El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados

Alejandro BOGANTES
Profesor Escuela de Ciencias Exactas y Naturales, Universidad Estatal a Distancia
San José, 11502/Montes de Oca, Costa Rica

RESUMEN

Debido a que la ciberseguridad se enfoca en la protección de los activos de información y de la infraestructura computacional, el objetivo de este artículo es compartir las normas de seguridad que se deben tomar en cuenta para evitar ser objeto de ataques cibernéticos y personas malintencionadas que desean obtener información personal confidencial, con el fin de adquirir un beneficio de forma ilegal, pero enfocado en el ámbito académico.

Aunado a lo anterior, es indispensable que en la educación formal universitaria, así como a la ciudadanía en general, se dote del conocimiento sobre las buenas prácticas en el uso de sistemas de información, dispositivos electrónicos, redes sociales, aplicando las técnicas de ciberseguridad, de manera que el sistema educativo de la Universidad procure brindar los conocimientos académicos y desarrollar las habilidades necesarias para enfrentar la vida tomando en cuenta los desafíos de la época debido al auge de la Cuarta Revolución Industrial.

El resultado de esta investigación muestra hallazgos con relación a las prácticas inadecuadas que realizan los estudiantes y personas asociadas a la Universidad para plantear un programa de divulgación y capacitación, con el fin de proteger la información sensible de los sistemas de información y de la infraestructura informática.

Palabras claves: ciberseguridad, delito informático, buenas prácticas, seguridad informática.

1. INTRODUCCIÓN

La Universidad Estatal a Distancia de Costa Rica (UNED), dentro de su Escuela de Ciencias Exactas y Naturales, ofrece a la comunidad estudiantil del país la carrera de Ingeniería Informática a nivel de Bachillerato y Licenciatura en distintos énfasis.

La UNED como parte de su visión institucional, promueve la búsqueda continua de la excelencia y exigencia académica en sus áreas fundamentales como docencia, investigación, producción de materiales didácticos para alcanzar los niveles educativos superiores deseados en condiciones de calidad, pertinencia y equidad, acordes con las demandas de los diversos grupos de la sociedad costarricense [1].

Por lo anterior, el programa de Ingeniería Informática adquirió la acreditación en Costa Rica del ente oficial encargado de este proceso, llamado Sistema Nacional de Acreditación de la Educación Superior (SINAES), el cual garantiza y exige que sus programas acreditados sean congruentes, pertinentes y actuales, como lo demanda la sociedad.

A raíz de la acreditación del programa de Ingeniería Informática, la UNED ha realizado programas y Seminarios de Actualización Profesional (SAP), tanto para estudiantes como para graduados de la carrera de Informática, esto en una actividad cuyo objetivo es, actualizar los conocimientos de los profesionales graduados, según las necesidades y tendencias en el área de las Tecnologías de Información y Comunicación (TIC), que se analizan cada dos años para definir las temáticas a desarrollar en cada SAP, según las necesidades de los estudiantes.

Los programas de actualización profesional SAP en el programa de Ingeniería Informática en la UNED, se llevan a cabo desde el año 2017, ofreciendo seminarios, charlas, cursos y talleres de actualización profesional tecnológica, haciendo frente a las actuales tendencias TIC en temas relacionados con el apogeo de la Cuarta Revolución Industrial, entre ellos: robótica, big data, ingeniería del software, desarrollo ágil, desarrollo de video juegos, calidad informática, inteligencia artificial, internet de las cosas, ciberseguridad y delitos informáticos.

Según el SAP (2018), "Con los avances de la ciencia y la tecnología se ha potenciado la preservación de la especie, de esta manera es como la Carrera Ingeniería Informática de la UNED, busca contribuir al desarrollo de la sociedad y del medio ambiente, a través de la formación de profesionales críticos, independientes, participativos, creativos, con espíritu emprendedor y con un dominio sólido de la Informática" [2].

Cada año, los temas elegidos para presentar en el SAP, corresponde a las necesidades que las mismas personas graduadas del programa responden mediante una encuesta aplicada meses antes de iniciar el seminario. Es por ello que, el tema de la Ciberseguridad y delitos informáticos es uno de los temas con más proyección e interés para los estudiantes y para el país, convirtiéndolo en uno de los favoritos y primordiales del seminario. Por lo tanto, se pretende mostrar los hallazgos con respecto a la aplicación de este tema en los estudiantes y en el país en general, con el objetivo de crear un programa de capacitación y concientización que promuevan el buen uso de la seguridad informática y así disminuir la incidencia de los delitos informáticos en Costa Rica.

2. OBJETIVOS

Objetivo general: Promover un programa de capacitación y concientización en la comunidad estudiantil del programa de Ingeniería Informática de la UNED, para aplicar las buenas prácticas tecnológicas y asumir un rol de apoyo en cuanto a seguridad informática se refiere, contribuyendo a minimizar el impacto de la reincidencia de los delitos informáticos en Costa Rica.

Los objetivos específicos se citan a continuación:

1. Describir las estadísticas sobre la reincidencia de los delitos informáticos más frecuentes en Costa Rica.
2. Establecer las buenas prácticas seguridad informática en el ámbito profesional y académico de la UNED.
3. Proponer la capacitación y divulgación sobre buenas prácticas en seguridad informática en la comunidad estudiantil de la UNED, que permita la concientización sobre el uso seguro y responsable del internet y las nuevas tecnologías.

3. CONCEPTOS TEÓRICOS

Para abordar los conceptos teóricos que tratan en este artículo, se presentan los siguientes:

Ciberseguridad: Para ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información), la ciberseguridad es 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" [3].

Seguridad de la información: Según la norma de calidad internacional ISO 2700, la cual se encarga de establecer el conjunto de estándares internacionales relacionados con la seguridad de la información, define la misma como la siguiente:

"Preservación de la confidencialidad, integridad y disponibilidad de la información" [4]. Lo anterior, quiere decir que, es importante implantar medidas preventivas y correctivas para garantizar la autenticidad, integridad y disponibilidad de la información, de manera que esta no sea alterable, ajena ni propensa a manipulación y ataques informáticos.

Para INCIBE, la protección de la información se expresa en torno a la protección de los tres pilares básicos de la ciberseguridad anteriormente mencionados, los cuales se definen a continuación:

*"*Confidencialidad*:* implica que la información es accesible únicamente por el personal autorizado".

*"*Integridad*:* hace referencia a que la información sea correcta y esté libre de modificaciones y errores". La información puede ser alterada intencionalmente o ser incorrecta, basando nuestras decisiones sobre ella.

"Disponibilidad*:* hace referencia a que la información esté accesible, a las personas o sistemas autorizados, cuando sea necesario" [5].

Delito informático: Lázaro Domínguez, indica que un delito informático es aquella acción delictiva, bien de tipo tradicional bien novedosa, que se comete a través de un nuevo medio -las redes informáticas- o con los recursos facilitados por aquellas: ordenadores y herramientas de software [6].

El Consejo de Europa, con motivo sobre un Convenio sobre la Ciberdelincuencia celebrado en el 2001, estableció unas categorías que desde entonces gozan de una gran aceptación dividendo los delitos informáticos en cuatro grupos:

1. Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Acá se pueden citar los actos como: el acceso no autorizado los sistemas de información y redes, manipulación de los datos, interferencias en el funcionamiento de las instalaciones y el empleo de aparatos y dispositivos que hagan posible lo anterior mencionado.
2. Delitos que se derivan de la falsificación, supresión o borrado de datos, generalmente para la obtención del algún beneficio, por ejemplo: remuneración económica.
3. Delitos relacionados con contenidos, como: pornografía infantil, difusión de pornografía.
4. Delitos relacionados con la vulneración de derechos de autor y propiedad intelectual.

Debido al apogeo del uso y crecimiento del Internet, redes sociales y el avance en la tecnología informática, así como otros aspectos culturales, políticos y sociales, hace que de la clasificación anterior, surjan otros delitos informáticos derivados del terrorismo, la corrupción, prostitución, estafas, fraudes, chantajes, abusos sexuales, amenazas, daños, extorsiones, cyberbulling, todos ellos haciendo uso de al menos un dispositivo electrónico, que son indispensables comprender y estudiar para crear mecanismos de concientización y divulgación de buenas prácticas para hacerle frente a la detención de esos actos delictivos.

4. DELITOS INFORMÁTICOS EN COSTA RICA

Costa Rica no está ajeno a los ataques cibernéticos y la frecuencia en que los delitos informáticos ocurren día a día, muchos suceden por el desconocimiento y falta de formación del público general, sobre el buen uso del internet y dispositivos electrónicos.

El Organismo de Investigación Judicial de Costa Rica (OIJ), es una institución de carácter público perteneciente al Gobierno que, al ser una dependencia de la Corte Suprema de Justicia, actúa como un ente auxiliar de los Tribunales Penales y del Ministerio Público, para garantizar la imparcialidad, honestidad y objetividad de las investigaciones criminales. Es por ello que dentro de este Organismo se encuentra la Unidad de Análisis Criminal, que dentro de sus tareas está ejecutar labores profesionales con el análisis y estadística criminal, así como recopilar, evaluar, procesar, analizar y comunicar información general o concreta sobre la actividad criminal, con el fin de apoyar la planificación estratégica y operativa de la acción policial contra el delito, realizar análisis comparativos de casos; de fenómenos criminales, de grupos de autores, entre otros [7].

Con base en las estadísticas obtenidas de dicha Unidad de Análisis Criminal, se muestra en la figura 1, los delitos informáticos más frecuentes en Costa Rica, durante el I semestre del 2019:

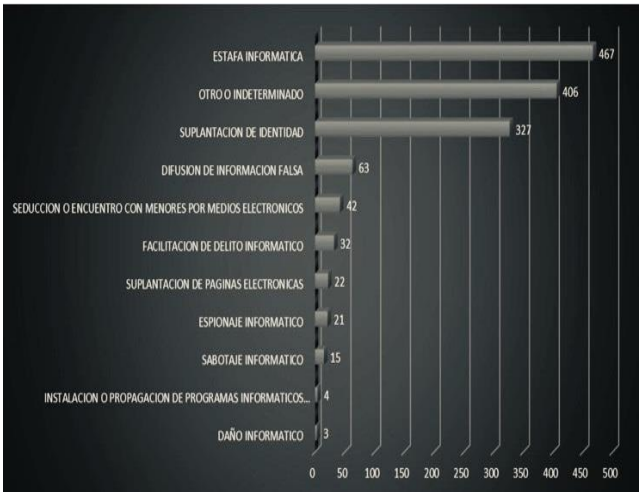


Figura 1. Incidencia de delitos informáticos por delito en Costa Rica, I semestre 2019.

Fuente: Unidad de Análisis Criminal, Organismo de Investigación Judicial de Costa Rica, 2019.

Según el gráfico anterior, se deduce que, de los 1402 delitos informáticos ingresados a la Oficina de Recepción de Denuncias del OIJ, un total de 467 se trata de estafa informática, 406 otro o indeterminado y 327 suplantación de identidad.

Se desprende entones que la estafa informática, es catalogada como aquella acción que, tiene relación con la obtención, alteración o borrado de la información, o bien, interferencia de un tercero (ilegítima) en el acceso a un sistema informático con el fin de obtener un beneficio propio generalmente monetario en perjuicio del tercero y de esta forma da origen al delito como tal.

Así mismo, se aprecia en la estadística del gráfico anterior que, otro de los delitos más frecuentes es la suplantación de identidad y esto tiene relación también con la creación de perfiles falsos en redes sociales y páginas WEB falsas que, hacen creer al público en general, que es el perfil o sitio de internet original y verdadero y es acá donde se origina la estafa y conlleva a un surgimiento de otros delitos informáticos reincidentes, entre ellos: acoso, extorsión, manipulación de la información, vulnerabilidad de la información personal, trata de personas y estafas informáticas.

De acuerdo a las zonas del país donde hay mayor incidencia de los delitos informáticos, se resume en el siguiente gráfico de la figura número 2 a continuación:

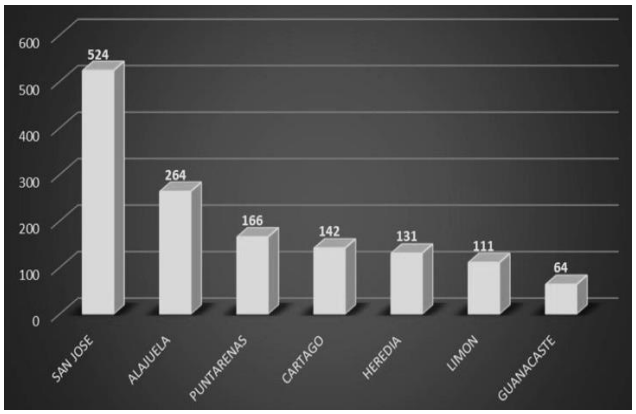


Figura 2. Incidencia de delitos informáticos por provincia en Costa Rica, I semestre 2019.

Fuente: Unidad de Análisis Criminal, Organismo de Investigación Judicial de Costa Rica, 2019.

Según la figura 2 anterior, la provincia de Costa Rica de mayor prevalencia es San José con 524 denuncias, seguido de Alajuela con 264 y Puntarenas 166, esto evidencia que en la zona capital donde se concentra la mayor parte de la población, así como se encuentran las mayores universidades y el entorno laboral, es donde se cometen más delitos informáticos.

De acuerdo a la información proporcionada por la Unidad de Análisis Criminal del OIJ de Costa Rica, para el año 2019 se concluye que, el delito de mayor incidencia fue la estafa informática para una cantidad de 467 delitos, donde la provincia del país más afectada fue San José y el mes de mayor incidencia al delito mencionado fue en julio.

En la figura 3 siguiente, se aprecia lo indicado anteriormente sobre la provincia de Costa Rica donde hay más concurrencia de delitos informáticos.

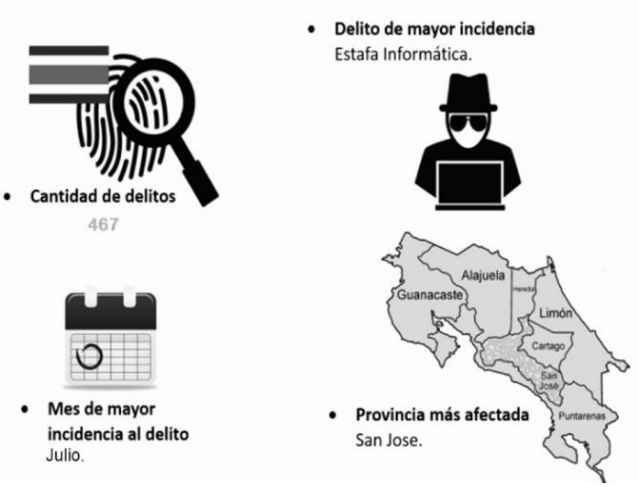
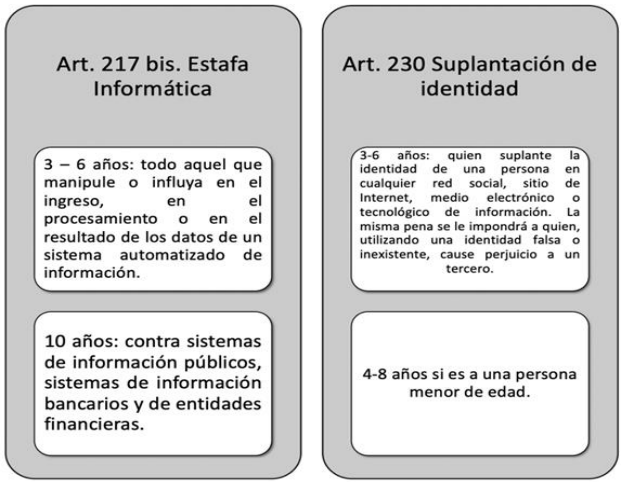


Figura 3. Estadísticas sobre la incidencia de delitos informáticos en Costa Rica, año 2019.

Fuente: Unidad de Análisis Criminal, Organismo de Investigación Judicial de Costa Rica, 2019.

Aun así, teniendo en cuenta los hallazgos mostrados, es importante indicar que, en Costa Rica, existe un código penal mediante una ley (Ley 9048) que hace frente a la respuesta en caso de incurrir algún delito informático de los indicados anteriormente, estableciendo una pena de prisión para todo aquel que lo cometa [8].

En la siguiente figura número 4, se muestra las principales penas de acuerdo a los delitos informáticos más reincidentes, entre ellos la estafa informática y la suplantación de identidad, las cuales deben aplicarse en caso de cometerse.



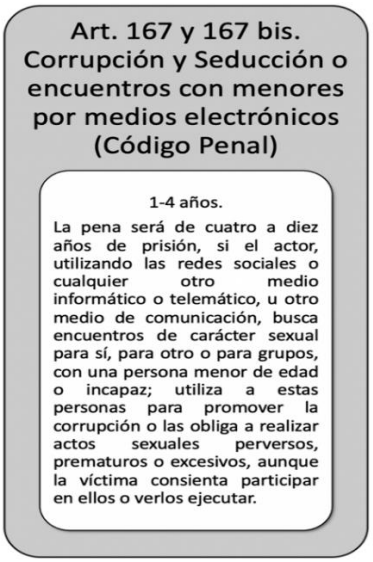


Figura 4. Ley 9048 sobre la pena de los delitos informáticos en Costa Rica.

Fuente: Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal, N.º 9048, Costa Rica.

5. RELACIÓN DE LAS ESTADÍSTICAS DE DELITOS INFORMÁTICOS CON EL ENTORNO ESTUDIANTIL

Según las estadísticas mostradas anteriormente, se apreció que en todo el territorio nacional se presentan denuncias relacionadas con delitos informáticos, por lo tanto, es necesario hacerle frente para tratar de minimizar esos datos, ya que la mayoría de los delitos ocurren por falta de conocimiento y de formación sobre ciberseguridad, tanto para la población con estudios tecnológicos como para el público en general.

Al ser la UNED, una Universidad de educación a distancia con una trayectoria de cuatro décadas y al ofrecer el programa de Ingeniería Informática en todo el territorio nacional debido a esta facilidad y al uso de plataformas virtuales en educación, permite comprometerse en que el estudiante asuma un proceso de aprendizaje que le permite concluir sus estudios con mayor accesibilidad y facilidad, conservando siempre los indicadores y estándares de calidad académica que su acreditación requiere.

Es por lo anterior que, la carrera de Ingeniería en Informática al tener acceso a todos los estudiantes del país, debe realizar, capacitar, promover y divulgar un programa de actualización profesional y formación sobre la ciberseguridad y atención a los delitos informáticos a nivel nacional, considerando que es un tema que los mismos profesionales graduados han solicitado capacitarse y tomando en cuenta los datos mostrados en las estadísticas anteriores, donde al estar viviendo en una era digitalizada, la incidencia de delitos informáticos en el país es

vital y se debe hacer frente a esto desde la educación y a todos aquellos futuros profesionales que están actualmente cursando una carrera de educación tecnológica. De manera que contando con la adecuada formación y acatando las buenas prácticas en ciberseguridad se logre disminuir la frecuencia de delitos informáticos en Costa Rica.

6. BUENAS PRÁCTICAS DE CIBERSEGURIDAD EN EL ÁMBITO ESTUDIANTIL Y EMPRESARIAL

Como parte de las buenas prácticas que todo profesional técnico y personal no técnico debería acatar y tener presente, tanto a nivel personal como empresarial, destacan a continuación los siguientes [9]:

1. Aprender a identificar aquellas amenazas tecnológicas que pueden ser intencionadas por terceros o accidentales, como: vandalismo, espionaje, robo de información confidencial y técnicas de ingeniería social.
2. Proteger los activos de toda organización, más que todo los dispositivos tecnológicos, así como definir responsabilidades de protección sobre los mismos.
3. Aprender la importancia de clasificar la información que permita aplicar las medidas de seguridad oportunas, para ello considerar siempre los tres pilares de la seguridad informática: confidencialidad, integridad y disponibilidad.
4. Realizar mecanismos de respaldos constantes y seguros de la información y de sus sistemas computacionales, con su debidos permisos y encriptación necesaria, de manera que solo este accesible por el personal permitido.
5. Realizar copias de seguridad para evitar la pérdida de datos, hasta la monitorización y el registro de las incidencias.
6. Asegurarse siempre el correcto funcionamiento de los equipos electrónicos, desde el tratamiento de la información, instalación y puesta en marcha, acatando la actualización de los mismos y protección ante software malicioso.
7. Documentar todas las tareas técnicas que todo personal realiza en una organización y así estar preparados ante cualquier incidente.
8. Garantizar que todo software o sistema que se utilice y se instale, se realice de acuerdo a los protocolos y guías de seguridad necesarias.
9. Aplicar actualizaciones constantes de todo equipo computacional y dispositivo electrónico, de manera que siempre cuente con el último software actualizado para hacer frente a las vulnerabilidades y ataques informáticos que puedan presentarse.
10. Verificar que todos los equipos cuenten con un antivirus apropiado y original, y que se realicen correctamente los análisis periódicos de los equipos, para evitar infecciones.
11. Contar con un sistema de monitoreo constante de los sistemas de información y equipos informáticos, con el fin de hacerle frente a pérdidas de servicio, fallas o incluso accesos no autorizados a los mismos.
12. Contar siempre con un plan de recuperación de la información ante desastres, que permita la restauración de los datos, el hardware y software crítico de una organización ante un desastre.
13. Uso de contraseñas seguras y adecuadas, para acceder tanto a los dispositivos personales, estudiantiles y organizacionales, así como tener una política segura en la creación, mantenimiento y cambio de contraseñas, con el fin de mantener la seguridad y privacidad de la información.
14. Descargar actualizaciones para nuestros dispositivos solamente desde su tienda o sitio oficial.
15. Atención a los correos electrónicos “no deseados”, eliminar aquellos que parezcan sospechosos o no conocidos, ya que se puede ser víctima de una suplantación de identidad.
16. Capacitarse en materia de ciberseguridad, ataques informáticos y gestión de incidentes, con el fin de tener la capacidad de hacerle frente a los ataques y delitos informáticos mediante los protocolos, herramientas y mecanismos de seguridad apropiados. Lo anterior, tanto para estudiantes como profesionales en el área, debido a que la tecnología cambia día a día y la actualización constante es esencial.

7. CONCLUSIONES Y RECOMENDACIONES

Con respecto a los hallazgos, interpretación de contenidos y buenas prácticas presentadas en este artículo, se obtienen las siguientes conclusiones y recomendaciones:

1. Asumir un rol de apoyo y aprendizaje en seguridad informática para el sector académico del programa de Ingeniería Informática de la UNED, con el fin de que contribuya en el desarrollo de actividades académicas y prácticas relacionadas con el tema de Ciberseguridad, de manera que este personal también asuma un compromiso de capacitación que ayude a inculcarlo a los estudiantes.
2. Continuar aplicando el tema de ciberseguridad y seguridad informática en el seminario de actualización profesional (SAP) que ofrece la UNED a los profesionales graduados del programa de Ingeniería Informática.
3. Hacer del conocimiento de la Escuela de Ciencias Exactas y Naturales, los expuesto en este artículo, con el fin de que puedan implementar mejoras en la formación de los estudiantes con respecto al tema tratado.
4. Crear un programa de formación, capacitación y divulgación sobre el tema de ciberseguridad, seguridad informática y delitos informáticos a toda la población estudiantil a nivel nacional, mediante cursos y talleres que permita aprovechar la metodología de enseñanza a distancia, haciendo frente a las tendencias actuales de TIC y a la cuarta revolución industrial, de manera que

permita aplicar las buenas prácticas citadas y minimizar el impacto de la incidencia de delitos informáticos en Costa Rica, creando conciencia sobre ello.

5. Como parte del entorno cultural y de bien social que caracteriza a la UNED, se recomienda crear un programa de formación y divulgación sobre buenas prácticas informáticas al público general del país, tanto en escuelas, colegios y otras universidades, de manera que el personal no técnico también se forme y aprenda sobre la materia.

8. REFERENCIAS

[1] Universidad Estatal a Distancia (2019) **Misión y visión de la UNED**. San José, Costa Rica. Obtenido en: https://www.uned.ac.cr/rectoria/myv

[2] Universidad Estatal a Distancia (2018) Acontecer, **Ingeniería Informática actualiza conocimientos en Inteligencia Artificial y Ciberseguridad**. San José, Costa Rica. Obtenido en: https://www.uned.ac.cr/acontecer/a-diario/gestion-universitaria/3299-ingenieria-informatica-actualiza-conocimientos-en-inteligencia-artificial-y-la-ciberseguridad

[3] ISACA (2019) Cibsersecurity. USA. Obtenido en: http://www.isaca.org/Search/Pages/DefaultResults.aspx?k=cybersecurity&s=Site%20Content&start1=0&ct=Site&cs=ISACA&scopes=People,Site%20Content,Conversations

[4] ISO 27000 (2019) Seguridad de la información. Madrid, España. Obtenido en: http://www.iso27000.es/glosario.html

[5] Instituto Nacional de Ciberseguridad España, INCIBE Cómo gestionar una fuga de información: una guía de aproximación para el empresario. Vol. 1, 2016, pp. 4-5, León, España.

[6] Francisco Lázaro Domínguez, Introducción a la Informática Forense, pp. 28-29. Editorial RA-MA. Madrid, España

[7] Organismo de Investigación Judicial (2019), Unidad de Análisis Criminal. San José, Costa Rica. Obtenido en: https://sitiooij.poder-judicial.go.cr/index.php/oficinas/oficina-de-planes-y-operaciones/unidad-de-analisis-criminal

[8] Procuraduría General de la República (2019). Sistema Costarricense de Información Jurídica. Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal N.º 9048, San José, Costa Rica. Obtenido en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

[9] Instituto Nacional de Ciberseguridad España, INCIBE Buenas prácticas en el área informática. Vol. 1, 2019, León, España.