2. Gestión de la Ciberseguridad

2.1. Introducción y objetivos

Este tema pretende sentar las bases y profundizar en las principales normas y estándares de seguridadque debe tener en cuenta toda organización para diseñar e implementar correctamente su ciberseguridad. Cada organización debe basar su seguridad en su política de seguridad y establecer un sistema de gestión de seguridad de la información (SGSI).

El pilar fundamental en el que ha de basarse la seguridad de la información de toda organización, ya sea pública o privada, es la definición de la política de seguridad. Una política de seguridad bien definida e implantada en una organización gestionada por procesos es la base para implantar un SGSI que regule y gobierne los procesos y procedimientos que han de implementarse en toda organización. Además, todo el personal, cada uno según su nivel, debe seguirla de forma coordinada para conseguir el objetivo de seguridad requerido por la organización, para protección ante cualquier tipo de amenaza interna o externa.

El objetivo fundamental de este tema es el de conocer en qué consiste una política de seguridad, a quién va dirigida y saber cómo diseñarla, analizar el concepto de SGSI y fases de las que consta, así como conocer las asociaciones y certificaciones relacionadas con la profesión de la seguridad de la información. Este conocimiento es esencial para comprender los conocimientos que son necesarios para convertirse en un profesional en el área.

Más concretamente, los objetivos de este tema son los siguientes:

* Estudiar en qué consiste la política de seguridad de una organización.
* Analizar las fases de las que consta una política de seguridad para comprender qué pasos hay que dar para diseñarla.
* Analizar en qué consiste un SGSI y sus fases.
* Entender y saber explicar el rol del profesional de la seguridad de la información con referencia al reconocimiento de la profesión por los clientes, el entorno académico y los conocimientos comúnmente requeridos.
* Conocer las fundamentales certificaciones en el área de la seguridad de la información y entender el proceso de certificación.

2.2. Política de seguridad

La política de seguridad de una organización es un conjunto de normas que rigen y determinan lo que se puede hacer y lo que no dentro de ella, coordinando todas las actividades de seguridad de todos los miembros de una organización, empezando por la dirección. Según el Internet Engineering Task Force (IETF, 1997), se define como «una serie de sentencias formales (normas) que deben cumplir todas las personas que tengan acceso a cualquier información y tecnología de una organización». Entre las características más importantes de toda política de seguridad se pueden destacar (Díaz, 2004):

* Define el comportamiento apropiado para cada caso.
* Establece qué herramientas y qué procedimientos son necesarios.
* Sirve para comunicar un consenso del uso de datos y aplicaciones dentro de la organización.
* Proporciona una base para la demostración del uso inapropiado de recursos por parte de empleados o de externos.

La política de seguridad de una organización es un concepto en constante movimiento que permite que el mantenimiento de la seguridad sea un proceso vivo y administrable de forma estructurada y organizada. Por tanto, la seguridad es un proceso que se tiene que alcanzar mediante el desarrollo de la política de seguridad, que ha de entenderse como algo dinámico que se tiene que actualizar observando una serie de principios de seguridad:

A screen shot of a phone

Description automatically generated

Tabla 1. Principios de seguridad. Fuente: elaboración propia.

Este apartado explica los tipos de normativas necesarias en una política de seguridad y las fases y actividades que llevar a cabo dentro del proceso de gestión de la seguridad de acuerdo con un conjunto de principios de seguridad. Además, explica cómo es la puesta en marcha del proceso de seguridad, que se puede escenificar como una rueda que incluye una serie de fases que conforman un SGSI.

Se ha de contemplar siempre el principio de privilegio mínimo, que consiste en tratar de minimizar el número de usuarios con privilegios de administrador, el conjunto de equipos externos con acceso a sistemas locales y el número de situaciones en las que alguien o algo tiene privilegios de acceso que no necesita para que el trabajo salga adelante.

A diagram of a diagram of a diagram

Description automatically generated with medium confidence

Figura 1. Política de seguridad. Fuente: elaboración propia.

Hay que implementar las salvaguardas de seguridad teniendo presentes los principios de defensa en profundidad y de diversidad de defensa. Se debe intentar tener más de un nivel de defensa y que sean de distinta naturaleza para, de esta forma, hacer más difícil el trabajo del supuesto atacante, que no solo debe vencer más de una defensa, sino que cada una lo obliga a tener distintos tipos de conocimiento.

También es importante seguir el principio del cierre completo, que consiste en garantizar que, ante un incidente de ataque con éxito a un componente, este queda aislado del resto de activos de la organización. Quizás el más importante y difícil de conseguir es el principio de simplicidad, que persigue que se cumplan todos los anteriores a la vez que se puede gestionar todo el sistema, de manera simple y entendible.

Es necesario remarcar que se debe cumplir, en toda política de seguridad, cualquier obligación legal en el marco de las leyes del país donde se quiera imponer la política.

Para conseguir el objetivo, se define un conjunto de normas, procesos y procedimientos relacionados con todos los ámbitos de la seguridad que se ejecutan de forma cíclica para eliminar todas las vulnerabilidades posibles. Algunas de las normas claves que estarán en cualquier política son:

* SGSI.
* Ciclo de vida de desarrollo seguro de *software*.
* Normas de uso aceptable de equipos y servicios.
* Normas de acceso remoto.
* Normas de protección de la información.
* Normas sobre la seguridad perimetral.
* Normas básicas de seguridad física.
* Normas sobre respuestas a incidentes.
* Encriptación aceptable.
* Proveedores de conexión a Internet aceptables.
* Proveedores de *software* aceptables.
* Seguridad en las adquisiciones.
* Auditoría.
* Valoración de riesgos.
* Contraseñas aceptables.
* Seguridad de portátiles.
* Seguridad de equipos en las zonas desmilitarizadas (*demilitarized zones*, DMZ).
* Redes privadas virtuales.
* Seguridad de los servidores.
* Laboratorios de prueba de problemas de seguridad.
* Antivirus.
* Seguridad de encaminadores y conmutadores.
* Comunicaciones *wireless*.
* Cortafuegos aceptables.

Varios estándares se pueden seguir para la implantación de una política de seguridad:

* Esquema Nacional de Seguridad, guía CCN-STIC-805 (Real Decreto 3/2010, 2010).
* ISO 27001 (ISO27001-5, 2020).
* COBIT 5 (Cuzme Rodríguez et al., 2017) para la seguridad de la información.

El proceso principal que emana de la política de seguridad es el SGSI, que, a su vez, debe implantar un ciclo de vida de desarrollo seguro de *software* para implementar la seguridad de las aplicaciones *online* desde el comienzo del desarrollo. Estos procesos son la base para implementar la seguridad y protección de los sistemas de información y comunicaciones de la organización.

2.3. Diseño de la política de seguridad

Las políticas tienen muchas utilidades. Por ejemplo, podrían ser un salvavidas durante un desastre o un requisito de una función reguladora. La política también puede proporcionar protección contra la responsabilidad debida a un trabajador o definir acciones para el control de los secretos comerciales.

Diferentes tipos de políticas

El término «política» es uno de esos términos que pueden significar varias cosas en seguridad de la información. Por ejemplo, existen políticas de seguridad en servidores que se refieren al control de acceso y la información de enrutamiento. Los estándares, procedimientos y directrices también se conocen como políticas en el sentido más amplio de la seguridad.

Aquí se hace referencia a las políticas como controles administrativos de carácter temático, a veces denominadas «políticas funcionales». Estas políticas detallan las políticas generales de la organización.

Políticas y su importancia

Las políticas no son directrices o estándares, ni tampoco, obviamente, procedimientos. Las políticas describen la seguridad en términos generales y no específicos; pueden considerarse las plantillas o requisitos generales que determinan cómo se diseñarán e implementarán los diferentes elementos de la seguridad.

La diferencia entre política e implementación es importante. Por ejemplo, si una política estableciese que el *login* único debe hacerse con un producto concreto de una empresa, cuando el mercado evolucione, puede que otros productos sean mejores. No parece razonable que el objetivo (que es lo que define la política) esté ligado a un producto o tecnología concreta, al menos en la mayoría de los casos. Ahora bien, la política sí que puede indicar la obligatoriedad de que, independientemente de la elección de producto final, se documenten las razones de por qué se ha seleccionado.

El diseño de políticas es importante porque estas definen los objetivos de la seguridad. Además, la participación de la dirección en la definición de las políticas proporciona un mensaje claro sobre la implicación y compromiso de la organización en sus niveles directivos. Las políticas se aplican a la organización entera, por lo que facilitan tener unos estándares de seguridad coherentes, y esto es algo que los clientes pueden apreciar y hace la gestión más sencilla.

Por último, las políticas son útiles para gestionar los litigios. Si se amonesta a un empleado por una acción relacionada con la seguridad y no había una política escrita, es complicado justificar esa amonestación. Desde una perspectiva más pragmática, la ausencia de políticas escritas correctamente simplemente impide la evaluación externa y la auditoría.

Secciones de una política de seguridad

De acuerdo con la guía CCN-STIC-805 del Centro Criptológico Nacional (CCN) (2011), las secciones típicas de una política de seguridad de la información son:

«1. Misión u objetivos del organismo

2. Marco normativo

3. Organización de seguridad

- Definición de comités y roles unipersonales

- Funciones

- Responsabilidades

- Mecanismos de coordinación

- Procedimientos de designación de personas

4. Concienciación y formación

5. Postura para la gestión de riesgos

- Plan de análisis

- Criterios de evaluación de riesgos

- Directrices de tratamiento

- Proceso de aceptación del riesgo residual

6. Proceso de revisión de la política de seguridad».

Misión y objetivos

Se describirá la razón de la existencia de la organización y los servicios que presta.

Marco normativo

El objetivo es definir por escrito las responsabilidades en que puede incurrir una organización por su naturaleza jurídica, sus obligaciones de cumplir con la normativa nacional o de la industria y sus obligaciones contractuales con terceros señalando la normativa correspondiente.

Organización de la seguridad

En esta sección del CCN-STIC-805 se detallan las siguientes actividades (CCN, 2011):

«- Se debe describir cómo se coordina el organismo para atender a las necesidades de seguridad, tanto TIC como en otras materias y cómo se distribuye la información y se toman decisiones corporativas. La guía CCN-STIC 402 (CCN STIC402, 2006) puede usarse como modelo.

- Se deben describir los roles unipersonales en materia de seguridad de la información. En particular la figura del responsable de Seguridad de la información, detallando sus funciones y responsabilidades.

- Se debe determinar la estructura de seguridad […]

- Cuando se traten datos de carácter personal, se hará mención explícita al Documento de Seguridad que refleja la postura de <el organismo> respecto de los mismos».

Concienciación y formación

El objetivo es comprender plenamente que la seguridad de la información concierne a todos los miembros y todas las actividades, de conformidad con el principio de seguridad total, así como la presentación clara de los medios necesarios para que todos los participantes en el proceso y sus responsables directos sean sensibles a los diversos riesgos a los que se están expuestos.

Gestión de riesgos

El análisis de riesgos será el pilar para determinar los controles de seguridad por implementar. Esta sección debe reflejar el compromiso y la obligación de los responsables del sistema de realizar análisis de riesgo y estudiar sus conclusiones. El análisis y tratamiento de riesgos debe ser una actividad que se repita periódicamente.

Proceso de aprobación y revisión

La política de seguridad de la información es un documento que será aprobado formalmente por la alta dirección y será vinculante para toda la organización. Asimismo, será objeto de un proceso periódico de revisión para adaptarlo a las nuevas circunstancias, técnicas u organizativas, y evitar que quede obsoleto. Por esta razón, se establecerá un proceso organizativo para garantizar que la puntualidad, relevancia, integridad, completitud y precisión de lo que establece la política se revisará periódicamente y se presentará a la alta dirección para su aprobación oficial. El proceso de preparación y aprobación debe estar claramente definido en la misma política.

Herramientas para implementar la política de seguridad

Dado que la política de seguridad está escrita en un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello, se utilizan otros instrumentos que reciben diferentes nombres. Los más comunes son los siguientes:

* Normas de seguridad.
* Guías de seguridad.
* Procedimientos de seguridad.

Las normas estandarizan el uso de aspectos específicos del sistema. Indican un uso correcto y responsabilidad del usuario y son obligatorias.

Una guía es de naturaleza educativa y está destinada a ayudar a los usuarios a aplicar las medidas de seguridad correctamente al proporcionar un razonamiento donde no se dispone de los procedimientos correctos. Por ejemplo, a menudo hay una guía para escribir procedimientos para configurar la seguridad de un sistema operativo o un servicio determinado. La orientación ayuda a evitar que se pasen por alto problemas de seguridad importantes, lo que se puede realizar de varias maneras.

Los procedimientos (operativos) seguros se ocupan de tareas específicas, mostrando cada paso que se debe realizar. Son muy útiles en tareas que son repetitivas, como puede ser un procedimiento de *backup* y recuperación de un sistema.

Las organizaciones no siempre separan claramente estos diferentes tipos de herramientas, pero, en ocasiones, se crean guías de usuario y manuales de seguridad que contienen un poco de todos los elementos mencionados en este artículo anterior, siempre buscando una mayor eficiencia en la sensibilización y formación de los usuarios del sistema. Aunque los manuales y los reglamentos mixtos pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre lo que se refiere a la política y su aplicación práctica. De esta forma, se puede ser más flexible y se consigue una cierta uniformidad de resultados incluso cuando evoluciona o cambia la tecnología o cualquiera de los mecanismos empleados.

2.4. Sistema de gestión de seguridad de la información

Como se ha dicho anteriormente, la política de seguridad de toda organización debe llevar a cabo la implementación de un sistema que gestione las medidas de seguridad en todos los niveles que hay que implantar para proteger adecuadamente los sistemas.

Un SGSI es para una organización el diseño, implantación y mantenimiento de un conjunto de procesos que permitan gestionar de forma eficiente la accesibilidad de la información y asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando, a la vez, los riesgos de seguridad de esta.

Un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como a los externos del entorno, gestionando el riesgo de forma dinámica con el objetivo de que el riesgo residual sea el mínimo posible.

Hay varios modelos que se pueden seguir para implantar un SGSI. Normalmente, siguen el esquema de fases plan-do-check-act (PDCA), que significa «planificar-hacer-controlar-actuar». Este es un enfoque de mejora continua basado en una monitorización constante del sistema que permite actualizar el riesgo residual de los activos de la organización de forma dinámica:

A close-up of a text

Description automatically generated

Tabla 2. Fases PDCA. Fuente: elaboración propia.

Tres de las implementaciones más importantes de SGSI son:

* ISO 27001.
* NIST SP 800-53. Rev. 5.
* Esquema Nacional de Seguridad (España).

ISO 27001

Este sistema (ISO27000, s. f.) sigue el enfoque de mejora continua de fases PDCA. Los aspectos y documentación más importantes por desarrollar en este esquema son:

* Alcance del SGSI.
* Procedimientos y controles que apoyan el SGSI.
* Descripción de la metodología de evaluación del riesgo.
* Informe resultante de la evaluación del riesgo.
* Plan de tratamiento de riesgos.
* Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.
* Registros.
* Declaración de aplicabilidad (*statement of applicability,* SoA).
* Procedimiento de gestión de toda la documentación del SGSI.

Las actividades más importantes por realizar en ISO 27001, dentro de un enfoque de mejora continua, son (Figura 2):

* Implicación de la dirección.
* Alcance del SGSI y política de seguridad.
* Inventario de todos los activos de información.
* Metodología de evaluación del riesgo.
* Identificación de amenazas, vulnerabilidades e impactos.
* Análisis y evaluación de riesgos.
* Selección de controles para el tratamiento de riesgos.
* Aprobación por parte de la dirección del riesgo residual.
* Declaración de aplicabilidad.
* Plan de tratamiento de riesgos.
* Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
* Definición de un método de medida de la eficacia de los controles y su puesta en marcha.
* Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
* Monitorización constante y registro de todas las incidencias.
* Realización de auditorías internas.
* Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
* Mejora continua del SGSI.

A diagram of a process

Description automatically generated

Figura 2. Actividades ISO 27001. Fuente: ISO27000, s. f.

Requisitos de documentación

La documentación del SGSI deberá incluir la política, alcance y objetivos del SGSI, así como los diferentes procedimientos y controles de seguridad del sistema. La documentación será más o menos amplia dependiendo de la organización y de las diferentes actividades que desarrolle. Por tanto, el alcance y complejidad de los requerimientos de seguridad variarán en función de estas circunstancias.

La dirección debe aprobar un documento de política de seguridad de la información que se deberá publicar y comunicar a todos los empleados y entidades externas relevantes. Se deben aprobar los documentos previamente a su distribución, revisando y actualizándolos periódicamente según las necesidades requeridas.

A diagram of a diagram of a diagram with Mediterranean Sea in the background

Description automatically generated with medium confidence

Figura 3. Jerarquía de documentación ISO 27001. Fuente: elaboración propia.

Compromiso de la dirección

La norma ISO 27001 especifica la obligación de suministrar evidencias del compromiso planteado, tanto en el desarrollo como en la implantación y mejora del sistema, en los siguientes aspectos:

* En el proceso de comunicación interna al personal de la organización del SGSI en la empresa.
* En el establecimiento de la política y los objetivos del SGSI de la empresa.
* En la revisión periódica del desempeño del SGSI.
* En el aseguramiento de la disponibilidad de los recursos necesarios para la plena efectividad del SGSI.

Responsabilidades

Las responsabilidades y sus correspondientes autoridades deben estar perfectamente definidas en cualquier organización o empresa. La norma ISO requiere que la alta dirección asegure que se cumplan estos requisitos y que las responsabilidades sean comunicadas dentro de la organización, valorando el tamaño, complejidad y cultura de esta. Se puede nombrar un representante de la dirección, quien tendrá la responsabilidad de:

* Asegurar que los procesos del SGSI se implanten y funcionen.
* Informar a la alta dirección sobre el desempeño del sistema y cualquier oportunidad de mejora.

Revisión por la dirección

La dirección debe desarrollar una actividad de revisión que implique la verificación de la eficacia y efectividad del SGSI para asegurar su plena validez. El proceso de revisión por la dirección no debería ser un planteamiento realizado solamente para satisfacer los requisitos de la norma o de los auditores, sino que debería ser una parte integral de los procesos de gestión de la organización.

NIST SP 800-53. Rev5

El Risk Management Framework (RMF) del National Institute for Standars and Technologies (NIST) es otro modelo de SGSI que aborda los problemas de seguridad de las organizaciones relacionadas con el diseño, desarrollo, implementación, operación y disponibilidad de los sistemas de información y los entornos en los que operan dichos sistemas.

El RMF del NIST se compone de los siguientes seis pasos (2020):

A diagram of a security system

Description automatically generated

Figura 4. Esquema RMF del SGSI según NIST 800-53. Rev. 4. Fuente: NIST, 2020.

* Clasificar el sistema de información basado en una evaluación de impacto (FIPS publicación 199).
* Seleccionar los controles de seguridad básicos aplicables con base en los resultados de la clasificación de seguridad y aplicar la adaptación de orientación (incluyendo el uso potencial de superposiciones).
* Aplicar los controles de seguridad y documentar el diseño, desarrollo y detalles de la implementación de los controles.
* Evaluar los controles de seguridad para determinar el grado en que los controles están implementados correctamente, operando como se pretendía y produciendo el resultado deseado con respecto al cumplimiento de los requisitos de seguridad del sistema.
* Autorizar la operación del sistema de información basada en una determinación del riesgo de las operaciones de la organización y de los activos, los individuos y otras organizaciones, resultante de la operación y el uso del sistema de información y la decisión de que este riesgo es aceptable.
* Supervisar los controles de seguridad en el sistema de información y el entorno de operación de forma permanente para determinar la efectividad del control, los cambios en el sistema/entorno y el cumplimiento de la legislación, órdenes ejecutivas, directrices, políticas, reglamentos y normas.

Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS) es el modelo de SGSI que sigue la administración pública española. El Real Decreto 3/2010 de 8 de enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos, así como las medidas de protección por implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte del CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

Se recomienda la visualización de la clase magistral *Esquema Nacional de Seguridad*, sobre el Esquema Nacional de Seguridad, de obligado cumplimiento en la Administración pública española.

Básicamente, la implantación del esquema consta de los siguientes pasos, que se representan en la Figura 5:

* Categorizar el sistema de información:
  + El responsable de la información manejada establece los niveles requeridos (anexo I del ENS y guía CCN-STIC-803).
  + El responsable de los servicios prestados establece los niveles requeridos (anexo I del ENS y guía CCN-STIC-803).
  + Se deduce automáticamente la categoría del sistema de información.
* Seleccionar medidas de seguridad:
  + El responsable de la seguridad realiza el pertinente análisis de riesgos.
  + El responsable de la seguridad determina la declaración de aplicabilidad, teniendo en cuenta los mínimos requeridos por el anexo II del ENS y las medidas adicionales que se estimen oportunas.
* Implantar las medidas de seguridad:
  + El administrador de seguridad del sistema se encarga de aplicar las medidas acordadas (guía CCN-STIC-804).
* Evaluar la seguridad del sistema de información:
  + Corresponde al sistema de gestión que se emplee. Pudiendo recurrir a auditorías externas cuando sea pertinente (guía CCN-STIC-808), se evalúa el riesgo residual.
* Autorización para operar:
  + El responsable de la información acepta el riesgo residual sobre la información que le compete.
  + El responsable del servicio acepta el riesgo residual sobre los servicios que le competen. Puede ser necesario un plan de mejora de la seguridad para atender a los riesgos que no son aceptables, regresando al paso 2.
* Monitorizar:
  + El administrador de seguridad del sistema recopila información sobre el desempeño del sistema de información en materia de seguridad.
  + El responsable de la seguridad monitoriza que el sistema de información se comporta dentro de los márgenes aceptados de riesgo.
  + Los responsables de la información y de los servicios son informados de desviaciones significativas del riesgo sobre los activos de los que son propietarios; si la desviación es elevada, el responsable del sistema puede acordar la suspensión temporal del servicio hasta que se puedan garantizar niveles aceptables de riesgo.

2.5. Profesión de gestión de la ciberseguridad

Una profesión puede caracterizarse por el desarrollo de los siguientes cinco criterios:

* La creación de un cuerpo organizado de conocimientos.
* El reconocimiento por parte de los clientes de la autoridad de la profesión.
* La aprobación de la comunidad de la autoridad de la profesión.
* Un código de ética.
* Una cultura profesional apoyada por la actividad académica y profesional.

En cuanto a la disciplina de la seguridad de la información, aunque no existe una carrera de grado específica para esta, sí se ha desarrollado claramente como disciplina independiente.

Aunque no hay una asociación profesional de clara aceptación general, el cuerpo de conocimiento (*body of knowledge*, BOK) del [Consorcio Internacional de Certificación de Seguridad de Sistemas de Información](https://www.isc2.org/) o (ISC)2 es un ejemplo de recopilación de requisitos en el área que puede considerarse como definitorio de qué debe saber un profesional de la seguridad de la información. También el (ISC)2 incluye en sus requisitos un código ético al que los certificados por la organización deben adherirse.

El reconocimiento de la profesión por la comunidad y los clientes parece más que evidente por la existencia de consultoras y empresas especializadas. Desde el punto de vista académico, existen conferencias académicas especializadas. También hay conferencias y eventos profesionales no específicos del ámbito académico.

Revistas y eventos especializados

Desde el punto de vista académico, un ejemplo de evento especializado sería la conferencia [ACM Conference on Computer and Communication Security](http://www.sigsac.org/ccs.html) (CCS), que se celebra desde 1993, organizada por el grupo de interés Security, Audit and Control (SIGSAC) de ACM.

Además de las conferencias, existen numerosas revistas especializadas:

*IEEE Security and Privacy* es un magacín técnico del IEEE. Como tal, los artículos publicados son breves. A pesar de quedar sometidos a evaluación por pares *(peer review),* según la política editorial, «en general, no son adecuados para su publicación los artículos que cubren un área técnica muy particular» (IEEE, s. f. a). Para estos artículos que no encajan, se nos sugieren otras revistas de IEEE más orientadas a la investigación.

Un ejemplo de esas revistas es [IEEE Transactions on Secure and Dependable System](http://www.computer.org/portal/web/tdsc)*.*

¿El *hacker* como profesional?

Existe mucha confusión sobre el término *hacker* y la connotación peyorativa que a veces se le ha asignado. Sin entrar en discusiones terminológicas, es importante resaltar que, actualmente, existe un concepto de «*hacking* ético» que implica el análisis de vulnerabilidades de sistemas mediante acciones ofensivas, pero excluyendo los motivos maliciosos o espurios. Por ello, el *hacker* ético actúa en coordinación con las empresas, que utilizan sus servicios para mejorar su seguridad.

El *hacker* ético es un profesional con unas capacidades muy concretas que normalmente realiza *penetration testing* de manera controlada y previo contrato o acuerdo con la empresa. La perspectiva de *hacking* ético tiene como elemento interesante el situar la seguridad desde el contexto del atacante.

Los eventos relacionados con el *hacking* son diferentes de las conferencias académicas. Ejemplos de estos eventos son el evento [DefCon](https://www.defcon.org/) y [HackerHalted](http://www.hackerhalted.com/). En ellos, se diseminan las técnicas y vulnerabilidades de seguridad que se encuentran en la práctica, las cuales pueden utilizarse de manera maliciosa o ética. Aunque realmente las técnicas son las mismas, son la intención o el uso los que las diferencian.

2.6. Certificaciones de ciberseguridad

El (ISC)2, fundado en 1989, es una organización sin ánimo de lucro con sede en Florida dedicada fundamentalmente a la formación y certificación en seguridad de la información.

Se recomienda la visualización de la clase magistral *Certificaciones de ciberseguridad*sobre principales certificaciones de gestión de la ciberseguridad.

Las certificaciones (ISC)2 incluyen:

* Certified Information Systems Security Professional (CISSP), que incluye:
  + Information Systems Security Architecture Professional (CISSP-ISSAP).
  + Information Systems Security Engineering Professional (CISSP-ISSEP).
  + Information Systems Security Management Professional (CISSP-ISSMP).
* Certified Secure Software Lifecycle Professional (CSSLP).
* Certification and Accreditation Professional (CAP).
* Systems Security Certified Practitioner (SSCP).

Probablemente la más conocida y extendida de todas ellas es la CISSP, que es una certificación profesional generalista muy amplia.

CISSP

La certificación CISSP es una de las más valoradas por su reconocimiento internacional. Una CISSP está certificada como profesional para definir la arquitectura, diseño, gestión y controles de los sistemasempresariales. Los certificados, además de contar con un valor añadido para su contratación, forman parte de la comunidad de (ISC)2, donde pueden actualizarse y tener oportunidades adicionales para interactuar con sus colegas.

La CISSP se estructura en diez dominios que conforman el Common Body of Knowledge (CBK):

* Seguridad de la información y gestión de riesgos *(information security and risk management).*
* Sistemas y metodología de control de acceso *(access control systems and methodology).*
* Criptografía *(cryptography).*
* Seguridad física *(physical security).*
* Arquitectura y diseño de seguridad *(security architecture and design).*
* Legislación, regulaciones, cumplimiento de estas e investigación*(legal, regulations, compliance, and investigation).*
* Seguridad de red y telecomunicaciones *(telecommunications and network security).*
* Planes de continuidad del negocio y de recuperación frente a desastres *(business continuity and disaster recovery planning).*
* Seguridad en el desarrollo de aplicaciones *(application development security).*
* Seguridad de operaciones *(operations security).*

Para la certificación CISSP se deben cumplir los siguientes requisitos:

* Aprobar el examen CISSP: consta de 250 preguntas de selección simple y seis horas de duración.
* Demostrar experiencia mínima de cinco años en al menos dos de los diez dominios del CBK.
* Adherirse al código ético de la (ISC)2.

Para mantener la certificación CISSP se debe realizar una cierta cantidad de actividades cuya finalidad es asegurar que el profesional se ha mantenido activo en el área de la seguridad en el tiempo. Cada una de estas actividades recibe cierta cantidad de créditos (CPE), de los cuales el profesional debe reunir 120 cada tres años.

CAP

La certificación CAP se dirige a certificar los conocimientos, las habilidades y las capacidades que necesitan los profesionales que evalúan riesgos y establecen parámetros de seguridad para contrarrestar los riesgos potenciales. Se ha preparado con la colaboración de la Oficina de Seguridad de la Información del Departamento de Estado de los EE. UU.

Esta certificación se centra en los siguientes dominios:

* Entender la autorización de seguridad de sistemas de información.
* Categorizar los sistemas de información.
* Establecer la línea de base de control de seguridad.
* Aplicar controles de seguridad.
* Evaluar controles de seguridad.
* Autorizar sistemas de información.
* Monitorizar los controles de seguridad.

Como se puede ver, es una certificación asociada a los procesos de autorización y certificación, no tan amplia como la CISSP.

La certificación ICSM de ISACA

La Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association, ISACA) es una asociación internacional fundada en 1967 que promueve y organiza el desarrollo de metodologías y certificaciones para las actividades de auditoría y control en sistemas de información. Entre sus productos más conocidos está el *framework* COBIT de control de sistemas de información o las certificaciones de auditoría.

ISACA ofrece también el Certified Information Security Manager (CISM o Gestor Certificado en Seguridad de la Información), dirigido específicamente al área de gestión en el contexto de la seguridad.

Los dominios que cubre el CISM son los siguientes:

* Gobierno de seguridad de la información.
* Gestión de riesgos de información y cumplimiento.
* Desarrollo y gestión del programa de seguridad de la información.
* Gestión de incidentes de seguridad de la información.

El proceso de certificación tiene bastantes puntos en común con el de CISSP. Concretamente, los pasos son los siguientes:

* Aprobar el examen CISM.
* Adherirse al código de ética profesional de ISACA.
* Estar de acuerdo en cumplir con la política de educación continua.
* Acreditar experiencia laboral en el ámbito de la seguridad de la información.
* Presentar una solicitud de certificación CISM.

A diagram of a system

Description automatically generated

Figura 5. Esquema Nacional de Seguridad (ENS). Fuente: elaboración propia.