintas funciones:

- Existan normas éticas para una profesión, esto quiere decir que un profesional, en este caso un técnico, es responsable de los aspectos técnicos del producto, como también de las consecuencias económicas, sociológicas y culturales del mismo.
- Sirven como un instrumento flexible, como suplemento a las medidas legales y políticas, ya que éstas en general van muy lentas comparadas con la velocidad del desarrollo de las tecnologías de la información. Los códigos hacen de la ley su suplemento y sirven de ayuda a los cuerpos legislativos, administrativos y judiciales.
- Sirven como concienciación pública, ya que crear unas normas así, hace al público consciente de los problemas y estimula un debate para designar responsabilidades.

- Estas normas tienen una función sociológica, ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera; es símbolo de sus estatus profesional y parte de su definición como profesionales.
- Estas normas sirven también como fuente de evaluación pública de una profesión y son una llamada a la responsabilidad que permiten que la sociedad sepa qué pasa en esa profesión; aumenta la reputación del profesional y la confianza del público.
- En las organizaciones internacionales estas normas permiten armonizar legislaciones o criterios divergentes existentes (o ausentes, en su caso) en los países individuales

Los códigos son un paso en la concienciación de las sociedades y organizaciones que quieren mejorar situaciones en las que los impactos sociales del desarrollo tecnológico son poco percibidos.

Estos tienen que evitar duplicar lo que ya existe en la ley.

La ley trata de la legalidad de las prácticas sociales, es normativa por definición y se impone con sanciones. Los códigos, en cambio, tratan del comportamiento según principios éticos, su normatividad es mostrar una declaración de intenciones sobre la "misión" de una institución y la coerción real con que se imponen es pequeña, aunque en algunos casos se incluyen expulsiones de la asociación en cuestión.

La ley es el acercamiento de más poder normativo y asigna con claridad los derechos, responsabilidades y deberes de cada uno.

Un código de ética se suma a un cambio de actitud por parte de la sociedad, respetando el accionar de la misma.

El objetivo de la ética informática busca más que proponer un análisis sobre "sociología de la informática" o sobre la evaluación social de las tecnologías (technology assessment), busca ir más allá en el sentido de proporcionar medios racionales para tomar decisiones en temas en los que hay en juego valores humanos y dilemas éticos.

Algunos de los códigos de ética que hacen referencia a la seguridad informática o a la informática, son los siguientes:

- Código de Ética del Ingeniero Mexicano (UMAI)
- Código de Ética de la IEEE

- American Society for Industrial Security (ASIS)
- Código de Ética de la Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A. C. (AMIPCI)

En el tema de Seguridad Informática, el Consorcio para la Certificación Internacional de Seguridad en Sistemas de Información (ISC2 – International Information Systems Security Certification Consortium) emite una de las más importantes certificaciones en el tema de Seguridad Informática, conlleva como requisito indispensable el compromiso y conocimiento del Código de Ética establecido por el Consorcio.

Dentro de los cánones a seguir, se indica lo siguiente:

- Proteger a la sociedad, a la comunidad y a la infraestructura

- Actuar en forma honorable, honesta, justa, responsable y legal

- Proveer servicios diligentes y competitivos a sus superiores

- Actuar siempre protegiendo y promoviendo el crecimiento de la profesión

ISC2 – International Information Systems Security Certification Consortium https://www.isc2.org/Request for Comments Editor http://www.rfc-editor.org/

Código de Ética de ISC2 https://www.isc2.org/cgi/content.cgi?category=12

Consideramos que las nuevas tecnologías informáticas han cambiado nuestro modo de vivir, este desarrollo ha conllevado a cambios en la forma de actuar y de pensar de los hombres y ha traído consigo nuevas pautas de comportamiento inherentes a la dignidad humana.

En los últimos años se están planteando a nivel internacional la necesidad de desarrollar e implantar el código ético y de seguridad informática que regule el saber informático.

1.1 PROBLEMAS ÉTICOS

No hay una manera precisa de definir el concepto de ética informática, pero sí podemos definir sus problemas en unos pocos apartados.

1. Impacto social
2. Delitos informáticos
3. Privacidad y Anonimato
4. Propiedad Intelectual
5. Responsabilidades de los profesionales
6. Globalización

1. Impacto social de los ordenadores en nuestras vidas

Como "herramienta universal" que puede, en principio, realizar casi cualquier tarea, resultan una amenaza para ciertos puestos de trabajo.

Aunque necesitan de vez en cuando la reparación, las computadoras no requieren sueldo, ellas no se cansan, no van a casa por enfermedad ni quitan tiempo de trabajo para el resto de sus actividades y la relajación.

Al mismo tiempo son a menudo más eficientes que los seres humanos en la ejecución de muchas tareas.

Por lo tanto, los incentivos económicos para sustituir a seres humanos por los dispositivos automatizados son muy altos y están siendo un hecho en varios mercados, cadenas de montaje de automóviles, cajeros, teleoperadoras, máquinas de comida, cirugía robótica, drones de rescate, son algunos de los sectores que hoy en día ya consideramos con normalidad que se encuentren automatizados sin ser conscientes de las implicaciones que conllevan a nivel socio económico.

Los ordenadores y la robótica tienen un gran potencial desarrollando tareas repetitivas y pesadas o que requieran un gran esfuerzo físico, de forma exacta y sin sufrir agotamiento, de hecho fueron concebidos para ello.

Sin embargo aunque a corto plazo la informática y robotización de algunos sistemas a desmejorado el mercado laboral también es cierto que han surgido y surgen cada día nuevas profesiones relacionadas con el mismo ya que todas la máquinas requieren cierta

atención humana para su monitorización y reparación. yendo más allá se necesitan ingenieros, desarrolladores de software, analistas de sistemas , profesores ...etc para permitir que el las necesidades de la sociedad en estos temas sean cubiertas, de done a largo plazo es posible que se estén generando más puestos de los que se quitan y esto simplemente conlleve a un cambio social en cuanto al mercado laboral se refiere.

2. Delito informático

Como vimos en el capítulo anterior la seguridad informática se divide en seguridad física y seguridad lógica, esta última Spafford, Heaphy y Ferbrache [Spafford, et al, 1989] la divide en cinco aspectos:

1. Aislamiento y secreto

2. Integridad -- asegurando que los datos y los programas no están modificados sin autoridad competente

3. Servicio intacto

4. La consistencia -- asegurándose de que los datos y el comportamiento que vemos hoy será igual mañana

5. Acceso que controla a los recursos

El malware proporciona un desafío significativo cuando hablamos de seguridad lógica.

Los delitos informáticos, tales como malversación, el espionaje industrial, las bombas de la lógica, los troyanos, entran en nuestros sistemas normalmente por el personal confiado en que tiene permiso de utilizar el sistema .

La seguridad del sistema por tanto debe también abarcar las acciones y costumbres o la reeducación en las buenas maneras de estos usuarios y cualquier otro que tenga acceso a nuestro sistema.

3. Privacidad y Anonimato

Dos puntos de importancia que no deben confundirse y sobre los que siempre hay mucha polémica y desconocimiento.

Anonimato según la rae es el carácter o la condición de anónimo y anónimo queda definido por el diccionario de la lengua española © 2005 Espasa-Calpe de la siguiente manera:

anónimo, ma

1. adj. y m. [Obra o escrito] que no lleva el nombre de su autor:
   novela anónima; recibió varios anónimos.
2. [Persona] de nombre no conocido:
   poeta, admirador anónimo.
3. Secreto de la persona que oculta su nombre:
   guardar el anónimo.

Por tanto el anonimato garantiza que nunca nadie pueda saber quién eres en el mundo presencial y es una necesidad para muchos activistas (especialmente para aquellos que luchan en países o entornos muy hostiles en los que puede peligrar su vida o la de sus familiares).

Sin embargo privacidad queda definido por el Diccionario de la lengua española © 2005 Espasa-Calpe como:

1. privacidad

f. Derecho y propiedad de la propia intimidad y vida privada

De donde ser anónimo significa ser desconocido, que no conozcan nuestros datos o nuestro nombre, podría entenderse como una cualidad de la privacidad en cierto sentido, salvaguardar nuestra privacidad proveyéndonos de anonimato en la red no sólo es aconsejable si no que es un derecho que nosotros mismos violamos ante la premisa de "Si yo no tengo nada que esconder".

Creer que en la red, por estar parapetados detrás de una pantalla, somos más anónimos es un error: la realidad es que todo lo que hacemos en la red queda recogido en un fichero *log*, es generalmente trazable y atribuible con más facilidad y posibilidades de éxito que en la vida *offline*, y puede y debe ser perseguido cuando lo que esté encima de la mesa sea la comisión de un delito de amenazas, injurias, difamación, u otros delitos

definidos como tales.

Pues bien planteémonos la siguiente pregunta:

¿Quién subiendo en el ascensor le cuanta a su vecina si se siente triste o contento porque ese mes no llega cubrir los gastos, o porque a tenido una aventura con el mejor amig@ de su novi@ , o que resulta que le ha salido un grano en la cara interna del muslo y necesita ver a un médico?. Nadie en su sano juicio, ya que en la vida real sí somos conscientes de que este tipo de cosas no se divulgan a los cuatro vientos, sin embargo por una misteriosa razón las publicamos en las redes sociales y las contamos por el washaap en ocasiones incluso con imágenes, y ¿donde creen que van a parar todas esas imágenes, datos e información?, ¿realmente creen que no es recolectada y almacenada?

Uno de los asuntos más tempranos de la ética informática para despertar interés público era la privacidad.

Por ejemplo, a mediados de los años sesenta el gobierno americano había creado ya bases de datos grandes de la información sobre los ciudadanos privados (datos de censo, expedientes de impuesto, expedientes del servicio militar, expedientes del bienestar, etcétera).

En el congreso de los E.E.U.U., las cuentas fueron introducidas para asignar un número de identificación personal a cada ciudadano y entonces recolectar todo el gobierno los datos sobre cada ciudadano bajo identificación correspondiente a un número.

Una protesta pública sobre el "gobierno del gran hermano" hizo a congreso desechar este plan y condujo a presidente de los E.E.U.U. a designar a comités para recomendar la legislación de la privacidad a principios de los 70

Podemos ver claramente con que facilidad las empresas y los gobiernos recolectan todo tipo de información sobre nosotros: sexo, edad, trabajo, gustos, afiliación política, orientación sexual, dirección, cuentas de correo, de banco... etc

Como si de un buffet libre sobre nuestras vidas se tratase ya que permitimos y divulgamos esta información por cualquier sitio de la red en el que vamos pasando y creyendo que todo esto en principio es utilizado sólo para ofrecernos publicidad de nuestro interés, pero ¿sólo para eso?, lo cierto es que crear servicios atractivos donde se requieran datos personales para acceder es una muy buena forma de hacerse con bases de datos sobre nuestros perfiles y poderlos utilizar en el momento más conveniente para lo que se considere oportuno.

Por todo lo anterior es importante en primer lugar tomar consciencia de la situación y hacer que la tomen en nuestro entorno y por otro lado proveernos de herramientas que faciliten salvaguardar nuestra privacidad, tales como navegación anónima, cifrado de nuestros correos, no divulgación de nuestros datos e imágenes y un largo etcétera.

4. Propiedad Intelectual

Una de las áreas más polémicas de las éticas informáticas se refiere a los derechos de característica intelectual conectadas con propiedad del software.

Alguna gente, como Richard Stallman que comenzó la fundación de Software Libre, cree que la propiedad del software no se debe permitir a todos.

Él demanda que toda la información debe estar libre, y todos los programas deben estar disponibles para copiar, estudiar y modificarse por cualquier persona que desee ya que considera el conocimiento como un bien de la humanidad y no como un producto sobre el cual se deba sacar beneficio, lo cual si lo pensamos detenidamente tiene bastante sentido.

¿se imaginan que Shakespeare no hubiese escrito su obra por problemas de copyright con su editor? , resulta absurdo sólo imaginarlo, sin embargo es una triste realidad en algunos casos hoy en día.

Del otro lado otros discuten que las compañías o los programadores del software no invertirían semanas y meses del trabajo y de fondos significativos en el desarrollo del software si no pudieran conseguir beneficios de estas inversiones en forma de licencias y patentes, por otro lado es justo caer en la cuenta de que estos desarrollos nacen de la necesidad del mercado de cubrir cierta característica y hay otras formas parte de la licencia para conseguir rédito por la inversión.

La industria del software es una parte de billones de dólares de la economía; y las compañías del software demandan perder mil millones de dólares por año con las copias ilegales.

La propiedad es una cuestión compleja, puesto que hay varios diversos aspectos del software que se pueden poseer y tres diversos tipos de propiedad: copyright, secretos comerciales, y patentes.

Uno puede poseer los aspectos siguientes de un programa:

1. El "código de fuente" que es escrito por el programador en un lenguaje de programación de alto nivel como Java o C++.

2. El "código de objeto", que es una traducción en lenguaje de máquina del código de fuente.

3. El "algoritmo", que es la secuencia de la máquina que permite que el código de fuente y el código de objeto se representen.

4. La parte gráfica de un programa, que es la manera el programa aparece en la pantalla y los interfaces con los usuarios.

Una edición muy polémica está poseyendo hoy una patente en un algoritmo de la computadora.

Una patente proporciona un monopolio exclusivo en el uso del artículo patentado, así que el dueño de un algoritmo puede negar a otros el uso de fórmulas matemáticas que son parte del algoritmo. Ultrajan, demandando que las patentes del algoritmo quitan con eficacia partes de matemáticas del dominio público, y de tal modo amenazan a los matemáticos y a los científicos lisiar ciencia.

Consecuentemente, solamente las compañías muy grandes con los presupuestos grandes pueden permitirse funcionar tal búsqueda.

Sin embargo es importante respetar las licencias, pero por suerte existen licencias libres que permiten la copia y divulgación de la información y del código y de los documentos técnicos generados, por ello lo importante es elegir cuidadosamente nuestra licencia.

5. Responsabilidades de los profesionales

Los informáticos se han especializado en el conocimiento de una materia compleja y a menudo tienen posiciones con autoridad y son respetados en la comunidad. Por esta razón, pueden tener un impacto significativo sobre el mundo.

Junto con tal energía de cambiar el mundo viene el deber para ejercitar esa energía de forma responsable [Gotterbarn, 2001].

Los informáticos se encuentran en una variedad de relaciones profesionales con la gente [Johnson, 1994], incluyendo:

patrón -- empleado

cliente -- profesional

profesional -- profesional

sociedad -- profesional

La complejidad de tales relaciones que implican una diversidad de intereses, pueden derivar en diferentes tipos de conflictos si no son tratadas con la ética y profesionalidad necesaria de donde es importante entender las implicaciones para ambas partes que cada una de estas relaciones conlleva para poder satisfacer a ambas partes con profesionalidad evitando el conflicto, esto normalmente lo suele dar la experiencia pero nunca está demás buscar consejo o referencias al respecto.

6. Globalización

La ética informática se está desarrollando hoy rápidamente en un campo más amplio y aún más importante, que se pudo razonablemente llamar el "ética global de la información".

Las redes globales como el Internet conecta a toda la gente a lo ancho y largo de la tierra.

Leyes Globales

¿Si los usuarios de la computadora en los Estados Unidos, por ejemplo, desean proteger su libertad del discurso en el Internet, que leyes se aplican?

Si tenemos un servidor p2p con contenido subido por los usuarios y ese servidor está replicado en otros cuatro en países distintos, ¿La ley de que país debería aplicarse en el caso de alguno de esos contenidos resultase ilegal?, es más hay que ser consciente de que lo ilegal en un país no tiene por que serlo en otro.

Por otro lado pongamos nos en el caso de un fraude electrónico en una compra por internet a china por ejemplo, ¿A quien debemos reclamar?.

Educación Global

¿Cuál será el impacto de esta "educación global repentina y profunda" sobre dictaduras políticas, comunidades aisladas, culturas coherentes, prácticas religiosas, el etc.?

Y después de tanta pregunta pasemos a algunas respuestas.

La ACM y IEEE ya a partir del año 1999 adoptaron un código ético que se puede leer en el siguiente enlace:

El Código de Ética y Práctica Profesional de Ingeniería del Software de la ACM / IEEE Computer Society

Se pueden resumir las principales funciones de los códigos de ética en los siguientes apartados [Bowyer, 1996]:

1) simbolizar una profesión;
2) proteger los intereses del grupo;
3) inspirar buena conducta;
4) educar a los miembros de tal profesión;
5) disciplinar a sus afiliados;
6) fomentar las relaciones externas;
7) enumerar los principios morales básicos;
8) expresar los ideales a los que se debe aspirar;
9) mostrar reglas básicas de comportamiento;
10) ofrecer guías de comportamiento;
11) enumerar derechos y responsabilidades.

2. Jerarquía de las normas jurídicas españolas, LSSI, LOPD, Código penal, ley informática en EE.UU, Australia, Brasil, India, China, Reino Unido.

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red organizacional.

Una norma de seguridad establece unos requisitos que se sustentan en la política y que regulan determinados aspectos de seguridad. Son por tanto, declaraciones a satisfacer. Una norma debe ser clara, concisa y no ambigua en su interpretación.

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

Objetivo: declaración del propósito o intención de la redacción del documento y de los objetivos de seguridad relacionados con la política que se intentan satisfacer.

Definiciones: Se indican las definiciones de aquellos términos que aparezcan en la norma y que pudieran ofrecer dificultad para su comprensión. Es una forma de eliminar la ambigüedad en la interpretación al establecer el significado en la norma de los términos utilizados.

Responsables del cumplimiento: se define dentro de la Organización qué departamento o responsable velará por el cumplimiento de la norma y revisará su correcta implantación o cumplimiento.

Incumplimiento: se establecen las consecuencias que se derivarán del incumplimiento de la norma cuando éste sea detectado o las acciones disciplinarias que ocasionarán.

Normas a aplicar: debe contener los requisitos de seguridad que se declaran de

obligado cumplimiento.
Podrán agruparse los requisitos por categorías, estableciendo apartados donde se agrupen los requisitos relacionados. También los enunciados pueden numerarse para poder posteriormente referenciarlos.

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

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

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

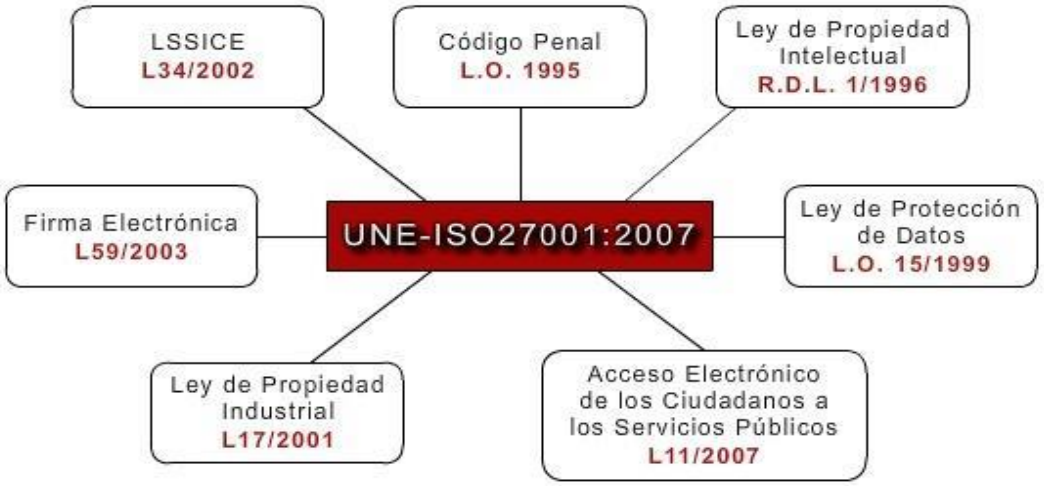
Debe estar bajo un control de versiones.

Normas: Con el fin de proporcionar un marco de Gestión de la Seguridad de Información utilizable por cualquier tipo de organización, independientemente de su tamaño o actividad, se ha creado un conjunto de estándares bajo el nombre de ISO/IEC 27000.

2.1 MARCO LEGAL Y JURÍDICO DE LA SEGURIDAD. NORMATIVAS DE SEGURIDAD.

Desde la publicación del la Ley Orgánica de Protección de Datos de Carácter Personal en el año 1999 hasta la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos del año 2007, hay una serie de leyes que, de una manera u otra, están relacionadas con la seguridad de la información, además de numerosas regulaciones sectoriales en diversos ámbitos: financiero, telecomunicaciones, agrario, etc.

LEGISLACIÓN ESPAÑOLA



Ley Orgánica 15/99 de Protección de Datos de Carácter Personal

Esta ley se complementa con el reglamento estipulado en el Real Decreto RD 1720/2007.

El objetivo de esta Ley es garantizar y proteger, en lo concerniente al tratamiento de los datos personales (automatizados o no), las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.
Los derechos recogidos en la LOPD son:

•Las personas de las que se almacena datos de carácter personal, tienen una serie de derechos amparados por esta ley:

o Derecho de información: Cuando alguien proporciona sus datos debe ser informado de que van a ser almacenados.
o Derecho de acceso, cancelación, rectificación y oposición: La persona puede ver la información que se dispone de él, puede cambiar esos datos para que sean correctos y exactos, cancelar la información que se almacene de él y oponerse a que se almacene.

Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (LSSI)

Esta Ley se encarga de regular las obligaciones de los prestadores de servicios y los

servicios que prestan. Entre las obligaciones que estipula la Ley están:

• Los prestadores de servicios deben facilitar sus datos de contacto.
• Deben colaborar con las autoridades, reteniendo los datos de conexión y tráfico durante 12 meses.
• Los que albergan datos proporcionados por un cliente, no serán responsables por la información almacenada a petición del destinatario, siempre que:

No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Cuando transmitan información de terceros, los proveedores de servicio no tendrán responsabilidad al respecto si:

• No modifican la información.
• Permiten el acceso a ella sólo a los destinatarios autorizados
• Actualizan correctamente la información.
• No utilizan su posición con el fin de obtener datos sobre la utilización de la información
• Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto sepan que ha sido retirada del lugar de la red en que se encontraba, o que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

Ley 32/2003, general de telecomunicaciones

El objeto de esta ley es la regulación de las telecomunicaciones. Entre los objetivos de esta Ley están:

• Fomentar la competencia.
• Garantizar el cumplimiento de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas.
• Promover el desarrollo del sector de las telecomunicaciones.
• Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones.
• Defender los intereses de los usuarios.
• Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.
• Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.
• Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea.

Ley 59/2003 de firma electrónica

Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.
La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel, por lo que tanto su generación como su utilización deben ser cuidadosamente controladas para evitar problemas.

R.D.L, 1/1996 Ley de Propiedad Intelectual

La propiedad intelectual de una obra literaria, artística o científica corresponde al autor y le da la plena disposición y el derecho exclusivo a la explotación de la obra. Las obras pueden estar expresadas en cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro como:

• Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, etc.
• Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería.
• Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia.
• Las obras fotográficas.
• Los programas de ordenador.
Al amparo de esta Ley, las organizaciones protegen su conocimiento y las obliga a respetar el de las demás. El otro punto relevante en el ámbito de la seguridad de la información es la obligación de contar únicamente con software original (propietario o libre), ya que la utilización de software sin licencia sería una infracción de la Ley.

Ley 17/2001 de Propiedad Industrial

Es la que regula los derechos sobre:
• Las marcas.
• Los nombres comerciales.
El organismo que se encarga de mantener el registro de marcas es la Oficina de Patentes y Marcas. Para tener derechos de propiedad sobre una marca hay que registrarla en dicha Oficina.
Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos
Los puntos más destacables de la Ley son:
• Los ciudadanos verán reconocidos nuevos derechos en sus relaciones con las administraciones públicas.

• Se creará la figura del Defensor del Usuario.
• Los trámites y gestiones podrán hacerse desde cualquier lugar, en cualquier momento.
• La administración será más fácil, más ágil y más eficaz.
• Los ciudadanos pasan a tomar la iniciativa en sus relaciones con la administración.

Contará con un Esquema Nacional de Seguridad y otro de Interoperabilidad, para que los servicios ofrecidos cuenten con un mínimo nivel de seguridad y las distintas administraciones puedan comunicarse con fluidez.

2.2 Estándares de las Políticas de Seguridad Informática

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

A continuación se incorpora una relación con la serie de normas ISO 27000 y una descripción de las más significativas aunque la trataremos con detalle un poco más adelante:

Familia de normas 27000	
Norma ISO/IEC	**Título**
ISO 27000	Gestión de la Seguridad de la Información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para un SGSI.
ISO 27002	Código de Buenas Prácticas.
ISO 27003	Guía de Implantación de un SGSI.
ISO 27004	Sistema de Métricas e Indicadores.
ISO 27005	Guía de Análisis y Gestión de Riesgos.
ISO 27006	Especificaciones para Organismos Certificadores de SGSI.
ISO 27007	Guía para auditar un SGSI.
ISO 2701X	Guías sectoriales.
ISO 27XXX	Futuras normas.

UNE-ISO 27001Esta norma es la definición de los procesos de gestión de la seguridad, por lo tanto, es una especificación para un SGSI y, en este momento, es la única norma Certificable, dentro de la familia ISO 27000.

ISO 27002La ISO 27002 viene a ser un código de buenas prácticas en el que se recoge un catálogo de los controles de seguridad y una guía para la implantación de un SGSI.

Cada uno de los dominios conforma un capítulo de la norma y se centra en un determinado aspecto de la seguridad de la información. En el siguiente dibujo se muestra la distribución de dichos dominios y el aspecto de seguridad que cubren:

Distribución de dominios de la Norma ISO 27002

ISO 27002 (documentación)

La pretensión de esta normativa es la elaboración de un SGSI que **minimice los riesgos** que se hayan detectado en los Análisis de Riesgos hasta un nivel asumible por la organización, en relación siempre a los objetivos de negocio. Es importante destacar que cualquier medida de protección que se haya implantado debe quedar perfectamente documentada.
La documentación que se genera con la implantación del SGSI se estructurará de la siguiente forma:

(Grafica)

Tipos de documentación

Donde las **Políticas** sientan las bases de la seguridad constituyendo la redacción de los objetivos generales y las implantaciones que ha llevado a cabo la organización. Pretenden indicar las líneas generales para conseguir los objetivos marcados sin entrar en detalles técnicos. Deben ser conocidas por todo el personal de la organización.

Los **Procedimientos** desarrollan los objetivos marcados en la Políticas. En ellos sí que

aparecerían detalles más técnicos y se concreta cómo conseguir los objetivos expuestos en las Políticas. No es necesario que los conozcan todas las personas de la organización sino, únicamente, aquellas que lo requieran para el desarrollo de sus funciones.

Las **Instrucciones** constituyen el desarrollo de los Procedimientos. En ellos se llega hasta describir los comandos técnicos que se deben realizar para la ejecución de dichos Procedimientos.

Y por último los **Registros** evidencian la efectiva implantación del SGSI y el cumplimiento de los requisitos. En este punto también es importante el contar con una serie de **indicadores** o **métricas** de seguridad que permitan evaluar la consecución de los objetivos de seguridad establecidos.

El Estándar ISO 17799 (El mismo 27002)

El estándar de seguridad ISO 17799 fue preparado por la British Standard Institution (con el nombre de BS 7799) y fue adoptado por el comité técnico de la ISO en Diciembre del año 2000.

Directrices del estándar 17799

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".
La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una

guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.
Con la aprobación de la norma ISO/IEC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la seguridad de la información, se espera que ISO/IEC 17799:2005 pase a ser renombrado como ISO/IEC 27002 en la revisión y actualización de sus contenidos en el 2007.

2.3 LEYES

Ley 1273 de 2009 (Colombia) [1]:
La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evita incurrir en alguno de estos tipos penales.

Artículos relevantes de la ley:

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.
- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
- Artículo 269D: DAÑO INFORMÁTICO.
- Artículo 269E: USO DE SOFTWARE MALICIOSO.
- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES.
- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

2.4 Legislación Europea

En materia de seguridad informática existen dos normativas legales relevantes:

1. Directiva 2009/136/CE/ del Parlamento Europeo y del Consejo, de 25 de noviembre. [2]
2. Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre. [3]

La **Directiva 2009/136/CE** modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones

electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

La **Directiva 2009/140/CE** modifica la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

Principales Leyes internacionales de privacidad. [4]

La siguiente lista contiene una serie de privacidad internacional en relación con las leyes del país y región. Siempre que sea posible, estos hipervínculos referencia a una traducción al Inglés de la ley.

- Argentina: Ley de Protección de Datos Personales de 2000 (también conocido como Habeas Data)
- Austria: Ley de Protección de Datos de 2000, Austria Gaceta de Leyes Federales I N º parte 165/1999 (Datenschutzgesetz 2000 o DSG de 2000).
- Australia: Ley de Privacidad de 1988
- Bélgica: Bélgica, la Ley de Protección de Datos y Privacidad de Datos Comisión Belga de Blog de privacidad
- Brasil: Privacidad en la actualidad regulado por el artículo 5 de la Constitución de 1988.
- Bulgaria: El búlgaro Ley de Protección de Datos Personales , fue aprobado el 21 de diciembre de 2001 y entró en vigor el 1 de enero de 2002. Más información en la Autoridad de Protección de Datos Bugarian
- Canadá: La Ley de Privacidad - julio de 1983
  Protección de Información Personal y Electrónica Datos de la Ley (PIPEDA) de 2000 (proyecto de ley C-6)
- Chile: Ley sobre la Protección de Datos de Carácter Personal, agosto de 1998
- Colombia: dos leyes que afectan a la privacidad de datos - Ley 1266 de 2008 : (en español) y la Ley 1273 de 2009 (en español) Además, la Constitución proporciona a cualquier persona el derecho a actualizar su información personal
- República Checa: Ley de Protección de Datos de Carácter Personal (en abril de 2000) N º 101
- Dinamarca: Ley de Tratamiento de Datos de Carácter Personal, Ley N ° 429, mayo de 2000.
- Estonia: Ley de Protección de Datos Personales de 2003 . Junio de 1996,

consolidado julio de 2002.

- Unión Europea: la Unión Europea la Directiva de Protección de Datos de 1998
- Internet de la Unión Europea Ley de Privacidad de 2002 (Directiva 2002/58/CE) Con un debate aquí.
- Finlandia: Ley sobre la modificación de la Ley de datos personales (986) de 2000.
- Francia: Ley de Protección de Datos de 1978 (revisada en 2004)
- Alemania: Federal Data Protection Act de 2001
- Grecia: la Ley No.2472 sobre la protección de las personas en lo que respecta al tratamiento de datos personales, abril de 1997.
- Guernsey: Protección de Datos (Bailía de Guernesey) de 2001
- Hong Kong: la Ordenanza Datos de Carácter Personal (el "Decreto")
- Hungría: Ley LXIII de 1992 sobre la Protección de Datos de Carácter Personal y la publicidad de los datos de los intereses públicos (extractos en Inglés).
- Islandia: la Ley de Protección de la Persona; Procesamiento de Datos de Carácter Personal (Enero 2000)
- Irlanda: Protección de Datos (Enmienda), Número 6 de 2003
- India: Ley de Tecnologías de la Información de 2000
- Italia: Código de Protección de Datos de 2003
  Italia: Procesamiento de la Ley de Datos Personales, enero de 1997
- Japón: Ley de Protección de Datos Personales (Ley) (Traducción Inglés Oficial)
  Resumen de la publicación de la Ley Jonesday
- Japón: Ley para la Protección de los datos informáticos procesados que poseen los órganos administrativos, de diciembre de 1988.
- Corea - Ley sobre Protección de Información Personal de los Organismos Públicos Ley de Información y Uso de la red de comunicación
- Letonia: Ley de Protección de Datos Personales, 23 de marzo de 2000.
- Lituania: Ley de Protección Jurídica de los Datos de Carácter Personal (junio de 1996)
- Luxemburgo: la Ley de 2 de agosto de 2002 sobre la Protección de las Personas con respecto al tratamiento de datos personales.
- Malasia - principio de la ley común de la confidencialidad de datos personales Ley de Protección (no finalizado) Bancos e Instituciones Financieras Ley de 1989 disposiciones sobre la privacidad.
- Malta: Ley de Protección de Datos (Ley XXVI de 2001), modificada de 22 de marzo 2002, 15 de noviembre de 2002 y el 15 de julio 2003
- México: Ley Federal para la Protección de datos personales en poder de los particulares (en español) - El acuerdo con la normativa los derechos de los interesados, la seguridad y las disposiciones de notificación de incumplimiento, el cloud computing, el consentimiento y los requisitos

de notificación, y la transferencia de datos. Buen resumen de la ley en Inglés en el Grupo de Derecho Informático
- Marruecos: Ley de Protección de Datos
- Países Bajos: Holandesa de Protección de Datos de Carácter Personal, de 2000 modificada por las Leyes de fecha 5 de abril de 2001, Boletín de leyes, ordenanzas y decretos 180 de 06 de diciembre 2001
- Nueva Zelanda: la Ley de Privacidad, mayo de 1993, Ley de Modificación de Privacidad de 1993, Ley de Modificación de Privacidad de 1994
- Noruega: Ley de datos personales (abril 2000) - Ley de 14 de abril 2000, N º 31 relativa al tratamiento de datos personales (Ley de datos personales)
- Filipinas: DATOS DE LA LEY DE PRIVACIDAD DE 2011 También hay un derecho reconocido de la intimidad en el derecho civil y un código de datos modelo de protección .
- Rumania: la Ley N º 677/2001 para la Protección de las Personas con respecto al tratamiento de datos personales y la circulación de estos datos
- Polonia: Ley de Protección de Datos de Carácter Personal (en agosto de 1997)
- Portugal: Ley de Protección de Datos de Carácter Personal (Ley 67/98, de 26 de octubre)
- Singapur - El Código de comercio electrónico para la Protección de Información Personal y Comunicaciones de los consumidores de comercio electrónico en Internet. Otros relacionados con las leyes de Singapur y las leyes de comercio electrónico .
- República Eslovaca: Ley N º 428 de 3 de julio de 2002, sobre Protección de Datos de Carácter Personal.
- Eslovenia: Personal Data Protection Act, RS N º 55/99.
- Sudáfrica: las Comunicaciones Electrónicas y la Ley de Transacciones de 2002
- Corea del Sur:
- España: LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos Personales
- Suiza: La Ley Federal de Protección de Datos de 1992
- Suecia: Personal Data Protection Act (1998:204), 24 de octubre 1998
- Taiwán: tratamiento informático Ley de Protección de datos - se aplica sólo a las instituciones públicas. (Traducción Inglés)
- Tailandia: Ley de Información Oficial, BE 2540 (1997) para las agencias estatales. (ley protección de datos personales en cuestión.)
- Reino Unido: UK Data Protection Act 1998
  Privacidad y comunicaciones electrónicas (Directiva CE) de 2003 el texto oficial, y un sitio orientado al consumidor en la Oficina del Comisionado de Información .

- Vietnam: La Ley de Transacciones Electrónicas 2008

Otras leyes de Seguridad informática:

Derecho informático: Es una rama de las ciencias jurídicas que considera la informática como instrumento y objeto de estudio.

Legislación informática La información como producto informático. La protección de los datos personales. La regulación jurídica de internet. Los delitos informáticos.

Delitos informáticos El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de caracteres tradicionales, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes.

Ley contra laso delitos informáticos en Colombia. El congreso colombiano aprobó un proyecto de ley que modifica el código penal para incorporar los delitos que violen la protección de informa formación de los datos.

Documento interesante, guía para el desarrollo del sistema de gestión de seguridad de la información.
1. http://www.slideshare.net/jennycala/contenidos-curso-sgsi

Links relacionados con el tema:

1. http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia
2. http://www.tareanet.edu.co/index.php?option=com_myblog&show=ley-1273-de-2010-delitos-informaticos-3768.html&Itemid=90
3. http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html
4. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:ES:PDF
5. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:ES:PDFhttp://www.informationshield.com/intprivacylaws.html

2.5 . Estándares internacionales de seguridad.

En un mundo cada vez más globalizado, los estándares nacionales se quedan cortos. Es necesaria la creación de unos estándares con una mayor cobertura de territorio.

De forma casi obligatoria para que existan estos estándares, es necesario que aparezcan organizaciones que los puedan crear, gestionar y ejecutar.

En los siguientes puntos echaremos una vistazo tanto a las organizaciones/instituciones existentes, como que estándares, normas o recomendaciones gestionadas por cada uno de ellos.

Instituciones de normalización

Según se ven en la figura 2, vamos a ver que instituciones de normalización son las que nos afectan directamente por nuestro territorio, clasificándolas por la cobertura de países que dan, dividiéndolas en europeas e internacionales.

Antes de entrar a verlas, abría que hacer una reseña a las Normas UNE (Una Norma Española) que como bien dice su nombre son las de ámbito de España.

Estas normas son creadas por AENOR, Antes las realizaba por Instituto Español de Normalización (IRANOR).

La forma de referencias a una norma UNE es con la palabra UNE seguido de un número, que corresponderá con el número de la norma.

Hay que diferenciar las normas UNE de las normas UNE-EN, que son una norma española con cobertura de la una norma europea (European Norm).

EUROPEAS

CEN (Comité Europeo de Normalización)

http://www.cen.eu/

Es una organización privada no lucrativa creada en 1961, encargada de desarrollar las estándares europeos (Los llamados EN) que no pertenezcan al sector eléctrico. También es el representante del CENELEC (European Committee for Electrotechnical Standardization) que es el encargado de las normas del sector eléctrico.

Además de estas normas, también elabora otros productos relacionados con otros tipos de normas.

ETSI (European Telecommunications Standards Institute)

http://www.etsi.org/

El Ministerio de industria y energía lo define como; Organismo sin ánimo de lucro creado al objeto de disponer del foro adecuado para la elaboración de las normas de telecomunicación que faciliten la estandarización del sector, y por lo tanto el avance hacia el Mercado Único Europeo. En el ETSI participan como miembros no sólo las Administraciones, sino también los operadores de red, la industria, los centros de investigación y los usuarios de los servicios de telecomunicación.

Los objetivos del ETSIse centran en la elaboración y el mantenimiento y actualización de normas ISOs técnicas a nivel europeo en los campos de las telecomunicaciones, tecnologías de la información y sistemas de radiodifusión y televisión.

Por tanto el ETSI es la organización clave en el contexto europeo para la elaboración de normas tanto en el sector de las telecomunicaciones como para la convergencia de este sector con los de tecnologías de la información y audiovisual.

Además el ETSI mantiene coordinación con los organismos internacionales de normalización, principalmente con ITUT e ITUR.

Algunos de los cuerpos de estandarización que podemos encontrarnos dentro de este organismo pueden ser:

- 3GPP (para redes UMTS)
- TISPAN (para redes fijas y convergencia con Internet).

INTERNACIONALES

ISO (International Standarization Organization)

http://www.iso.org

En 1926 fue creada la Federación Internacional de Asociaciones Nacionales de Normalización (International Standardization Associates, ISA). Esta fue disuelta en 1942 por la segunda guerra mundial. El 23 de febrero de 1947, se reunieron en Londres 64 delegados de 25 países, creando la ISO (Organización Internacional de Normalización), que vendrá a continuar el trabajo de la ISA.

El nombre no viene dado por las siglas, si no del griego isos, que significa igual. Su misión es promover en el mundo el desarrollo de la normalización y actividades relacionadas, en la mayoría de los campos técnicos, es la mayor entidad de desarrollo y publicación de Estándares Internacionales.

Es una red compuesta por los institutos nacionales de estandarización de 164 países, un miembro por Estado. La Secretaría General está en Ginebra (Suiza), que realiza operaciones de coordinadora del sistema.

Para acceder a los estándares, el público corriente tiene que comprar el documento. Los documentos están protegidos por derechos de copyright.

La organización está compuesta por tres clases de miembros:

- Miembros Natos: La representación es unitaria y recae sobre los organismos nacionales de normalización de cada país.
- Miembros Correspondientes: Son países sin organismos nacionales de normalización, normalmente en vía de desarrollo. No intervienen activamente en las decisiones pero son informados de ellas.
- Miembros Suscritos: Países con reducidas economías, a los que se les pide un pago menor.

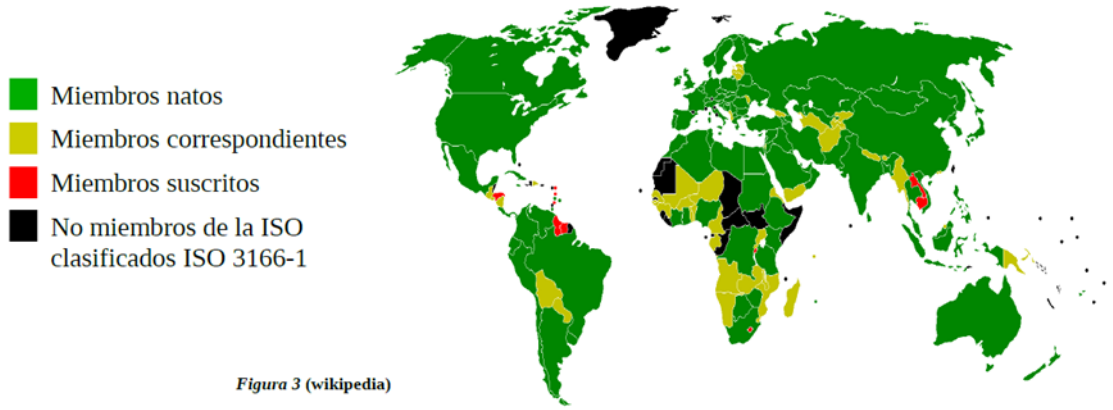


Figura 3 (wikipedia)

El costo de operación anual para la ISO se calcula en 97 millones de euros. El 60% se obtiene a través de cuotas a sus miembros, el 40% restante se obtiene a través de la venta de publicaciones y otros servicios.

A nivel interno, la estructura de ISO queda de la siguiente forma:

- Consejo Técnico: Encargado de aprobar los proyectos de normas.
- Comités Técnicos: Comités subordinados al Consejo Técnico. Su función es estudiar los principios científicos de la norma.
- Subcomités Técnicos: Subordinados a los Comités Técnicos. Aquí se encuentran cada uno de los países que conforman la organización.

Como punto importante ISO no realiza ninguna actividad de certificación. Ni de productos, servicios o de sistemas de gestión de la calidad. Solo elabora las normas que otros organismos emplean para poder certificar productos, servicios y sistemas de gestión de la calidad.

IEC (Comisión Electrotécnica Internacional)

http://www.iec.ch/

Para ver el origen de las normativas internacionales tendríamos que remontarnos a 1906, cuando se inició la normalización internacional en el ámbito de la electrotécnica, a través de la Comisión Internacional de Electrotécnica (International Electrotechnique Comittee, IEC).

Los estatutos de la CEI engloban a todas las tecnologías electrotécnicas:

- La electrónica
- El magnetismo y electromagnetismo
- La electroacústica
- Las tecnologías multimedia
- Las telecomunicaciones
- La producción y distribución de energía
- Las disciplinas generales relacionadas como; compatibilidad electromagnética, medición y rendimiento, seguridad y medio ambiente...

Numerosas normas se realizan conjuntamente entre la IEC y la ISO. Estas normas van precedidas por ISO/IEC. Existen tres formas de participación ante la IEC:

- Miembro pleno
- Miembro asociado
- Miembro preasociado

ITU-T (Sector de Normalización de las Telecomunicaciones de la UIT)

http://www.itu.int/ITU-T

Unión Internacional de Telecomunicaciones (engloba CCITT y CCIR) y es parte autónoma del UIT. Surge en 1992 como sucesora de la CCITT. Está caracterizada por poseer unos procesos ágiles para la elaboración de las normas. Desde la propuesta inicial de un borrador hasta la aprobación final de una recomendación, es un proceso tan sólo de unos pocos meses pudiendo ser menor.

Esta forma de trabajar permite que los progresos tecnológicos estar en mayor medida recogidos y normalizados.

La ITU-T clasifica sus recomendaciones en series, nombradas desde la serie A hasta la serie Z. Algunas de las series a destacar serian:

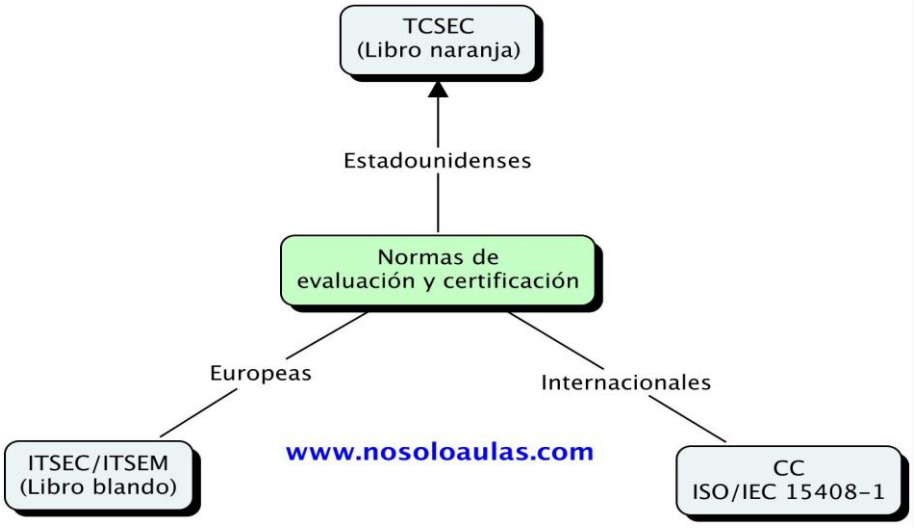
- Serie X; Redes de datos y comunicación entre sistemas abiertos y seguridad.
- Serie Y; Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación

También se debe hacer mención dentro de este punto a la British Standards Institution (BSI). La British Standards Institution, es una empresa privada multinacional cuyo fin se basa en la creación de normas para la estandarización de procesos. BSI es un organismo colaborador de ISO y proveedor de estas normas, mas adelante veremos la ISO 27001. Entre sus actividades principales se incluyen la certificación, auditoría y formación en las normas; distinguiéndose en este punto de la mayoría de las organizaciones anteriormente mencionadas.

Normas de evaluación y certificación

Ahora que conocemos las instituciones de certificación pasaremos a ver como las normas de evaluación y certificación en las que de una manera u otra participan.

Con las normas se persigue conseguir el cumplimiento de unos requisitos específicos para proporcionar una garantía escrita sobre puntos de negocio, proceso, producto,

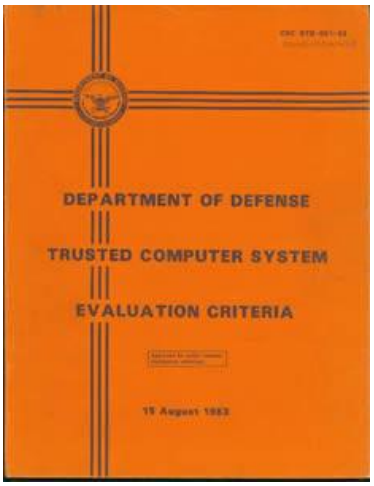


servicio y sistema de gestión de las empresas.

Todo esto se hace a través de procedimientos de evaluación y monitorización de empresa (totalmente de forma voluntaria). Veremos las tres principales normas. Empezaremos con los vetustos antecedentes de la norma CC (criterios comunes) de mano de la normativa estadounidense TCSEC y de la normativa europea ITSEC.

TCSEC (Trusted Computer System Evaluation Criteria)

Esta norma nace en 1983 con la meta de aplicar la política de seguridad del departamento de defensa estadounidense.



Principalmente se centra en definir criterios para mantener la confidencialidad de la información clasificada a nivel nacional. El departamento de defensa americano saco una serie de publicaciones de seguridad conocidas como las Rainbow Series, siendo el primer tomo de tapas naranjas el que cubría la TCSEC. Pasando a ser llamado coloquialmente el libro naranja.

El Libro Naranja fue desarrollado por el NCSC (National Computer Security Center) del Departamento de Defensa de EEUU. Actualmente, la responsabilidad la ostenta un organismo civil, el NIST (National Institute of Standards and Technology).

Los TCSEC definen 7 niveles de criterios de evaluación llamados clases, que a su vez se distribuyen en 4 grupos diferenciados por tener la misma letra en el nombre y tener unas características de nivel de seguridad parecidas.

Las 7 clases son las siguientes:

- D Protección mínima. Sin seguridad.
- C1 Limitaciones de accesos a datos.
- C2 Acceso controlado al sistema informático. Archivos de log y de auditoría del sistema.
- B1 Equivalente al nivel C2 pero con una mayor protección individual para cada fichero.
- B2 Los sistemas deben estar diseñados para ser resistentes al acceso de personas no autorizadas.
- B3 Dominios de seguridad. Los sistemas deben estar diseñados para ser altamente resistentes a la entrada de personas no autorizadas.

- A1 Protección verificada. En la práctica, es lo mismo que el nivel B3, pero la seguridad debe estar definida en la fase de análisis del sistema.

ITSEC/ITSEM (Information Technology Security Evaluation Criteria)

Es el equivalente al libro naranja americano (TCSEC) pero de generado por Europa en 1990. Se le conoce como el libro blanco. Tiene un mayor alcance y es más moderno que su homólogo americano.

Cuando se publicó en 1991 la versión 1.2 de ITSEC vino acompañada del ITSEM (Information Technology Security Evaluation Manual), que consiste en un manual de evaluación de la seguridad de TI cuya misión es describir los métodos y procedimientos para realizar las evaluaciones de seguridad de los diferentes criterios.

En el ITSEC al igual que en el TCSEC, hay una escala de 7 clases o niveles de evaluación. Esta empieza en E0 que incida una confianza no adecuada, hasta un E6 que representa el nivel de confianza más alto.

CC (Criterios Comunes) o ISO/IEC 15408-1

Surgen en 1990, siendo el resultado de la necesidad de conocer qué requisitos de seguridad satisfacía un determinado software, hardware o firmware. Mediante la combinación de los criterios aplicados en Inglaterra, Estados Unidos y Canadá, se constituyó y adoptó por la ISO los Criterios Comunes de Evaluación de Seguridad para Tecnologías.

El principal objetivo es poner de acuerdo a clientes, desarrolladores y testers sobre qué requisitos de seguridad cumple un determinado producto. CC se basa principalmente en 4 puntos:

- Perfil de protección.
- Objetivo de evaluación.
- Objetivo de seguridad.
- Nivel de evaluación de seguridad.

Al estilo de las anteriores normativas, los CC también están divididos en 7 niveles que van desde el EAL1 al EAL7:

- EAL1 (funcionalidad probada)
- EAL2 (estructuralmente probado)
- EAL3 (probado y verificado metódicamente)
- EAL4 (diseñado, probado y revisado metódicamente)
- EAL5 (diseñado y probado semi - formalmente)
- EAL6 (diseño verificado y probado semi - formalmente)
- EAL7 (diseño verificado y probado formalmente)

Correlación de los niveles ITSEC, ITSEC y CC.

US TCSEC	European ITSEC	Common criteria	Description
D	E0	EAL1	Functionally tested
C1	E1	EAL2	Structurally tested
C2	E2	EAL3	Methodically tested and checked
B1	E3	EAL4	Methodically designed, tested and reviewed
B2	E4	EAL5	Semi-formally designed and tested
B3	E5	EAL6	Semi-formally verified design and tested
A1	E6	EAL7	Formally verified design and tested

2.5. La familia de normas ISO/IEC 27000 (27001 / 27002)

La serie 27000 son varios estándares publicados por ISO e IEC. Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Las normas base de la serie 27000 consta de la ISO/IEC 27001 y ISO/IEC 27002, siendo consideradas las siguientes como normas complementarias. La numeración de las ISOs van desde 27000 a 27019 y de 27030 a 27044.

Algunas de estas normas son:

- ISO/IEC 27000; define el vocabulario estándar empleado en la familia 27000.
- ISO/IEC 27001; norma que especifica los requisitos para la implantación del SGSI.
- ISO/IEC 27002; código de buenas prácticas para la gestión de la seguridad.
- ISO/IEC 27003; guía de implementación de SGSI e información del uso del modelo PDCA.
- ISO/IEC 27004; especifica métricas y técnicas para la gestión de seguridad de la información.

- ISO/IEC 27005; gestión de riesgos en seguridad de la información.
- ISO/IEC 27006; requisitos a cumplir por las organizaciones emisoras de certificaciones.
- ISO/IEC 27007; Es una guía para auditar al SGSI según las normas 27000.
- ISO/IEC 27011; guía de gestión de seguridad de la información específica para telecomunicaciones.
- ISO/IEC 27031; guía de continuidad de negocio.
- ISO/IEC 27032; guía relativa a la ciberseguridad.
- ISO/IEC 27032; guía de seguridad en aplicaciones.

Tal como muestra la figura 7, la norma 27000 ha tenido un recorrido por varias entidades certificadoras y por varias versiones. Empezó como la norma BS 7799 de BSI, en 1995, con el fin de proporcionar un conjunto de buenas prácticas de gestión de seguridad a cualquier empresa que lo necesitara.

La norma BS 7799-1 se creó como guía de buenas prácticas no certificable. En cambio la norma BS 7799-2, definió los requisitos para la certificación de un SGSI. Se publicó por primera vez en 1998. En 1999, estas dos normas se resisaron. En 2002, se revisó BS 7799-1 para adecuarse a las normas ISO 17799. En 2005, la norma BS 7799-2 se publicó como ISO 27001. También se revisó y actualizó ISO 17799:2000 renombrándose como ISO 27002:2005.

En 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006. A partir de este punto, ISO continuó y continúa desarrollando las demás normas dentro de la series 27000 siendo la única norma certificable la 27001.

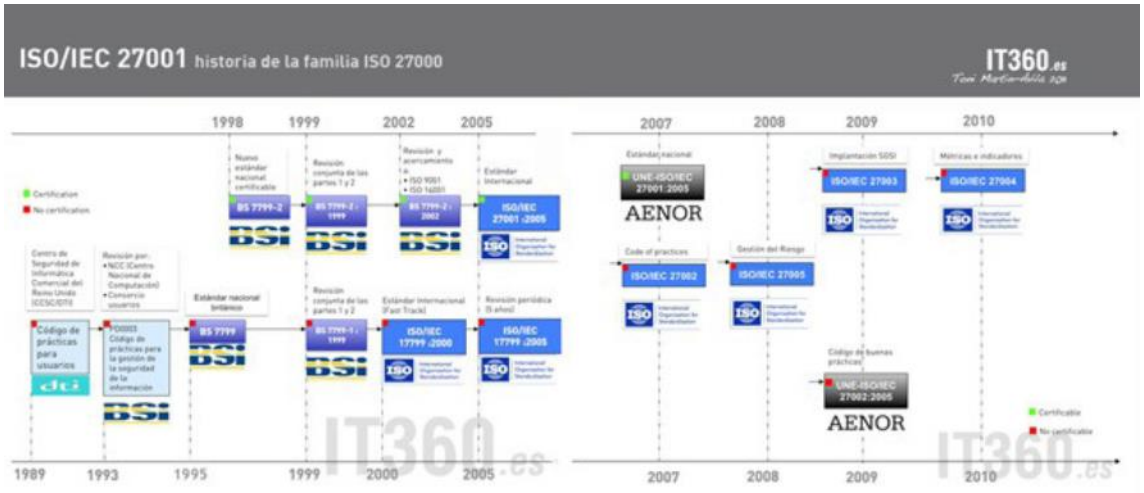


Figura 7 autor **Toni Martín-Avila IT360.es**

Ahora que tenemos la visión general de unas cuantas normas que componen la norma

27000 y cómo ha sido su historia pasaremos a analizar las dos normas base:

- ISO/IEC 27001
- ISO/IEC 27002
- ISO/IEC 27001

Esta norma especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado, definiendo los requisitos para implantar los controles de seguridad personalizados de la empresa. Esta norma es certificable, y para certificar una empresa según esta norma, se deberá conocer el proceso completo, siguiendo los pasos del tema ”Sistemas de Gestión de Seguridad de la Información” que sigue al actual.

La auditoría de certificación consiste en que un equipo auditor externo a la empresa la auditará, comprobando que tengamos cumplidos los puntos que establece la norma. En caso positivo, obtendremos la certificación y sello de que cumplimos con la ISO 27001.

Se usa el modelo PDCA (Plan-Do-Check-Act) para los procesos de la organización que estén incluido en el SGSI. Veremos en el tema “Sistemas de Gestión de Seguridad de la Información” este punto completamente desarrollado.

Beneficios que puede aportar entre otros la certificación son:

- Mejora de rendimiento al estar constantemente evaluándose el sistema.
- Demuestra que se cumple con las leyes pertinentes.
- Demuestra preocupación de la empresa por la seguridad de la información.
- Nos hace conscientes de los riesgos que pueden sufrir algunos departamentos.
- Etc.

Las principales claves para implantar esta norma son:

- Identificar los objetivos de negocio; el propósito de la certificación es garantizar la gestión de la seguridad sin olvidar que esto debe contribuir al desarrollo de los servicios o procesos de negocio
- Seleccionar un alcance adecuado; hay que tener siempre en mente el sistema que queremos construir y ajustar los recursos a esa meta.
- Determinar el nivel de madurez ISO 27001; hay que conocer de antemano el punto de partida para la certificación, ya que no será el mismo si partimos desde cero como si ya tenemos elaborada algo a través de otro proceso de calidad.

- Analizar el retorno de inversión; Es vital hacer ver que todo el proceso para la certificación de la ISO no es un gasto si no una inversión.

ISO/IEC 27002

Esta norma se puede considerar como un código de buenas prácticas o como una guía que permite saber qué pasos puedes seguir para mejorar la seguridad de la información. Esta norma no es certificable.

Define secciones o áreas sobre las que actuar, siendo estas las siguientes:

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Gestión de activos.
- Seguridad ligada a RRHH.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad de negocio.
- Conformidad.

Dentro de cada una de estas secciones o áreas, hay que tener en cuenta dos cosas:

- Objetivos de control; aspectos a asegurar (controles) dentro de cada área/sección. La suma de todos los controles de todas las secciones son 133 especificados en el anexo de la norma, pero no hay que aplicarlos todos, solo los que necesite la empresa.
- Controles: mecanismos para cada objetivo de control, dados como guía de implantación. Para asegurarlos.

2.6 Sistemas de Gestión de Seguridad de la Información (SGSI)

Es posible que nos encontremos esta "herramienta" de gestión por sus siglas en ingles, ISMS (Information Security Management System).

Un SGSI pone a disposición de la empresa las más eficaces herramientas necesarias para conocer y administrar la información de la empresa. También ofrece herramientas para minimizar los incidentes de seguridad que pudiera tener la empresa. Usa la norma 27001 como guía de referencia para su implantación. Al poder ser auditada, también puede ser certificada.

Algunas de las empresas dedicadas a estas son: SGS, Bureau Veritas Certificación y DNV entre otras. De forma reducida un SGSI consiste en un conjunto de:

- Estructura organizativa.
- Activos físicos (Hard y soft)
- Conocimientos
- Procedimientos
- Recursos humanos

Objetivos	**Desde el punto de vista de dirección:** **• Garantizar confidencialidad.** **• Reducir los riesgos a niveles aceptables.** **Desde el punto de vista implantador SGSI:** **• Definir un SGSI certificable.** **• Implantar metodología de trabajo óptima para asegurar la información.**
Beneficios de un SGSI	A nivel interno: • Documentar y estandarizar las actividades. • Disminuir riesgo; al tener elementos de control inicial para proyectos nuevos, estos se pueden asegurar desde el momento de diseño. • Rentabilidad a corto y medio plazo; esto se consigue al disminuir la posibilidad de pérdidas y fugas de información. • Sistema que autoaprende; por cada ciclo que se recorre en un SGSI se afinada cada vez mas. • Optimización de los recursos; nos informa de la situación de la empresa. A nivel externo: • Cumplir con leyes y reglamento; se percibe mejor una empresa que se sabe que cumple con la ley. • Protección del negocio; dando mayor estabilidad y posicionamiento en su mercado. • Imagen corporativa; entre otros motivos de mejora de imagen es estar auditado y certificado por una empresas y/o organismos externos. • Reducción de costes; aunque al principio se ve como un coste a la larga compensa. Detecta focos de problemas • Más competitiva. • Mejor calidad. No hay que abarcar todo el ámbito de la empresa para desarrollar una SGSI, es necesario restringirlo a un ámbito manejable. Posteriormente y si se ve que es necesario se puede ir ampliando hasta dar cobertura plenamente. El ámbito manejable no tiene que ser por departamentos o divisiones de la empresa. Se recomienda que en el primer acercamiento a la implantación de un SGSI, si se quiere hacer que cubra completamente toda la empresa, que se realice del menor tamaño posible de cada departamento. Luego abra tiempo de ampliarlo y mejorarlo. Se puede decir que hay dos ciclos diferenciados que se repetirán mientras la actividad de la empresa se continué realizando: Diseño, Mantenimiento. Implantar un SGSI puede llevar de 6 meses a 1 año dependiendo del tamaño de la empresa y de lo compleja que sea. Que no supere el año, es para que el trabajo que se realiza al principio no caduque. Hay que tener en mente que en el desarrollo de una SGSI tiene que primar que sea sencilla de desarrollar, implementar y mantener.

Modelo PDCA

Para numerar la fases de un SGSI se usa el modelo de gestión PDCA (Plan / Do / Check / Act) en español PHVA (Planificar / Hacer / Verificar / Actuar). El modelo de gestión PDCA es cíclico. Una vez que se a pasado por todos y cada una de las fases que lo compone, se volverán a realizar.

Por cada ciclo que se realiza se adquiere experiencia, detectando donde hemos fallado y que soluciones son las más idóneas para resolverlo. También detectaremos nuestros puntos fuertes.

¿Cuántas veces será esto? Los ciclos se seguirán haciendo mientras se continué con la actividad de la empresa. Mejorando, simplificando y ampliando el alcance por cada vuelta que se da. Por norma, cuando se aplica un PDCA a una empresa se realiza en dos vertientes, una para la detección de objetivos y los procesos que van de la mano de estos, y por otra, la resolución de problemas. En el caso de un SGSI se solapan los dos en una sola vertiente.

Según el Instituto Nacional de Tecnología de la Comunicación las fases y pasos de un SGSI quedan de la siguiente forma.

Fases

Fase 1 Plan	Fase 2 Do (hacer)	Fase 3 Check	Fase 4 Act
En esta primera fase se realiza un estudio de la situación de la Organización (desde el punto de vista de la seguridad), para estimar las medidas que se van a implantar en función de las necesidades detectadas. Hay que tener en cuenta que no toda la información de la que dispone la organización tiene el mismo valor, e igualmente, no toda la información está sometida a los mismos riesgos. Por ello un hito importante dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así mismo se hace necesario una Gestión para dichos riesgos de cara a reducirlos en la medida de lo posible. El resultado de este Análisis y Gestión de Riesgos será establecer una serie de prioridades en las tareas a realizar para minimizar dichos riesgos. Puesto que los riesgos nunca van a desaparecer totalmente, es importante que la Dirección de la Organización asuma un riesgo residual, así como las medidas que se van a implantar para reducir al mínimo posible dicho riesgo residual.	En esta fase se lleva a cabo la implantación de los controles de seguridad escogidos en la fase anterior. En dicha implantación se instalarán dispositivos físicos (hardware, software,...), pero también se creará o revisará la documentación necesaria (políticas, procedimientos, instrucciones y registros). Dentro de esta fase es muy importante dedicar un tiempo a la concienciación y formación del personal de la empresa de cara a que conozcan los controles implantados.	Es importante que la Organización disponga de mecanismos que le permitan evaluar la eficacia y éxito de los controles implantados. Es por esto que toman especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.	En esta fase se llevarán a cabo las labores de mantenimiento del sistema así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se suele llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se suele esperar a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

Pasos del SGSI

Usando el modelo de gestión PDCA podemos subdividirlo en las siguientes fases/pasos

Establecimiento del SGSI

- Inicio del Proyecto
- Asegurar el compromiso de la Dirección.
- Seleccionar y entrenar a los miembros del equipo inicial que participan en el proyecto.
- Definición del SGSI
- Identificación del alcance del SGSI y de la Política de Seguridad del SGSI.
- Recopilar los documentos de seguridad existentes en la organización.
- Preparar los procedimientos relacionados con la gestión y la operación del SGSI.
- Análisis de Riesgos
- Definición de una metodología para la clasificación de los riesgos.
- Creación de un inventario de activos.
- Evaluación de los activos a ser protegidos.
- Identificación y evaluación de amenazas y vulnerabilidades de los activos.
- Cálculo del valor de riesgo asociado a cada activo.
- Gestión de Riesgos
- Identificar y evaluar alternativas posibles para tratar los riesgos.
- Seleccionar e implantar los controles correctos que le permitan a la organización reducir el riesgo a un nivel aceptable.
- Redactar el documento de declaración de aplicabilidad (documento de selección de controles), que debe ser firmado por Dirección.
- Identificar los riesgos residuales que han quedado sin cubrir y obtener la firma de Dirección.
- Preparar el Plan de Tratamiento de Riesgos Preparar procedimientos para implantar los controles.

⇩

Implantación y operación

- Implantación del SGSI
- Implantar el plan de tratamiento de riesgos.
- Implantar políticas y procedimientos del SGSI.
- Implantar los controles seleccionados.
- Formación y sensibilización
- Impartir formación entre los empleados sobre los nuevos procedimientos que se van a implantar.
- Concienciar a la plantilla de la importancia que el proyecto de seguridad tiene para la Organización.

⇩

Monitorización y revisión

- Monitorización del SGSI
- Ejecutar procedimientos de monitorización para detectar errores de proceso, identificar fallos de seguridad de forma rápida y acciones a realizar.
- Revisión del SGSI
- Revisiones periódicas de la política y alcance del SGSI, así como de su eficacia.
- Revisiones de los niveles de riesgos residuales y riegos aceptables.
- Auditorías internas/externas del SGSI.

⇩

Mantenimiento y mejora

- Mantenimiento del SGSI
- Comunicar resultados de las auditorías a las partes interesadas.
- Adoptar acciones correctivas y preventivas.
- Mejora Continua
- Medir el rendimiento del SGSI.
- Implantar las mejoras identificadas en las revisiones del SGSI.