Revista Científica Mundo de la Investigación y el Conocimiento

DOI: 10.26820/recimundo/4.(1).esp.marzo.2020.173-181
URL: http://recimundo.com/index.php/es/article/view/793
EDITORIAL: Saberes del Conocimiento
REVISTA: RECIMUNDO
ISSN: 2588-073X
TIPO DE INVESTIGACIÓN: Artículo de Revisión
CÓDIGO UNESCO: 33 Ciencias Tecnológicas
PAGINAS: 173-181

Las Tics como herramienta para la gestión de riesgos

The Tics as a tool for risk management

Os tiques como uma ferramenta para gerenciamento de riscos

César Augusto Pazmiño Zabala[1]; Anita Karina Serrano Castro[2]; Martha Magdalena González Rivera[3]

RECIBIDO: 20/11/2019 **ACEPTADO:** 29/01/2020 **PUBLICADO:** 05/03/2020

1. Magister en Gerencia de Proyectos Educativos y Sociales; Magister en Gerencia Educativa; Diploma Superior en Diseño de Proyectos; Diploma Superior en Gestión y Planificación Educativa; Especialista en Liderazgo y Gerencia; Arquitecto; Universidad Estatal de Bolívar; Bolívar, Ecuador; cpazmino@ueb.edu.ec; https://orcid.org/0000-0003-4481-7031
2. Magister en Gerencia de Riesgos y Desastres; Especialista en Gestión Educativa; Ingeniera en Marketing; Licenciada en Ciencias de la Educación Mención Informática Educativa; Universidad Estatal de Bolívar; Bolívar, Ecuador; aserrano@ueb.edu.ec; https://orcid.org/0000-0002-0347-1823
3. Magister en Agroecología y Ambiente; Ingeniera Agroforestal; Licenciada en Contabilidad y Auditoria; Universidad Estatal de Bolívar; Bolívar, Ecuador; mgonzalez@ueb.edu.ec; https://orcid.org/0000-0003-3211-4988

CORRESPONDENCIA
César Augusto Pazmiño Zabala
cpazmino@ueb.edu.ec

Bolívar, Ecuador

RESUMEN

Las tecnologías de la información y la comunicación (TIC) son aquellas tecnologías que facilitan la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y difusión de la información. Son desarrolladas mediante la convergencia de la informática, las telecomunicaciones, la electrónica y la microelectrónica. La Organización Internacional para la Estandarización (ISO) indica que el riesgo es la probabilidad de que una amenaza determinada se materialice, explotando las vulnerabilidades de un activo o grupo de activos, causando daño o pérdidas a la organización. Los riesgos se pueden dividir en tres categorías según el impacto ocasionado: daños a las operaciones, daños a la reputación y daños legales de la organización. Para ejecutar el análisis y posterior gestión del riesgo, se tiene que seguir un modelo que incluya algunas etapas: planificar, hacer, verificar y actuar. La metodología propuesta utiliza como base el modelo Ciclo PDCA también llamado como Círculo de Deming, constituye una estrategia de mejora continua de la calidad en cuatro pasos, también se lo denomina espiral de mejora continua y es muy utilizado por los diversos sistemas utilizados en las organizaciones para gestionar aspectos tales como calidad (ISO 9000), medio ambiente (ISO 14000), salud y seguridad ocupacional (OHSAS 18000), o inocuidad alimentaria (ISO 22000). Se aplicó una metodología descriptiva, con un enfoque documental, es decir, revisar fuentes disponibles en la red, con contenido oportuno y relevante para dar respuesta a lo tratado en el presente artículo.

Palabras clave: TIC, ISO, Riesgo, Planificar, Realizar, Verificar, Corregir, Actuar, Informar.

ABSTRACT

Information and communication technologies (ICT) are those technologies that facilitate the acquisition, storage, processing, evaluation, transmission, distribution and dissemination of information. They are developed through the convergence of information technology, telecommunications, electronics and microelectronics. The International Organization for Standardization (ISO) indicates that the risk is the probability that a given threat will materialize, exploiting the vulnerabilities of an asset or group of assets, causing damage or losses to the organization. Risks can be divided into three categories according to the impact caused: damage to operations, damage to reputation and legal damages of the organization. To execute the analysis and subsequent risk management, a model must be followed that includes some stages: planning, doing, verifying and acting. The proposed methodology uses the PDCA Cycle model, also known as the Deming Circle, as a basis; it constitutes a four-step continuous quality improvement strategy, it is also called a continuous improvement spiral and is widely used by the various systems used in organizations. to manage aspects such as quality (ISO 9000), environment (ISO 14000), occupational health and safety (OHSAS 18000), or food safety (ISO 22000). A descriptive methodology was applied, with a documentary approach, that is, reviewing sources available on the network, with timely and relevant content to respond to what is discussed in this article.

Keywords: ICT, ISO, Risk, Plan, Carry Out, Verify, Correct, Act, Inform.

RESUMO

Tecnologias de informação e comunicação (TIC) são aquelas que facilitam a aquisição, armazenamento, processamento, avaliação, transmissão, distribuição e disseminação de informações. Eles são desenvolvidos através da convergência de tecnologia da informação, telecomunicações, eletrônica e microeletrônica. A Organização Internacional de Padronização (ISO) indica que o risco é a probabilidade de uma determinada ameaça se materializar, explorando as vulnerabilidades de um ativo ou grupo de ativos, causando danos ou perdas à organização. Os riscos podem ser divididos em três categorias, de acordo com o impacto causado: danos às operações, danos à reputação e danos legais à organização. Para executar a análise e o subsequente gerenciamento de riscos, é necessário seguir um modelo que inclua algumas etapas: planejamento, execução, verificação e atuação. A metodologia proposta utiliza o modelo PDCA Cycle, também conhecido como Círculo de Deming, como base; compreende uma estratégia de melhoria contínua da qualidade em quatro etapas, também é chamada de espiral de melhoria contínua e é amplamente utilizada pelos vários sistemas usados nas organizações. gerenciar aspectos como qualidade (ISO 9000), meio ambiente (ISO 14000), saúde e segurança ocupacional (OHSAS 18000) ou segurança alimentar (ISO 22000). Foi aplicada uma metodologia descritiva, com abordagem documental, ou seja, revisando as fontes disponíveis na rede, com conteúdo oportuno e relevante para responder ao que é discutido neste artigo.

Palavras-chave: TIC, ISO, Risco, Plano, Realizar, Verificar, Corrigir, Atuar, Informar.

Introducción

La posibilidad de conexión ha permitido el desarrollo de un nuevo espacio en el cual se llevan a cabo transacciones ilimitadas que van desde el simple intercambio de información, hasta la realización de actividades comerciales. Estas posibilidades han revolucionado la vida social, cultural y económica a nivel orbital, transformando las modalidades de comunicación entre personas, la manera de hacer los negocios entre las empresas, la forma de trabajar, etc.

Adicionalmente, surgen aplicaciones específicas en diferentes ámbitos, por ejemplo, en la administración pública se permite la realización de trámites como el pago de impuestos (e-gobierno); en la salud se busca desarrollar un sistema sanitario con una cobertura independiente de la situación geográfica y horaria (e-salud); en el ámbito del trabajo se entienden nuevos esquemas de funcionamiento (teletrabajo); en la banca se ofrecen nuevos servicios (e-banca), etc.

En la actualidad, son múltiples los riesgos asociados a equipos y sistemas de información y comunicaciones que no cuenten con controles de seguridad. Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Una alarma encendida para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, ameritando la necesidad de una estrategia completa de seguridad, para prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

A continuación se explicará la repercusión de estos riesgos para las organizaciones y como minimizarlos.

Metodología

Esta investigación está dirigida al estudio del tema “Las Tics como herramienta para la gestión de riesgos“. Para realizarlo se usó una metodología descriptiva, con un enfoque documental, es decir, revisar fuentes disponibles en la red, como google académico, con contenido oportuno y relevante desde el punto de vista científico para dar respuesta a lo tratado en el presente artículo y que sirvan de inspiración para realizar otros proyectos. Las mismas pueden ser estudiadas al final, en la bibliografía.

Resultados

Las tecnologías de la información y la comunicación (TIC) son aquellas tecnologías que facilitan la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y difusión de la información. Son desarrolladas mediante la convergencia de la informática, las telecomunicaciones, la electrónica y la microelectrónica. Es un sistema tecnológico con un amplio campo de aplicación, por ejemplo: donde se requiere procesar grandes cantidades de datos, integrar las actividades industriales y de servicios, y el uso de inversiones tangibles como investigación y desarrollo, software, formación de personal, etc.

Los rasgos más relevantes de las TIC propuestos en una investigación realizada por Sánchez y González son (Sanchéz-González, Junio 2012):

Tecnologías para actuar sobre la información, sino también información para actuar sobre la tecnología.

Tienen gran capacidad de penetración y efecto en la economía, debido a que la información en un momento oportuno, genera dividendos o disminuye pérdidas o costos.

La capacidad y lógica de interconexión

que todo sistema de Tics utiliza desarrollan una interconexión rápida y barata.

Permiten el reprogramar y re-equipar a las organizaciones, ganando eficiencia.

Convergencia de tecnologías específicas para el desarrollo de múltiples área: financieras, humanas, marketing, etc.

Características de las Tics

Inmaterialidad: asociada al hecho que la materia prima es la información, generar y procesar información, es un mundo interconectado, donde toda la información se puede localizar, exponer, intercambiar, transferir, recibir, vender o comprar en cualquier lugar, en tiempo real. La economía tiene uno de sus pilares en la información.

Interactividad: permiten al usuario una interacción total: no sólo elaborar mensajes, sino también decidir la secuencia de información, establecer el ritmo, cantidad y complejidad de la información que se desea y elegir el tipo de código con el que quiere establecer relaciones con la información (Chávez, 2019).

Instantaneidad: se rompen las barreras temporales y espaciales de naciones y culturas, puesto que nuestro mundo es más pequeño e interconectado. Destaca la dificultad de los Estados y Gobiernos para controlar el flujo de información, debido a que las TIC invisibilizan las fronteras, dificultando el control y la legislación sobre el ciberespacio. La supresión de las barreras espacio temporales es la característica más valiosa desde la perspectiva educativa; favorece el aprendizaje independiente, el autoaprendizaje colaborativo y en grupo.

Innovación: busca la mejora, el cambio y la superación cualitativa y cuantitativa de sus predecesoras. Esto ocasiona un problema debido a la escasa capacidad que presenta la sociedad, o las diferentes generaciones para incorporar y asimilar las tecnologías que surgen y que pueden originar actitudes negativas, de rechazo o resistencia al cambio (Cañón, Mayo 2016).

Elevados parámetros de calidad de imagen y sonido: el objetivo de las TIC no es sólo manejar información con celeridad y poder transportarla a lugares remotos, sino que la calidad y la fiabilidad de la información sea elevada. La calidad de imagen de las Smart TVs, reproductores de Mp3/Mp4, tablets, móviles, etc., es una prueba fehaciente sobre la capacidad de equipos destinados al consumo doméstico.

Digitalización: capacidad de transformar información codificada analógicamente en códigos numéricos, facilitando su manipulación y distribución; favorece la transmisión de todo tipo de información por los mismos canales, facilitando compartir archivos, hacer múltiples copias (manteniendo la calidad) etc.

Influencia de procesos sobre productos: afectan más a los procesos que a los productos, alcanzando ciertos resultados informativos e incluso permiten un mayor desarrollo de los procesos implicados en la obtención de dichos resultados. Nuestra forma de trabajar, de estudiar o de comunicarnos se transforma, por ejemplo trabajar desde casa, equipo de trabajo de diferentes países.

Interconexión: las TIC tienen altas probabilidades de interrelacionarse de forma independiente. La unión de diferentes tecnologías conlleva un mayor impacto que las tecnologías individuales (multi direccionalidad y multi formato).

Diversidad de funciones que pueden desempeñar: desde almacenar información hasta permitir la interacción entre usuarios, incluye la incorporación de nuevos hardware (cámara, GPS, etc.) multiplica esta diversidad, siendo el ejemplo más familiar y extendido los smartphones, cuyo número de aplicaciones aumenta exponencialmente.

Riesgo informático

La Organización Internacional para la Estandarización (ISO) indica que el riesgo es la probabilidad de que una amenaza determinada se materialice, explotando las vulnerabilidades de un activo o grupo de activos, causando daño o pérdidas a la organización. Los riesgos se pueden dividir en tres categorías según el impacto ocasionado: daños a las operaciones, daños a la reputación y daños legales de la organización (Arévalo-Cedillo, Agosto 2017).

Elementos del Riesgo:

Activos de información: son cualquier elemento que contenga información; los activos forman uno de los 14 dominios que trata el estándar ISO/IEC 27002, contiene 3 objetivos de control y 10 controles, siendo uno de los objetivos de este dominio que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la gestión de riesgos. De acuerdo al estándar, los activos de información deben ser clasificados de acuerdo a la sensibilidad y punto crítico de la información que contienen o de acuerdo a la funcionalidad que cumplen y rotulados, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Amenazas: son vulnerabilidades de un activo que pueden ser aprovechadas por una o más causas potenciales de un incidente, puede ocasionar daño a los activos y por consiguiente a la organización; las amenazas son los elementos que pueden dañar o alterar la información de una u otra forma, estas generalmente pueden ser encontradas a partir de una vulnerabilidad existente. Las amenazas se pueden clasificar en varios tipos: de origen natural, del entorno, por defecto de aplicaciones, causadas por personas de forma accidental o de forma deliberada (Burgos-Campos, 2008).

Vulnerabilidades: los activos se ven afectados por una serie de amenazas; la probabilidad de que se materialice dichas amenazas y la degradación implícita a un activo es lo que se conoce como vulnerabilidad. Las vulnerabilidades deben ser expresadas en una escala numérica para poder posteriormente cuantificar su impacto, se sugiere que éstas sean identificadas y valoradas individualmente. La vulnerabilidad se puede expresar mediante la fórmula (Burgos-Campos, 2008):

$$\text{Vulnerabilidad} = \text{Frecuencia estimada Días al año}$$

Impacto: mide lo que puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando la misma se materializa sobre un activo. El valor se estima conociendo el valor de los activos y su degradación causada por las amenazas (Chicaiza, 2015):

$$\text{Impacto} = \text{Valor} \times \text{Degradación del activo}$$

Análisis de Riesgos

El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización y permite determinar la naturaleza, el costo y la protección que tiene un sistema. Al implantar este plan se debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la dirección de la organización. El riesgo se puede estimar mediante el producto entre la probabilidad de que ocurra y el impacto que causa dicho riesgo.

La Gestión de Riesgos es una disciplina que existe para hacer frente a los riesgos no especulativos, que son aquellos riesgos de los cuales sólo puede ocurrir una pérdida para la organización. Suele tener los siguientes objetivos vinculados (Altamirano, Junio 2019):

Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación.

Determinar a qué amenazas están expuestos dichos activos

Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización de la amenaza).

Llegando finalmente a un concepto medible que es el riesgo al que la entidad queda expuesta, es decir a una vulnerabilidad provocada por una amenazada.

Para ejecutar el análisis y posterior gestión del riesgo, se tiene que seguir un modelo que incluya algunas etapas: planificar, hacer, verificar y actuar, (ilustrado en la siguiente figura). La familia de estándares ISO 27000 se refiere directamente al ciclo Plan-Do-Check-Act (ciclo PDCA), conocido por la gestión clásica de calidad de Deming, que enfatiza en la necesidad de la orientación al proceso, así como la integración del planeamiento de las operaciones y la verificación constante de la implementación conforme a lo planificado (Cañón, Mayo 2016).

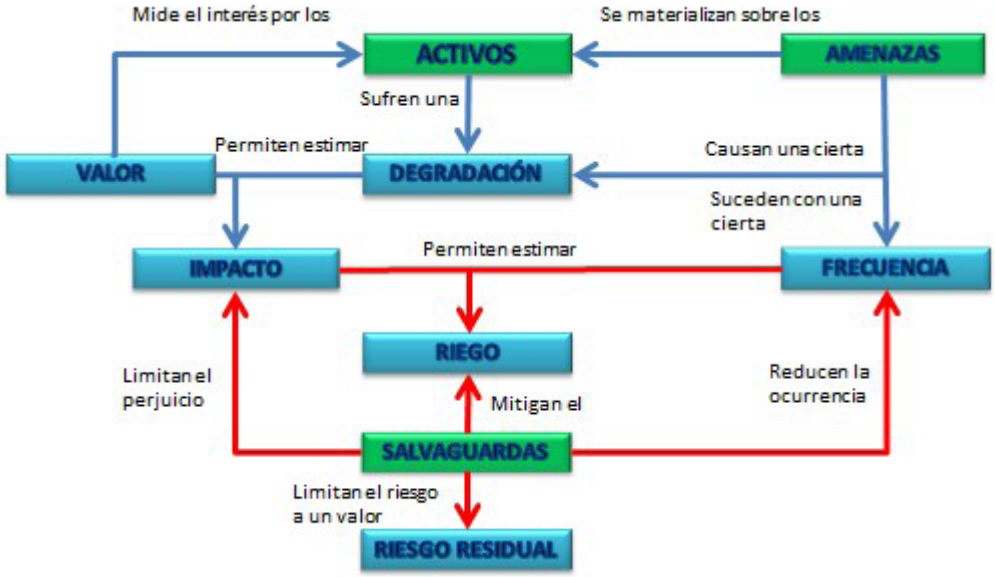

Grafico 1. Flujograma de Riesgo

Fuente: (Samblás, 2014)

La metodología propuesta utiliza como base el modelo Ciclo PDCA también llamado como Círculo de Deming, ya que fue el Dr. Williams Edwards Deming, constituye una estrategia de mejora continua de la calidad en cuatro pasos, también se lo denomina espiral de mejora continua y es muy utilizado por los diversos sistemas utilizados en las organizaciones para gestionar aspectos tales como calidad (ISO 9000), medio ambiente (ISO 14000), salud y seguridad ocupacional (OHSAS 18000), o inocuidad alimentaria (ISO 22000).

Se implanta dentro de la organización siguiendo los siguientes pasos (Sanchéz-Toledo, 2017):

a. Planificar: se establecen los objetivos, procesos y procedimientos para la gestión de riesgos tecnológicos. La finalidad de esta etapa es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Se define el plan de comunicaciones y el análisis del contexto organizacional actual para medir el alcance de la gestión de riesgos tecnológicos.

b. Hacer: se realiza la implementación y operación de los controles, procesos y procedimientos e incluye también la operación e implementación de las políticas definidas, la valoración y tratamiento de los riesgos.

c. Verificar: se evalúa y se mide el desempeño de los procesos en relación a la política y los objetivos de seguridad. Se debe informar los resultados obtenidos.

d. Actuar: se establece la política para la gestión de riesgos tecnológicos y se implementan los cambios requeridos para la mejora de los procesos. En las etapas verificar y actuar, se incluye el monitoreo y la mejora continua, donde se verifican los cambios y el cumplimientos de indicadores establecidos en la etapa de planificación.

La implementación de los controles muestra como en tiempo previo al estudio, distintas compañías de gran tamaño enfrentaron crisis de seguridad de información. Como conclusiones del informe se muestra que el 69% de los participantes dijo estar confiado o muy confiado sobre la efectividad de la organización para enfrentar retos de seguridad provenientes del exterior. Sin embargo, sólo el 56% mostró esta confianza para enfrentar las amenazas internas (Sanchéz-González, Junio 2012).

Las empresas, si bien están constituidas por activos físicos (edificios e infraestructura), y activos de información (contenido digital), varias de las compañías administran los riesgos de seguridad físicos y de información como entidades separadas y distintas, lo que puede implicar pérdida de oportunidades. Es conveniente que las empresas eviten una serie de riesgos de seguridad, entre los que incluyen robo de identidad, fuga de información, fraude y otros, por lo que es necesario contar con un marco de gobernabilidad en relación a la seguridad de la información.

De esta forma, uno de los puntos más importantes para definir controles de seguridad de la información, es instaurar políticas claras al respecto, que establezcan un marco regulatorio para las actividades que deben ser llevadas a cabo en este contexto.

Parámetros para establecer Políticas de Seguridad de la Información (PSI)

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, debe estar avalado y contar con respaldo de la dirección y/o máxima gerencia, debido a que sin este apoyo, su implementación será más compleja e incluso puede fracasar. Es importante que al momento de formular las políticas de seguridad de la información, se consideren por lo menos los siguientes aspectos:

Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

Reunirse con los departamentos dueños de los recursos, ya que ellos son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad. Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en proteger los activos críticos en su área.

Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.

Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Razones que impiden o limitan la aplicación de las políticas de seguridad informática.

Debe ser capaz de convencer a los altos ejecutivos de la necesidad y beneficios de

buenas políticas de seguridad informática, sino los esfuerzos de su implementación pueden ser desperdiciados. Otros inconvenientes lo ilustran los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos de las empresas a no comprender exactamente la razón o motivos de las inversiones. Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensible y por ende su imagen.

Los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos. Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencia en las proyecciones y utilidades de la compañía.

Es importante destacar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

Conclusiones

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la entidad buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. Existe una serie de estándares, protocolos, métodos, reglas, herramientas y Leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Una de las técnicas que permite evaluar en una entidad u organización su nivel de seguridad es realizar un análisis de riesgos. El estudio debe incluir la visión de negocio, la realización del análisis de riesgos proporciona a las organizaciones una visión de la situación en cuanto al nivel de protección de los sistemas de información. Por este motivo, se constituye como uno de los pilares fundamentales a la hora de conocer de manera de detallada la infraestructura y el funcionamiento interno.

No hay duda que el uso y el acceso a la información son factores críticos en el desarrollo de la economía actual y son las Tecnologías de la Información y las Comunicaciones (TIC) las que han permitido que el acceso a los grandes volúmenes de información sea relativamente sencillo, eficiente y eficaz, por lo cual se puede afirmar que parte de la consolidación de la sociedad de la información ha sido posible gracias al desarrollo vertiginoso de las TIC.

En una economía que funciona en redes, tanto al interior de la empresa, como entre empresas, y entre redes de empresas relacionadas, es una economía articulada globalmente que funciona como una unidad en tiempo real, es decir, la nueva economía tiene la capacidad tecnológica que permite el trabajo y la interacción de forma globalizada y coordinada; la capacidad organizativa que permite acceder de forma directa o indirectamente a mercados globales; y la capacidad institucional que permite la regulación o desregulación para permitir la participación y la generación del nuevo escenario.

Los estándares sobre gestión de la seguridad de la información son complementados con otros que tratan el tema de la gestión de riesgos. Entre los más conocidos están OCTAVE, MAGERIT, ISO/IEC 27005

(ISO/IEC, 2008) y NIST SP 800-30 (NIST, 2012). La seguridad informática se encarga de la salvaguarda de la tecnología y de la información contenida en ella, mientras que la seguridad de la información se ocupa de los riesgos, beneficios y procesos involucrados en la manipulación de la información dentro de la organización, independientemente de cómo sea creada, manejada, transportada, o almacenada. Un buen sistema de seguridad debe proteger los sistemas vulnerables ante el posible acceso físico o remoto de intrusos no autorizados.

Bibliografía

Altamirano, M. (Junio 2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. Avances, 21(1), 248 - 263. Obtenido de www.ciget.pinar.cu

Arévalo-Cedillo. (Agosto 2017). Metodología Ágil para la Gestión de Riesgos Informáticos. Revista Killkana Técnica, 1(2), 31 - 42. Obtenido de www.kilkana.ucacue.edu.ec

Burgos-Campos. (18 de Septiembre de 2008). Modelo Para Seguridad de la Información en TIC. Revista UDA, 21(2), 234 - 253. Obtenido de www.academia.edu

Cañón, G. &. (Mayo 2016). Tecnologias de la informacion y la comunicación: evolucion del concepto y características. Revista Internacional de Investigación e Innovación Educativa., 6(1), 218 - 230. Obtenido de https://www.upo.es

Chávez, M. (Junio de 2019). Tecnología de Información y Comunicación (Tics). Obtenido de Universidad Nacional de Educación: http://repositorio.une.edu.pe

Chicaiza, A. (Diciembre de 2015). Metodología autoguiada para gestión de riesgos de tecnologías de la información adaptada a las pymes ecuatorianas en el área de tic. Obtenido de Universidad Tecnológica Equinoccial: http://repositorio.ute.edu.ec

Samblás, A. (21 de Febrero de 2014). Gestión del Riesgo. Obtenido de ABAST: http://calidadtic.blogspot.com

Sanchéz-González. (Junio 2012). La Sociedad de la Información: Génesis, Iniciativas, Concepto y su Relación con Las TIC. Revista UIS Ingenierías., 11(1), 113 - 129. Obtenido de https://www.redalyc.org

Sanchéz-Toledo. (Julio de 2017). Ciclo pdca - estrategia para la mejora continua. Obtenido+ de Calidad & Gestión: http://www.calidad-gestion.com.ar

CITAR ESTE ARTICULO:

Pazmiño Zabala, C., Serrano Castro, A., & González Rivera, M. (2020). Las Tics como herramienta para la gestión de riesgos. RECIMUNDO, 4(1(Esp)), 173-181. doi:10.26820/recimundo/4.(1).esp.marzo.2020.173-181