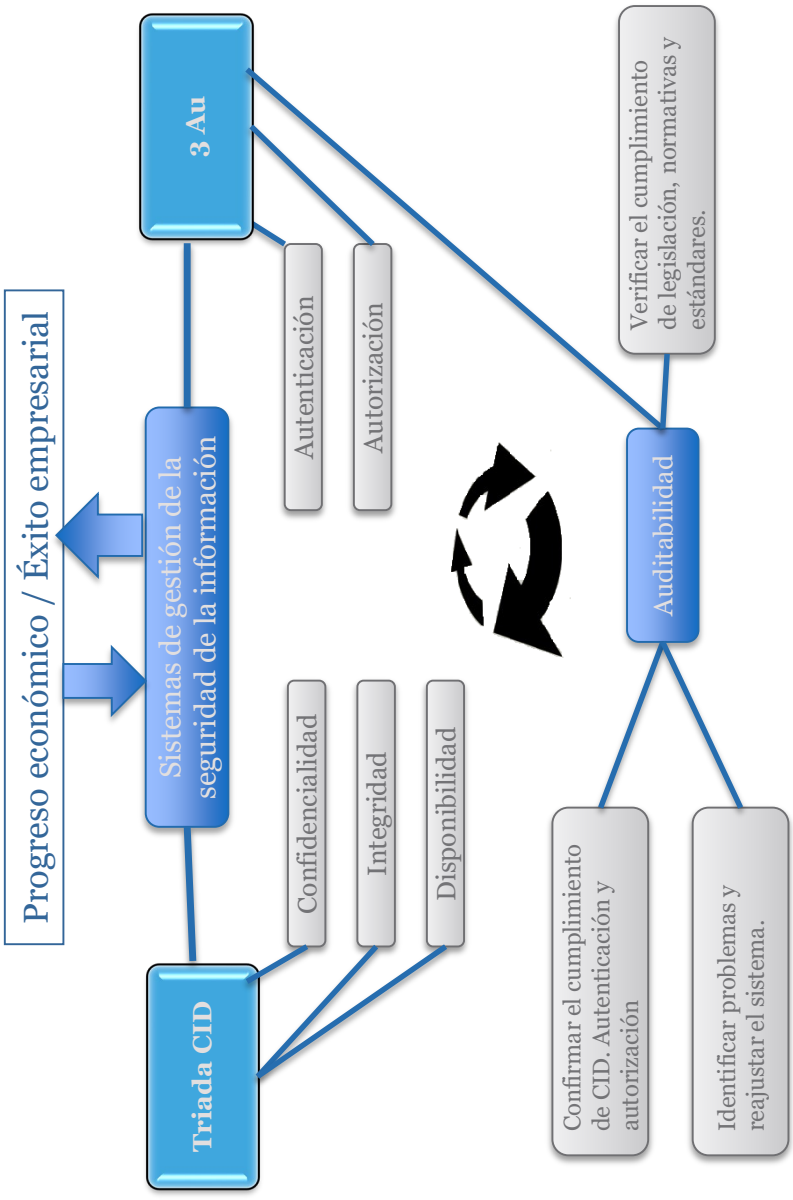
Introducción a los sistemas de gestión de seguridad de la información

TEMA 1

Esquema



Ideas clave

1.1. ¿Cómo estudiar este tema?

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

El objetivo de este tema es comprender que es un sistema de gestión de seguridad de la información y su importancia para la organización de cara a mantener el riesgo dentro de unos umbrales establecidos por la organización. De esta forma, los ingenieros informáticos monitorizan uno de los mayores activos de las organizaciones, como es la información, ofreciendo una protección adecuada y eficaz de la misma de cara a minimizar los posibles daños económicos que pueda sufrir la organización.

Así, se subrayará se subrayará la importancia de la seguridad de la información en el contexto económico actual. Asimismo se presentarán los **principios fundamentales** con base en los cuales se define el concepto de seguridad de la información:

- CID: confidencialidad, integridad y disponibilidad.
- Reglas Au: autenticación, autorización y auditabilidad.
- La seguridad de la información como un proceso y no como un producto: importancia de la auditoría informática.

1.2. Principios fundamentales de los sistemas de gestión de la seguridad de la información (SGSI)

En las últimas décadas se ha ido gestando una creciente interdependencia entre la actividad económica y las denominadas t**ecnologías de la información y de la comunicación** (en adelante TIC).

Desde la propuesta del primer ordenador ENIAC pasando por el desarrollo de la red a partir de las propuestas de DARPA y Tim Berners-Lee sobre la W3C, se ha producido un desarrollo de las tecnologías para la generación, tratamiento y compartición de información.

Casi todas nuestras actividades cotidianas cuentan con algún elemento TIC que en muchos casos se nos muestra como absolutamente indispensable. El nuevo escenario es etiquetado como **ciberespacio** y constituye el marco esencial de las relaciones sociales y empresariales.

En efecto, hoy en día es prácticamente imposible hablar de éxito empresarial y progreso económico sin incluir convenientemente las TIC en nuestra idea de negocio(Katz, 2009).

Ahora bien, el uso de las TIC no está exento de riesgos. El carácter sistémico de las TIC les confiere una **complejidad** que dificulta mucho la comprensión de los principios de diseño subyacentes, así como de las implicaciones de los mismos.

La mejora y proliferación de ordenadores personales han ido acompañados de productos *software* orientados a aprovechar las posibilidades de esos medios tecnológicos pero también de **programas cuya meta es la interceptación de información** sensible sin autorización o la **obstaculización de un uso eficiente de las TIC**.

De este modo, la **ciberseguridad** tiene una importancia económica incontestable en el actual escenario tecnológico. Dicha importancia reside no solo en los costes directos derivados de la reimplantación o recuperación de sistemas y de tecnologías, sino también en lo relativo al **deterioro de la imagen de nuestra empresa** de cara a potenciales usuarios o clientes de nuestros productos (Montes, 2018).

La **seguridad de un sistema de información** no queda circunscrita a la aplicación de una serie de procedimientos y a la implantación de un cierto conjunto de tecnologías. Los objetivos de seguridad son parte importante del modelo de negocio de cualquier iniciativa empresarial en la actualidad. Una negligencia en el despliegue de medidas de seguridad tiene un **efecto inmediato** en nuestra organización (desarrollo de nuevas estrategias de protección, implementación de nuevas medidas *software*, etc.) pero **también un efecto mediato** a través del menoscabo de la **reputación de nuestro negocio** con respecto a potenciales clientes/usuarios.

Por tanto, se puede definir un sistema de gestión de seguridad de la información (en adelante SGSI) como un conjunto de políticas y procedimientos para gestionar de forma sistemática los activos de información de una organización. El objetivo de un SGSI es **minimizar el riesgo** y garantizar la continuidad de negocio de forma proactiva, limitando el impacto de una violación de la seguridad.

Normalmente, el SGSI monitoriza el comportamiento de los empleados, los procesos, así como los datos y la tecnología, aunque puede orientarse hacia un particular conjunto de datos como pueden ser los datos de los clientes.

Para crear el SGSI se dispone de la norma **ISO 27001:2013**, que no incluye acciones específicas y concretas, sino que se limita a orientar sobre documentación a generar, auditorías internas, mejora continua y acciones preventivas y correctivas. Si nos atenemos a la definición que nos facilita la norma en su revisión 2013, en sistema de gestión para la seguridad de la información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una empresa u organización. (ISO27001, 2015).

Una correcta metodología de uso de TIC requiere establecer el conjunto de expectativas y el conjunto de elementos necesarios para satisfacerlas. La especificación de expectativas de seguridad en primer lugar obliga a dictaminar qué es lo que queremos proteger. En este punto hay que tener en cuenta que tiene sentido proteger solo aquello que tiene un cierto valor para nuestra empresa.

En el contexto de los sistemas de gestión de seguridad de la información, tal y como muestra la siguiente figura, se utiliza el término de **activo de información** para referir aquellos **elementos que poseen un valor para una empresa u organización**.

Figura 1. Elementos que poseen un valor para una empresa u organización.

1.3. Reglas de oro de los SGSI

Según hemos visto en la gráfica anterior, la naturaleza de los activos de información es muy variada porque comprende desde la plantilla de una empresa hasta documentos digitales. No obstante, ya sea de modo directo o por impacto indirecto, las **expectativas de seguridad sobre nuestros activos de información** se pueden concretar en objetivos de la seguridad de la información específicos.

De modo general dichos objetivos se dividen en **tres grandes categorías** (**tríada CID** de la figura siguiente):

- Objetivos de confidencialidad.
- Objetivos de integridad.
- Objetivos de disponibilidad de los activos de información.

Figura 2. Tríada CID.

La tríada CID constituye la base de definición de los SGSI. La **confidencialidad** de un activo se garantiza cuando dicho **recurso sólo puede ser accedido por usuarios legítimos**. La **integridad** de los activos de información se consigue si se **impide su modificación por parte de usuarios no autorizados**. Por su parte, si se exige **disponibilidad** de un activo se está creando un conjunto de procedimientos que hacen posible **acceder/hacer uso de dicho activo siempre que se desee**.

Cada una de las propiedades de los SGSI está acompañada de un conjunto de amenazas que no son sino los posibles ataques que se pueden efectuar para erosionar tales sistemas.

Teniendo en cuenta el flujo normal de información entre un origen y un destino puedes distinguir cuatro tipos de ataques, como se muestra en la figura:

- Ataques por interceptación del flujo de información.
- Ataques por interrupción del flujo de información.
- Ataques por modificación del flujo de información.
- Ataques por generación e inyección de información.

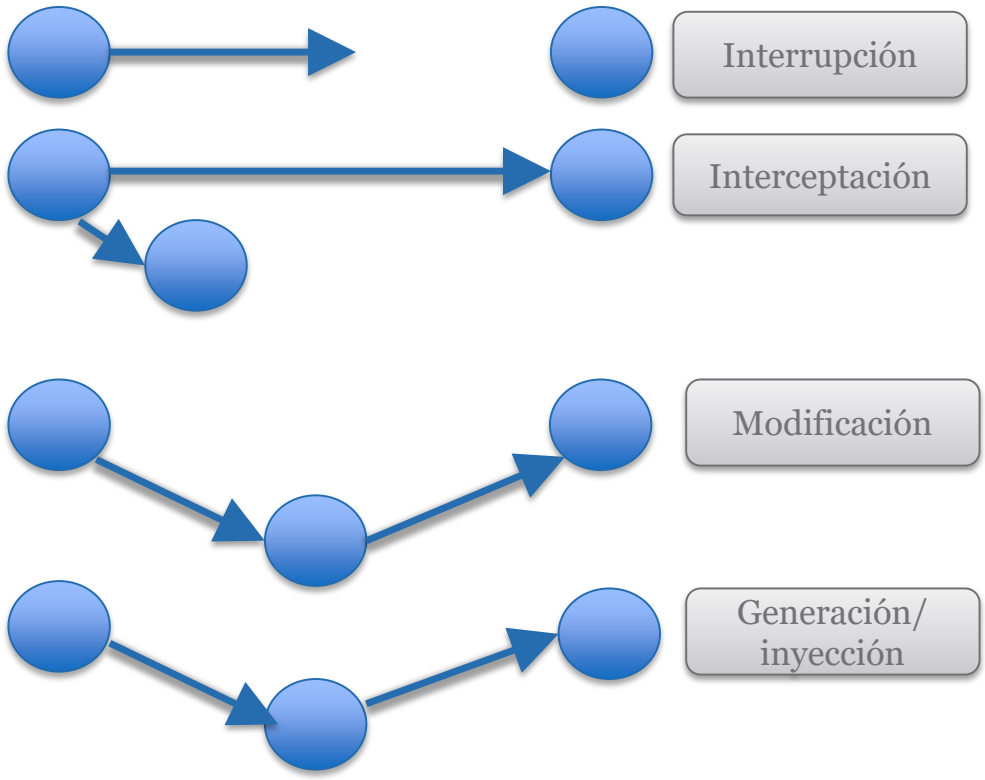


Figura 3. Tipos de ataques.

La puesta en marcha de cada uno de estos ataques involucra diversos tipos de agentes.

Como agentes más significativos en el ámbito de las amenazas a los SGSI tenemos:

- ***Hackers***:
  - **Usuarios avanzados** de las TIC que llevan procedimientos para la identificación de vulnerabilidades de cara a plantear futuras soluciones.
  - Los *hackers* no son ***crackers.*** Estos últimos buscan vulnerabilidades para sacar provecho de las mismas.

- **Enmascarados**:
  - Usuarios **legítimos** de un sistema que hacen **uso de credenciales** (contraseña, certificados, etc.) de terceros para acceder a información no autorizada.

- **Actividad no autorizada** por parte de usuarios **legítimos.**

- **Descarga de ficheros y almacenamiento** sin respetar los controles de acceso establecidos:
  - **Reubicación de ficheros** de un entorno protegido a un entorno que no lo está.

- **Troyanos**:
  - *Software* malicioso que el usuario interpreta como inofensivo pero que permite que un atacante realice de modo remoto acciones sobre nuestro sistema. Entre las posibles acciones figura la captura de información sensible.

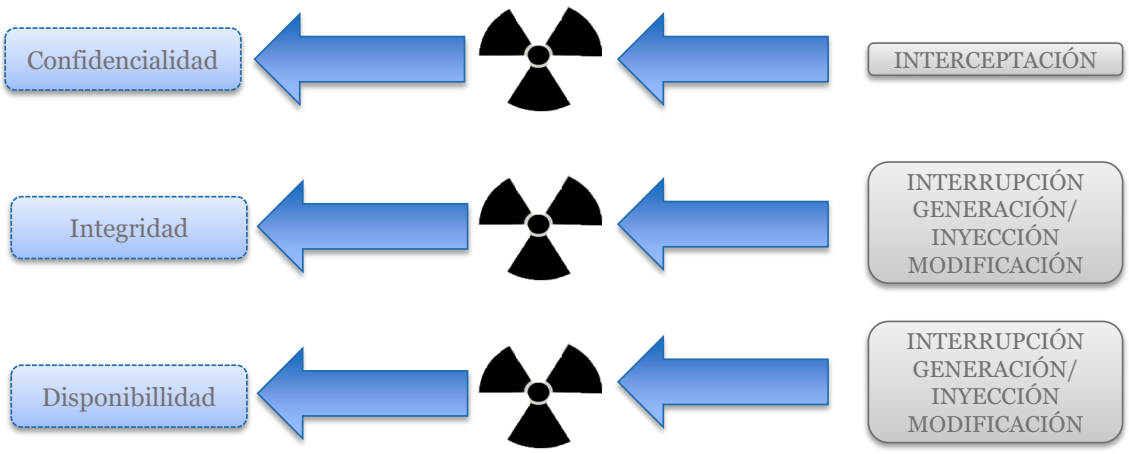


Figura 4. Relación entre tipos de ataques y la tríada CID.

Los anteriores agentes y los ataques que despliegan pueden relacionarse con la tríada CID según se muestra en la figura anterior. Ahora bien la protección frente a dichas

amenazas no puede garantizarse sin más que exigir la confidencialidad, la integridad y la disponibilidad de los activos de información.

En efecto es preciso controlar el acceso a activos, la identificación del origen de las comunicaciones y la incorporación de procedimientos para la identificación de eventos y su registro de cara a una ulterior revisión.

De esta forma la tríada CID ha de ser extendida y mejorada mediante las llamadas reglas de oro, **las 3 Au de los SGSI**.

De cara a implantar una robusta estrategia de protección de nuestros activos de información, además de la tríada CID se exige el cumplimiento de los siguientes requisitos:

- **Autenticación:** mediante este requisito se persigue evitar el acceso a nuestro sistema de usuarios no autorizados.
- **Autorización:** implica asignar permisos de acceso a cada una de las identidades o grupo de identidades creadas mediante el sistema de autenticación diseñado.
- **Auditabilidad:** concierne a la captura de eventos destacados y de su almacenamiento en ficheros *log* o en bases de datos, con el objeto de detectar posteriormente posibles problemas de seguridad.

1.4. Papel de la auditoría informática en los SGSI

Una de las principales consecuencias de la alta complejidad de los vigentes sistemas de gestión de la información es el carácter tentativo de las soluciones adoptadas para preservar su seguridad. Tomando en consideración que la seguridad es un proceso y no un producto, el diseño e implementación de una arquitectura para la gestión de información requiere partir de una serie de principios y asunciones.

En el caso de la seguridad de los activos sostenidos por tal arquitectura, tales asunciones incluyen los procedimientos, metodologías y elementos técnicos necesarios para garantizar la confidencialidad de recursos para verificar la integridad de los mismos y sostener su disponibilidad siempre que se desee usarlos.

El perfecto ensamblaje de todas esas herramientas y soluciones además exige la puesta en marcha de mecanismos de verificación de la identidad de los usuarios que intentan acceder a los distintos activos de información.

Asimismo, la autenticación debe ir acompañada de la constatación de que las acciones que los usuarios desean realizar corresponden con el tipo de operaciones que el sistema establece que pueden efectuar.

En definitiva todo usuario, una vez autenticado, **debe estar autorizado** para llevar a cabo una cierta acción. Por último y una vez efectuado el acceso al recurso con la consiguiente ejecución de la acción para la que se tiene autorización es necesario dejar evidencias suficientes sobre el tipo de acceso y la operación específica llevada a cabo.

Este rastro es parte fundamental de la auditoría informática, pieza crítica en el engranaje de los SGSI que permite e impulsa la coherencia entre nuestras expectativas de seguridad y los resultados reales observados en la puesta en práctica de nuestros sistemas.

De acuerdo con la RAE, la auditoría es la «revisión de la contabilidad de una empresa, de una sociedad, etc., realizada por un auditor».

En el caso de la **auditoría informática** los apuntes contables a **revisar** son **los flujos de información y el uso de los recursos**, esto es de los activos de información de una empresa u organización.

El objetivo esencial es **verificar el correcto funcionamiento de los sistemas TIC** de la empresa pero también **fomentar la confianza** de los componentes de un organismo en dichos sistemas y de los usuarios/clientes en el servicio proporcionado por la empresa.

La **confianza en nuestro negocio** es otro **activo** más, quizás el más importante de los **que tiene que proteger un SGSI**.

La auditoría informática no es un mero registro de incidencias sino que también trata de prevenir ulteriores problemas de seguridad en nuestro sistema. Para ello analiza todos los componentes de nuestra infraestructura empresarial, empezando por las políticas y directrices de seguridad, pasando por procedimientos y metodologías de protección de activos y terminando como protocolos de seguridad física. Podemos afirmar que **la**

auditoría informática no es simplemente un mecanismo de acumulación enumerativa del cumplimiento de requisitos sino que **es una medida de seguridad** (Kassa, 2016).

Para concluir y en la línea de la promoción de la confianza hay que señalar que la auditoría informática también responde a **obligaciones de carácter normativo o legislativo**.

Con respecto a la naturaleza normativa de la auditoría informática hay que reseñar el interés y necesidad de muchas empresas de probar el cumplimiento de estándares como la **norma ISO 27001** (*Information Security Management System -ISMS-standard*) (ISO, 2013).

El hecho de que una empresa cumpla esta norma proporciona credibilidad de la misma de cara a otras empresas, organismos o simplemente de cara a clientes o usuarios finales. En muchas situaciones tal cumplimiento es condición innegociable para proporcionar o aspirar a proporcionar ciertos servicios (por ejemplo, en el caso de que se desee conseguir un contrato con un organismo gubernamental es más que plausible que sea un requerimiento de la oferta).

Con respecto a la legislación, la auditoría debe presentar pruebas y evidencias suficientes respecto al manejo adecuado de datos personales y del cumplimiento del marco legal vigente para operaciones comerciales.

En el caso de España esto exige que se salden con éxito el conjunto de requerimientos de la **Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPD)** para el caso de datos personales y la **Ley de Servicios de la Sociedad de la Información (LSSI)** para todo lo relativo a comercio electrónico.

Así, a modo de ejemplo, el Real Decreto 951/2015, (RDL 951/2015, de 23 de octubre), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica establece que la seguridad de los sistemas de información de una organización será auditada en los siguientes términos:

- Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- Que existen procedimientos para resolución de conflictos entre dichos responsables.

- Que se han designado personas para dichos roles a la luz del principio de «separación de funciones».
- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- Que se cumplen las recomendaciones de protección descritas en el anexo II sobre medidas de seguridad, en función de las condiciones de aplicación en cada caso.
- Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

Esta auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

- Documentación de los procedimientos.
- Registro de incidentes.
- Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
- Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el artículo 18 «Adquisición de productos y contratación de servicios de seguridad».

1.5. Referencias bibliográficas

ISO. (2013). *Norma ISO 27001*. [S. l.]: ISO. Recuperado de https://normaiso27001.es/

Kassa, S. G. (2016). Information System Security Audit: an ontological framework. *ISACA Journal 5*, 1-8. Recuperado de https://www.isaca.org/Journal/archives/2016/volume-5/Documents/Information-Systems-Security-Audit_joa_Eng_0916.pdf

Katz, T. (2009). *El papel de las TIC en el desarrollo: propuesta de América latina a los retos económicos actuales*. Barcelona: Ediciones Ariel y Fundación Telefónica. Recuperado de https://www.fundaciontelefonica.com.pe/publicaciones-listado/pagina-item-publicaciones/itempubli/13/

Montes, M. J. (31 de octubre de 2018). Fuga de información, la mayor amenaza para las empresas [blog post]. Recuperado de https://blogs.protegerse.com/2018/10/31/fuga-de-informacion-la-mayor-amenaza-para-las-empresas/

España. Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. *Boletín del Estado,* 4 noviembre de 2015, núm. 264, pp. 104246-104267 Recuperado de https://www.boe.es/eli/es/rd/2015/10/23/951

Lo + recomendado

No dejes de leer…

Information Security Management System (ISMS)

Al-Dhahri, S., Al-Sarti, M. y Abdul, A. (2017). Information Security Management System. *International Journal of Computer Applications 158*(7), 29-33.

Artículo académico publicado en la International *Journal of Computer Applications*, donde los profesores Al-Dahri, S., Al-Sarti, M. y Aziz, A. A., de la Universidad King Abdulaziz de Arabia Saudí, proporcionan una visión global de los diferentes aspectos a afrontar en el desarrollo de un SGSI/ISMS.

Accede al artículo desde el aula virtual o a través de la siguiente dirección web: https://www.ijcaonline.org/archives/volume158/number7/aldhahri-2017-ijca-912851.pdf

ISO 27001 – Importancia de la formación sobre seguridad SGSI

SGSI. (13 de mayo de 2014). ISO 27001 – Importancia de la formación sobre seguridad SGSI [Blog post].

En este blog editado por ISO Tools Excellence sobre los Sistemas de Gestión de Seguridad de la Información, encontramos este artículo donde se profundiza en la importancia de la formación sobre seguridad SGSI.

Accede al artículo desde el aula virtual o a través de la siguiente dirección web: https://www.pmg-ssi.com/2014/05/iso-27001-importancia-de-la-formacion-sobre-seguridad-sgsi/

Cómo gestionar una fuga de información

INCIBE. (2016). *Cómo gestionar una fuga de información: una guía de aproximación para el empresario*. León: INCIBE.

Guía emitida en 2016 por el Instituto Nacional de Ciberseguridad de España, donde proporciona a los empresarios los pasos a seguir cuando se produce una fuga de información dentro de la empresa.

Accede al documento desde el aula virtual o a través de la siguiente dirección web: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

Implantación de un SGSI en la empresa

INTECO. (S. f.). *Implantación de un SGSI en la empresa*. Madrid: INCIBE.

El Instituto Nacional de Tecnologías de la Comunicación nos presenta un documento a modo de guía para la implantación de un SGSI en la empresa.

Accede a la guía desde el aula virtual o a través de la siguiente dirección web: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

Los códigos secretos

Singh, S. (2000). *Los códigos secretos*. Madrid: Debate.
Disponible en el aula virtual en virtud del artículo 32.4 de la Ley de Propiedad Intelectual.

Este libro muestra una muy buena introducción a los entresijos de la seguridad de la información en particular.

No dejes de ver...

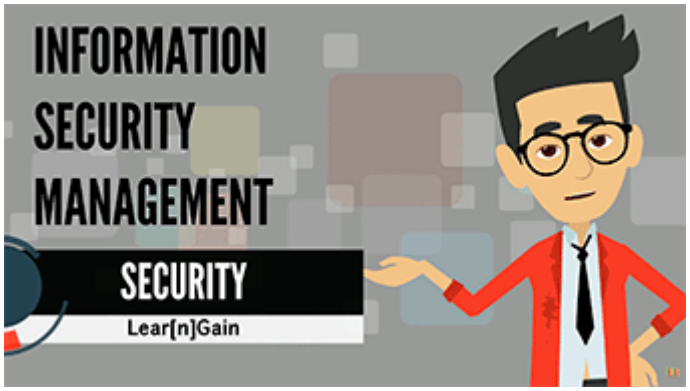
El arte y la ciencia en la seguridad informática de la empresa

Charla de Chema Alonso en un ESET Security Day en Valencia 2018 en la que se habla del «arte y la ciencia» de gestionar la seguridad informática en una empresa.

Accede al vídeo desde el aula virtual o a través de la siguiente dirección web:
https://youtu.be/l8ckZEovuGo

Information Security Management

En este vídeo en inglés de 2016 se refuerzan, brevemente, los conceptos de la triada CIA: confidencialidad, integridad y disponibilidad.



Accede al vídeo desde el aula virtual o a través de la siguiente dirección web:
https://youtu.be/XsgNlriPs40

ISO 27001.2013 and Internal ISMS Audit

En este vídeo de 2018, Steve Watkins, jefe del ISO/IEC 27001 User Group, proporciona una visión general acerca del proceso de auditoría interna bajo la norma ISO 27001.

Accede al vídeo desde el aula virtual o a través de la siguiente dirección web:
https://youtu.be/42uI1fpDosw

TED: ¿Qué hay de malo en su contraseña?

En este sitio existe una serie de vídeos dedicados a la temática de la seguridad. Todos los vídeos están en inglés pero incorporan subtítulos en español. De entre todos ellos es especialmente relevante el dedicado a la gestión de contraseñas y que corresponde a una charla impartida por Lorrie Faith Cranor. Uno de los elementos que una auditoría de seguridad debe cumplir es la verificación de que se cumple una política de seguridad robusta en la gestión de contraseñas de identificación de usuarios.

Accede al vídeo desde el aula virtual o a través de la siguiente dirección web:
https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_word?utm_campaign=tedspread&utm_medium=referral&utm_source=tedcomshare

+ Información

Enlaces relacionados

Portal de la ISO 27001 en español

Página web de la norma ISO 27000, donde, entre otros, proporciona los aspectos básicos y fundamentales de la norma 27001 y su implicación con el SGSI antes de la revisión de 2013. Tiene su utilidad como punto de partida del SGSI.

Accede al blog desde el aula virtual o a través de la siguiente dirección web:
http://www.iso27000.es/sgsi.html

The Top cyber securities blogs and websites 2020

La Universidad de San Diego nos proporciona esta entrada donde se recogen los mejores blogs y sitios web sobre ciberseguridad para el año 2020.

Accede al blog desde el aula virtual o a través de la siguiente dirección web:
https://onlinedegrees.sandiego.edu/top-cyber-security-blogs-websites/

ENISA

Página web de The European Union Agency for Cybersecurity (ENISA), creada por la Unión Europea y establecida en Grecia, donde se puede acceder a las últimas novedades en ciberseguridad.

Accede al blog desde el aula virtual o a través de la siguiente dirección web:
https://www.enisa.europa.eu/

Bibliografía

Arcos, S. (2011). *Ingeniería social: psicología aplicada a la seguridad informática*. Barcelona: Universidad Politécnica de Cataluña. Recuperado de http://upcommons.upc.edu/handle/2099.1/12289

Computerworld. (2 de julio de 2013). Un incidente grave de seguridad TI puede costar 500 000 euros a la gran empresa [Blog post]. Recuperado de https://www.computerworld.es/tendencias/un-fallo-grave-de-seguridad-ti-puede-costar-500000-euros-a-las-empresas

+ Información

Lectura: Importancia de la auditoría informática (robo de datos en *iCloud*

La lectura debe consistir en un análisis crítico del problema de seguridad en iCloud.

Deberás leer los siguientes artículos:

http://www.cnet.com/es/noticias/apple-sabia-del-problema-en-icloud-antes-de-filtracion-de-famosas/
http://alt1040.com/2014/09/icloud-fotos-famosas
http://www.elladodelmal.com/2014/09/robar-fotos-de-apple-icloud-de-un.html
http://www.cope.es/detalle/Tim-Cook-Apple-reforzara-la-seguridad-de-iCloud.html

Tendrás que responder a las siguientes preguntas:

¿Crees que un problema como el de *iCloud* supone una pérdida económica para una empresa? ¿Por qué?
Teniendo en cuenta que uno de los principios fundamentales de la seguridad informática ha de ser la transparencia, ¿consideras que el problema *iCloud* debería haber sido enfocado de otro modo?
¿Crees que una auditoría informática en rigor hubiera evitado el problema de seguridad de *iCloud*? ¿Por qué?

Objetivos

Describe las consecuencias de la mala política de seguridad en el caso específico de iCloud. Discute cómo se podría y debería haber evitado este problema en una auditoría informática.

Extensión de la actividad

Dos páginas con fuente Georgia 11 e interlineado 1,5.

Test

1. Los tres principios fundamentales de los SGSI son:

A. Confidencialidad, integridad y autenticación.

B. Cifrado, integridad y disponibilidad.

C. Confidencialidad, integridad y disponibilidad.

2. Un ataque por interceptación afecta a:

A. La disponibilidad de los datos.

B. La autenticación de los datos.

C. La confidencialidad de los datos.

3. ¿Qué es un activo de información?

A. Todo aquel elemento que posee un valor para nuestra empresa y que es necesario para poder llevar a cabo su actividad de negocio.

B. El conjunto de documentos de una empresa.

C. El conjunto de documentos y equipos de una empresa.

4. Las reglas de oro de los SGSI son:

A. La privacidad y el anonimato.

B. La autenticación y la autorización.

C. La autenticación, la autorización y la auditabilidad.

5. Si una persona no autorizada modifica la información disponible en nuestra base de datos, está afectando a:

A. Integridad.

B. Disponibilidad.

C. Confidencialidad.

6. La auditoría informática es necesaria para:

A. Conseguir las certificaciones de calidad de nuestro sistema de información.

B. Detectar posibles problemas de seguridad, aconsejar cómo solucionarlos y evitar posibles ataques o errores de seguridad que menoscaben la actividad de nuestra empresa y su prestigio.

C. Asegurar que los costes de producción no exceden a los beneficios que reporta nuestro negocio.

7. Los ficheros de *log* son fundamentales para:

A. Realizar auditorías.

B. Garantizar la integridad de los activos de información.

C. Implementar sistemas de autorización.

8. Al principio según el cual un usuario autorizado tiene posibilidad de acceder a un recurso en cualquier momento y hacer uso del mismo de forma ininterrumpida, se le llama:

A. Identificación.

B. Disponibilidad.

C. Cifrado.

9. La integridad depende de:

A. Autorización.

B. Auditabilidad.

C. Autenticación.

10. ¿Cuál de las siguientes acciones no constituye una buena práctica en la gestión de la seguridad?

A. Revisar logs de acceso para detectar conductas o comportamientos no autorizados.

B. Supervisar el rendimiento de los trabajadores en su puesto de trabajo.

C. Investigar al respecto de nuevas tendencias, prácticas de intrusión.