Volumen 3, Número 7 – Abril – Junio – 2017

ISSN 2410-4019

Revista del Desarrollo Urbano y Sustentable

ECORFAN®

ECORFAN-Bolivia

Indización

Google Scholar

Research Gate

REBID

Mendeley

RENIECYT

La Revista del Desarrollo Urbano y Sustentable, Volumen 3, Número 7, de Abril a Junio-2017, es una revista editada mensualmente por ECORFAN-Bolivia. Loa 1179, Cd. Sucre. Chuquisaca, Bolivia. WEB: www.ecorfan.org, revista@ecorfan.org. Editora en Jefe: RAMOS-ESCAMILLA, María. PhD, Co-Editor: IGLESIAS-SUAREZ, Fernando. ISSN: 2410-4019 Responsables de la última actualización de este número de la Unidad de Informática ECORFAN. ESCAMILLA-BOUCHÁN, Imelda. PhD, LUNA-SOTO, Vladimir. PhD, actualizado al 30 Junio 2017.

Presentación

ECORFAN, es una revista de investigación que pública artículos en las áreas de: Desarrollo Urbano y Sustentable

En Pro de la Investigación, Docencia, y Formación de los recursos humanos comprometidos con la Ciencia. El contenido de los artículos y opiniones que aparecen en cada número son de los autores y no necesariamente la opinión del Editor en Jefe.

Como primer artículo presentamos, *Visión y propuestas de la Comunidad Universitaria sobre la gestión y manejo integral de los residuos. Caso Centro Universitario de Ciencias Biológicas y Agropecuarias (CUCBA), de la Universidad de Guadalajara*, por LOZA-LLAMAS, Juana America, ROMO-REYES, María Magdalena y BRITO-PALACIOS, Hermila, con adscripción en la Universidad de Guadalajara, como siguiente articulo presentamos, *Metodología para establecer el empaque más adecuado de las sales gourmet Huixtocihuatl*, por ESTRADA-GARCÍA Israel, MENDOZA-CANO, Sergio Farid, AVILA-BADILLO, Filimon, GUERRERO-CASTILLO, Juan, con adscripción en la Universidad Tecológica de la Huasteca Hidalguense, como siguiente articulo presentamos, *Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas*, por RAMOS-ESCALANTE, Fernando, ROMERO-ROMERO, Araceli, GASCA-LEYVA Michael y LÓPEZ-BOTELLO, Felisa Yaerim, con adscripción en la Universidad Autónoma del Estado de Morelos, como siguiente articulo presentamos, *Adición de Tule (Typha Dominguensis) al Mortero Portland como refuerzo: Estudio de las propiedades Mecanicas*, por ESPINOSA-SOSA, Enrique Esteban, PULIDO-BARRAGÁN, Eder Uzziel, LUGO-DEL ANGEL, Fabiola Erika y CRUZ-NETRO, Liz del Carmen, con adscripción en el Instituto Tecnológico de Ciudad Madero, como siguiente articulo presentamos, *Globalización y su Impacto Multidisciplinario en las Explotaciones Agropecuarias,* por NÚÑEZ-OLIVERA, José Manuel, CABRAL-PARRA, Rodolfo, NORIEGA-GARCÍA, Miguel Ángel y LOMELI-RODRIGUEZ, Sandra Eva, con adscripción en la Universidad de Guadalajara, como siguiente articulo presentamos, *El uso del cine en la enseñanza de valores y competencias ciudadanas entre grupos de infantes en situación vulnerable*, por GUTIÉRREZ-ZENTENO, Sheila Xoloxochitl, ENRRIQUEZ-GARCÍA, Roldán, GÁLVEZ-RENDÓN, Marco Antonio y GUTIÉRREZ-ZENTENO, Candida Aremí, con adscripción en la Universidad Autónoma de Chiapas, como último artículo presentamos, *Diseño de sistema de captación de agua pluvial como alternativa para el ahorro de agua potable en la UTVT*, por MARTÍN-DEL CAMPO S, Ma. Guadalupe, GONZÁLEZ-ESCOBAR, José Luis, PEDROZA-BENITEZ, Socorro y MARTÍNEZ-HIDALGO, Ana Karina.

Contenido

Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas

RAMOS-ESCALANTE, Fernando*†, ROMERO-ROMERO, Araceli, GASCA-LEYVA Michael y LÓPEZ-BOTELLO, Felisa Yaerim

Universidad Autónoma del Estado de Morelos, Av. Universidad No. 1001, Col Chamilpa, Cuernavaca, Morelos, México. C.P. 62209

Recibido Abril 18, 2017; Aceptado Junio 23, 2017

Resumen

Al hablar de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas (PyMEs), tiene como fin evaluar y mejorar la eficacia y eficiencia de una organización, los sistemas deben estar sometidos a controles de calidad y auditoría informática debido a que las computadoras y los centros de procesamiento de datos son susceptibles a los delitos informáticos, la delincuencia y el terrorismo. Conocer los aspectos que las organizaciones deben de asegurar en us procesos de negocio y nuevos proyectos en conjunto con los constantes cambios de las tecnologías de la información y comunicación, de tal forma que cubran las necesidades de sus clientes de manera eficiente y oportuna y al mismo tiempo ayude a cumplir con las disposiciones generales de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares certificando que los proveedores de las empresas aplicables además de proporcionar un tratamiento adecuado a la información que garantice su uso para los fines convenidos dentro del marco de contrato.

Información, Seguridad Informática, Auditoría Informática

Abstract

Speaking of computer security, applied to service providers of small and medium-sized enterprises, it aims to evaluate and improve the effectiveness and efficiency of an organization, the systems must be subjected to quality controls and information technology audit since computers and data processing centers are susceptible to computer-related crime, crime and terrorism. Know what organizations should ensure in us business processes and new projects in conjunction with the constant changes in information and communication technologies, so that they meet the needs of its customers in an efficient and timely manner and at the same time help to comply with the General provisions of the Federal law of protection of personal data in the possession of individuals certifying that the providers of the applicable companies also provide treatment appropriate to information that ensures its use for the agreed purposes within the framework of the contract.

Information, Computer Security, Information Technology Audit

Citación: RAMOS-ESCALANTE, Fernando, ROMERO-ROMERO, Araceli, GASCA-LEYVA Michael y LÓPEZ-BOTELLO, Felisa Yaerim. Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas. Revista del Desarrollo Urbano y Sustentable. 2017. 3-7: 16-23.

* Correspondencia al autor (Correo electrónico: Fernando.ramose@gmail.com)
† Investigador contribuyendo como primer autor.

1. Introducción

La seguridad de la información es la protección de información de una gama amplia de amenazas para asegurar la continuidad comercial, minimizar el riesgo comercial, y aumentar al máximo el retorno en las inversiones y las oportunidades de negocios, se logra implementando un conjunto conveniente de controles, incluyendo, políticas, procesos, procedimientos y funciones del hardware y software. Estos controles deben ser establecidos, implementados, supervisados, revisados y mejorados, en conjunto con los procesos de negocio para garantizar la integridad de la información y los objetivos de la organización (Escuela Colombiana de Ingeniería Julio Garabito, 2008).

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener cuatro características (Empresa Oficial de Servicios Públicos de Yumbo Colombia, 2010):

Las aplicaciones deberán estar protegidas para que la comunicación entre las bases de datos, otras aplicaciones y los usuarios se realice de forma segura, atendiendo a los principios básicos de la seguridad de la información (Integridad, Confidencialidad, Disponibilidad e Irrefutabilidad).

1.1 Justificación

La Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas (PyME), pretende servir como apoyo a las empresas en el sector público y privado, que requieran subcontratar operaciones o procesos a través de outsourcing y que mediante esta estrategia proporcionen información de Personas Físicas a terceros.

Que operen con escalas bajas de producción, utilizan tecnologías adaptadas y sean de propiedad familiar o su financiamiento proceda de fuentes propias, dedicadas a la venta, administración y producción de bienes y servicios.

1.2 Problema

La seguridad de la información y la infraestructura crítica del negocio es importante para ambos sectores público y de negocios del sector privado, funciona como un detonador para lograr el e-government o el e-business y evitar o reducir los riesgos pertinentes. La interconexión de las redes públicas y privadas y el compartir recursos de información aumentan la dificultad de lograr el control de acceso. La tendencia a la informática distribuida también ha debilitado la efectividad del control central, especializado.

La confianza que puede lograrse a través de los medios técnicos es limitada y debe apoyarse por una gestión apropiada y por los procedimientos. Identificando qué controles deben ser implementados, requiere planificación cuidadosa y atención al detalle. La gestión de la seguridad de la información requiere como mínimo la participación de todos los empleados de la organización, la participación de los accionistas, proveedores, clientes o terceras partes externas, la asesoría y consejo de especialistas en la materia también puede necesitarse.

1.3 Hipótesis

Identificar la necesidad que tienen las PyME de requerimientos de invulneravilidad, con el propósito de proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.

ISSN: 2410-4019

1.4 Objetivos

1.4.1 Objetivo General

Geerar una metodología para protección de los datos personales en posesión de los particulares, al regular y controlar su tratamiento legítimo para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

1.4.2 Objetivos específicos

- Planear y establecer estrategias de seguridad de la información de acuerdo a lineamientos principios y necesidades institucionales.
- Realizar diagnósticos y evaluaciones que garanticen la integridad de la información para identificar y minimizar los riesgos en los diferentes niveles funcionales, operativos y de sistema.

2. Marco Teórico

En la actualidad la información es considerada uno de los objetos de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación presentan un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales y en muchos casos, llegando a tener un valor superior (Academia Latinoamericana de Seguridad Informática, 2003).

Por esto y otros motivos, la sovencia de la información es un asunto tan importante para todos, ya que afecta directamente a los negocios de una empresa o de un individuo. Una de las preocupaciones de la seguridad de la información es proteger los elementos que forman parte de la comunicación. Estos elementos buscan proteger: La información, equipos que la soportan y las personas que la utilizan.

2.1. Aspectos de la Seguridad Informática

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener cuatro características (Empresa Oficial de Servicios Públicos de Yumbo Colombia, 2010): Integridad; Confidencialidad; Disponibilidad; Irrefutabilidad.

Se le llama activos a los valores para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados. Son tres elementos que conforman lo que se denominan activos:

- Información: Son los elementos que contienen información registrada, en medio electrónico o físico.
- Equipos que la soportan: Cualquier componente disponible para sustentar, almacenar y procesar información sustancial para los procesos de negocio de una entidad o procesos de negocio.
- Software: Programas de computadora que se utilizan para la automatización de procesos, es decir, acceso, lectura, tránsito y almacenamiento de la información.
- Hardware: Infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento.
- Organización: Aspectos que componen la estructura física y organizativa de las empresas.
- Usuarios: Son los individuos que utilizan la estructura tecnológica y de comunicación de la empresa y que manejan la información.

ISSN: 2410-4019

Los mecanismos de la Seguridad Informática son técnicas o herramientas que se utilizan para fortalecer los principios básicos de la seguridad de la información ya antes mencionados, y según su función se clasifican en (Universidad de las Américas Puebla, 2000):

Preventivos

Los mecanismos de prevención son un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran

Detectivos

Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema, se caracterizan por enviar un aviso y registrar la incidencia.

Recuperación

Se implementa cuando ha fallado el mecanismo de prevención y define los pasos que deben adoptarse después o durante un ataque, ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar porque tuvo lugar, a reparar el daño que causo y a implementar un plan de contingencia si existe. Tanto la estrategia de Prevención como la de Recuperación funcionan para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que pudieran ser causados.

Por otro lado; las funciones de la seguridad informática tienen mucho que ver con "donde se emplean", principalmente se consideran (Omar Alejandro Herrera Reyna, 2007):

- La función centralizada, que permite un mejor control y desempeño de las funciones de seguridad informática.
- La función distribuida, para algunas organizaciones hace más sentido distribuir la función de la seguridad ya que esto permite tener un mejor desempeño operativo a costa de menor control y desempeño.

La información es un recurso o activo que, como otros recursos importantes del negocio, es esencial en una organización y en su operación, por consiguiente, necesita ser protegida adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta interconectividad creciente, la información se expone a una variedad más amplia de amenazas y vulnerabilidades.

3. Metodología de Investigación

Se realizó un diagnóstico de los dominios y controles de seguridad que deberán ser adoptados por los terceros de las Pequeñas y Medianas empresas que almacenen o procesen información de personas físicas. El objetivo principal es definir los controles de seguridad base con los que deberán cumplir los proveedores, de acuerdo al servicio que proporcionen, los terceros deberán apegarse a las recomendaciones para lograr un ambiente seguro, estos controles deberán ser implementados por terceros considerando su naturaleza o giro, el tamaño de la infraestructura y el riesgo que represente para las PyMEs.

3.1 Evaluación de riesgos

La evaluación de riesgos es la tarea más compleja del proyecto; su objetivo es definir las reglas para identificar los activos, las vulnerabilidades, las amenazas, las consecuencias y las probabilidades, como también definir el nivel aceptable de riesgo. Si esas reglas no están definidas claramente, las PyMEs podrían encontrarse en una situación en la que obtendría resultados inservibles.

ISSN: 2410-4019

La evaluación de riesgos se realiza identificando y evaluando activos, vulnerabilidades y amenazas. Una vulnerabilidad es una debilidad en un activo, proceso, control, etc. que pueda ser explotado por una amenaza. Una amenaza es cualquier causa que pueda infligir daño a un sistema u organización. Un ejemplo de una vulnerabilidad es la falta de software antivirus; y una amenaza relacionada es el virus informático.

Pasos básicos para la valuación y el tratamiento:

- Definir y documentar la metodología y distribuirlos a todos los propietarios de activos de la organización.
- Organizar entrevistas con todos los propietarios e identifiquen sus activos y las vulnerabilidades y amenazas relacionadas. Con su respectiva evaluación de probabilidad e impacto si ocurriera un riesgo en particular.
- Consolidar los datos en una única hoja de cálculo, calcular los riesgos e indicar qué riesgos no son aceptables.
- Para cada riesgo que no sea aceptable, escoger uno o más controles de la ISO 27001 y calcular cuál sería el nuevo nivel de riesgo luego de la implementación de esos controles.

3.2 Tratamiento de riesgos

Implementar lo que se definió en el paso anterior. Lo importante es obtener una visión integral de los peligros sobre la información de su organización. El objetivo es, reducir los riesgos no aceptables, redactar un informe sobre la evaluación de riesgos que documente todos los pasos tomados durante el proceso de evaluación y tratamiento de riesgos. Luego de finalizar su proceso de tratamiento de riesgos, sabrá exactamente qué controles se necesitan, hay un total de 133 controles, pero, probablemente, no los necesite a todos.

ISSN: 2410-4019

Posteriormente la redacción del plan de tratamiento del riesgo, cuyo objetivo es definir claramente cómo se implementarán los controles de la DdA, quién lo hará, cuándo, con qué presupuesto, etc. Éste plan de implementación está enfocado sobre los controles de sus terceros (proveedores); sin el cual, usted no podría coordinar los pasos siguientes del proyecto. La siguiente etapa determina, cómo medirá el logro de los objetivos establecidos tanto para cada control aplicable de la Declaración de aplicabilidad.

3.3 ¿Cómo hacer funcionar la Metodología de Evaluación de Seguridad?

La metodología más importante son los "registros"; sin registros, resultará muy difícil probar que una actividad se haya realizado realmente, se puede supervisar qué está sucediendo, sabrá realmente si sus empleados, están realizando sus tareas según lo requerido. La dirección tiene que saber qué está sucediendo; es decir, si todo el mundo ejecutó sus tareas, si se obtienen los resultados deseados, etc. Con base a estos aspectos, la dirección debe tomar algunas decisiones importantes.Asimismo se requiere que las medidas correctivas y preventivas se apliquen sistemáticamente; es decir, que se identifique la raíz de una no conformidad, se solucione y se controle.

4. Resultados

Propuesta de cuestionario para la evaluación de seguridad informática

El cuestionario de seguridad propuesto a continuación, se basa en la utilización recomendaciones de las mejores prácticas en la gestión de la seguridad de la información de ISO/IEC 27000 (27001-27002), estos controles proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

RAMOS-ESCALANTE, Fernando, ROMERO-ROMERO, Araceli, GASCA-LEYVA Michael y LÓPEZ-BOTELLO, Felisa Yaerim. Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas. Revista del Desarrollo Urbano y Sustentable. 2017.

El cuestionario se comparte para ser completado por los proveedores, se divide en una serie de secciones independientes y aspectos particulares de la garantía de la información. La información proporcionada por los proveedores en este cuestionario será utilizada por las PyMEs para evaluar los controles de seguridad durante la Evaluación de Seguridad Informática y se utilizarán como una declaración por parte del proveedor.

4.1.1 Estructura del Cuestionario de Seguridad

El cuestionario de seguridad deberá tener una estructura clara, por lo que deberá contar con información que le permita completar el cuestionario de manera adecuada, en la primera sección se deberá poder identificar información con respecto a los controles requeridos y el dominio al que pertenecen (tabla 1).

ID	Sección	Dominio / Subdominio	Control

Tabla 1 Identificar información (controles requeridos y el dominio al que pertenecen)
Fuente: Elaboración propia 2017

Es responsabilidad del proveedor responder al nivel de implementación de cada uno de los controles, así como la descripción detallada de las medidas que se consideran para cada uno de los controles de seguridad. (Tabla 2).

Implementación			Descripción del control
SI	Parcial	NO	

Tabla 2 Nivel de Implementación
Fuente: Elaboración propia 2017

De igual forma se deberá considerar una sección para que el evaluador pueda describir los controles revisados durante la Evaluación de Seguridad Informática, así como, las evidencias que sustenten la implementación de los controles. (Tabla 3).

Comentarios del Evaluador	Evidencias Presentadas

Tabla 3 Controles del Evaluador
Fuente: Elaboración propia 2017

La información proporcionada en este cuestionario será utilizada por las PyMEs para evaluar los controles de seguridad implementados al momento de la evaluación y podrán ser consultados para cualquier trabajo que haya de realizarse.

4.1.2 Política de Seguridad de la Información (PSI)

A continuación, se ejemplifica en las tablas 4, 5 y 6 la aplicabilidad y controles de seguridad, pero esto se tiene que replicar para cada dominio de la PSI en la que se consideran 3 subdominios y 9 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles PS-100, 101, 103 y 108 considerados para cada dominio. Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. El número total de controles suma 144 entre todas las secciones, aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

PSI-100	D1.1	Administración y Soporte para la Seguridad de la Información	Existe una política de Seguridad Documentada?
PSI-101			Hay una persona que le de mantenimiento y revise la Política de Seguridad?
PSI-102			Se realiza una revisión y aprobación formal por la gerencia de las Políticas de Seguridad por lo menos anualmente?
PSI-103			Tiene procedimientos que segueen que la Política es leída por todo su personal?
PSI-104			Se proporcionan las políticas al personal por lo menos cada 12 meses?

Tabla 4 Administración y Soporte para la Seguridad de la Información
Fuente: Elaboración propia. 2017

PSI- 105	D1.2	Clasificación de la información	Cuenta con una política de clasificación de la Información documentada?
PSI- 106			Existen procedimientos que incluyan los métodos para el manejo de información de acuerdo a su clasificación?

Tabla 5 Clasificación de la Información
Fuente: Elaboración propia. 2017

ISSN: 2410-4019

PS-107	D1.3	Uso aceptable y Excepciones	Dentro de la política se cubren los requisitos de uso aceptable?
PS-108			Para las excepciones a la política se requiere hacer una evaluación formal de riesgo?

Tabla 6 Uso Aceptable y Excepciones
Fuente: Elaboración propia. 2017

5. Conclusiones

La propuesta de una Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas (PyMEs), tiene como fin evaluar y mejorar la eficacia y eficiencia de una organización, los sistemas de TI deben estar sometidos a controles de calidad y auditoría informática debido a que las computadoras y los centros de procesamiento de datos son susceptibles a los delitos informáticos, la delincuencia y el terrorismo. Sus beneficios son:

- Cuidado y mejora de la imagen pública.
- Generación de confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Genera un balance de los riesgos en TI.

Las fases que componen la metodología propuesta de auditoría informática son

- Planear, obtener y entender los procesos de negocio.
- Analizar y evaluar los controles de seguridad implementados para determinar la probable efectividad y eficiencia de los mismos.
- Aplicación de pruebas para verificar la efectividad de los procedimientos de control.
- Informar los resultados de la auditoría, con el fin de reportar las sugerencias correspondientes a las oportunidades de mejora encontradas
- Efectuar el seguimiento para evaluar el nivel del cumplimiento y el impacto de las recomendaciones realizadas.

El objetivo de llevar a cabo esta metodología es que las organizaciones aseguren que sus procesos de negocio y nuevos proyectos en conjunto con los constantes cambios de las tecnologías de información cubran las necesidades de sus clientes de manera eficiente y oportuna y al mismo tiempo ayude a cumplir con las disposiciones generales de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares certificando que los proveedores de las empresas aplicables proporcionen un tratamiento adecuado a la información que garantice su uso para los fines convenidos dentro del marco de un contrato.

Para alcanzar la Propuesta de la Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas (PyMEs), que accedan a información de Personas Físicas, es indispensable conocer la naturaleza de las organizaciones y hacer un análisis de riesgos y posibles amenazas sobre la información, identificando, analizando y diseñando controles de seguridad, ofreciendo a las empresas un estudio de su esquema de seguridad en relación a la norma ISO 27000.

6. Referencias

Academia Latinoamericana de Seguridad Informática (2009). *Unidad 1 Introducción a la Seguridad Informática. Modulo 1. Obtenido en agosto 2016* http://carolinacols.files.wordpress.com/2012/03/fundamentos-bc3a1sicos-de-seguridad-informc3a1tica.pdf

ISSN: 2410-4019

Escuela Colombiana de Ingeniería Julio Garabito (2008). *Seguridad y Protección de la Información, Introducción a los Conceptos de Seguridad de la Información*. Fascículo 2 *Obtenido en* agosto 2016. https://docs.google.com/:profesores.is.escuelaing.edu.co

Empresa Oficial de Servicios Públicos de Yumbo Colombia (2010). *Seguridad Informática. Obtenido en Agosto 2016* http://www.espyumbo.com/portalespy/index.php?option=com_content&view=article&id=78:seguridad-informatica&catid=41:notibanner

ISO 27000 (2005). *Sistema de Gestión de la Seguridad de la Información*. Obtenido en setiempre 2016. http://www.iso27000.es/sgsi.html

Omar Alejandro Herrera Reyna (2007). *Comentarios, Experiencias y Tips sobre Seguridad de la Información*. Obtenido en setiempre 2016. Candado digital, http://candadodigital.blogspot.mx/2007/10/la-funcin-de-seguridad-informtica-en-la.html#!/2007/10/la-funcin-de-seguridad-informtica-en-la.html

Portal de ISO 27002. Obtenido en febrero 2017. http://www.iso27000.es/iso27002.html

SeguInfo dominios ISO 27001 y 27002 (2010). Obtenido en febrero 2017. https://seguinfo.wordpress.com/2010/06/28/dominios-de-iso-27001-e-iso-27002/

Universidad de las Américas Puebla (2000). *Conceptos Básicos de Seguridad Informática*. Obtenido en setiempre 2016. http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf

ISSN: 2410-4019

Revista del Desarrollo Urbano y Sustentable

2410 4019
ISSN 2410 - 4019
www.ecorfan.org