La seguridad informática en la empresa

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la Bibliografía Básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha Bibliografía.

¡Bienvenido a Seguridad Informática! En esta materia, se abordarán los riesgos y vulnerabillidades a los que se encuentra expuesta una infraestructura tecnológica desde un enfoque que te dotará de una visión crítica a la hora de abordar un proyecto, considerando no solo aspectos funcionales de las soluciones, sino, además, teniendo en cuenta que, si bien es importante que una solución resuelva el problema para el cual ha sido diseñada, también es importante que lo haga de forma segura.

La Seguridad Informática es básicamente una actividad de protección en la cual lo que se trata de proteger son tres atributos fundamentales: la Confidencialidad, la Integridad y la Disponibilidad de los activos sobre los que se basa una infraestructura de tecnología.

Cualquiera sea la infraestructura de tecnología, ésta siempre tendrá como objetivo procesar información, con lo cual, la información que circule a través de ella se reconoce como el activo mas relevante, ya sea que se trate de un entorno hogareño, corporativo o gubernamental.

Ahora bien, la información puede encontrarse en distintos medios y formas, digitalizada y almacenada, en soporte papel, como conocimiento empírico, etc., entonces, si la información es “el activo” a proteger, resulta insuficiente abordar su protección con un enfoque basado exclusivamente en la Seguridad Informática.

Es aquí adonde surge la Seguridad de la Información como un concepto global e integrador de todas las acciones de protección en un contexto empresarial, adonde la Seguridad Informática cumple un rol importante, pero en la misma medida también lo hacen otros factores, como la seguridad física del entorno y de las personas, aspectos culturales de los recursos humanos involucrados, controles de acceso físico, seguridad juridica, seguridad de los servicios provistos por terceros, entre otros.

Es importante tener presente esto ultimo pues es común encontrar en distintas fuentes referencias erroneas a la Seguridad Informática y a la Seguridad de la Información como sinónimos.

En esta materia se aborda la seguridad de una infraestructura tecnológica con un enfoque basado en la Seguridad Informática, pero sin perder de vista todo el contexto que implica la Seguridad de la Información.

Por ultimo, en linea con las Competencias Específicas definidas en el plan de la carrera, el entorno en el cual se enfoca la materia es principalmente en el ambito de las empresas y organizaciones.

La Seguridad Informática en la empresa

Toda organización tiene una misión. La misión es el objetivo mismo de la empresa. Si la infraestructura tecnológica sobre la cual se basan sus procesos se ve comprometida, el impacto puede resultar desde un simple inconveniente hasta algo tan crítico que comprometa el cumplimiento de esa misión, por lo tanto, dotar de seguridad a los activos involucrados se vuelve una tarea elemental y estratégica en un contexto de planificación y gestión empresarial.

En este sentido, el primer principio que se debe incorporar es que la seguridad al 100% es un objetivo dificil de alcanzar y sostener a lo largo del tiempo, pues involucra recursos, humanos y económicos, que en el ambito de una organización se encuentran delimitados, con lo cual, deben ser gestionados de forma eficiente.

Por lo tanto, para elaborar una estrategia de seguridad adecuada la organización debe definir qué seguridad pretende, dando respuesta a los siguientes interrogantes:

- ¿Qué activos quiere asegurar?
- ¿Contra qué amenazas lo quiere asegurar?
- ¿Cómo lo quiere asegurar?
- ¿Cuándo y en qué condiciones?

La respuesta a estos interrogantes no puede surgir de forma arbitraria, debe estar sustentada en un proceso metodológico y de rigor científico, medible y repetible; se trata del Análisis de Riesgos, que se aborda, de forma breve, a continuación.

Análisis de riesgos

Se trata de un proceso metodológico que permite identificar los activos tecnológicos y de información de la organización, sus vulnerabilidades, las amenazas a las que se encuentran expuestos, analizar la probabilidad de que dichas amenazas se materialicen, es decir, su nivel de riesgo, y determinar el impacto que pueden provocar a la organización si se materializan.

Es importante tener en claro los conceptos que utiliza el Análisis de Riesgos:

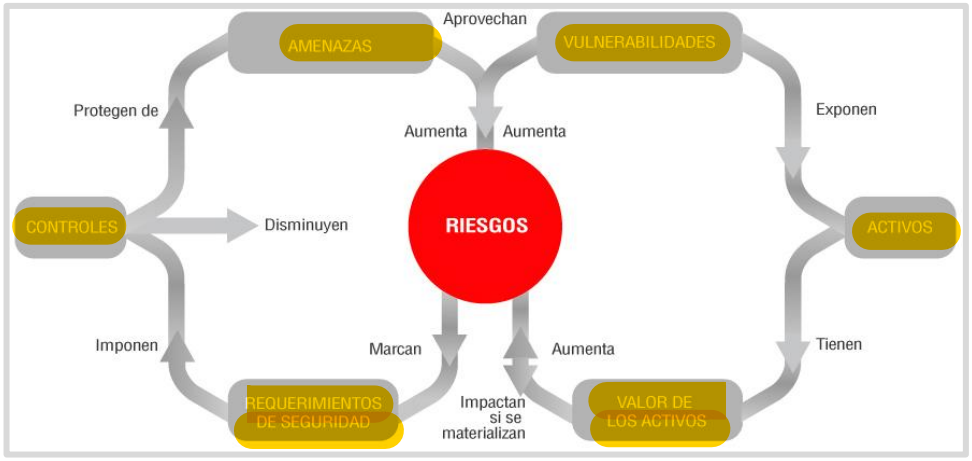
"**Activos:** Recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su Dirección". (Magerit Ver. 3, 2012, 3.1.1, p. 22).

"**Amenaza:** Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. (ISO/IEC 27002:2009, 2009, 2.16, p. 13)".

"**Vulnerabilidad:** Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza". (Magerit Ver. 3, 2012, 3.1.5, p. 35).

"**Riesgo:** El riesgo informático o riesgo de seguridad de la información se relaciona con la posibilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a una organización". (ISO/IEC 27002:2009, 2009, 2.9, p. 13).

Figura 1: Riesgos



Fuente: Secure & IT, 2016. Recuperada de: https://goo.gl/ME2kp4

En base a los resultados del análisis, se inicia una instancia de evaluación de los riesgos identificados que permite guiar a la toma de decisiones en la

determinación de los riesgos a tratar y la prioridad para implementar los tratamientos.

La evaluación de los riesgos tiene dos aspectos, por un lado el grado de probabilidad de que éste se materialice, y por otro lado su criticidad, qué tan importante es su ocurrencia.

La criticidad es específica de la organización y requiere un proceso de clasificación.

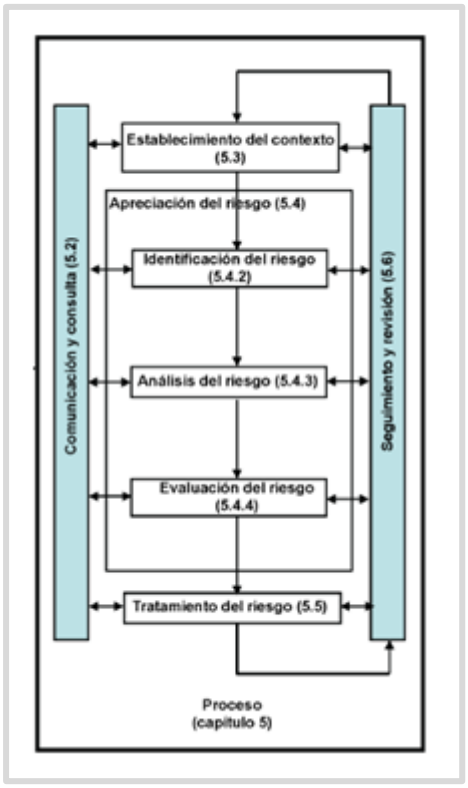
En cuanto al tratamiento del riesgo, implica la implementación de controles que permitan reducir el nivel de probabilidad de materialización de las amenazas. Las opciones de tratamiento pueden incluir lo siguiente:

- Evitar el riesgo optando por descartar la actividad que lo causa.
- Aceptar o incrementar el riesgo con el objeto de buscar una oportunidad.
- Eliminar aquello que provoca el riesgo.
- Modificar la probabilidad de que el riesgo se materialice.
- Atenuar el impacto del riesgo.
- Compartir el riesgo con terceras partes (Seguros).
- Retener el riesgo en base a una decisión informada.

Las amenazas a las infraestructuras tecnológicas y a la información que procesan y almacenan no son estáticas, esto se debe a que son afectadas por un conjunto de factores que van desde fallos en la implementación de las soluciones hasta el dinamismo del mundo de las organizaciones, adonde nuevas regulaciones son establecidas modificando sus procesos, y si el contexto cambia, se deben reevaluar las amenazas.

Esta característica dinámica de las amenazas requiere que el Análisis de Riesgos sea frecuentemente revisado, convenientemente, debe formar parte de un proceso, y como todo proceso, debe ser gestionado.

Figura 2. Gestión del Riesgo



Fuente: ISO/IEC 31000, 2009, Gestión de Riesgos.

Existen diversas metodologías de Análisis de Riesgos, muchas de ellas, soportadas a través de herramientas automatizadas que permiten llevar a cabo las tareas implicadas de formas muy eficientes, a continuación se citan algunas.

- ISO/IEC 31000 Gestión del Riesgo. Principios y Directrices.
- ENS MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Norma Española.
- ISACA COBIT Control Objectives for Information and Related Technologies.
- SEI OCTAVE Operationally Critical Threat, Asset and Vulnerability Evaluation.
- NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments.

Sistemas de Gestión de la Seguridad de la Información

Gestionar la seguridad de la información de una organización implica generar confianza, confianza en que los riesgos a los se encuentra expuesta tanto su infraestructura tecnológica como la información que procesa y almacena, son gestionados de forma adecuada.

Esta confianza a la que se hace referencia, en el ambito de las organizaciones, se genera a través de la implementación y certificación de Normas Estándares.

Para gestionar la seguridad se requieren una serie de procedimientos, procesos y controles que involucra de forma transversal a toda la organización. Se requiere de un sistema de gestión, basado en procesos y buenas prácticas e inmerso en un ciclo de mejora continua que garantice que estos procesos serán cada vez mas eficientes y eficaces.

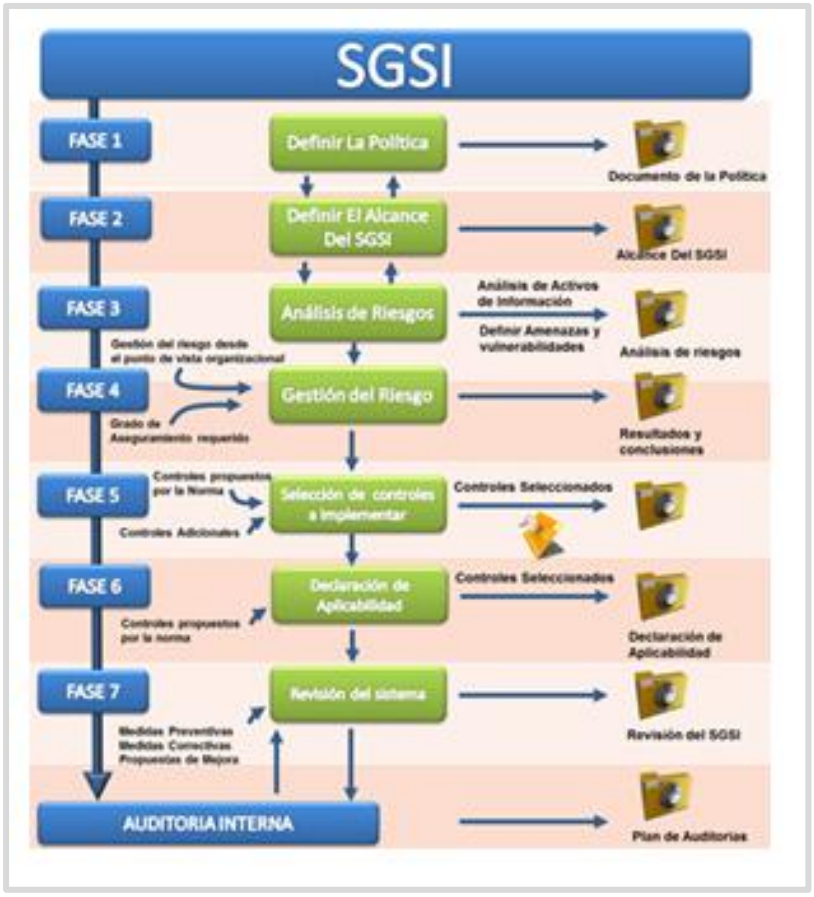
El Estándar de referencia, por excelencia, en el marco de los Sistemas de Gestión de la Seguridad de la Información es la Norma ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información[1].

La Norma ISO/IEC 27002[2] Códigos de buenas prácticas para la Gestión de la Seguridad de la Información, es un complemento de la Norma ISO/IEC 27001, por ende no es certificable. Esta extiende las especificaciones de la Norma ISO 27001, brindando directrices detalladas sobre cada ítem del Anexo A "Referencias sobre Objetivos de Control y Controles" de la citada Norma, describiendo los dominios de control y controles que pueden ser implementados dentro de una organización.

El Sistema de Gestión incluye: estructura organizacional, políticas, planificación, actividades, responsabilidades, prácticas, procedimientos, procesos, recursos.

[1] ISO/IEC 27001 Tecnologías de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la información. Requerimientos. De https://www.iso.org/standard/54534.html
[2] ISO/IEC 27002 Tecnologías de Información. Técnicas de seguridad. Código de Prácticas para controles de seguridad de la Información. De https://www.iso.org/standard/54533.html

Figura 3: Sistema de gestión de seguridad de la información basado en ISO/IEC 27001:2013



Fuente: Nomas ISO, 2017. Recuperada de https://goo.gl/zdUX2A

En resúmen, la Seguridad Informática es una actividad de protección. Lo que se protege son los atributos de Confidencialidad, Integridad y Disponibilidad de los activos.

En las empresas, esta actividad, forma parte de un concepto mas amplio conocido como Seguridad de la Información.

La gestión de la seguridad se basa en el Análisis de Riesgos como piedra angular de un Sistema de Gestión de la Seguridad de la Información, que cuando se basa en una Norma Estándar, como las expuestas, permite generar confianza en que los activos de la organización son gestionados de forma segura.

A forma de síntesis, se puede decir que la gestión de la seguridad de la información se deriva del Análisis y Gestión de Riesgos.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática*. 2° Edición. Madrid, España: Ra-Ma.

ISO/IEC 27001. (2013). *Tecnologías de información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requerimientos. Suiza: Organización Internacional de Estandarización* (ISO). Recuperado de: https://www.iso.org/standard/54534.html.

ISO/IEC 27002. (2013). *Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. Suiza: Organización Internacional de Estandarización* (ISO). Recuperado de: https://www.iso.org/standard/54533.html.

ISO/IEC 31000. (2009). *Gestión de Riesgos. Suiza: Organización Internacional de Estandarización* (ISO). Recuperado de: https://www.iso.org/standard/54533.html.

Ministerio de Hacienda y Administraciones Públicas. (2012). *Metodología de análisis y gestión de riesgos de los sistemas de información.* Recuperado de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Information Systems Audit and Control Association, ISACA. (2012). *COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Recuperado de: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx?utm_referrer=

National Institute of Standards and Technology, NIST. (2012). *SP 800-30 Rev. 1 Guía de Evaluación de Riesgos* (traducción propia). Estados Unidos. Recuperado el de http://csrc.nist.gov/publications/PubsSPs.html#800-30

Software Engineering Institute, SEI. (2012). *OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation* (Traducción propia). Recuperado el 03/2017 de http://www.cert.org/resilience/products-services/octave/

Secure & IT. (2016). *Análisis y gestión de riesgos*. Recuperado de: https:// www.secureit.es/procesos-y-gobierno-it/analisis-y-gestion-de-riesgos/

Normas ISO. (2017). *ISO 27001 Gestión de la Seguridad de la Información [Imagen].* Recuperado de: http://www.normas-iso.com/wp-content/uploads/2012/02/SGSI.png

Políticas de Seguridad de la Información

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la Bibliografía Básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha Bibliografía.

Políticas de Seguridad de la Información

Todos los aspectos relacionados con las Políticas de Seguridad de la Información se encuentran bien definidos en la familia de Normas Estándares ISO/IEC 27000 Gestión de la Seguridad de la Información[1]. Específicamente, en ISO/IEC 27002[2], su capítulo "5 Política de Seguridad", constituye una guía completa para el abordaje de este documento.

No obstante esto, en la presente Lectura, se presenta una breve revisión de éste requisito que constituye la base sobre la cual se asienta un Sistema de Gestión de Seguridad de la Información en un entorno organizacional, cuya estructura se ilustra a continuación.

Figura 1. Estructura de una Política de Seguridad de la Información

Fuente: Gómez Vieites, M. Enciclopedia de la Seguridad Informática, p. 72.

Política de Seguridad

La Política de Seguridad es una Declaración de la Dirección de la Organización en la que se define el compromiso, los objetivos, alcances, responsabilidades, entre otros aspectos, del Sistema de Gestión de Seguridad de la Información. En otras palabras, la Política de Seguridad sienta las bases del Sistema de Gestión de la Seguridad de la Información.

[1] ISO/IEC 27000. Familia de Normas Estándares de Gestión de Seguridad de la Información. De https://www.iso.org/isoiec-27001-information-security.html
[2] ISO/IEC 27002 Tecnologías de Información. Técnicas de seguridad. Código de Prácticas para controles de seguridad de la Información. De https://www.iso.org/standard/54533.html

Plan de Seguridad

También conocido como Plan Director de Seguridad, se trata de una planificación detallada en la que se definen los proyectos que se deberán llevar a cabo para implementar la Política de Seguridad. Comprende proyectos de nivel técnico, legal y organizativo.

Procedimiento de Seguridad

Es una especificación de los pasos que se deben llevar a cabo para la realización de tareas determinadas, relacionadas siempre con los objetivos definidos por la organización en la Política de Seguridad.

Características de las Políticas de Seguridad

La Política de Seguridad debe reunir las siguientes características:

- Debe ser posible implementarla a través de guías que especifiquen los pasos necesarios de una forma detallada.
- Debe contener y divulgar guías de uso responsable por parte del personal involucrado.
- Deben delimitar de forma clara las responsabilidades exigidas al personal involucrado.
- Debe alinearse con las exigencias del marco jurídico que regula la actividad de la organización.
- Debe ser auditada de forma periódica y adaptada a las nuevas exigencias de la organización, del entorno tecnológico y del marco jurídico.
- Debe mantenerse en un grado de abstracción elevado, de forma tal que no impida o limite la aplicación de medidas necesarias (Normativas, Procedimientos) ante cambios de contextos internos o externos, esto es, debe ser atemporal.
- Los servicios, aplicaciones y usuarios deben tener asignados los privilegios mínimos necesarios para llevar a cabo sus tareas.
- Los sistemas deben ser desarrollados e implementados para que, en caso de fallas, se sitúen en un estado seguro.
- No debe limitarse al cumplimiento de requisitos impuestos jurídicos o a exigencias de terceros, sino que debe estar alineada con las necesidades de negocio de la organización.
- Debe ser independiente del Hardware y del Software.

Definición de las Políticas de Seguridad

Las Políticas de Seguridad deben contener:

- Especificación del Alcance, en el que se indiquen los activos, procesos, personal, terceros externos a la organización, y cualquier otro recurso afectado por la Política.
- Especificación de los Objetivos que se pretenden alcanzar.
- Declaración de compromiso de la Dirección de la organización con la Política de Seguridad.
- Clasificación de la información.
- Identificación de los activos a proteger a través de Análisis y gestión de riesgos.
- Recursos involucrados en la implementación de las medidas de seguridad.
- Asignación de responsabilidades en los distintos niveles de organizativos.
- Definición clara y precisa de los comportamientos exigidos y de los que están prohibidos por parte del personal.
- Identificación de las medidas, normas y procedimientos de seguridad a implementar.
- Abordar las relaciones con terceros a través de un modelo de gestión.
- Planes de contingencia y de continuidad del negocio en respuesta a la materialización de incidentes.
- Cumplimiento de la legislación vigente.
- Definir las consecuencias ante incumplimiento y violaciones de la Política.

En la definición de las Políticas de Seguridad deben participar los siguientes roles de la organización:

- Directivos y responsables de los distintos departamentos y áreas funcionales de la organización.
- Personal del departamento de Informática y de Comunicaciones.
- Miembros del Equipo de Respuesta a Incidentes de Seguridad Informática, en caso de que éste exista.
- Representantes de los usuarios que pueden verse afectados por las medidas adoptadas.
- Consultores externos expertos en Seguridad Informática.
- Asesores Legales de la organización.

Por ultimo, y no menos importante, se deben llevar a cabo acciones de concientización para todas las partes involucrados, se debe generar conciencia colectiva pues la seguridad es responsabilidad de todos.

Políticas de Seguridad de la Información en el ámbito Público

En Argentina, la Oficina Nacional de Tecnologías de Información (ONTI), dependiente de la Jefectura de Gabinete de Ministros de la Nación[3], se encarga de regular las normativas relacionadas con las tecnologías de información y seguridad de la información en el ámbito público.

En este marco, desde el año 2005, publica el documento "Política de Seguridad de la Información Modelo"[4] basado principalemente en la familia de Normas Estándares ISO/IEC 27000, ya citada anteriormente en ésta Lectura.

Los organismos públicos alcanzados por este Modelo están definidos en la Desición Administrativa N° 669/2004[5].

Si bien su ámbito de aplicación apunta a organismos públicos, el Modelo es igualmente válido y puede tomarse como plantilla o referencia para el sector privado.

Este Modelo presenta la siguiente estructura:

[3] Jefatura de Gabinete de Ministros. Argentina. https://www.argentina.gob.ar/jefatura
[4] ONTI. Política de Seguridad Modelo. De: http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219163/norma.htm
[5] Decisión administrativa N° 669/2004. De http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/102188/norma.htm

Figura 2. Estructura de una Política de Seguridad de la Información

Fuente: Administración Pública Nacional, ONTI, 2013. Recuperado de: https://goo.gl/Rc2Vhm

En conclusión, la Política de Seguridad es la base del Sistema de Gestión de la Seguridad de la Información. Se trata de un documento de alto nivel de abstracción en el que la dirección de la organización fija cuales son los objetivos que se persiguen para garantizar la seguridad de la información y como ésta será protegida.

En concreto, constituye un marco flexible que da cabida a todas las Normas y Planes que regulan los procesos de seguridad en toda la organización.

Por otra parte, los Planes y Procedimientos son los medios a través de los cuales se implementan esos objetivos de seguridad. Si la Política de Seguridad es el "qué se pretende" en relación a la seguridad, los Planes y Procedimientos serán el "cómo lograr" esos objetivos.

La seguridad es una responsabilidad institucional de la dirección de la organización, por ende, debe decidir los lineamientos de la Política de Seguridad, respaldarla, asignarle los recursos necesarios y lograr conciencia colectiva de seguridad, involucrando a todos los actores de la organización, pues la seguridad es, a la vez, responsabilidad de todos.

Por ultimo, la revisión de las Normas Estándares, Guías y Referencias expuestas en esta Lectura, es de carácter obligatoria para profundizar los conceptos presentados.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática*. (2° Ed.) Madrid, España: Ra-Ma.

ISO/IEC 27001. (2013). *Tecnologías de información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requerimientos. Lugar: Suiza, Organización Internacional de Estandarización* (ISO). Recuperado de: https://www.iso.org/standard/54534.html.

ISO/IEC 27002. (2013). *Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. Lugar: Suiza, Organización Internacional de Estandarización* (ISO). Recuperado de: https://www.iso.org/standard/54533.html.

Jefatura de Gabinete de Ministros. (2005). *Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional.* Argentina: Oficina Nacional de Tecnologías de Información, ONTI. Argentina. Recuperado de: http://www.enre.gov.ar/web/bibliotd.nsf/042563ae0068864b04256385005ad0be/725d3547f18529530325705900436194/$FILE/Disp.%206-Anexo.pdf

Seguridad del sistema y del entorno

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la Bibliografía Básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha Bibliografía.

El dominio de la seguridad abarca todo aquello en el entorno de los sistemas de información que puede tener un impacto en la Disponibilidad, Integridad y Confidencialidad de la información.

Un desastre natural es un ejemplo de una amenaza física. Las medidas son también de una variedad muy diversa, como los circuitos cerrados de vigilancia. A pesar de que este dominio físico de la seguridad de la información puede parecer el más alejado de la profesión en sí, es importante entenderlo, ya que el firewall mejor configurado no será suficiente si alguien es capaz de acceder físicamente al Servidor que lo ejecuta.

Como muestra de la importancia de la seguridad, es interesante conocer algún caso de instalación con medidas bien diseñadas de seguridad física.

Un ejemplo es el búnker Pionen de la empresa Bahnhof[1], que cuenta con Wikileaks[2] como uno de sus clientes más reconocidos. Aunque construir un centro de datos en un búnker parece más bien una operación de marketing que una necesidad física, sus características son interesantes para ilustrar el diseño conjunto físico-lógico de sistemas seguros.

Entre los aspectos que sus creadores tuvieron en cuenta fueron la estabilidad geológica y el aislamiento frente a ataques físicos externos. No obstante, dado que uno de los mayores riesgos físicos **es el acceso no autorizado**, en ese aspecto la ubicación del Centro no aporta ningún beneficio adicional.

[1] Para más información sobre Bahnhof Internet Service Provider, consulte: https://www.bahnhof.net/
[2] Para más información sobre Wikileaks, consulte: https://www.wikileaks.org/

Figura 1. Centro de Datos Pionen de Bahnhof, situado en un antiguo búnker de la segunda guerra mundial en las montañas de Estocolmo

Fuente: Centro de datos Pionen, Bahnhof, 2016. Recuperada de https://goo.gl/hIzkpb

Seguridad del Sistema

La Seguridad del Sistema, también conocida bajo el nombre de Seguridad Lógica, consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas o agentes (procesos y servicios) autorizadas. Una premisa bien conocida en este marco define que *todo lo que no está permitido debe estar prohibido*.

Otra de las premisas es la *seguridad por defecto*, adonde los controles de seguridad sobre los activos son llevadas a su maximo nivel.

Los objetivos que se plantean en este marco son los siguientes:

- Limitar el acceso a los recursos del sistema, tales como aplicaciones y archivos.
- Asegurar que el personal pueda trabajar sin la necesidad de controles exhaustivos, y no sean capaces de acceder a recursos sin autorización.
- Asegurar la utilización de los recursos del sistema sea acorde a los procedimientos de uso definidos.
- Asegurar que las comunicaciones sean establecidas exclusivamente entre los interlocutores y que no intervengan terceros no autorizados.
- Asegurar la integridad en las comunicaciones de forma tal que la información no sea alterada durante los procesos de transmisión.

- Implementar planes de contingencia, como redundancia en las comunicaciones, de forma tal que se cuenten con canales alternativos de comunicación.

Existen dos grandes fuentes de amenazas a la Seguridad del Sistema o Lógica:

- Las relativas a Usuarios que intentan vulnerar la seguridad.
  - Escalada de privilegios, usurpación de identidad, acceso no autorizado, programación insegura, entre otras.
- Las relativas a programas maliciosos con el mismo objetivo.
  - Malware, bombas lógicas, virus, troyanos, entre otras.

Controles de Acceso

Los Controles de Acceso constituyen una de las piedras angulares en la Seguridad del Sistema, puesto que se pueden implementar a nivel del Sistema Operativo, Software de Negocio, Software de Base de Datos, soluciones de seguridad y cualquier otro tipo de aplicación.

Estos controles permiten:

- Proteger al sistema ante utilización o modificaciones no autorizadas.
- Asegurar la integridad de la información a través de la restricción de la cantidad de usuarios y procesos con accesos permitidos.
- Resguardando la información sensible de accesos no autorizados.

Las consideraciones relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso solicitado por un Usuario, a un determinado recurso, son planteadas por el National Institute for Standards and Technology[3] (NIST) en el NIST SP 800-12 Handbook[4] donde se encuentran resumidos los siguientes esquemas para dotar de seguridad a cualquier sistema:

- **Identificación y Autenticación**
  Se trata de la primera línea de defensa implementada en una infraestructura de tecnología. Se trata de evitar el ingreso de personas no autorizadas que permite, además, efectuar un seguimiento de las actividades de los usuarios. **Autentificación** es la comprobación que se efectúa en base a la identificación. **Identificación** es la presentación y reconocimiento del usuario una vez presentado ante el sistema.

3 Para más información sobre NIST, consulte: https://www.nist.gov/
4 Para más información sobre NIST SP 800-12 Handbook, consulte: https://goo.gl/l5d6VN

- **Roles**

  El acceso a la información puede limitado en base a la necesidad de conocer de los usuarios, agrupándolos por roles. Ejemplo de roles, pueden ser Personal administrativo, Logístico, Técnico, entre otros.

- **Transacciones**

  Los controles de acceso en transacciones se basan en la solicitud de una clave al momento de procesar una transacción específica.

- **Limitaciones a los Servicios**

  Estos controles se basan en limitar el uso concurrente de ciertos servicios, en base a criterios previamente definidos. Un ejemplo de ello, puede ser limitar el uso simultáneo de software de facturación a un cierto número de usuarios; cualquier intento de acceso por parte de otro usuario será denegado por el sistema.

- **Privilegios de Acceso**

  Se refiere al privilegio con el cual se permite el acceso al Usuario sobre los recursos y la información. Estos privilegios pueden ser:

  - **Lectura**: habilita lectura o visualización de la información. No es posible modificarla, no obstante, la información puede ser copiada o impresa.
  - **Escritura**: habilita la alteración de la información, modificación.
  - **Ejecución**: habilita a la ejecución aplicaciones.
  - **Borrado**: habilita a la eliminación de recursos del sistema como aplicaciones y archivos.
  - **Todas las anteriores**

  Además, existen otros privilegios de acceso especiales:

  - **Creación**: concede permiso para la creación de archivos, registros o campos.
  - **Búsqueda**: concede permiso para búsqueda de contenidos dentro de un directorio específico.

- **Ubicación y Horario**

  Es posible restringir el acceso a los recursos del sistema en base a la ubicación física o lógica, tanto de los datos como del Usuario. En relación al horario, se puede inhabilitar el acceso de acuerdo a rangos horarios previamente definidos, manteniendo de esta manera un control más extendido del acceso a los recursos del sistema, siempre que sean complementados con los controles expuestos anteriormente.

- **Control de Acceso Interno**

  Estos controles definen los privilegios con los que cuentan los usuarios sobre los recursos del sistema. Estos privilegios, como ya se planteó pueden además estar definidos por grupos o roles de usuarios. NIST detalla cinco métodos de control de acceso interno, entre ellos las Listas de Control de Acceso.

- **Control de Acceso Externo**

  Se trata de controles que operan como un elemento de protección durante la interacción del sistema con servicios, sistemas y entidades

externas a la organización. Son para de estos controles dispositivos de control de puertos, firewalls, proxys, solo por citar algunos.

- **Administración**
  Luego de definir las medidas de control de acceso sobre la infraestructura de tecnología y los recursos que la integran, se debe llevar a cabo una administración minuciosa de las éstas. Se requiere implementación, comprobación y testeos sobre los privilegios concedidos. La Política de Seguridad que se desarrolle respecto a la Seguridad del Sistema debe guiar en las decisiones referidas a la determinación de los Controles de Acceso, especificando las concesiones necesarias para establecer los perfiles de Usuario.

Se recomienda una revisión de la Norma Estándar ISO/IEC 27002[5] que presenta recomendaciones relacionadas al tema expuesto, a largo de los dominios que la componen.

Seguridad del Entorno

La Seguridad del Entorno, también conocida como Seguridad Física, abarca controles tan diversos como las amenazas. Las áreas fundamentales que deben considerarse pueden resumirse en las que se presentan a continuación.

Controles administrativos

Incluyen todos los procedimientos administrativos, en oposición a los controles propiamente físicos o técnicos.
Se pueden mencionar los siguientes como hitos fundamentales:

- Planificación de los requisitos de las instalaciones.
- Gestión de la seguridad de las instalaciones.
- Controles administrativos al personal.

Controles del entorno y de la habitabilidad

Son los controles físicos esenciales para mantener la operación de los sistemas y del personal que los opera. Las siguientes son las áreas principales:

[5] ISO/IEC 27002 Tecnologías de Información. Técnicas de seguridad. Código de Prácticas para controles de seguridad de la Información. De https://www.iso.org/standard/54533.html

- Suministro eléctrico.
- Detección y supresión de incendios.
- Calefacción, ventilación y aire acondicionado.

Controles técnicos y físicos

En este apartado se agrupan los controles que no son puramente administrativos, a pesar de tener aspectos administrativos. Las principales áreas son las siguientes:

- Control del inventario de equipos. Esencialmente, control del robo y el daño a los equipos.
- Dispositivos de control de acceso a las instalaciones.
- Control de las condiciones de las instalaciones.
- Detección de intrusos y alarmas.
- Requisitos de los medios de almacenamiento.

En este marco, la Norma Estándar ISO/IEC 27002 presenta en su capítulo 9 Seguridad Física y del Entorno, una guía pormenorizada y de lectura obligatoria para complementar lo expuesto en éste material.

En resumen, abordar la Seguridad del Sistema y del Entorno es una tarea compleja y crítica en el marco de la gestión de la seguridad de una infraestructura tecnológica y su información.

Incluir o excluir un control de seguridad será determinante en el estado general de la seguridad, pues implica mitigar correctamente una amenaza o, por el contrario, dejar a la organización totalmente expuesta.
Se trata, en definitiva, de determinar de forma certera la superificie de ataque, o en otras palabras, el perímetro de seguridad de la organización e identificar las vulnerabilidades que pueden presentar los activos allí presentes.

Las Normas Estandares como las planteadas, NIST SP 800-12 o ISO/IEC 27002, surgen en este contexto como herramientas validas, aunque no únicas ni mucho menos exclusivas, para delimitar el perímetro de seguridad bajo un proceso metodológico y establecer los controles de seguridad adecuados al contexto objeto de análisis.

Es de destacar también que el Análisis de Riesgos, ya sea aplicado en el marco de una Norma Estándar o fuera de ella, contribuye en la clasificación de los riesgos, que presentes en la superficie del sistema y en su entorno, deben ser tratados.

Por ultimo, es oportuno reflexionar acerca del concepto de perímetro de seguridad, esa división tanto física como lógica que determina lo que está dentro de la red y lo que está fuera de ella. Este límite tal como se conocía tradicionalmente se ha extendido de forma radical, producto de la aparición de facilidades como el Cloud Computing[6], el Bring Your Own Device[7], o el Teletrabajo[8], solo por citar algunos. Entonces, cabe preguntarse ¿cuál es el perímetro de seguridad del caso bajo estudio? Identificarlo de forma precisa contribuirá en mayor medida a identificar las amenazas físicas y lógicas que deberán ser analizadas.

[6] Para más información sobre *Cloud computing*, consulte: https://es.wikipedia.org/wiki/Computación_en_la_nube
[7] Para más información sobre BYOD, consulte: https://es.wikipedia.org/wiki/Bring_your_own_device
[8] Para más información sobre Teletrabajo, consulte: https://es.wikipedia.org/wiki/Teletrabajo

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática*. (2° Ed.) Madrid, España: Ra-Ma.

ISO/IEC 27002. (2013). *Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. Lugar: Suiza, Organización Internacional de Estandarización* (ISO). Recuperado de: https://www.iso.org/standard/54533.html

National Institute of Standards and Technology (NIST). (2017). *Special Publication 800-12 (DRAFT). Revisión 1. Introducción a la Seguridad de la Información* (Traducción propia). Recuperado de http://csrc.nist.gov/publications/drafts/800-12r1/sp800_12_r1_draft.pdf

National Institute of Standards and Technology (NIST). (1995). *The NIST Handbook* (Traducción propia). Recuperado de http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Bahnhof (2016). *Centro de Datos Pionen.* [Imagen]. Estocolmo, Suecia. Recuperada de: https://www.bahnhof.net/

Protección y detección

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Protección y detección

La lectura del presente material es meramente complementaria a la Bibliografía Básica. Definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha Bibliografía.

Protección

Las medidas de protección deben ser eficaces y eficientes para las amenazas que pretenden contrarrestar.

Estas medidas poseen ciertas características y tipificaciones que es importante conocerlas para tener presente al momento de determinar de qué forma tratar a una amenaza.

Las medidas de protección se definen en las Normativas Estándares y Guias de Seguriad de la Información bajo algunos de los siguientes términos:

- Medidas de seguridad. (MAGERIT v3. Libro 1, 2012, 8.8.1, p. 102).
- Salvaguardas: o contra medidas, son procedimientos o mecanismos tecnológicos que contribuyen a reducir el riesgo. (MAGERIT v3. Libro 1, 2012, 8.8.1, p. 103).
- Control: medida que está modificando el riesgo. (ISO/IEC 31000, 2009, 2.26, p.13).

Existen amenazas que no requieren medidas de protección, se contrarrestan simplemente con una organización adecuada, otras requieren elementos técnicos (programas o equipos), otras requieren seguridad física y, por último, está la política de personal.

Selección de medidas de protección

Ante la amplia diversidad de posibles medidas de protección a considerar, es necesario realizar una preselección inicial acotando aquellas que son relevantes para lo que se debe proteger. En esta preselección se deben tener en cuenta los siguientes aspectos:

- Tipificación de los activos que deben ser protegidos, dado que cada tipo de activo requiere de medidas específicas de seguridad.
- Servicios de seguridad que deben ser protegidos, esto es, su confidencialidad, integridad o autenticación.
- Amenazas contra las que se requieren medidas de seguridad.
- Posibles medidas alternativas seguridad.

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

- Centrarse en los activos más valiosos y desestimar aquellos que sean menos relevante para el negocio.
- Centrarse en los riesgos cuyas amenazas representen una mayor probabilidad de materialización.
- Evaluar el grado de eficacia que ofrecen las medidas alternativas.

Esto conlleva a dos tipos de definiciones para excluir una cierta medida del conjunto de las que conviene analizar:

- No aplica. Cuando una medida no es oportuna dado que técnicamente es inadecuada al activo que se pretende proteger, no ofrece el servicio de seguridad necesario o no ofrece seguridad ante la amenaza evaluada.
- No se justifica. Cuando la medida ofrece la protección pretendida, pero su implementación implica recursos superiores al valor del activo que se pretende proteger.

Como resultado de estas consideraciones se dispondrá de una "declaración de aplicabilidad" de medidas que deben ser analizadas como posibles componentes del sistema de protección.

Efectos de las medidas de protección

En el contexto de un cálculo de riesgo (MAGERIT Versión 3.0, 2012), las medidas de protección afectan de dos maneras:

- **Reducen la probabilidad de las amenazas.** Se conocen como medidas preventivas. Las medidas ideales tienen la capacidad de impedir la materialización de la amenaza.
- **Limitan el daño provocado**. Existen medidas que limitan la posible degradación, mientras que otras permiten detectar el ataque y evitar que la degradación se profundice. Existen medidas que se limitan a realizar una restauración del sistema en caso de que una amenaza lo destruya.

En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

Tipos de medidas de protección

Conocer qué tipo de protección otorga una medida determinada, permite entender de qué forma se está abordando una amenaza. La siguiente tipificación es bien conocida:

- **Prevención.** Una medida es preventiva cuando reduce las oportunidades de que un incidente ocurra.
- **Disuasión.** Una medida es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven a atacar.
- **Eliminación.** Una medida elimina una amenaza cuando impide que ésta tenga lugar.
- **Minimización del impacto / Limitación del impacto.** Una medida minimiza o limita el impacto de una amenaza cuando acota las consecuencias de su materialización.
- **Corrección.** Una medida es correctiva cuando, habiéndose producido un daño, lo repara.
- **Recuperación.** Una medida ofrece recuperación cuando permite regresar al estado anterior al incidente.
- **Monitorización.** Son medidas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido.
- **Detección.** Una medida funciona detectando un ataque cuando informa de que el ataque está ocurriendo.
- **Concientización.** Son las actividades de formación de las personas involucradas en el sistema que pueden tener una influencia sobre él.
- **Administración.** Son medidas relacionadas con los componentes de seguridad del sistema.

En la siguiente tabla se relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad.

Tabla 1. Relación efecto de medidas de protección vs tipo de protección

Efecto	Tipo
Preventivas. Reducen la probabilidad de una amenaza (riesgo).	- Preventivas - Disuasorias - Eliminación
Acotan la degradación que provoca una amenaza.	- Minimizadoras - Correctivas - Recuperación
Consolidan el efecto de las demás	- De monitorización

	- De detección - De concientización - Administrativas

Fuente: MAGERIT versión 3, 2012, 3.1.4, p. 34.

Eficacia de la Protección

Las medidas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden contrarrestar. La medida ideal es 100% eficaz, eficacia que combina 2 factores:

- Desde el punto de vista técnico:
  - es técnicamente idónea para enfrentarse al riesgo que protege.
  - se emplea siempre.
- Desde el punto de vista de operación de la medida:
  - está perfectamente desplegada, configurada y mantenida.
  - existen procedimientos claros de uso normal y en caso de incidencias.
  - los usuarios están formados y concientizados.
  - existen controles que avisan de posibles fallos.

Es posible representar el grado de idoneidad de las medidas de protección asociándolas con un factor dentro de un rango entre 0% y 100%. A la vez, estos factores se pueden corresponder con niveles de madurez de las medidas, tal como se presenta en la siguiente tabla.

Tabla 2. Grados de eficacia de medidas de protección

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / Ad Hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

Fuente: MAGERIT versión 3, 2012, 3.1.5, p. 34.

Medidas de Protección recomendadas

Diversas Guías y Normas Estándares incluyen recomendaciones de medidas de protección aplicables frente a una amenaza determinada. A continuación se citan algunos de éstos recursos.

- ISO/IEC 27002:2014. Código de prácticas para controles de seguridad de la información.
- ISO/IEC 27033:2012. Guía para diseño e implementación de seguridad en Red.
- ISO/IEC 27034:2011. Seguridad en Aplicaciones.
- ISACA COBIT v.5:2012. Seguridad de la Información. Objetivos de control.
- MAGERIT v.3:2012. Libro 1 – Método. Capítulo 6. Catálogo de Elementos.
- NIST Cibersecurity Framework. Guías y Prácticas para infraestructuras críticas.
- PCI-DSS v.3.2:2016. Industria de Tarjetas de Pago. Normas de Seguridad de Datos.
- ITIL v3:2011. Capítulo 3.4 - Gestión de la Seguridad.

Detección

Las detección es una instancia clave en la seguridad de una infraestrctura tecnológica, mas bien en la gestión de los riesgos que subyace en ella.

Existen diversos mecanismos y herramientas capaces de detectar anomalías y alertar de forma automática a los responsables de seguridad.

Estos mecanismos soportan la configuración de las políticas de seguridad de la organización a través de reglas y operaran en función de ellas.

Se presenta a continuación una breve mención de las principales soluciones disponibles.

- **IDS/IPS:** Intrusion Detection Systems / Intrusion Prevention Systems. Sistemas de Detección de Intrusión / Sistemas de Prevención de Intrusión. Son soluciones basadas en reglas, capaces de detectar y prevenir anomalías y violaciones a políticas de seguridad y emitir alertas de forma automática. En cuanto a su presentación, existen en versiones software y hardware. En cuanto a su aplicación, existen en versiones Host y Red. El primero se encarga de monitorizar los eventos en un Host específico, mientras que el segundo se encarga de monitorizar los eventos en la Red.

- **SIEM**: Security Information and Event Management. Sistemas de correlación de Eventos. Son soluciones basadas en reglas, que se encargan de reunir información de registros de los distintos sistemas operativos, servicios y protocolos desplegados y los analiza en busca de fallas, actividades sospechosas y violaciones de políticas.

- **OSSIM**: Open Source Security Information Management. Conocidos también como Open Source SIEM, se trata se soluciones similares características a las que presenta un SIEM, con la ventaja del licenciamiento GPL (General Public Licence).

- **UTM**: Unified Threat Management. Gestión Unificada de Amenazas. Se trata de soluciones que implementan múltiples soluciones de seguridad en una misma herramienta. Algunas de las funcionalidades que incluyen son: Antispam, Antiphishing, Antivirus, Antispyware, Filtrado de contenidos, IDS/IPS, VPN, por citar algunas.

- **Firewalls**: Cortafuegos. Se trata de soluciones basadas en reglas que controlan el acceso de un recurso desde y hacia una red. Existen en versiones software y hardware.

- **Antivirus**: Las soluciones Antivirus forman también parte de los mecanismos de detección con los que se cuenta en una organización, seguramente con implementaciones más complejas y centralizadas que en un contexto de usuario final.

En resumen, para proteger de forma adecuada una infraestructura tecnologica y su información, se deben definir medidas de protección. Se trata de acciones destinadas a contrarrestar amenazas presentes en el perímetro de seguridad que han sido previamente identificadas, analizadas evaluadas y seleccionadas a través de un proceso de Análisis y Gestión de Riesgos. Estas medidas tienen características propias que es oportuno conocerlas para tener presente de qué forma y con qué eficacia contribuirán a proveer seguridad.

En especial, los mecanismos de detección, se abordará con mayor profundidad en los siguientes módulos de la materia.

Guias y Normativas de Seguridad como las expuestas, brindan catalogos de de medidas de protección aplicables ante amenazas específicas en cualquier contexto abordado.

Por otra parte, los mecanismos de detección, son herramientas de seguridad que soportan la configuración de reglas basadas en las Políticas

de Seguridad de la organización, y operan en busqueda de presencia y prevención de las amenzas que se han definido contrarrestar.

Se recomienda la revisión de la bibliografía detallada en la sección de Referencias para profundizar lo expuesto en la presente Lectura, en particular la Norma española MAGERIT v3 dado que se trata de un recurso estructurado y completo.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática*. (2° Ed.) Madrid, España: Ra-Ma.

ISO/IEC 27002. (2013). *Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información*. Suiza: Organización Internacional de Estandarización, ISO. Recuperado de: https://goo.gl/clY16p.

ISO/IEC 27033. (2012). *Tecnologías de información. Técnicas de seguridad. Seguridad en Redes.* Suiza: Organización Internacional de Estandarización, ISO. Recuperado de: https://goo.gl/aVpa8R.

ISO/IEC 27034. (2011). *Tecnologías de información. Técnicas de seguridad. Seguridad en Aplicaciones*. Suiza: Organización Internacional de Estandarización, ISO. Recuperado de: https://goo.gl/RrsLJ9.

Information Systems Audit and Control Association, ISACA. (2012). *COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Estados Unidos. Recuperado de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx?utm_referrer=

Ministerio de Hacienda y Administraciones (2012). Plan de seguridad. En *MAGERIT Versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I. Método*. Madrid, España: Centro de Publicaciones. Recuperado de: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

National Institute of Standards and Technology (NIST). (2014). *Framework for improving Critical Infraestructure Cibersecurity. Version 1.0.* (Traducción propia) Recuperado de: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Industria de Tarjetas de Pago (PCI). (2016). *PCI DSS v. 3.2. Norma de Seguridad de datos. Requisitos y Procedimientos de evaluación de seguridad*. Recuperado de https://es.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

Río Huercanos, S. (2014). *ITIL v3. Manual Integro. Manual de ITIL*. En español. Recuperado el 03/2017 de: http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf