SEGURIDAD Y CERTIDUMBRE EN LA EXPLOTACION DE LAS TIC EN NUESTRO CONTEXTO

Padilla Vedia Carmen Janeth[1]

[1] Docente Departamento de Informática y Sistemas. Facultad de Ciencias y Tecnología, Universidad Autónoma Juan Misael Saracho.

Dirección para correspondencia: Janeth Padilla Vedia. Calle Méndez N°1586

INTRODUCCION

Los trabajos de investigación sobre seguridad y confianza ocupan gran parte en investigaciones de otros países con un acceso diferente a las TIC.

Pero en menor proporción existen trabajos en nuestro país, sin embargo tenemos un reto que enfrentar cuando frecuentemente se escucha a través de diferentes medios la situación por la que atraviesa nuestro país con respecto a la seguridad y confianza que los usuarios tienen con respecto a la utilización de las TIC.

En este trabajo se presenta un vistazo que trata de reflejar el efecto que tienen las TIC sobre la confianza y seguridad de los usuarios tanto en instituciones privadas, públicas y sociedad en su conjunto.

INTRODUCCION

Hoy por hoy la creciente incorporación de las tecnologías de información nos hace sentir la dependencia de las organizaciones y de la sociedad en general de una tecnología absorbente y necesaria en el mundo globalizado en el que nos toca vivir. Es evidente que esta tecnología avanza a un ritmo acelerado en el que las organizaciones deben tratar de circunscribirse para permanecer en el mercado.

Siguiendo a Castell (1998), la infraestructura de la vida cotidiana se ha vuelto tan compleja y esta tan entrelazada que su vulnerabilidad ha aumentado de forma exponencial. Aunque las nuevas tecnologías mejoran la seguridad, también hacen la vida diaria más vulnerable en todo aspecto.

Esta situación nos hace pensar que cada día que pasa en nuestro medio el precio a apagar por protección es mayor, hay que considerar vivir en un sistema de cerrojos electrónicos, sistemas de alarmas y sistemas de cámaras de video y otros que se tornaran necesarios.

Las TIC en las Empresas

A nivel de empresa y de la cadena de valor se evidencia una importancia creciente del manejo del conocimiento, que es la base del uso de TIC.

En la forma en que las nuevas tecnologías son usadas por las empresas se puede diferenciar entre el uso infraestructural o genérico y el especializado. En el primer caso la tecnología soporta funciones como la comunicación audio-visual (telefonía fija, móvil o VOIP), la comunicación escrita (e-mail, SMS, chat), el acceso a datos gracias a la digitalización, almacenamiento y distribución de documentos de la empresa y la búsqueda de información en Internet.

En el segundo caso, el de uso especializado de las nuevas tecnologías, las empresas se benefician a través de soluciones que apoyan los diferentes procesos internos de su negocio y aquellos externos que lo relacionan con su cadena de valor, como ser:

En la **gestión estratégica** los directivos o dueños de las empresas pueden disponer de instrumentos que les permiten aplicar e implementar conceptos de programación y orientación estratégica del negocio, así como monitorear en todo momento, gracias a sistemas de captura automática de datos, el grado de cumplimiento de su acción empresarial con los objetivos establecidos.

- Como soporte a la gestión empresarial, la definición de su estrategia y la identificación de debilidades y oportunidades, se hace uso de sistemas de inteligencia empresarial (o business intelligence, BI). Estos sistemas analizan los datos generados por la organización y elaboran información útil para la toma de decisiones. Estos sistemas pueden también integrarse con software para la gestión de procesos (Business Process Managment).

En la **gestión financiera**, existen aplicaciones que facilitan el monitoreo de la situación económica y financiera de la empresa, así como su capacidad de generar rédito y utilidades.

Estos sistemas suelen ser muy sofisticados y dirigidos a empresas de gran tamaño, pero existen algunas soluciones que se adaptan a las necesidades de empresas medianas y hasta pequeñas.

En la **producción** se utilizan sistemas de diseño de producto y de procesos productivos del tipo CAD/CAM (Computer Aided Design y Computer Aided Manufacturing), y de desarrollo de prototipos y manufactura (Rapid Prototyping and Manufacturing – RPM), integrados con Las TIC en el desarrollo de la Pyme sistemas de monitoreo de la calidad, que reducen los tiempos y costos de producción y hacen un uso más eficiente de insumos y maquinarias.

En la **gestión de la cadena de suministro** (Supply Chain Management o SCM), las empresas disponen de aplicaciones que permiten gestionar los stock y planificar el suministro, emitir órdenes de compra, verificar las entregas, administrar la logística y gestionar la relación financiera de la empresa con sus proveedores.

La **gestión de clientes** también se beneficia de aplicaciones y soluciones basadas en la web. Con estos sistemas las empresas pueden gestionar su relación con clientes, brindar servicios post-venta, analizar las pautas de ventas, procesar facturas y gestionar pagos, comunicarse con los clientes para conocer sus intereses y preferencias, etc.

La **promoción** de la empresa, de sus servicios y productos, ya no puede hacerse sin tener una clara estrategia de mercadeo e imagen corporativa en la web. En la actualidad, es la primera vitrina de la empresa y punto de contacto importante para potenciales clientes, aún cuando no compran por Internet. La estrategia web (la cual con más frecuencia está haciendo uso de las redes sociales como Facebook o Twitter), es importante para fidelizar clientes y relevar información acerca de productos y mercados potenciales.

Cuando acompaña al **comercio exterior,** la tecnología permite procesar rápidamente documentación de aduanas para certificar origen y calidad de productos. Muchas veces una documentación completa y verificable es un requisito para acceder a ciertos mercados. Hoy en día estos procedimientos son casi siempre basados en una plataforma sobre Internet.

En el área de **recursos humanos** se usan aplicaciones para la gestión de personal, la formación y la búsqueda y selección de trabajadores para la empresa.

La infraestructura tecnológica de la empresa se torna entonces en un elemento esencial de su estrategia de digitalización y abarca tanto la creación de redes internas (por cable o inalámbricas), el uso de sistemas móviles para comunicación de voz y datos, el almacén de datos, la seguridad y el acceso a Internet.

La Innovación Tecnológica en las Organizaciones

La innovación tecnológica es la que comprende los nuevos productos y procesos y los cambios significativos, desde el punto de vista tecnológico, en productos y procesos, algunos de cuyos rasgos sobresalientes son:

- Realimentación entre la tecnología de la información disponible y la posibilidad de su aplicación general.
- La informática proporciona una extensión de las capacidades humanas, por lo que la interacción hombre- máquina adquiere gran protagonismo.
- Las aplicaciones informáticas poseen tal universalidad y globalidad que capitalizan a toda la organización y sus actividades, internas y de relación.

- No parece existir la próxima estabilización de la innovación tecnológica , lo que supone un permanente ciclo de innovación
- La tecnología crea tantos o más problemas que los que resuelve

Innovaciones incrementales y su aplicabilidad: Son aquellas que producen cambios en tecnologías ya existentes para mejorarlas, pero sin alterar sus características fundamentales.

Ocurren con frecuencia en las actividades de producción y corresponden a mejoras en los procesos productivos existentes, atribuibles fundamentalmente al personal encargado de la producción y no tanto a una actividad deliberada de Investigación + Desarrollo (I + D). Son el resultado de “Aprender haciendo” y “Aprender usando”.

- Cambios en los sistemas tecnológicos: Son combinaciones de innovaciones radicales e incrementales, que unidas a innovaciones en actividades organizativas y gerenciales, provocan efectos en diferentes esferas de la producción o permiten el surgimiento de otras; dando lugar a mejorar la producción con elementos tecnológicos apropiados y aplicables.

- Cambios en los paradigmas tecnológicos: Son los que han promovido las revoluciones industriales y corresponden a tecnologías o cambios en los sistemas tecnológicos, cuyo amplio espectro de aplicación afecta las condiciones de producción de todos los sectores de la economía.

Medidas y Hábitos de Seguridad

Las medidas y hábitos de seguridad definen el nivel de riesgo que asume el usuario. Para minimizarlo es indispensable observar una serie de medidas, además de mantener unos hábitos en el tiempo. De esta forma se minimiza el riesgo y los peligros asociados a las nuevas tecnologías.

Medidas automatizables y no automatizables: nivel de implantación y evolución

En función del nivel de participación del usuario, las medidas de seguridad se clasifican en automatizables y no automatizables.

- Las medidas automatizables o de carácter pasivo son aquellas que, por lo general, no requieren una actuación específica por parte del usuario, o cuya configuración permite una puesta en marcha automática. En general, se podrían considerar herramientas de seguridad en sentido estricto.
- Las medidas no automatizables o de carácter activo requieren la participación del usuario para su funcionamiento. Más que de herramientas, se trata de acciones llevadas a cabo por el usuario que redundan en una mayor seguridad (por ejemplo: utilización de contraseñas, realización de copias de seguridad, partición de disco duro, etc.).

Desarrollo económico y seguridad

Debemos tener claro que es imposible mantenerse al margen de la globalización las cambiantes dependencias de la tecnología que afectan la economía y el medio ambiente, Sin seguridad no podrá haber un desarrollo económico sostenible. Y la situación en nuestro país nos demuestra que la pobreza permanente de amplios sectores de la sociedad atenta a su vez contra la estabilidad estatal. La dependencia de las organizaciones respecto de la información y de los sistemas que la administran, la archivan y transportan es evidente con el fin de lograr sus propios fines ya sean estos públicos o privados, utilizan de forma rápida y creciente los activos relacionados con la información y los sistemas informáticos.

Algunos autores hacen mención al término nueva economía cuando hacen referencia al sector productivo que surge de la producción y explotación de las tecnologías de información y comunicaciones.

Pero en lo que a la seguridad de la información se refiere , la frontera entre las nuevas actividades productivas y las restantes no aparece claramente por cuanto el uso de las tecnologías de información y comunicaciones son empleadas de acuerdo a sus actividades productivas, independientemente si son físicamente tangibles los productos resultantes.

En el ámbito de la economía la información puede ser considerada como una nueva materia prima esencial para los procesos involucrados en las actividades productivas.

Sin embargo es necesario prestar atención y trabajar las cuestiones de confianza y seguridad para los usuarios, considerando estos atributos en las aplicaciones que garanticen la intimidad, protejan de problemas ya que los consumidores necesitan sentirse seguros de que las empresas no violan la intimidad y que no usan la información con otros fines; porque en nuestro medio tenemos una sociedad culturalmente diferenciada y en algunos sectores poco flexibles.

El recelo en nuestro medio con respecto a las tecnologías de información es frecuente sobre todo cuando se plantea la cuestión de confianza en los ordenadores y dispositivos relacionados. Es comprensible este aspecto, ya que frecuentemente se escucha por diferentes medios las noticias relativas a la falta de incorporación de medidas de seguridad en el uso de medios tecnológicos que originan susceptibilidades en algunos directivos y ejecutivos de las organizaciones.

Los profesionales informáticos dedicados a la seguridad son los que deben alertar a cerca de los riesgos que pudieran no estar controlados en los medios tecnológicos a fin de mejorar la confianza y seguridad de la información manipulada a través de las tecnologías e información y comunicación.

La seguridad debiera abarcar claramente en nuestro país desde el gobierno y sus diferentes niveles incorporando políticas de seguridad a ser aplicadas en los diferentes niveles políticos, económicos, social y ser aplicadas en organizaciones públicas, privadas, académicas y otras. Sin embargo la generación y la permanencia de la confianza es un fenómeno complejo que tiene más que ver con la percepción del usuario de la seguridad que con la protección rigurosamente demostrable.

La dependencia respecto de la tecnología de la información, y la necesidad de un desarrollo sostenido de la sociedad de la información reclama establecer fundamentos sólidos de esa confianza. Lo que significa aplicar salvaguardas o defensas técnicas y administrativas para controlar el riesgo; así como disponer de legislación que sirva para marcar las reglas del juego, disminuir las discrepancias y castigar el delito. Se trata de actuaciones complejas en sí mismas, pero no es posible demorarse en su establecimiento. Solo así se podrá aprovechar efectivamente y de forma tranquila los recursos y las oportunidades que la sociedad de la información ofrece a las relaciones económicas o personales.

La realidad nos dice que no podemos abarcar todo, sin embargo podemos investigar y analizar el contexto tecnológico en nuestro país y a partir de ello conociendo lo que se está haciendo en el mundo asimilarlo para poder aplicar en nuestras organizaciones.

Una Empresa innovadora debe comprender tres elementos fundamentales:

- Eficiencia
- Competitividad
- Calidad

Nuestro país en cuanto a las innovaciones tecnológicas de acuerdo al informe de ranking sobre la utilización de las TIC para potenciar el crecimiento económico y la competitividad en un total de 142 países desarrollados y en vías de desarrollo se encuentran liderados por los países nórdicos.

En concreto Suiza se hace con el primer puesto de esta lista gracias a que su rendimiento es excepcional en todos los aspectos, tanto en términos de utilización a nivel personal y empresarial de las TIC, como de contenidos digitales o infraestructura.

Mientras que nuestro país ni siquiera es tomado en cuenta en ninguna estadística y sólo sea mencionada como la más atrasada y pobre, la figura es clara, las principales instituciones no están dirigidas de acuerdo a las competencias requeridas por el área. En el caso de la Ciencia y la Tecnología es necesario trabajar e invertir en proyectos realmente aplicables a nuestra realidad, por ejemplo considerar el acceso a banda ancha o considerar la escases de capacitación de una buena parte de la población para hacer uso de las TIC con confianza y seguridad permitiendo modificar el ranking que se tiene de conectividad por internet, Bolivia se sitúa en el puesto 120 entre 148 países evaluados.

Desde la perspectiva de la región latinoamericana, el país se encuentra en el antepenúltimo lugar, solo por encima de Nicaragua (124) y Haití (143).

Según Chuquimia, (2014), del colectivo "Más y Mejor Internet", el lugar que ocupa el país se explica porque la cobertura es muy pobre en el país. Según el INE, solo el 1% de las viviendas del área rural tiene acceso al servicio de internet y solo un 9% de las poblaciones urbanas. En cambio, un 30% de los hogares del país cuenta con acceso a una computadora.

"El primer elemento es que si bien el Gobierno está enfocado en mejorar la cobertura a través del satélite (Túpac Katari) hacia los sectores rurales, esto es insuficiente cuando se trata de hablar de la calidad del servicio", señaló Chuquimia

Es importante analizar el contexto donde el cambio no será trascendente mientras no mejoremos la forma de educar en el uso apropiado de las tecnologías de información y comunicación, considerando que la mayoría de la población no está preparada para hacer uso de la tecnología. No solo es de tener acceso, sino de formar hábitos correctos de consumo en la que se vea el uso de las TIC como un beneficio y no un gasto.

Ante esta situación es importante que el comité Plurinacional de Tecnologías de Información y Comunicación **(COPLUTIC)** se enmarca en el Artículo 9 en su numeral IV en el que menciona “principios de la descolonización del conocimiento, la seguridad informática, la soberanía tecnológica del Estado Plurinacional y el uso de software libre y estándares abiertos”.

También es importante que el Consejo sectorial de Telecomunicaciones y Tecnologías de Información y Comunicación (COSTETIC) participe activamente en el marco del Artículo74 de la Ley No 164.

Seguridad en la utilización de las TIC

Las cuestiones básicas tratan que hay que proteger, que es proteger, contra que, y cuanto invertir en protección.

Lo que hay que proteger son los activos, es, la información y otros recursos de la organización relacionados con ella, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Para conseguir la seguridad de dichos activos en especial de la información hay que atender cuatro sub estados o aspectos de dicha seguridad relacionados con la autenticación, confidencialidad, integridad y disponibilidad (ACID).

Los activos han de ser protegidos frente a las amenazas, que son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales.

La protección ha de ser proporcionada a los riesgos siempre hay una traducción económica del riesgo que puede asumir o aceptar una organización o usuario. Las medidas de seguridad se miden también en términos económicos.

Es importante considerar que los usuarios son el punto más vulnerable en la cadena de seguridad, ya que su desconocimiento de unas buenas prácticas de seguridad puede ocasionar incidentes que ponen en riesgo la confidencialidad e integridad de información sensible. Razón por la cual la capacitación a los trabajadores de cualquier empresa (independientemente de su tamaño o actividad) debe ser constante para reducir actuaciones que pueden provocar un problema de seguridad para la protección de los activos de cualquier empresa, mostrando la forma más correcta de actuar ante una selección de las situaciones más habituales en nuestro trabajo diario.

Algunas recomendaciones a considerar para proteger la información en las organizaciones de nuestro país:

- La probabilidad de daño causado por una violación que incluya datos personales se reduce considerablemente si una organización reduce la cantidad de datos de carácter personal que utilice, recaude, y guarde.
- Las políticas y las tecnologías deben ponerse en práctica para proteger la información confidencial de la empresa. Estos controles tienen que garantizar la capacidad de obtener información sobre la red, así como la oportunidad de manejar los datos que entran y salen de la empresa. Si bien las políticas y la tecnología son ciertamente una parte crítica de cualquier programa de Seguridad de la Información, estas medidas por sí solas no pueden ofrecer la suficiente seguridad en la práctica.
- La concienciación de los riesgos, y las protecciones disponibles son la primera línea de defensa para la seguridad. Los empleados son el perímetro real de la red de la organización y su comportamiento es un aspecto vital de la seguridad. La protección de las organizaciones comienza con asegurarse de que los empleados comprendan sus funciones y responsabilidades en la protección de los datos sensibles y la protección de los recursos de la empresa, y ayudar a la organización en el mantenimiento de los equipos y de seguridad de la red.
- La globalidad, generadora de formidables fuerzas productivas, engendra también formas de delito también globales, que amenazan seriamente en nuevo contexto que surge de la revolución de la información.

El precio de la no seguridad en nuestro país

Este aspecto es crucial ya que en nuestro medio se escuchan diversas justificaciones dentro de los ámbitos empresariales con o sin fines de lucro para la no implantación de medidas de seguridad sobre todo preventivas por el hecho de significar un costo adicional a la adquisición e implantación de las tecnologías de información y comunicaciones , lo que es difícil de entender a pesar de las constantes noticias que pasan por diferentes medios de comunicación, a la vez que se trata de comprender la situación económica de muchas instituciones que operan en nuestro medio y que hacen pensar en incorporar políticas que incentiven a la incorporación de medidas de seguridad.

Motivos alegados para no utilizar medidas de seguridad

El desconocimiento del uso apropiado de las TIC en nuestro país por un buen porcentaje de la población sobre todo en el área rural se convierte en una barrera principal para que los usuarios no apliquen las medidas de seguridad automatizables (excepto en el caso de los programas de control parental y antivirus, que se usan con más frecuencia en el área urbana). Cabe destacar que es probable que estas funcionalidades las encuentre ya en su sistema antivirus, puesto que la tendencia de la industria hoy en día es aglutinar en un solo producto (que históricamente se sigue llamando antivirus) varias protecciones que previenen contra peligros más actuales.

También la sensación de que este tipo de medidas entorpecen el trabajo es habitual entre los usuarios que no implementan estas herramientas.

De nuevo el desconocimiento es la razón principal para no eliminar los archivos temporales y cookies o para no particionar el disco duro. La intención de no utilizar contraseñas, alegando no ser necesarias.

Recomendaciones básicas de seguridad en el internet

A continuación se ofrece una visión del nivel de adopción de hábitos seguros en la utilización de Internet, agrupándose en 6 categorías:

- Navegación por Internet;
- Correo electrónico
- Chats y mensajería instantánea
- Banca en línea y comercio electrónico
- Redes peer to peer
- Redes sociales.

Navegación por Internet

Analizar, manual o automáticamente, con un antivirus todo archivo que se descarga de Internet antes de abrirlo / ejecutarlo.

Correo electrónico

La popularidad y facilidad de uso del correo electrónico lo ha hecho objetivo número uno de atacantes y estafadores.

- No responder a correos electrónicos sospechosos de ser falsos ni a cadenas de correo.
- No descargar y abrir ficheros adjuntos a correos electrónicos procedentes de desconocidos, o que yo no haya solicitado
- Analizar todos los ficheros adjuntos en el correo electrónico con un antivirus antes de abrirlos.
- Borrar el historial de destinatarios cuando reenvío un correo electrónico a múltiples direcciones.

Chats y mensajería instantánea

Aunque está perdiendo fuerza frente a las redes sociales, sistemas de chat y mensajería instantánea siguen siendo populares entre los usuarios de Internet.

- Nunca facilitar datos confidenciales (contraseñas, nombre de usuario
- Evitar pinchar en invitaciones a visitar sitios web que proceden de desconocidos.
- Rechazar las invitaciones / mensajes de usuarios que no son conocidos de los que no quiero recibir mensajes
- Borrar los ficheros adjuntos que no fueron solicitados por mensajería instantánea.

Banca en línea y correo electrónico

- Cerrar la sesión al terminar de realizar operaciones online con el banco.
- Evitar el uso de equipos públicos o compartidos (cibercafés, estaciones o aeropuertos)
- Vigilar periódicamente los movimientos de la cuenta bancaria en línea.
- No facilitar al banco cuando pide los datos personales o contraseñas por correo electrónico o por teléfono.
- Para realizar transacciones en línea (pagos, compras, transferencias) comprobar el uso de una conexión segura (protocolo https, validez y vigencia del certificado).

Redes

- Analizar con el programa antivirus todos los archivos descargados a través de redes P2P.
- No compartir todos los archivos que tengo en mi ordenador con el resto de usuarios P2P
- Hacer funcionar el programa de P2P con un usuario con permisos limitados.

Redes Sociales

- El uso de las redes sociales es una realidad cada vez más frecuente entre los internautas en nuestro país
- El perfil de usuario de las redes sociales almacenan habitualmente datos personales que requieren que se aplique una privacidad adecuada de ahí que solo debe ser visto por contactos conocidos
- Estas acciones también comprometen a otros actores que tienen influencia a la hora de garantizar la seguridad de la información:
- Desarrolladores de software, que deberían programar aplicaciones fiables, seguras y exentas de vulnerabilidades.
- Empresas antivirus y desarrolladores de software de seguridad, encargados de suministrar soluciones de seguridad a los usuarios finales.
- Proveedores de Internet, responsables de administrar las redes que los usuarios emplean para conectarse a Internet.
- Entidades de registro de dominios y reguladoras de nombres, que tienen el poder de desactivar dominios maliciosos.

Conclusiones

Algunos indicadores de la gestión 2012 son la penetración de telefonía fija 7,74%, la penetración en telefonía móvil 92,26%, en banda ancha fija 0,65% (65.869 accesos), en banda ancha móvil 3,91% (320 mil accesos) y en televisión por pago 1,43%. El informe plantea que el país carece de una agenda digital, aunque advierte que sí tiene un plan de e-gobierno gestionado por la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia y el Programa Satelital “Tupak Katari”.

"Bolivia presenta –dice un compendio de la situación mundial– los niveles más bajos de penetración de banda ancha fija, que no alcanzan 2% de la población, lo que contrasta con los altos niveles de penetración alcanzados por países desarrollados como Dinamarca, con cerca de 40% de la población atendida con banda ancha fija".

Con base en distintos indicadores, Bolivia está en el puesto 106 del ranking mundial de los sistemas de e-gobierno, cuando el promedio regional es 56,55. Entre los países de la región, Bolivia ocupa el puesto 16 entre similar número de estados. El índice integral de desarrollo TIC 2013 contiene información sobre las dimensiones institucional, económica, de infraestructuras y de capital humano.

Las fortalezas del país están en el fuerte crecimiento de la penetración en telefonía móvil, el alto porcentaje de usuarios de internet y desarrollo de la industria satelital propia, mientras que las debilidades son una insuficiente normativa, baja asequibilidad de los servicios y menores penetraciones y escasa tecnificación/conectividad en los hogares respecto al resto de países, insuficiente desarrollo de las infraestructuras móviles, reducido ancho de banda internacional por usuario de internet, falta de infraestructuras locales para internet, industria TIC poco desarrollada traducida en bajo volumen de exportaciones de bienes y servicios y en consecuencia también existe un reducido desarrollo de seguridad y confianza en la sociedad de la información.

BIBLIOGRAFIA

Arroyo, L. (2005). Internet en las PyMEs. Edición Electrónica Gratuita. Texto completo en: www.anetcom.es/servicios/respdescargas.asp

Acevedo, C. (2009). Plan Estratégico para la Unidad de Transferencia de Tecnología de la FCyT. Trabajo de grado, Facultad de Ciencias y Tecnología, UMSS, Cochabamba-Bolivia

Ameconi, O. (2004). Microempresas en Acción PyMEs, 1ª Edición, Ed. Macchi, Buenos Aires-Argentina.

Castells M (1998). Estado de Red

CEPAL. (2005). Documentos de proyectos Tecnología de información y las comunicaciones (TIC) para el fomento de las pymes exportadoras en América.

Chuquimia, M. (2014). Activistas del colectivo Más y Mejor Internet para Bolivia (MMIB),

Guaipatín, C. (2003) Observatorio MIPYME: Compilación Estadística para 12 Países de la Región. Inter-American Development Bank, Washington, D.C., abril.

Infocomm Development Authority (IDA) (2004), Executive Summary of Annual Survey on Infocomm Usage Businesses for 2003," Singapore, junio.

Instituto Nacional de Estadística, Geografía e Informática (INEGI) (2001). Micro Pequeña, Mediana y Gran Empresa. Censos Económicos 1999. Estratificación de los Establecimientos. México, Diciembre.

Guillent, C. (2007). Las TICs en la Estrategia Empresarial. Edición Electrónica gratuita. Texto completo
www.anetcom.es/servicios/respdescargas.asp

Medisan 2000; 4(4):3Fernando Maciá, Web 2.0 y comercio electrónico: la nueva ventaja competitiva, 8/5/2009, publicado en http://www.fernandomacia.com/web-20/web-20-y-comercio-electronico-la-nueva-ventaja-competitiva/

http://www.inteco.es, Protocolos y Seguridad en Red, Herrero M, López A.

Regalado R. y otros: (2007) Las MIPyMES en Latinoamérica, Edición electrónica gratuita. Texto completo en:www.eumed.net/libros/2007b/274/

Vidaurre G., (2005). Análisis del Desarrollo Empresarial en las MiPyMEs y utilización de las TICs, Documento de Trabajo No 5. Cámara de Industrias, La Paz, Bolivia.

Artículo Académico

Recibido: 29 de septiembre de 2015
Aprobado: 8 de octubre de 2015