Dom. Cien., ISSN: 2477-8818
Vol. 3, núm. mon., agos., 2017, pp. 200-217

DOI: 10.23857/dc.v3i3 mon.636

Número Publicado el 05 de agosto de 2017

Ciencias de la computación
Artículo de investigación

Ciberseguridad en los sistemas de información de las universidades

Cybersecurity in university information systems

Cibersegurança em sistemas de informação universitária

[I] Carlos E. Anchundia-Betancourt
ceab221984@gmail.com

Recibido: 12 de enero de 2017 *** Corregido:** 23 de febrero de 2017 *** Aceptado:** 14 julio de 2017

[I] Ingeniero en Sistemas ; Programa de Revalidación de la Maestría de Gestión Estratégica de Tecnologías de la Información, Facultad de Ingeniería; Universidad de Cuenca, Campus Central, Cuenca, Ecuador.

Resumen

El impacto de la globalización que va acompañando la creciente implantación de las tecnologías, están trayendo grandes beneficios a organizaciones y empresas de toda índole, pero a la vez están produciendo grandes problemas de seguridad y de protección de datos y privacidad con los cuales las organizaciones tendrán que enfrentarse. El objetivo de esta investigación es revisar el estado actual del conocimiento en la ciberseguridad en los sistemas de información en el contexto universitario, con algunas implicaciones en el Ecuador. A partir de una revisión documental, usando como recursos plataformas como Sciencedirect® y Google Académico®, entre otros, se identificaron áreas de interés general, dada la escasa literatura de ciberseguridad en el contexto universitario. Aunque la ciberseguridad es un fenómeno de mucho impacto en este entorno globalizado, la productividad científica en este tema es escasa; lo que dificulta un análisis profundo de la situación en el contexto universitario; sin embargo, al ser, la ciberseguridad, un fenómeno global y generalizado a todo tipo de organización, pueden extrapolarse las amenazas al sector universitario. Así, la universidad está llamada a jugar un papel protagónico en el establecimiento de una necesaria cultura de ciberseguridad que exige una labor de capacitación de todos los sectores de la sociedad; las instituciones universitarias no pueden quedarse ajenas y deben participar en el proceso, contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de ciberseguridad, apoyada en una cultura de seguridad y defensa, dentro de la Universidad y desde la Universidad a la sociedad.
Palabras clave: ciberseguridad; universidad; Ecuador.

Abstract

The impact of globalization, which is accompanying the growing deployment of technologies, are bringing great benefits to organizations and companies of all kinds, but at the same time they are producing great problems of security and data protection and privacy with which organizations will have to confront. The objective of this research is to review the current state of knowledge in cybersecurity in information systems in the university context, with some implications in Ecuador. Based on a documentary review, using platforms such as Sciencedirect® and Google Académico®, among others, areas of general interest were identified, given the scarce literature on cybersecurity in the university context. Although cybersecurity is a phenomenon of great impact in this globalized environment, the scientific productivity in this subject is scarce; which makes difficult an in-depth

analysis of the situation in the university context; However, since cybersecurity is a global and generalized phenomenon for all types of organization, threats to the university sector can be extrapolated. Thus, the university is called to play a leading role in the establishment of a necessary culture of cybersecurity which requires training of all sectors of society; university institutions can not remain alien and must participate in the process, contributing to create a safe university cyberspace and leading the establishment of a culture of cybersecurity, supported by a culture of security and defense, within the University and from the University to the society.

Keywords: cybersecurity; university; Ecuador.

Resumo

O impacto da globalização, que acompanha a crescente implantação de tecnologias, está trazendo grandes benefícios para organizações e empresas de todos os tipos, mas ao mesmo tempo estão produzindo grandes problemas de segurança e proteção de dados e privacidade com quais organizações terão para confrontar. O objetivo desta pesquisa é revisar o estado atual do conhecimento em segurança cibernética em sistemas de informação no contexto universitário, com algumas implicações no Equador. Com base em uma revisão documental, utilizando plataformas como Sciencedirect® e Google Academic®, entre outras, foram identificadas áreas de interesse geral, dada a escassa literatura sobre segurança cibernética no contexto universitário. Embora a segurança cibernética seja um fenômeno de grande impacto neste ambiente globalizado, a produtividade científica neste assunto é escassa; o que torna difícil uma análise aprofundada da situação no contexto universitário; No entanto, uma vez que a segurança cibernética é um fenômeno global e generalizado para todos os tipos de organização, as ameaças ao setor universitário podem ser extrapoladas. Assim, a universidade é chamada a desempenhar um papel de liderança no estabelecimento de uma cultura necessária de segurança cibernética, que requer formação de todos os setores da sociedade; as instituições universitárias não podem permanecer estrangeiras e devem participar do processo, contribuindo para criar um ciberespaço seguro da universidade e liderando o estabelecimento de uma cultura de segurança cibernética, apoiada por uma cultura de segurança e defesa, dentro da Universidade e da Universidade à sociedade.

Palavras chave: cibersegurança; universidade; Equador.

Introducción

En las últimas décadas, las nuevas tecnologías, los servicios electrónicos y redes de comunicación se han visto cada vez más integradas en el quehacer diario; las empresas, la sociedad, el gobierno y la defensa nacional dependen del funcionamiento de las tecnologías de la información y comunicaciones (TICs) y de la operación de las Infraestructuras Críticas de Información (ICIs); el transporte, las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y servicios públicos se sustentan en la disponibilidad, integridad y confidencialidad de la información que fluye a través de estas infraestructuras (Leiva, 2015).

El primer cuarto del Siglo XXI, constituye un lugar común de insistir en la dependencia de las sociedades occidentales de sus sistemas de información, ya sean estos públicos o privados; la actividad cotidiana de los ciudadanos, de los profesionales, de las empresas, de las entidades públicas, del Estado, en suma, depende de que ese conjunto de herramientas tecnológicas a las que se han denominado sistemas de información (computadores y redes de comunicaciones, esencialmente), propiedad u operados por el sector público, por las organizaciones privadas o por los propios ciudadanos, se permanezcan operativos y en condiciones de prestar los servicios que de ellos se esperan (Galán & Galán, 2016).

El enorme desarrollo de las Nuevas Tecnologías, la informática y las telecomunicaciones, y especialmente el efecto sinérgico entre ambas, está suponiendo un cambio trascendental en la sociedad; trabajo, economía, administración y ocio son algunos de los aspectos que están variando a pasos agigantados, dirigiendo a los usuarios hacia esa sociedad cada vez más global, en la que la esfera de influencia supera el entorno mediato, y lo que ocurre en las antípodas ya forma parte de las circunstancias; en este nuevo modelo social, al que se ha bautizado como Sociedad de la Información, juega un papel determinante Internet como vehículo de transmisión e intercambio de todo tipo de información, produciéndose una sinécdoque entre la parte y el todo, Internet por Sociedad de la Información (Salom, 2010).

Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes (Pons, 2017). El aumento de la conectividad a Internet provoca que cada vez más personas estén conectadas en un espacio público y transaccional, proporcionando una plataforma dinámica y de crecimiento que permite que avance la

comunicación, la colaboración y la innovación; sin embargo, los ataques cibernéticos y el robo de información crítica se han convertido en una gran amenaza derivado de las consecuencias económicas y sociales que conllevan (López, 2015).

Abordar el tema de la seguridad en entornos digitales invita a reflexionar sobre los beneficios que aporta el uso de internet a la sociedad del siglo XXI; sin embargo, es preciso tener en cuenta los riesgos que genera la navegación y, en algunos casos, la sobreexposición a los recursos mediáticos (Castillejos, Torres & Lagunes, 2016).

Existe una tendencia en la ciberseguridad en el mundo actual de masificación e hiperconectividad a nivel mundial que hace que cada dispositivo represente un nuevo blanco de ataques para los ciberdelincuentes, si no se conocen las medidas necesarias para prevenirlos (Vallés, 2016). En general, se podría decir que la Ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (Leyva, 2015).

A nivel internacional, la ciberseguridad está cobrando unos marcados matices de relevancia y de urgencia, a medida que la economía digital se ha ido desarrollando en los últimos 15 años, las empresas así como los consumidores son más dependientes que nunca de los sistemas de información; la relevancia de la ciberseguridad sigue viéndose incrementada debido a la aparición de una nueva ola de sistemas ciber-físicos como son los dispositivos "inteligentes" para el hogar, vehículos autónomos y sistemas aéreos no tripulados; sin embargo, en este contexto de transformación digital, es cada vez más claro que tanto el público como el sector privado no pueden seguir el ritmo de las amenazas de ciberseguridad (Machín & Gazapo, 2016).

En la actualidad, la seguridad como elemento político clave en la escena internacional, se compone de nuevas dimensiones que se suman a las consideradas tradicionales, como son la militar y la política; en ese sentido, van paulatinamente adquiriendo relevancia las facetas económica, la científica-tecnológica-comunicacional, la medioambiental, la social-cultural-étnica, la ilegal-narcotráfico, delito cibernético, el tráfico de personas, el lavado de activos, etc.- la alimentaria, entre otras; en estos términos, es fácil percatarse que las políticas públicas de los Estados -cada vez más impregnadas por la variedad de elementos que hacen a la seguridad-, están obligadas a acompañar los cambios impuestos por una pléyade cada vez más amplia de riesgos (Ibarra & Nieves, 2016).

Por otro lado, las concepciones tradicionales de seguridad, defensa, seguridad externa, seguridad interna, seguridad multidimensional, seguridad humana y otros, no solo que se traslapan, sino que se refuerzan y contraponen, abriendo la posibilidad a nuevas miradas teóricas y epistemológicas de la seguridad y la defensa, que sean capaces de dar cuenta del comportamiento de las amenazas y sus nuevas lógicas (Vargas, Recalde & Reyes, 2017).

El impacto de la globalización, su desarrollo subsecuente, y los fenómenos inherentes que afectan a las organizaciones en general, impactan también a las universidades. El objetivo de esta investigación es revisar el estado actual del conocimiento en la ciberseguridad en los sistemas de información en el contexto universitario, con implicaciones en el Ecuador.

Materiales y métodos

A objeto de cumplir con el objetivo, se plantea una investigación documental. La búsqueda de la información se basó en los recursos como ScienceDirect® y Google Academic®, entre otros; combinando campos de búsqueda con conceptos como ciberseguridad, seguridad informática, universidad, entre otros, los cuales se utilizaron tanto en inglés como en español. Luego se elaboró una estructura para la presentación y discusión de los resultados que parte de la concepción global de la ciberseguridad, hasta llegar al entorno universitario, y sus implicaciones en el Ecuador.

Resultados y discusión

La difusión masiva que se está produciendo de la computación en nube unido a la creciente implantación de las tecnologías de la información y comunicación, están trayendo grandes beneficios a organizaciones y empresas de toda índole, pero a la vez están produciendo grandes problemas de seguridad y de protección de datos y privacidad que será preciso afrontar; algunos informes rigurosos de empresas del sector de la seguridad informática consideran que a las grandes ventajas que traen consigo podrán traer grandes riesgos y amenazas contra la ciberseguridad, simplemente porque su facilidad de uso puede traer consigo la difusión de todo tipo de virus y amenazas de muy diversa índole (Joyanes, 2010).

Ciberseguridad es un término reciente que se utiliza para designar diversos campos de investigación, desarrollo e innovación; relacionados con el tratamiento del ciberespacio desde el punto de vista de su seguridad y fiabilidad para el usuario y el dominio público (Paya, Cremades & Delgado, 2017).

A principios de 2011, un grupo de trabajo bilateral rusoestadounidense del EastWest Institute (EWI) y la Universidad de Moscú elaboró un marco de terminología internacional; así, definieron la Ciberseguridad como "una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse" (Rauscher & Yashenko, 2011). La ciberseguridad es definida en líneas generales como la seguridad de la información digital almacenada en redes electrónicas, aunque aún hoy no hay un consenso en su definición (Ibarra & Nieves, 2016). ISACA define la ciberseguridad como la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

La ciberseguridad es definida como "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno; los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno; la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno; las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y la confidencialidad" (Caro, 2010).

La Ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información; es decir, es donde los controles de Ciberseguridad son eficaces y el ciberespacio es considerado confiable, flexible y seguro para las TICs; sin embargo, donde los controles de Ciberseguridad están ausentes, incompletos, o mal diseñados, el ciberespacio es considerado como tierra de nadie (Leiva, 2015).

La conectividad a Internet acelera el crecimiento económico de las naciones y crea oportunidades para los negocios y el comercio; es por ello que la seguridad del ciberespacio debe ser una parte central de la planeación gubernamental; sin embargo, estas oportunidades siempre traen sus riesgos asociados ya que las tecnologías de Internet aún no están maduras y los delincuentes las pueden explotar fácilmente (López, 2015).

La Ciberseguridad, no es un concepto de fronteras perfectamente definidas; muy al contrario, en su configuración intervienen, se superponen, se integran y, en ocasiones, se erosionan mutuamente, conceptos, métodos, procedimientos, herramientas y regulaciones que construyen una realidad multiforme y multidisciplinar (Galán & Galán, 2016).

Se puede decir que en la medida que la sociedad se vuelve más dependiente de las TICs, la protección y la disponibilidad de estos activos críticos se convierte cada vez más en un tema de interés nacional; los incidentes que causan la interrupción de las infraestructuras críticas y los servicios de TICs podrían causar importantes impactos negativos en el funcionamiento de la sociedad y la economía; como tal, el ciberespacio seguro se ha convertido en uno de los retos más importantes del siglo, y por lo tanto la seguridad informática se considera cada vez más como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad (Leiva, 2015).

La falta de seguridad en el ciberespacio deteriora gravemente la confianza entre la comunidad TIC que está sufriendo una de las revoluciones más importantes en la historia de la humanidad; la seguridad y la prosperidad de cualquier país está conectada a la protección de las redes TIC, a través de las cuales la población puede ejercer sus libertades de expresión, asociación e información (Carlini, 2016).

Cuando se aborda el tema del perfil del universitario, es primordial considerar sus actuaciones como gestor de información y conocimiento en la Red; por tal hecho, resulta necesario identificar los factores que lo caracterizan como internauta (Castillejos, Torres & Lagunes, 2016). El desarrollo de Políticas o Estrategias de Ciberseguridad no es una tarea fácil, y no se basa solo en la aplicación de la ley, la gestión y la tecnología, requiere una forma consensuada y armoniosa de actuar y resaltar la necesidad de innovación (Leyva, 2015).

La consecución de una cultura de ciberseguridad no es posible a través de meras acciones de divulgación, aun cuando éstas sean necesarias, sino que requiere de una ingente labor formativa especializada que tenga en cuenta en ese proceso de enseñanza/aprendizaje a todos los sectores de la sociedad; sin embargo, esta cultura de ciberseguridad no puede ser eficaz si no se inserta dentro de una cultura de seguridad y defensa (De Tomas, 2014).

La ciberseguridad implica problemas complejos y su resolución exige una voluntad política de diseño e implementación de un plan de desarrollo de infraestructuras y servicios digitales que comprenda una estrategia multidisciplinaria, coherente, eficaz y controlable (Rodríguez, 2016). La Ciberseguridad ya

no es una opción; la dependencia de las sociedades occidentales de sus sistemas de información (públicos y privados) es de tal magnitud que no puede abordarse ningún proyecto de interés nacional que no contemple la seguridad de los sistemas de información, la información tratada y los servicios prestados, como requisitos tan importantes como la propia prestación de aquellos servicios (Galán & Galán, 2016).

Cada vez más, las organizaciones se enfrentan a una realidad digitalmente modificada, donde las nuevas tecnologías permean cada uno de los ambientes organizacionales y personales; la creciente expansión digital genera nuevos riesgos y necesidades de protección, hecho que invita a la reflexión en aras de proteger la información en un mercado más competido y exigente; en el entorno de la cuarta revolución industrial, los ejecutivos de seguridad se enfrentan a unos escenarios cambiantes y dinámicos que demandan reacciones rápidas, que contemplan la anticipación y la conciencia para proteger la información (Almanza, 2017).

A pesar de las posibilidades de desarrollo personal y profesional que brinda el ciberespacio, la amenaza cibernética ocupa un lugar destacado entre los riegos y amenazas que atenazan la seguridad interna e internacional (De Tomas, 2014). El intercambio de información entre el sector público y privado, a nivel nacional, es necesario para tener una visión completa de cuáles podrían ser las posibles y diferentes amenazas, y así desarrollar tecnologías para responder rápidamente a las amenazas cibernéticas sin sufrir daños importantes (Carlini, 2016).

Las estrategias de seguridad adoptadas por los Estados que gozan de una democracia avanzada constituyen un instrumento eficaz para la implantación de una cultura de ciberseguridad en sus respectivas sociedades, pero requieren de un eficaz desarrollo legislativo y un verdadero compromiso por parte del Gobierno y de las Administraciones y organismos públicos para que su arraigo sea una realidad y además, el adecuado (De Tomas, 2014).

Fenómenos como la transnacionalidad, el terrorismo, la tecnología, Internet no solo han eventualmente condicionado la agenda internacional de los últimos tiempos, sino que resumen en materia de ciberseguridad una característica sustancial de la sociedad internacional; la idea de la Sociedad de la Información, en la que es de orden la noción de autodeterminación en línea en términos de la libertad informática del individuo, implica contemplar elementos como conexión a la Red, software, el dominio de la tecnología por las grandes corporaciones, el rol del propio Estado en

términos de defensa de un derecho humano como es el acceso a Internet, entre otros (Ibarra & Nieves, 2016).

El establecimiento de una cultura de ciberseguridad exige una labor de capacitación de todos los sectores de la sociedad, para la que está llamada a jugar un papel protagonista la Universidad; las instituciones universitarias no pueden quedarse ajenas y deben participar en el proceso, contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de ciberseguridad, cimentada en una cultura de seguridad y defensa, dentro de la Universidad y desde la Universidad a la sociedad (De Tomas, 2014).

La seguridad socioeconómica de personas y Estados depende de nuevos actores que en la sociedad global se han configurado como muy relevantes; organizaciones multilaterales, de integración regional, grandes empresas con PIB superior al de estados son entes que un análisis riguroso no puede ignorar; Internet, como en los casos anteriores, abre posibilidades de mejora en áreas como la educación, pero también intensifica los efectos perversos de un modelo de relaciones productivas que pretende reducir la influencia de la variable humana a la mínima expresión; la seguridad laboral y social de los seres humanos puede quedar seriamente comprometida a causa de la creciente automatización y externalización (Rodríguez P., 2016).

En el actual momento histórico, en el que la tendencia general es de una progresiva informatización de las sociedades, y de una creciente dependencia individual y colectiva respecto a las innovaciones tecnológicas, todo indica que la importancia de estas nuevas formas de delincuencia aumentará exponencialmente en el futuro próximo. Además de la cuestión meramente técnica, del carácter cambiante de la ciberdelincuencia se desprende una dificultad añadida en su prevención y persecución: La perfectibilidad de los instrumentos legales y jurídicos de los que se dispone en la actualidad (Paya, Cremades & Delgado, 2017).

Sobre la ciberseguridad hay mucho trabajo que hacer y uno de los desafíos más importantes es lograr un compromiso real de los Estados en la generación de políticas públicas específicas, y en la construcción de una cultura de ciberseguridad; para alcanzar este objetivo, primero deben lograrse articulaciones y puntos de coincidencia desde las organizaciones internacionales afines, el sector público y privado, de manera de ofrecer a los Estados herramientas efectivas, tanto de protección y cuidado de los individuos, como de lo que se considera información crítica para los gobiernos (Ibarra & Nieves, 2016).

La llamada "digitalización de la sociedad" exige garantizar que las herramientas tecnológicas utilizadas tienen la capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas prestan o hacen accesibles (Galán & Galán, 2016).

En España, el marco jurídico de la ciberseguridad, entendido como el conjunto de regulaciones que vienen a ordenar de un modo u otro el adecuado uso de los sistemas de información para la prevención o tratamiento de los ciberincidentes (accidentales o deliberados), es muy extenso. Los países más avanzados en materia de ciberseguridad -entre los que ya se encuentra España-, han diseñado estrategias nacionales (de repercusión internacional) tendentes a afrontar los retos que supone operar en el ciberespacio. De nuestra actividad, de nuestro celo, de nuestra profesionalidad, en suma, depende que los servicios públicos españoles, presentes y futuros, posean el nivel de confiabilidad que nos permita crecer como Estado, como ciudadanos y como personas. (Galán & Galán, 2016).

El desarrollo del ciberespacio ha facilitado enormemente el desarrollo de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales. Hoy en día se ha encaminado el control de muchos procesos mundiales a través del ciberespacio. Por lo que no hay duda de que actualmente el ciberespacio constituye un bien valioso. Y de que la seguridad del ciberespacio ha crecido en importancia (González, 2010).

A pesar de los riesgos que conlleva una sociedad cada vez más interconectada digitalmente y cada vez más olvidada de los procedimientos tradicionales, la tendencia digital es imparable; lo que significa que hay que afrontar el futuro como es y gestionar los riesgos asociados. Los riesgos asociados son numerosos, entre los que destacan, una mayor y más compleja actividad criminal desarrollada por grupos organizados o delincuentes individuales; una más prolífica actividad terrorista que hace uso del ciberespacio ampliamente para actividades terroristas y para apoyo a ellas; una mayor y más compleja actividad de espionaje, ya sea industrial, militar o político; una mayor variedad y cantidad de ataques a las infraestructuras críticas nacionales, a las libertades públicas y a todo tipo de servicios en los que se basa el funcionamiento de las sociedades modernas; un mayor índice de ataques camuflados, orquestados por Estados y encubiertos bajo apariencia de ataques con origen en bandas criminales, activistas políticos, etc.; una mayor participación de ciudadanos particulares en acciones maliciosas, ya sea por ignorancia, por curiosidad, por diversión, por reto o por lucro; y un largo

etcétera de riesgos como causa de la atracción que el ciberespacio produce al ofrecer una mayor rentabilidad, globalidad, facilidad e impunidad para todo este tipo de actividades (Ganuza, 2010).

La formación y la capacitación del personal implicado directamente en la lucha contra la ciberdelincuencia es una labor fundamental que implica a administraciones públicas, organizaciones empresariales e instituciones académicas; sin embargo, todo programa formativo que se dirija a capacitar a sus participantes en las técnicas y procedimientos requeridos para el adecuado tratamiento de la ciberdelincuencia nace condenado a la obsolescencia en un periodo de tiempo cada vez más breve; ello se debe, en primer lugar, al carácter cambiante de la amenaza, cuya sofisticación, complejidad y dimensiones aumenta día tras día, lo que conlleva a una aparición continua de nuevas técnicas y procedimientos para eludir las medidas de seguridad de los sistemas informáticos a los que, normalmente, los especialistas en ciberseguridad únicamente pueden responder de manera reactiva (Paya, Cremades & Delgado, 2017).

Las tecnologías de la información y las innumerables formas en las que se utilizan siguen evolucionando a un ritmo acelerado y están alterando constantemente la industria, al igual que las vulnerabilidades que traen consigo los actores y amenazas que buscan aprovecharse de estas; esta tendencia continuará y se intensificará, transformando cada uno de los pasos de la manera en la que se relaciona, produce, distribuye y consume; es por ello que las economías y sociedades deben prepararse para que puedan aprovechar estas ventajas de manera exitosa (López, 2015).

La ciberseguridad afecta al bienestar digital de la sociedad, de las organizaciones y de los países; dentro de la sociedad afecta a distintas dimensiones: dimensión política, social, económica, legal, justicia y policial, técnica y de gestión; los desafíos son complejos y satisfacerlos requiere de la voluntad política para diseñar e implementar una estrategia global para el desarrollo de infraestructuras de información que incluyan una estrategia de ciberseguridad coherente y efectiva; una respuesta firme a las dimensiones humana, legal, económica y tecnológica de las necesidades de seguridad de infraestructuras de información puede construir confianza y genera un crecimiento del bienestar económico que beneficie a toda la sociedad (Caro, 2010).

En el marco de la cuarta revolución industrial, con ambientes cada vez más volátiles, inciertos, complejos y ambiguos, es necesario que los responsables de la seguridad de la información en las organizaciones tengan una atención plena y consciente, frente a los nuevos desafíos (Almanza, 2017).

El caso Ecuador

Según el Índice Global de Ciberseguridad (IGC), de la Unión Internacional de Telecomunicaciones (UIT), de julio de 2017, en el que se mide el compromiso de los Estados frente al tema de seguridad informática, Ecuador se encuentra en el sexto puesto de 19 países de América Latina (Ministerio de Telecomunicaciones y Sociedad de la Información, 2017); y ocupa el puesto 66 en el listado global de los 193 países que formaron parte del estudio (Dávila, 2017).

Como lo señalan Vargas, Recalde & Reyes (2017), en el Ecuador, aunque el acceso a internet ha registrado un elevado incremento durante los últimos 5 años, las evidencias muestran que la reflexión en este tema de ciberseguridad es aún incipiente y se requieren esfuerzos interagenciales para su institucionalización. Destacan estos autores que, al menos en Ecuador, las estadísticas referentes a violaciones a la seguridad han sido en su mayoría dentro del sistema financiero; agregando que, un incremento en sus cifras ha convertido a la ciberseguridad en un tema preocupante, especialmente para la banca ecuatoriana.

El Gobierno ecuatoriano, en su esfuerzo por minimizar estos problemas, tomó algunas decisiones de tipo político-coyuntural y También se promulgaron políticas más sustentables; además, ha dispuesto el uso obligatorio de las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información, las cuales contemplan un conjunto de directrices para viabilizar la implementación de la seguridad de la información en las entidades públicas. No obstante, han sido muy pocas las que han implementado en parte el esquema y sus medidas, que dan mediada confianza a los ciudadanos de la administración pública (Vargas, Recalde & Reyes, 2017).

Refiriéndose a las instituciones gubernamentales en el Ecuador, Alarcón, Barriga, Picón & Alarcón (2016), señalan que la seguridad informática es uno de los requerimientos más importantes, ya que en la mayoría de las aplicaciones y servicios que se brindan a la ciudadanía, no se toman en cuenta medidas de seguridad o análisis de posibles puntos débiles; agregan que, toda institución gubernamental que no cuente con un esquema de seguridad establecido, siempre será un fácil objetivo para terceras personas (cibercriminales) que aprovechan las vulnerabilidades de los sistemas para obtener información que pueden involucrar datos de tipo sensibles, críticos y confidenciales de los ciudadanos y de las operaciones de la institución, por lo cual surge la necesidad, que toda institución pública u otras organizaciones deben manejar un ciclo de mejora continua en los procesos de seguridad implementados.

En este contexto, el debate en torno a la ciberseguridad y ciberdefensa en el Ecuador debe ser enfocado desde los conceptos fundamentales: el Estado, su seguridad, su desarrollo y defensa. Es imprescindible desarrollar una estrategia nacional de seguridad que incluya al ciberespacio y que agregue valor e influya a todos los niveles de decisión; y estos, a su vez, se conecten, de forma matricial, con las normas o estándares que son aplicables, con los sectores estratégicos involucrados, con el método de implementación y con los objetivos de seguridad que se van a plantear. Vargas, Recalde & Reyes (2017).

Dado que los sistemas de información forman parte integral de las prácticas de negocio, los cuales entregan beneficios tales como: eficiencia en operaciones, mejora en la toma de decisiones, mejora en la atención de clientes, etc., y que, sin embargo, los mismos se enfrentan a riesgos propios del ambiente en los cuales se desarrollan, y que el incremento de regulaciones y leyes exigen mayor cumplimiento, se plantea la necesidad de establecer un marco para el Gobierno de la Seguridad de la Información, la cual puede ser aplicada a cualquier tipo de empresa ya sea pública o privada. A menudo este campo, se percibe con un enfoque limitado que únicamente abarca los Sistemas de Información y Tecnología relacionada; sin embargo, la Seguridad de la Información tiene un enfoque más amplio, por lo cual es necesario aplicar prácticas de Gobierno y Gestión de Seguridad de la Información. Ante esta realidad, la Superintendencia de Bancos y Seguros del Ecuador, ha planteado cambios que las instituciones controladas deben tomar como referencia la ISO/IEC 27000 o la que lo sustituya (Ochoa, 2015).

Con el uso de las normas internacionales para los Sistemas de Gestión de Seguridad de la Información (SGSI), las organizaciones pueden desarrollar e implementar un marco para gestionar la seguridad de sus activos de información y preparar la evaluación independiente de su SGSI en materia de seguridad de la información, y además, pueden ser usadas por las organizaciones para prepararse ante una evaluación independiente de su SGSI aplicada a la protección de la información (ISO, 2016). En esta familia de normas, además de la 27.000 que presenta una descripción general y terminología, la 27.001 y 27.006 que especifican requisitos, la 27.002, 27.003, 27.004 y 27.005 que describen directrices generales, y las 27.10, 27.011 que describen directrices especificas generales, entre muchas otras. Se destaca la norma 27.0032 (ISO, 2012), que aborda la seguridad del Ciberespacio o cuestiones de Ciberseguridad que se concentran en tender puentes entre los diferentes vacíos del Ciberespacio; en particular, proporciona una guía técnica para abordar riesgos de Ciberseguridad comunes.

Conclusiones

El impacto de la globalización que va acompañando la creciente implantación de las tecnologías, están trayendo grandes beneficios a organizaciones y empresas de toda índole, pero a la vez están produciendo grandes problemas de seguridad y de protección de datos y privacidad con los cuales las organizaciones tendrán que enfrentarse.

Aunque la ciberseguridad es un fenómeno de mucho impacto en este entorno globalizado, la productividad científica en este tema es escasa; lo que dificulta un análisis profundo de la situación en el contexto universitario; sin embargo, al ser, la ciberseguridad, un fenómeno global y generalizado a todo tipo de organización, pueden extrapolarse las amenazas al sector universitario.

La universidad está llamada a jugar un papel protagónico en el establecimiento de una necesaria cultura de ciberseguridad que exige una labor de capacitación de todos los sectores de la sociedad; las instituciones universitarias no pueden quedarse ajenas y deben participar en el proceso, contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de ciberseguridad, apoyada en una cultura de seguridad y defensa, dentro de la Universidad y desde la Universidad a la sociedad.

Sobre la ciberseguridad hay mucho trabajo que hacer y uno de los desafíos más importantes es lograr un compromiso real de los Estados en la generación de políticas públicas específicas, y en la construcción de una cultura de ciberseguridad, este es un rol que definitivamente, debe liderar la universidad.

Aunque los ranking mundiales ubican al Ecuador en una posición destacada, es mucho el trabajo que queda pendiente, en cuanto a su investigación y desarrollo en el ámbito general, y en particular los entes gubernamentales, y el universitario. El tema de la ciberseguridad, y en general los sistemas de gestión de seguridad de la información, tales como la familia ISO 27.000, podría constituirse en una línea de investigación y desarrollo que involucre el sector gubernamental, el sector empresarial y a la universidad como ente vinculante.

Referencias bibliográficas

Alarcón, P.; Barriga, R.; Picón, C. & Alarcón, J. (2016). La importancia de la seguridad informática en las instituciones gubernamentales (Ecuador). Revista Caribeña de Ciencias Sociales. Consultado el 8 de octubre de 2016. En línea: http://www.eumed.net/rev/caribe/2016/11/seguridad.html

Almanza, A. (2016). Encuesta nacional de seguridad informática 2016. Desafíos de la cuarta revolución industrial. Sistema, 143, 18-36.

Caro, M. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 49-82. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. IEEE Documento de opinión, 67, 1-16.

Castillejos, B.; Torres, C. & Lagunes, A. (2016). La seguridad en las competencias digitales de los millennials. Apertura, 8(2), 54-69. DOI: http://dx.doi.org/10.18381/Ap.v8n2.914

Dávila, E. (2017). ¿Cómo está Ecuador en materia de Ciberseguridad? El Comercio, disponible en [http://www.elcomercio.com/guaifai/ecuador-seguridad-internet-hackeo-ciberataque.html].

De Tomas, S. (2014). Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". Especial referencia al ámbito universitario. ICADE, 92, 14-47.

Galán, C. & Galán C., C. (2016). La ciberseguridad pública como garantía del ejercicio de derechos. Derecho & Sociedad, 47, 293-306.

Ganuza, N. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 167-214. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

González, J. (2010). Estrategias legales frente a las ciberamenazas. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 85-127. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Ibarra & Nieves, (2016). La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad. Memorias "VIII Congreso de Relaciones Internacionales", 16 p. Universidad Nacional de La Plata, Argentina.

ISO (2012). ISO/IEC 27032:2012. Information technology - Security techniques -- Guidelines for cybersecurity. Ginebra: International Organization for Standardization.

ISO (2016). ISO/IEC 27000:2016 Preview. Information technology -- Security techniques -- Information security management systems - Overview and vocabulary. Ginebra: International Organization for Standardization.

Joyanes, L. (2010). Introducción: estado del arte de la ciberseguridad. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 13-46. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176.

López, A. (2015). Ciberseguridad en los países del MINT. Revista de Tecnologías de la Información, 2(3), 155-167.

Machín & Gazapo, 2016). La ciberseguridad como factor crítico en la seguridad de la unión europea. Revista UNISCI, 42, 47-68.

Ministerio de Telecomunicaciones y Sociedad de la Información (2016). Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad. Quito: Gobierno Nacional de la República del Ecuador: Portal MINTEL, Disponible en [https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/].

Ochoa, P. (2015). Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio. Revista Tecnológica ESPOL - RTE, 28(3), 1-17.

Paya, C.; Cremades, A. & Delgado, J. (2016). El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad de Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. Revista Policía y Seguridad Pública, 7(1), 237-270. DOI: http://dx.doi.org/10.5377/rpsp.v7i1.4312

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20, 80-93. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563

Rodríguez, G. (2016). Ciberseguridad realidad y tendencias en Venezuela. Cuestiones Jurídicas, 10(1), 13-39.

Rodríguez P., 2016). ¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades, 18(36), 391-415. DOI: http://dx.doi.org/10.12795/araucaria.2016.i36.17

Salon, J. (2010). El ciberespacio y el crimen organizado. En "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio", 131-164. Cuadernos de estrategia, 147. España: Ministerio de Defensa.

Vallés, L. (2016). La ciberseguridad en el mundo actual. TINO, 50, 585-620.

Vargas, R.; Recalde, I. & Reyes, R. (2016). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20, 31-45. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571