UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

"ANÁLISIS PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA APLICADO EN EMPRESAS CORPORATIVAS". Revisión de la Literatura"

Trabajo de investigación para optar el grado de:

Bachiller en Ingeniería de Sistemas Computacionales

Autor:

Oscar Antonio Pérez Vilca

Asesor:

Mg. Lupe Yovani Gallardo Pastor

Lima - Perú

2018

ACTA DE AUTORIZACIÓN PARA PRESENTACIÓN DEL TRABAJO DE INVESTIGACIÓN

El asesor Lupe Yovani Gallardo Pastor, docente de la Universidad Privada del Norte, Facultad de Ingeniería, carrera profesional de Ingeniería de Sistemas Computacionales, ha realizado el seguimiento del proceso de formulación, desarrollo, revisión de fondo y forma (cumplimiento del estilo APA y ortografía) y verificación en programa de antiplagio del trabajo de Investigación del o los estudiantes(s)/egresado(s):

- ❒ Oscar Antonio Pérez Vilca

Por cuanto, **CONSIDERA** que el trabajo de Investigación, titulado "Análisis para la Gestión de la Seguridad Informática aplicado en Empresas Corporativas", para optar al grado de bachiller por la Universidad Privada del Norte, reúne las condiciones adecuadas en forma y fondo, por lo cual **AUTORIZA** su presentación.

Los Olivos 20 de Julio de 2018

_____

Mg. Lupe Y. Gallardo Pastor

Asesor

ACTA DE EVALUACIÓN DEL TRABAJO DE INVESTIGACIÓN

El Sr(a) ,

ha procedido a realizar la evaluación del trabajo de investigación del (los) estudiante(s): *Oscar Antonio Pérez Vilca* para aspirar al grado de bachiller con el trabajo de investigación: "ANÁLISIS PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA APLICADO EN EMPRESAS CORPORATIVAS"

Luego de la revisión del trabajo en forma y contenido expresa:

( ) Aprobado

Calificativo: ( ) Excelente [20 - 18]

( ) Sobresaliente [17 - 15]

( ) Bueno [14 - 13]

( ) Desaprobado

Ing./Lic./Dr./Mg.

Evaluador

DEDICATORIA

A mis padres, Victoria Vilca y Olimpio Pérez, por el esfuerzo en darme educación, apoyo incondicional y plena confianza.

A mis 04 hermanas por el aliento constante en terminar este proyecto y seguir superándome personal y profesionalmente

AGRADECIMIENTO

A mi asesora por su apoyo invalorable y constante para la elaboración del presente trabajo de investigación.

A la Universidad Privada del Norte por la metodología y procesos que emplean para el desarrollo de la carrera.

A mis compañeros de clase, que desde el inicio de la carrera mostraron el apoyo y colaboración en el desarrollo de los cursos.

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

La seguridad informática es un aspecto relevante hoy en día en el área de las redes y comunicaciones, por lo cual es importante contar con soluciones integrales que permitan gestionar de manera eficiente las amenazas informáticas que tratan de comprometer la disponibilidad de los servicios o lucrarse con información confidencial.

La presente investigación tiene como objetivo realizar una revisión sistemática de la literatura basada en artículos y libros publicados en idioma español a través de un análisis completo de la publicación, diseño de investigación, sector corporativo, instrumentos y variables de acuerdo con el estudio; características para la gestión de la seguridad informática aplicado en empresas corporativas. La búsqueda de la información se realizó en la base de datos de E-Libro y Redalyc. Las publicaciones seleccionadas como unidad de estudio estuvieron conformado por 05 publicaciones y estuvieron sujetos a una evaluación del contenido sobre la seguridad informática, además se puede afirmar que los artículos presentaron uniformidad en la información y no sugieren una metodología formal. Adicionalmente, el análisis indica a la gestión de seguridad informática como un elemento clave para la protección y funcionamiento de los recursos informáticos en las redes corporativas.

PALABRAS CLAVES: revisión sistemática, gestión de la seguridad, seguridad informática, recursos informáticos.

CAPÍTULO I. INTRODUCCIÓN

En la actualidad, uno de los activos más valiosos para cualquier empresa es la información que maneja. Estos activos pueden ser un conjunto de datos, software, sitios web, y en general todo recurso tecnológico que esté a disposición de los usuarios. Bajo esta premisa se hace necesario contar con medios y herramientas que protejan toda la red informática en una empresa. Por lo expuesto, surge el termino seguridad informática que tiene como objetivo prever y evitar incidentes que perjudiquen la operación en las organizaciones.

Verificando la definición de Costas, S.J. 2014) la gestión de la seguridad consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Baca, U. G. (2016) afirma que la seguridad informática tiene como objetivo proteger dichos activos, por lo que la primera labor será identificarlos para establecer los mecanismos necesarios para su protección y analizar la relevancia de los mismos en el proceso de negocio de la organización. No tiene sentido gastar miles de dólares en proteger activos no importantes para el negocio o que no tengan un valor que justifique ese gasto.

Según, Gil Vera, V., & Gil Vera, J. (2017) en los últimos años, el uso de la informática se ha extendido a la mayoría de actividades profesionales y humanas a nivel mundial. Las redes de comunicación y los recursos informáticos se han convertido en un factor esencial para el desarrollo económico y social de las naciones. Debido a lo anterior, garantizar la seguridad de la información se ha convertido en una tarea de vital importancia y preocupación para empresas, organizaciones e instituciones públicas y privadas.

Para Álvarez, M. G., & Pérez, G. P. P. (2004) actualmente, la estrategia de control de intrusos más utilizada es la perimetral, basada en la utilización de cortafuegos y routers. Estos

dispositivos actúan como las rejas con pinchos y las puertas con doce cerrojos. Sirven para mantener fuera a los intrusos, es decir, sirven al propósito de prevenir ataques o intrusiones en la red interna por ellos protegida.

Según, Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013) la mayoría de expertos coinciden en que no existe ningún sistema totalmente seguro e infalible al 100%, se debe tratar de proteger la información y el sistema que la utiliza para ofrecer un nivel de seguridad razonable a los usuarios. Para que un sistema se pueda considerar razonablemente seguro se debe garantizar que se cumplen los principios básicos de la seguridad informática: integridad, confidencialidad y disponibilidad.

En un estudio sobre seguridad informática, el CERT informa que en el año 2003 se han producido más de 100.000 incidentes de seguridad y que se ha informado de más de 3.000 vulnerabilidades. Si se comparan estos datos con los primeros publicados en 1988, que recogían 6 incidentes y 171 vulnerabilidades, uno se puede dar cuenta de lo mucho que ha evolucionado la seguridad informática, o inseguridad, según se mire, en los últimos 15 años. (Álvarez, M. G., & Pérez, G. P. P. 2004)

En atención a la problemática expuesta, la búsqueda sistemática de análisis en la base de datos de E-Libro y Redalyc revela la carencia de estudios que resalten la gestión efectiva de la seguridad informática en empresas corporativas. Desde esta perspectiva, un Firewall cumple un rol primordial en las redes corporativas y se hace necesario para bloquear ataques externos con una adecuada administración; y con ello aumentar la confiabilidad en el manejo de las redes informáticas en la empresa.

Ante lo expuesto, se realizó la presente investigación a fin de responder a la pregunta ¿Cuáles son las características para la gestión de la seguridad informática frente a las amenazas en las redes corporativas? Considerando los casos más relevantes a nivel mundial en los últimos años.

Así, el objetivo de estudio fue analizar las principales características de la gestión de seguridad informática aplicado en empresas corporativas mediante una revisión sistemática. Para ello se recurre a diversos artículos publicados previo análisis completo de acuerdo al diseño de investigación y estudio.

CAPÍTULO II. METODOLOGÍA

2.1 Selección de estudios

La recopilación de las fuentes de información se realizó en los meses de mayo y junio del 2018 sobre estudios relacionados con la investigación “Gestión de la Seguridad Informática aplicado en empresas corporativas”. Se consideraron los siguientes criterios de inclusión:

(a) Artículos de estudios prácticos en empresas de mediana o gran envergadura y sus áreas específicas en el contexto Latinoamericano. Además, todos ellos se encuentren en versión digital y en idioma español.

(b) El periodo de publicación comprendan entre los años 2006 y 2017 con el objetivo de identificar las principales características en la gestión de la seguridad informática aplicado en empresas corporativas en los últimos quince años, para con ello abordar el tema planteado en el problema. Asimismo, se excluyeron estudios referidos a la implementación del sistema de gestión de seguridad informática y documentos que emplean características en un contexto no corporativo.

(c) Para iniciar la búsqueda de la investigación se consideró el título y campo de acción del tema planteado en la investigación. Se tomaron en cuenta las palabras claves que abarquen un amplio aspecto del tema: gestión de la seguridad, seguridad, red corporativa**.** La muestra estuvo conformada por medianas y grandes empresas. La situación socio demográfico por gerentes, ingenieros, supervisores, jefes y personal técnico de sistemas.

Se realizaron tres pasos para desarrollar el proceso de búsqueda de la literatura:

a) Como primer paso, se realizó una indagación de la literatura para encontrar estudios relacionados con el tema en la base de datos en la biblioteca virtual E-Libro y Redalyc.

b) En el segundo paso, ya contando con los resultados obtenidos de la indagación de la literatura, se filtró la cadena de búsqueda considerando los títulos, palabras claves y bibliografía que arrojó el primer paso de búsqueda.

2.2 Codificación de datos

Después de extraer los artículos más importantes se elaboró la codificación de los artículos seleccionados (Tabla 1). Los artículos fueron codificados de acuerdo con las características de los libros y publicaciones (año de publicación, nombre de artículo, tipo de estudio, características de la Seguridad y objetivo).

Tabla 1:
Características de la unidad de análisis respecto al año de publicación, nombre de artículo, tipo de estudio, características de la Seguridad y objetivo

Año	**Nombre del artículo**	**Tipo de estudio**	**Tipo de seguridad informática**	**Objetivo**
2014	Seguridad Informática para empresas y particulares	1 (experimental)	Seguridad Activa y Pasiva	Ofrecer una visión de la seguridad de la información completa y muy práctica a todos los usuarios del sector TI y en general que sientan la necesidad de proteger sus recursos informáticos
2002	Seguridad Informática	1 (descriptivo - correlacional)	Seguridad Activa	Conocer las innovaciones en ataques y vulnerabilidades más actuales en materia informática, haciéndonos más prevenidos y realizar acciones totalmente seguras.
2016	Introducción a la seguridad informática	1 (descriptivo)	Seguridad Pasiva	Conocer las herramientas y distinguir los principales tipos de seguridad informática para plantear argumentos que sustenten que la información es valiosa para cualquier organización
2004	El mito de la seguridad informática	1 (experimental Descriptivo)	Seguridad Pasiva	Identificar los factores críticos relacionados con la seguridad informática en base a experiencias de ataques de virus a empresas corporativas.
2014	Gestión de incidentes de seguridad informática	1 (descriptivo)	Seguridad Activa y Pasiva	Calcular y utilizar adecuadamente los recursos necesarios para aplicar correctamente estas medidas de prevención, detección y corrección de incidentes de seguridad informática

Tabla 2

Características de la unidad de análisis respecto a la revista de publicación, diseño de investigación, muestra, instrumentos y variables asociadas

Año	**Nombre del artículo**	**Tipo de estudio**	**Tipo de seguridad informática**	**Objetivo**
2017	Seguridad Informática organizacional: un modelo de simulación basado en dinámica de sistemas	1 (descriptivo - experimental)	Seguridad Activa	Desarrollar un modelo de simulación que permita evaluar el nivel óptimo de seguridad que deben tener las organizaciones considerando aspectos relacionados con la reducción del riesgo y la obtención de beneficios empresariales.
2002	Antivirus y Seguridad Informática: El nuevo	1 (descriptivo - experimental)	Seguridad Activa	Prevenir con aplicaciones posibles daños que puedan afectar el buen funcionamiento del sistema informático.

CAPÍTULO III. RESULTADOS

Se identificaron 24 artículos de acuerdo con el título de la investigación, de los cuales según evaluación fueron separados 12 por estar dentro de los criterios de exclusión. Por lo tanto, se examinaron 12 de ellos que fueron analizados a detalle. Tres artículos consistían en dar una reflexión sobre la seguridad informática basado en opiniones de expertos. Dos investigaciones correspondían a presentar soluciones de implementación para protección de las redes domésticas. En un artículo la investigación estuvo basado en la gestión de los incidentes de la seguridad informática, no correspondiendo al objetivo de estudio.

Finalmente, en un artículo se estudia únicamente un tipo de solución empleada para la seguridad de las redes informáticas. Por lo tanto, la unidad de análisis quedó establecida por 05 artículos científicos (figura 1),

.

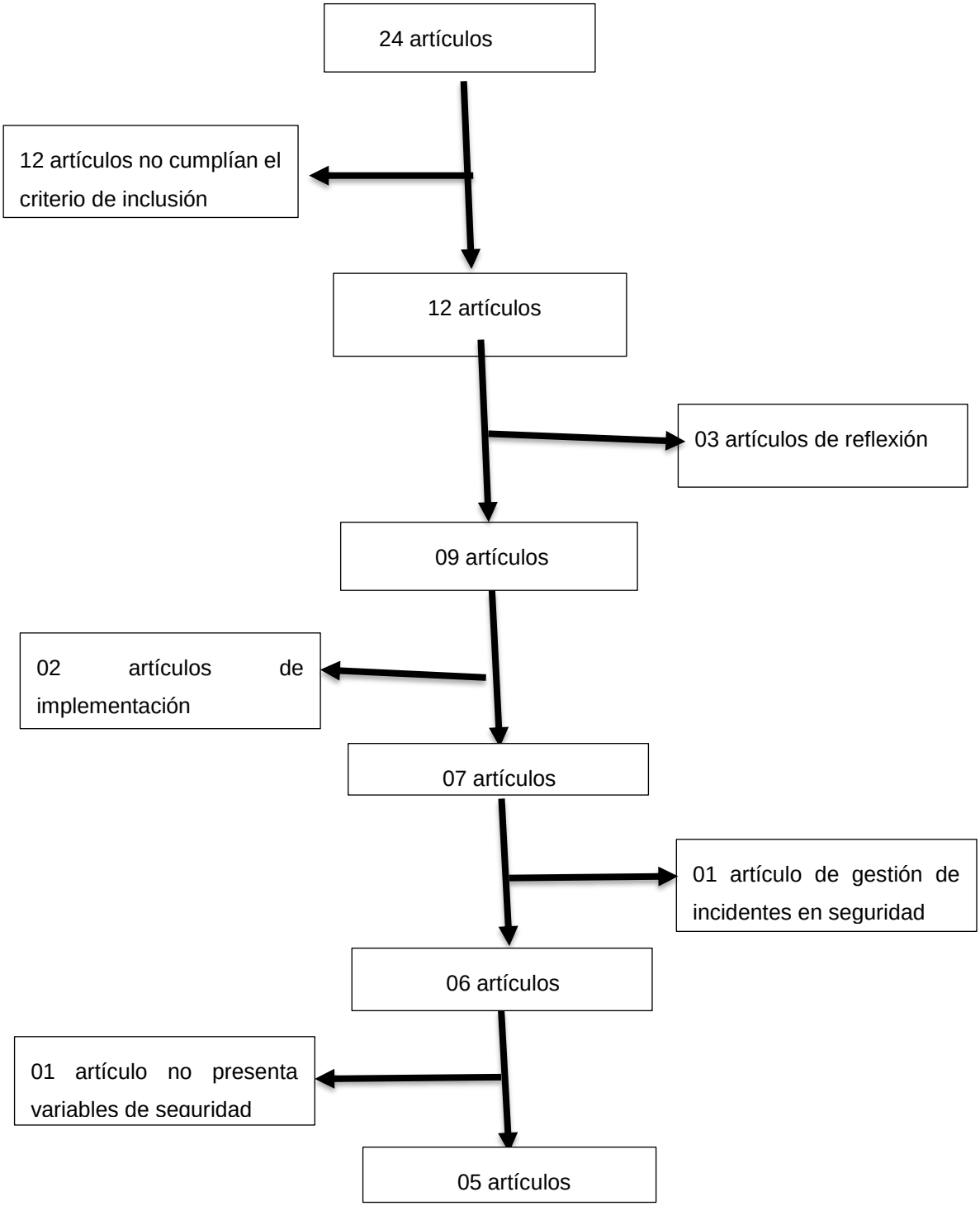

Figura 1. Procedimiento de selección de la unidad de análisis

3.1 Artículos y publicaciones.

En la fase de análisis, de acuerdo a los artículos revisados, el total corresponde al área de Ingeniería Informática (100 %). De acuerdo con los registros, 4 artículos corresponden a la biblioteca virtual E-Libro (80%) y 01 se encuentran en Redalyc (20%). Los artículos de investigación fueron editados en idioma español.

En el análisis del periodo de publicaciones, estas inician el año 2002 con un artículo en el año 2002. Dos artículos en 2014 y finalmente dos artículos en los años 2017 y 2017.

Indicar que el 100 % de autores de los artículos revisados son Ingenieros de Sistemas Informáticos de profesión.

3.2 Diseño de investigaciones

En el diseño de investigación con relación a los estudios realizados de seguridad informática se encontraron 02 tipos, en función de lo que se quiere proteger: Seguridad activa, que consta de medidas preventivas (65%) y seguridad pasiva, mediante medidas correctivas (35%). En tal sentido, Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013), afirma que la seguridad activa se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca; por ejemplo, la utilización de contraseñas. Y la seguridad pasiva comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad; por ejemplo, las copias de seguridad.

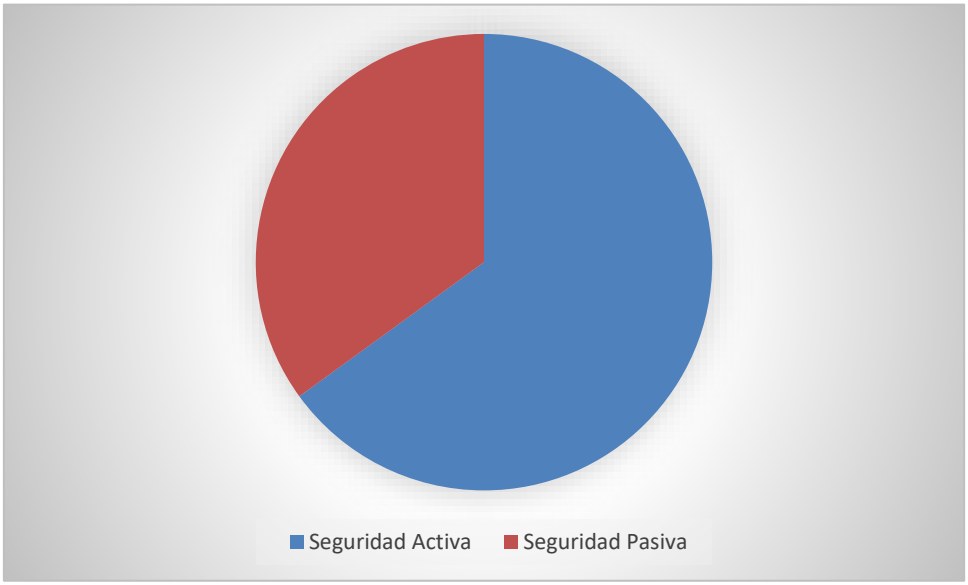

Figura 2. Tipos de seguridad informática consideradas en el estudio

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

Esta investigación revisa estudios de la gestión de la seguridad informática de diferentes países desde los años 2002 hasta 2017, encontrándose 2 artículos empíricos basado en experiencias propias de los autores, E-Libro y Redalyc fueron las dos fuentes principales consideradas en la investigación. El objetivo principal de esta investigación fue encontrar las características que debe considerarse en una gestión de seguridad informática, sobre todo aplicado en organizaciones o empresas corporativas. Para este fin se encontraron 03 artículos que describían a detalle las mejores normas y prácticas mas no evidenciaban casos de estudio en alguna empresa corporativa. Cabe indicar que para esta investigación no se encontraron artículos que describan en seguridad informática casos críticos basado en los últimos casos de ataques a empresas y organizaciones, puntualmente el último de gran impacto en todo el mundo, al caso Ransonware.

Asimismo, el presente estudio contribuye significativamente a los sectores empresariales, corporativos y organizacionales porque proporciona una visión general de investigaciones ya realizadas en donde se identifican, explora y sistematiza la literatura acerca de la gestión de la seguridad informática aplicada principalmente en el sector corporativo.

Conclusiones

Para la presente revisión sistemática sobre las características de la gestión de seguridad informática aplicado en empresas corporativas se aplicó la metodología de búsqueda sistemática de la literatura basada en métodos utilizados en la medicina, pero en este caso adaptado a la Ingeniería.

Se analizaron 5 artículos para dar solución a la pregunta propuesta en la revisión sistemática y con los estudios seleccionados se realizó un recuento de la propuesta de los autores. Esto artículos revisados presentaron diversas informaciones sobre gestión de seguridad, pero se puede aseverar que todos estos presentan uniformidad en su contenido. Los instrumentos estuvieron de acuerdo al tipo de investigación para encontrar los factores determinantes en el nivel de gestión de la seguridad informática en diversos sectores organizacionales no considerando para este estudio las pequeñas y medianas empresas.

Asimismo, esta revisión sistemática analizó los tipos de seguridad informática, los cuales indicaron que el empresario o director de la organización y su plana jerárquica deben admitir la gestión de la seguridad informática como elemento clave de protección y prevención. Desde una perspectiva más amplia, también se debe considerar la estrategia, el factor humano, mecanismos de apoyo, herramientas y técnicas y la propia organización. Además, el estudio revela la importancia de conocer la realidad sobre la gestión de la seguridad informática en empresas corporativas que se vienen aplicando en todo el mundo, dado que las redes corporativas pueden sufrir ataques desde cualquier computador ubicado en algún lugar remoto con el simple hecho de estar conectado a internet.

REFERENCIAS

Roa, B. J. F. (2013). Seguridad informática. Retrieved from http://ebookcentral.proquest.com

Costas, S. J. (2014). Seguridad informática. Retrieved from http://ebookcentral.proquest.com

Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Retrieved from http://ebookcentral.proquest.com

Gómez, V. Á. (2014). Auditoría de seguridad informática. Retrieved from http://ebookcentral.proquest.com

Chicano, T. E. (2014). Auditoría de seguridad informática (mf0487_3). Retrieved from http://ebookcentral.proquest.com

Baca, U. G. (2016). Introducción a la seguridad informática. Retrieved from http://ebookcentral.proquest.com

Gómez, V. Á. (2014). Gestión de incidentes de seguridad informática. Retrieved from http://ebookcentral.proquest.com

Álvarez, M. G., & Pérez, G. P. P. (2004). Seguridad informática para empresas y particulares. Retrieved from http://ebookcentral.proquest.com

Austin, R. D., & Darby, C. A. (2004). El mito de la seguridad informática. Retrieved from http://ebookcentral.proquest.com

Chicano, T. E. (2014). Gestión de incidentes de seguridad informática (mf0488_3). Retrieved from http://ebookcentral.proquest.com

Ficarra, F. (2006). Antivirus y seguridad informática: el nuevo. Retrieved from http://ebookcentral.proquest.com

Fundación, S. Y. D. (Ed.). (2007). Informe especial: perspectivas de seguridad 2006, balance de seguridad 2005. Retrieved from http://ebookcentral.proquest.com

Correa Medina, J., & Carlos Pérez, H., & Velarde Martínez, A. (2006). Virus informáticos. Conciencia Tecnológica, (31), 54-57.

Gil Vera, V., & Gil Vera, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia Et Technica, 22 (2), 193-197.