IMPACTO DE LA CONFIDENCIALIDAD EN LAS BASES DE DATOS DE LAS APLICACIONES DE COMERCIO ELECTRÓNICO (E-COMMERCE)

**CHRISTOPHER JIMÉNEZ**

**JOMEL MCDONALD**

**CAROLINA VALDÉS**

**JOSE LUIS RIASCOS**

1Licenciatura En Desarrollo De Software – Campus Dr. Víctor Levi Sasso – Universidad Tecnológica De Panamá

Resumen- La confidencialidad de la información es uno de los puntos esenciales a destacar cuando hablamos de seguridad informática. Ella representa una parte fundamental de lo que conlleva lograr que un sistema sea más seguro o menos vulnerable. A través de este artículo, se analizará de forma teórica y práctica, los conceptos que sustentan las formas viables para la protección y confidencialidad de la información del usuario, en aplicaciones orientadas al comercio electrónico.

Palabras claves- confidencialidad, confianza, información, seguridad.

Abstract– The confidentiality of information is one of the essential points to highlight when we talk about computer security. It represents a fundamental part of what means make a system safer or less vulnerable. Through this article, will be analyzed in a theoretical and practical way, the concepts that support the viable ways for the protection and confidentiality of user information, in applications oriented to electronic commerce.

Keywords**–** confidentiality, trust, information, security.

1. Introducción

La confidencialidad de la información es uno de los puntos esenciales a destacar cuando hablamos de seguridad informática. Ella representa una parte fundamental de lo que conlleva lograr que un sistema sea más seguro o menos vulnerable. A través de esta investigación, se expondrá de forma teórica y práctica, conceptos que sustentan formas viables para la protección y confidencialidad de la información del usuario, en aplicaciones orientadas al comercio electrónico. Apreciando también, diferencias en tanto a ventajas y desventajas de poseer un buen mecanismo para mantener de forma segura datos personales, como también los posibles riegos al no tenerlo.

En el Capítulo 1, se habla sobre el tema y objetivo principal de este texto, sobre el problema al cual nos estamos enfrentando y las restricciones que tenemos para poder resolverlo, como también la forma de cómo se va a puntualizar, apuntando a una mejor comprensión hacia el lector.

Más adelante, se especificará con detalle en el Capítulo 2, la presencia de antecedentes e investigaciones afines a este tema, como también el surgimiento y posibles implementaciones de soluciones propuestas a lo largo del estudio dado hacia éste. Seguido de esto, en el Capítulo 3, específicamente en el Marco Metodológico, se habla acerca de los procesos, forma e implementación del mecanismo elegido y requerido a solventar el planteamiento del problema, detallando los algoritmos y tipos de criptografía utilizados en la metodología. Al final de dicho capítulo, se demuestran los resultados esperados a través de las implementaciones en ejemplos prácticos y puntuales, con el objetivo de llegar a una conclusión a través de los hechos.

Luego de haber presenciado todos los capítulos, se podrá verificar y consultar las fuentes bibliográficas y referencias de cada uno de los conceptos introducidos para apoyar el contenido de algunos de los capítulos de los cuales requerían de información externa.

Justificación y Limitaciones

En la actualidad, los comercios electrónicos con sitios web o aplicaciones móviles, le es más conveniente que los usuarios se autentiquen o se registren en sus bases de datos. El motivo de esto es garantizar el seguimiento, comodidad y seguridad de los datos de los clientes.

Debido a esto, las empresas deben brindarle la mayor confianza y confidencialidad de la información de sus usuarios, ya que, hablamos de aplicaciones en donde hay flujos de efectivos, cuentas de ahorros, validaciones de tarjetas de crédito y más aún cuando el negocio de éstas es a través de las compra y ventas de artículos en línea. Muchos usuarios de generaciones pasadas no confían en brindar sus datos para lo que sería un registro en algún sistema, como su contraseña, números de tarjetas o cuentas de ahorró para poder realizar alguna transacción de manera electrónica y por Internet. También pueden llegar a desconfiar en los administradores de dichos sistemas.

Por ende, como justificación a este proyecto, proponemos que las empresas deben implementar mecanismos para cifrar y salvaguardar la confidencialidad de toda información de sus clientes y sin tenerla comprometida hacia externos.Para este tema, tenemos algunas limitantes o restricciones a implementar los resultados de este proyecto:

• El sector orientado a aplicar estos mecanismos de seguridad sería en el mercado de Comercio Electrónico (e-commerce)

• La tecnología que tendrá un mayor efecto sobre esta investigación es en los dispositivos móviles.

• En primer lugar, y como experimentación, se pondrá a prueba la implementación en la autenticación de una aplicación móvil dirigida a compras y venta por internet.

• La implementación se hará de forma local, en una base de datos interna como prueba de los resultados.

La idea de todo esto, es que los desarrolladores y analistas funcionales de sistemas, tengan en cuenta que la imparcialidad y confidencialidad es algo que no se puede negociar en la industria de los comercios electrónicos y posiblemente en cualquiera. La confianza de un cliente radica en la seguridad e integridad de sus datos personales en un sistema el cual el pueda acceder, permitiendo el ingreso de contraseñas, tarjetas y otros medios de identificación financiera, sin miedo a que algo o alguien, tenga acceso o atente contra la integridad de algunos de estos.

Antecedentes investigativos

Existen diversos trabajos investigativos acerca de la confidencialidad en las bases de datos de las plataformas de e-commerce, muchas de estas datan de los años 80’s, cuando los primeros bancos empezaban a poner en disposición dichos servicios y se lanzaban los primeros sistemas de compras en línea. Para nuestro trabajo de investigativo, tomaremos en cuenta aquellas investigaciones realizadas desde el año 2000, que es cuando surgen las plataformas m-commerce(comercio electrónico usando el teléfono móvil).

Entre los antecedentes investigativos de la confidencialidad en las bases de datos en el mundo e-commerce y m-commerce, hemos seleccionado los siguientes, para fundamentar nuestra investigación:

• Privacidad y protección de datos: un análisis de legislación comparada. “El trabajo presenta un análisis de la privacidad y protección de datos desde la perspectiva del comercio electrónico. Se presentan los principios y las garantías de protección de datos que deben prevalecer y su aplicación e interpretación en un ambiente de comercio electrónico.” (Mok, 2010)

• Customer’s Information Security Management System in E-commerce. (Yazdanifard, Kar Hoe, Rabiul Islam, & Pouya Emami, 2011). El artículo nos propone un Sistema para la gestión de seguridad de la información del cliente en el comercio electrónico.

• Database Security and Confidentiality: Examining Disclosure Risk vs. Data Utility through the R-U Confidentiality Map. (Duncan, Keller-McNulty, & Stokes, 2004). Este reporte técnico trata de la seguridad y confidencialidad en las bases de datos, examinando el riesgo de divulgación frente a la utilidad de datos a través del mapa de confidencialidad R-U (diagrama x-y en el plano cartesiano, donde la vertical corresponde al riesgo de divulgación y la horizontal responde a la utilidad de los datos).

• Comercio Electrónico y Protección de Datos. Este artículo de revista, desde un punto de vista legal fundamenta que: “La contratación electrónica permite realizar contratos relativos a la prestación de bienes y servicios con ventajas evidentes: mayor competitividad, reducción de costes y mayor celeridad en las relaciones comerciales.” (Clemente, 2013). Junto a estas ventajas, han de señalar que “el nuevo sistema contractual plantea problemas que afectan a la protección de los derechos de los consumidores. Por eso es necesario definir los límites de acceso a la intimidad y el respeto a los derechos de la persona humana” (Clemente, 2013).

Vulnerabilidades más comunes

Las infracciones de seguridad de las transmisiones por Internet y las bases de datos permiten el uso no autorizado de información confidencial de los clientes (por ejemplo, nombre, dirección, contraseña, seguridad social y números de tarjetas de crédito) y a menudo resultan en robo de identidad. (Yazdanifard, Kar Hoe, Rabiul Islam, & Pouya Emami, 2011). El mejoramiento de las técnicas de estafas y suplantación de identidad han aumentado y cada día afectan a más internautas. Una transacción básica a través de una plataforma e-commerce da al proveedor acceso a datos personales, como dirección, número de teléfono y detalles financieros.

a. La necesidad de brindar información personal

Las telecomunicaciones permiten a los proveedores recoger, analizar, almacenar y usar la información con gran facilidad y eficiencia. Su uso meramente comercial puede propiciar la utilización en otros ámbitos sociales y con otras finalidades, por lo que se pone de relieve el nacimiento de un nuevo problema en el tratamiento y respeto de datos personales: la necesidad del establecimiento de mecanismos para protección en sus diferentes etapas. Esto es, desde la recogida, pasando por el tratamiento y almacenamiento, hasta su posible cesión a terceros; y todo ello con independencia del soporte en que se encuentren. (Clemente, 2013).

El comercio tanto en su forma tradicional como electrónica exige la identificación de cualquier individuo que participe en una transacción; la homologación en este proceso representa un serio peligro para proteger la intimidad del cliente y preservar la confidencialidad en sus datos cuando estos circulan por la red.

b. Interconexión de archivos

Existe la posibilidad de que la información de usuarios esté interconectada desde la creación de su perfil para conocer con detalle todas las transacciones que realiza o llevar un seguimiento de donde se encuentre ubicado.

“La interconexión de bases de datos permite la recopilación masiva, instantánea e indiscriminada de datos sobre una persona desde cualquier parte del mundo. Es fácil incorporar información personal en bases de datos y transferirla a terceros u otras bases de datos ubicadas en cualquier parte del mundo” (Mok, 2010). Adicional esta información puede ser unificada y compilada en un instante, con el fin de obtener datos personales, de vivienda, árbol familiar, información laboral, financiera, médica, ideológica, académica, policiaca, así como información de las afinidades del cliente: pasatiempos, hábitos, viajes, comunicaciones, ente otros. Es totalmente fácil, previa o no autorización de un proveedor, que terceros obtengan información excesiva sin que el usuario lo haya autorizado o sea notificado de esta acción.

c. La autorización para el almacenamiento de cookies

Existen diferentes mecanismos de seguridad que adoptan las plataformas de e-commerce en sus bases de datos para salvaguardar la información de sus clientes, pero existe una vulnerabilidad mayor: “el consumidor puede fijar el nivel de seguridad de los “cookies”, y lo cierto es que, la mayoría de los consumidores, no tienen conocimiento sobre ellos, por lo tanto, aceptan niveles bajos de protección de “cookies” sin conocer lo que son, ni sus implicaciones.” (Mok, 2010).

“Almacenar las cookies en la actualidad representa un beneficio para los sitios web, y mejora significativamente la experiencia del usuario en el sitio, pero en las prácticas ilícitas es donde reside la invasión de la intimidad del usuario y, por consiguiente, la vulneración de la confidencialidad. Además, una vez obtenidos esos datos de forma ilícita, el consumidor no podrá nunca controlar el fin para el que podrían ser utilizados, incluso podrían trascender el simple ámbito publicitario.” (Mok, 2010)

d. No utilización de certificados

Skyler Slade, cofundador de Coefficient, una empresa encargada del almacenamiento de datos sugiere a los dueños de sitios web e-commerce a usar certificados SSL en las páginas de pago, páginas de registro y páginas de inicio de sesión. Ya que los certificados SSL evitan que los atacantes identifiquen y detecten el tráfico web de los usuarios e imposibilitando que roben datos sensitivos como sus contraseñas e información de su tarjeta de crédito.

La utilización de certificados agrega una capa adicional de seguridad, y también le da al cliente una buena impresión, al inspirarle confianza. Gran número de los usuarios de compran en línea han aprendido a asociar las siglas "https" con los estándares más altos de seguridad. Por lo que, su implementación en un sitio probablemente generará confianza y hará que los compradores se sientan más cómodos para completar la transacción.

Medidas preventivas ante vulnerabilidades

a. Concientizar a los usuarios

Promover en los usuarios el desempeño de un rol activo en la protección de sus datos. Informarles sobre la información recopilada, enseñarles cómo detectar comportamientos sospechosos en el sitio y avisarle en caso de que algo salga mal.

b. Asumir medidas con los administradores de base de datos

Esto radica en reglamentar la forma en que se maneja o se trata la información. Por un lado tendremos que prevenir malas prácticas cumpliendo las políticas de seguridad; para ello podemos firmar acuerdos de confidencialidad, en los que los que regularemos los aspectos relativos a la seguridad y la confidencialidad de la información en la prestación del servicio, incluyendo las sanciones en caso de incumplimiento.

c. Encriptar

Siempre se deben cifrar las contraseñas y cualquier otra información confidencial a manera de precaución, en caso de que los datos caigan en las manos equivocadas.

Al almacenar datos se debe considerar la encriptación del disco duro y usar servicios de encriptación de datos en las bases donde reside la información. De ese modo, si en algún momento la información de la base de datos queda expuesta, los datos de los usuarios no se verán comprometidos.

d. Implementar sistemas que permitan detectar la intrusión

Si en la red ocurren acciones de aspecto sospechoso, como que alguien o algo que intente entrar de forma ilegal, la detección de intrusos se activará. Los sistemas de detección de intrusos monitorean de forma continua el comportamiento de la red en busca de cualquier acción ilícita y lo identifican para su revisión. Estos sistemas no solamente pueden llegar a bloquear esa acción, sino que también recopilan información sobre él y alerta a los administradores. Pero a pesar de todo esto, las brechas de seguridad se siguen dando. Es por eso que es importante tener un plan de respuesta ante una violación de datos. Hay que estar preparado para entrar en acción con un sistema eficaz, que garantice un conjunto de instrucciones para sellar la violación y todo lo que conlleva.

e. Utilización de protocolos y certificados

La red madre considerada internet es una red insegura y muchas de las transacciones e intercambio de información entre organizaciones y clientes se dan ahí. Para protegernos de que nuestra información privada quede expuesta en todo Internet, existen diferentes estándares y protocolos de cómo se envía la información a través de esta red.

Las conexiones cifradas y las páginas seguras con protocolos HTTPS pueden ocultar y proteger los datos enviados y recibidos en los navegadores. Para crear canales de comunicación seguros, los profesionales de seguridad de Internet pueden implementar protocolos TCP/IP (con medidas de criptografía entretejidas) y métodos de encriptación como Secure Sockets Layer (SSL) o TLS (Transport Layer Security).

Impacto y consecuencias de la materialización de un posible ataque

Según Kaspersky Lab y B2B International, los ataques cibernéticos han costado en promedio de 1.3 millones de dólares por empresa en 2017 en los Estados Unidos de América, un 11% más que en 2016. Para las pequeñas y medianas empresas, el costo promedio de la recuperación asciende a 117 mil dólares. Estas estimaciones incluyen tanto el costo de negocio perdido, las mejoras de software y sistemas y los gastos extra en personal interno y en asesoramiento experto. Sin embargo, el activo que más está en riesgo es la reputación corporativa. Aquellas empresas que no saben gestionar correctamente un ataque y la comunicación de este a clientes y accionistas están en peligro de sufrir una aparatosa caída de reputación. Un informe de Forbes Insights indica que el 46% de las organizaciones que han experimentado ataques también han sufrido daños en la reputación y en el valor de su marca como resultado de un ataque.

Los daños causados por los ataques, independientemente de la fuente, se dividen en dos categorías principales: la filtración de datos y la pérdida de servicio.

a. Filtración de datos

La filtración de datos siempre da lugar a noticias sensacionalistas, pues la extracción de información corporativa confidencial va a parar a manos de criminales o competidores. Los daños causados por las filtraciones de datos son visibles y muy graves. Pueden ser daños de carácter financiero (pérdida de ingresos, costos legales y normativos, costos derivados de procesos judiciales y multas), costos de imagen (pérdida de la confianza y fidelidad de los clientes) y pérdida de competitividad (como resultado de la pérdida de propiedad intelectual).

Después de sufrir filtraciones de información, las empresas se gastan cantidades enormes de tiempo y dinero en tareas de detección y corrección técnica, en la identificación y el bloqueo de ataques, así como en la valoración de los daños causados y en la aplicación de medidas correctivas. Además, los casos de filtración de datos generan una publicidad negativa que dura mucho más que el ataque en sí.

b. Pérdida de servicio

Los ataques por denegación de servicio resultan en la degradación o en la total inoperatividad de los sistemas informáticos, tanto de estaciones de trabajo como de servidores web, de aplicaciones o de bases de datos. Pero los daños colaterales en el ámbito financiero de estos daños también pueden ser catastróficos. El comercio se paraliza o se detiene por completo, lo cual repercute directamente en los ingresos. Los procesos cotidianos se interrumpen o los empleados no pueden desempeñar sus tareas porque la red está fuera de servicio.

Propuesta de solución

Las normas ISO son estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer guías relacionadas con sistemas de gestión y aplicables a cualquier tipo de organización, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización.

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento; entendiendo confidencialidad como el principio donde la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Nuestra propuesta se basa en aplicar los estándares ISO 27001, para reducir las vulnerabilidades más comunes, con el objetivo de tomar medidas preventivas, y así evitar la materialización de un ataque de impacto:

Adoptar métodos para identificar los requisitos de seguridad

Las formas sistemáticas de identificación pueden prevenir algunos aspectos de ser olvidado o pasado por alto. Los ejemplos de métodos de evaluación de las políticas y reglamentos. Modelar las amenazas o realizar revisiones de incidentes.

Especificar los requisitos de seguridad

Dentro del apartado 1.4.1.1 de la norma ISO 27001 sobre el análisis de los requisitos de seguridad de la información y especificación, establece que los requisitos para proteger la información tienen que incluirse en los requisitos del producto de software.

Evaluar los requisitos según el valor de la información para el negocio

Las personas que mejor pueden evaluar los requisitos son los que utilizan el producto. Se debe elegir a diferentes personas que tengan diferentes roles en la organización. La seguridad adecuada refleja el valor de la información para la organización, por ende, todos los requisitos deben priorizarse según con los propósitos de negocio que se encuentran destinados a protegerse.

Integrar los requisitos a la solución

Cuanto antes se tenga en consideración la seguridad, más opciones existen de tratar las situaciones de riesgo. Se piensa en las políticas y el propio proceso de desarrollo del proyecto.

Definir criterios de aceptación

En algún momento se debe demostrar que lo que se propone para el sistema realmente se puede conseguir, y que los procedimientos establecidos fueron seguidos de una manera correcta. La principal recomendación es proporcionada por el control en la norma ISO 27001, se tiene que definir todos los parámetros de una manera clara y los resultados se deben cumplir. Estas son las bases para el desarrollo de los procedimientos de prueba.

Lanzar piloto en un ambiente replicado de producción

Se tiene que llevar a cabo la mejor identificación de las distintas vulnerabilidades y la fiabilidad de dichas pruebas. Este punto puede ser crítico cuando la prueba supone la utilización de las bases de datos, ya que los datos reales de las pruebas pueden suponer riesgos para sí mismos y que no estén relacionados con el producto.

Realizar diferentes tipos de pruebas

Se tiene que establecer una rutina de actividades que se tienen que realizar con respecto a todas las entradas y las salidas. De esta manera usted puede asegurarse que la prueba se repite si sucede algún error. Las primeras pruebas que se llevan a cabo por el equipo de desarrollo son para comprobar que los requisitos de funcionamiento se cumplen. Se deben corregir de forma rápida todos los errores de código más simples. Se tiene que establecer la garantía de seguridad realizando pruebas independientes.

## *Resultados De La Implementación*

Jomel hasta aqui

2. Diseño de la Página

Una forma sencilla de cumplir con los requisitos de formato del artículo es utilizar este documento como una plantilla y escribir el texto en él.

Su artículo debe tene un tamaño de página correspondiente a A4, la cual es 210mm de ancho y 285mm de largo. Los márgenes deben configurarse de la siguiente forma:

\* Corresponding author:

Alexis.Tejedor@utp.ac.pa

Superior = 15mm

Inferior = 15mm

Izquierda = 20mm

Derecha = 15mm

Su artículo debe estar en un formato de dos columnas con un espacio de 4.4mm entre las columnas.

2.1. La estructura del artículo debe ser la siguiente

1. Título del artículo

2. Afiliación de los autores

3. Resumen en español e inglés (250 palabras máximo)

4. Palabras claves en español e inglés

5. Introducción – incluir la motivción, objetivos, una vista general, y la estructura del artículo.

6. Cuerpo principal – explicación de los métodos, algoritmos, datos usados, instrumentación (sensores, sistemas, etc.), resultados and discusión

7. Conclusiones

8. Referencias

Su meta es que el artículo cumpla con el formato establecido lo más estrechamente posible.

3. Estilo de Página

Todos los párrafos deben tener sangría. Todos los párrafos deben estar justificados.

3.1. Fuente del Texto

La fuente del texto de todo el documento debe ser Times New Roman. El tamaño de la fuente está especificado en la Tabla 1.

3.2. Títulos y Datos del/los Autor/Autores

El título y datos del/los autor/autores deben aparecer en una sola columna and centrados.

Cada palabra en el título debe ser en mayúscula, excepto palabras cortas tales como: “un”, “una”, “y”, “como”, “en”, “por”, “para”, “desde”, “si”, “dentro”, “sobre”, “o”, “de”, “el/la”, “con”.

Los datos del autor no deben mostrar ningún título profesional (e.g. gerente o director), ningún título académico (e.g. Dr.) o membresiía de ninguna organización profesional (e.g. miembro de la IEEE).

Para evitar confusiones, el apellido debe ser escrito como la última parte del nombre de cada autor (e.g. John A.K. Smith).

Cada afiliación debe incluir los siguientes elementos: unidad a la que está adscrito, entidad a la que está afiliado y el correo electrónico. El último elemento es obligatorio porque facilita la comunicación entre el autor y el lector.

**Table 1.** Especificaciones para las fuentes

|  |  |  |
| --- | --- | --- |
| Tamaño | Fuente en Times New Roman | |
| Regular | Negrita |
| 8 | Título de la tabla, centrado  Título de la figura, centrado |  |
| 9 | Afilicación de los autores, centrado  Nombres de las columnas en las tablas, centrado |  |
| 10 | Párrafo,  Cuerpo del resumen,  Cabecera de 3er nivel, justificado a la izquierda | Afiliación del autor, centrado  Cabecera de 3er nivel, justificado a la izquierda |
| 11 |  | Nombre del autor, centrado |
| 20 |  | Título del artículo, centrado |
| 12 |  | Título del resumen y palabras claces |
| 14 |  | Título de la referencia,  Título de reconocimiento, Cabecera de 1er nivel, justificado a la izquierda |

3.3. Títulos de las Secciones

No deben utilizarse más de 3 niveles de títulos (sección y subsecciones). Otros títulos (subsecciones) deben tener una fuente de 10pts excepto los títulos de primer nivel. La letra inicial de cada palabra en el título debe ser en mayúscula excepto para las palabras cortas.

Título nivel-1: un título en el nivel 1 debe estar justificado a la izquierda, fuente Times New Roman, tamaño 14ptos y enumerado con números arábigos seguido por un punto, ejemplo: ver el título “3. Estilo de Página” de este documento. Los títulos “Reconocimientos” y “Referencias” no deben ser enumerados.

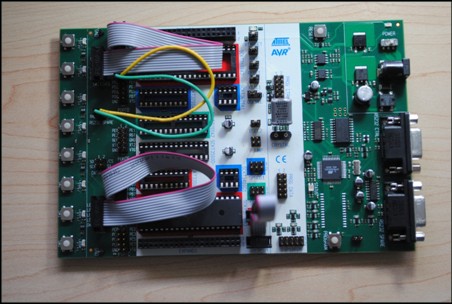
Título nivel-2: un título en el nivel 2 debe estas justificado a la izquierda y enumerado con números arábigos seguido por un punto. Por ejemplo, ver el título “3.3. Títulos de las secciones”.

Título Nivel-3: un título en el nivel 3 debe estar enumerado con números arábigos. El contenido debe seguir inmediatamente del título en un párrafo independiente.

3.4. Figuras y Tablas

Los gráficos y otras figuras enumeradas deben aparecer en el texto tan cerca de su mención como sea posible. Las figuras no deben infringir sobre los bordes de las páginas.

Las figuras y las tablas deben estar centradas en la columna. Las figuras y tablas de gran tamaño pueden estar en una columna con el objetivo de que puedan apreciarse con más claridad. Además, deben estar posicionadas en la parte superior o inferior de la página.“Figura 1.” debe ser usada, incluso al inicio de la oración.

****

**Figura 1.** Un ejemplo de un gráfico de líneas con colores que contrastan bien en pantalla como en una copia impresa en blanco y negro.

**3.4.1. Título de la figura**

Las figuras deben ser enumeradas con números arábigos y fuente regular de 8pts Regular. Los títulos de una sola línea (e.g. Figura 2) deben ser centrados, en cambio, un título multi-línea debe estar justificado (e.g. Figura 1). La mención de una figura en el texto del artículo debe realizarse antes de su aparición, tal como se aprecia con la Figura 1.



**Figure 2.** Ejemplo de una imagen con resolución aceptable.

3.4.2. **Títulos de las Tablas**

Las tablas deben enumerarse con números arábigos. Los títulos de las tablas deben centrarse con una fuente regular de 8pts. Cada palabra en el título de una table debe estar en mayúscula. La mención de una tabla en el texto del artículo debe realizarse antes de su aparición, tal como se aprecia con la Tabla 1.

3.5. Enlaces (Links) y Marcadores (Bookmarks)

Los enlaces y marcadores deben ser removidos del artículo durante el proceso de elaboración. Si usted necesita hacer referencia a un URL en su artículo, usted debe escribir completamente la dirección URL con una fuente regular.

3.6. Ecuaciones

Las ecuaciones deben enumerarse secuencialmente a lo largo del artículo. El número de la ecuación debe encerrarse entre paréntesis ubicado al margen derecho como en (1). Las ecuaciones deben escribirse en Times New Roman (por favor, no use otra fuente). Para crear ecuaciones multiniveles es necesario tartar las ecuaciones como un gráfico e insertarla en el artículo.

 (1)

4. Estilo de las Referencias

El título de la sección de Referencias no debe ser enumerado. Todas las referencias deben ser escritas en fuente de 9pts. Por favor, use estilo de letra regular como se muestra en la sección “Referencias”. Las referencias deben enumerarse secuencialmente y el número va entre corchetes (e.g. [1]).

Cuando haga referencia a una cita en el texto del artículo, por favor utilice simplemente el número de referencia, como en [2]. No utilice “Ref. [3]” o “Referencia [3]”excepto en el comienzo de la oración, e.g. “La referencia [3] muestra…”. Múltiples referencia deben enumerarse en corchetes separados (e.g. [2], [3], [4-6]).

Ejemplos de diferentes categorías de referencias mostradas en la sección de “Referencias” son las siguientes:

* Libro

e.g. Kevin R. Fall, W. Richard Stevens, TCP/IP Illustrated, Volume 1: The Protocols, 2nd ed., Addison-Wesley, USA, 2011.

* Artículo de un journal:

e.g. Mayank Suhirid, Kiran B Ladhane, Mahendra Singh, Vishwas A Sawant, "Lateral Load Capacity of Rock Socketed Piers Using Finite Difference Approach", Scientific & Academic Publishing, Journal of Civil Engineering Research, vol.1, no.1, pp.1-8, 2011.

* Artículo de una conferencia

e.g. Mohemed Almorsy, John Grundy and Amani S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework" , in Proceedings of 2011 IEEE 4th International Conference on Cloud Computing, pp. 364-371, 2011.

* Webiste:

e.g. Online Available: http://journal.sapub.org/ajb

* Tesis de maestría o disertación doctoral

e.g. A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP", M. Eng. thesis, Indian Institute of Science, India, 1999.

* Reporte Técnico

e.g. J. Padhye, V. Firoiu, D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control", Univ. of Massachusetts, Tech. Rep. 99-02, 1999.

* Estandar o norma

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

5. Conclusiones

Esta es la primera versión de este instructivo y ha sido diseñada por SAP -Scientific & Academic Publishing ([www.sapub.org](http://www.sapub.org))-. La mayoría de las instrucciones en este document han sido compiladas por SAP Productions. SAP Productions ofrece plantillas en una hoja A4 para Microsoft Word. SAP Productions ha hecho su mejor esfuerzo para asegurar que las plantillas tengan la misma apariencia.

RECONOCIMIENTOS

El título de la sección de Reconocimiento no debe ser enumerado. SAP Productions desea reconocer a todos colaboradores por desarrollar y mantener esta plantilla.

REFERENCiaS

1. Kevin R. Fall, W. Richard Stevens, TCP/IP Illustrated, Volume 1: The Protocols, 2nd ed., Addison-Wesley, USA, 2011.
2. Mayank Suhirid, Kiran B Ladhane, Mahendra Singh, Vishwas A Sawant, "Lateral Load Capacity of Rock Socketed Piers Using Finite Difference Approach", Scientific & Academic Publishing, Journal of Civil Engineering Research, vol.1, no.1, pp.1-8, 2011.
3. Mohemed Almorsy, John Grundy and Amani S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework" , in Proceedings of 2011 IEEE 4th International Conference on Cloud Computing, pp. 364-371, 2011.
4. Online Available: http://journal.sapub.org/ajb.
5. A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP", M. Eng. thesis, Indian Institute of Science, India, 1999.
6. J. Padhye, V. Firoiu, D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control", Univ. of Massachusetts, Tech. Rep. 99-02, 1999.
7. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.