Revista Especializada de Ingeniería y Ciencias de la Tierra
Vol: 2 N°2 Enero - Junio 2023
ISSN: L2805 -1874

Seguridad de los Sistemas Informáticos Universitarios: Retos Pendientes

Security of University Computer Systems: Pending Challenges

Bohen Gisela Solís Tejedor[1], Humberto Valderrama Castrellón[2], Elzebir Tejedor De León[3], Donatila Vásquez de Ayala[4]

[1]Licenciada en Sistemas, Licenciada en Tecnología Educativa, Magíster en Auditoría de Sistemas, Especialista en Docencia Superior. Docente de la Universidad de Panamá. Correo: bohen.solis@up.ac.pa https//orcd.org/0000-0002-2159-3584

[2]Licenciado en Sistemas Informáticos, Especialista en Docencia Superior. Docente de la Universidad Especializada de las Américas https://orcid.org/0000-0003-3024-5036 Correo: humberto.valderrama.8@udelas.ac.pa

[3] Doctora en Ciencias de la Educación, Especialista en Docencia Universitaria. Docente de la Universidad de Panamá. https://orcid.org/0000-0001-7836-9287 Correo: elzebir.tejedor@up.ac.pa

[4]Licenciada en Humanidades con especialización en Español. Especialista en Docencia Superior. Docente de la Universidad de Panamá. Correo: donatila.vasquez@up.ac.pa https//orcid.org/ 0000-0002-0366-836X

RESUMEN

El objetivo de este artículo es analizar los retos de la seguridad de los sistemas informáticos de las universidades. Metodológicamente, este artículo es descriptivo y documental y se basó en la redacción del planteamiento de una serie de retos de la seguridad de los sistemas informáticos universitarios. Para el desarrollo de este artículo se realizó una búsqueda en la base de datos de Google Académico, además, se indicó en este motor de búsqueda el filtro de "intervalo específico", que correspondió al período comprendido entre 2018 y 2022, ordenado por relevancia. Se especificó mediante la cadena de búsqueda, el idioma y el tipo de documento; se descartaron posteriormente ciertos tipos de documentos. Se incluyeron trabajos de un período de cinco años respecto a la fecha de realización de esta investigación (2022): artículos de revistas (indexadas), informes de conferencias, capítulos de libros, libros y tesis de fin de grado, de maestría y doctorales. La búsqueda estuvo basada

en tres criterios: título, resumen y palabras clave (las más utilizadas fueron: sistemas informáticos, universidad, seguridad informática, políticas de seguridad informática, entre otras). Se concluye que los retos de la seguridad de los sistemas informáticos son: la gestión de la seguridad informática, el establecimiento de políticas de seguridad informática, aplicación de estándares, adopción de metodologías para la incorporación de los elementos de seguridad informática acordes a la realidad universitaria, el establecimiento de marcos jurídicos, el establecimiento de un gobierno universitario de tecnología, la formación y capacitación de los colaboradores, análisis de vulnerabilidades de la seguridad informática y finalmente, se plantea la necesidad que tiene la Universidad de realizar auditorías externas a su sistema informático.

Palabras clave: seguridad, sistemas informáticos, universidad, equipos informáticos, análisis de vulnerabilidades.

ABSTRAC

The objective of this article is to analyze the security challenges of university computer systems. Methodologically, this article is descriptive and documentary and was based on the drafting of a series of security challenges for university computer systems. For the development of this article, a search was carried out in the Google Scholar database, in addition, the "specific interval" filter was indicated in this search engine, which corresponded to the period between 2018 and 2022, ordered by relevance. Specified by search string, language, and document type were subsequently dropped, certain books. Papers from a period of five years with respect to the date of completion of this research (2022) were included: journal articles (indexed), conference reports, book chapters, books and end-of-degree, master's and doctoral theses. The search was based on three criteria: title, abstract and keywords (the most used were: computer systems, university, computer security, computer security policies, among others). It is concluded that the security challenges of computer systems are: computer security management, establishment of computer security policies, application of standards, adoption of methodologies for the incorporation of

computer security elements according to the university reality. , the establishment of legal frameworks, the establishment of a university government of technology, the training and training of collaborators, analysis of computer security vulnerabilities and finally, the need for the University to carry out external audits of its computer system.

Key words: Security, computer systems, university, computer equipment, vulnerability analysis.

INTRODUCCIÓN

En las dos primeras décadas del Siglo XXI, el Internet, las tecnologías, las comunicaciones, y la digitalización, se han convertido en factores claves de una organización, por lo que Téllez, et al. (2016), señala que la auditoría de los sistemas informáticos se ha convertido en un factor clave para el cumplimiento de los objetivos organizacionales, comprobando su correcta utilización para así, poder obtener el máximo provecho de los servicios tecnológicos-informáticos.

Los sistemas de información y la informática juegan un rol cada vez más importante en las empresas, por lo que es necesaria la realización de auditorías informáticas para medir su eficiencia y evitar problemas informáticos en la empresa (Infante-Moro, et al, 2016). Entonces, el éxito de una organización se basa, en gran medida, en su capacidad para gestionar los riesgos, y es precisamente allí, donde radica la importancia de las auditorías informáticas, ya que permiten determinar las fortalezas y debilidades de su sistema de información (Arcentales-Fernández y Caycedo-Casas, 2017).

Bracho-Ortega, et al (2017), afirma que es sumamente importante conocer los riesgos de los sistemas de información e informáticos de una institución y que para ello se deben considerar canales, y el modo en que se considera la aplicación de medidas para calcular el riesgo de cada canal y las principales son: la porosidad (OpSec), los controles y las limitaciones. Estas medidas permiten, una vez analizado el canal correspondiente, determinar valores numéricos para cada ítem establecido y poder hacer recomendaciones en cuanto a los canales auditados.

Como ya se ha establecido, los avances tan marcados que han presentado las Tecnologías de Información y Comunicación (TIC, de aquí en lo sucesivo) y la inclusión de ellas, "en las actividades que pueden llevar al éxito a una organización, por otro lado, también pueden aumentar la probabilidad del surgimiento de problemas, conflictos y errores al realizar alguna de las tareas en la ejecución de procesos" (Salgado, et. al, 2017, p. 1).

La Universidad (como toda organización), también tiene la necesidad de contar con una herramienta de apoyo para la gestión de la información y de la seguridad informática para poder realizar diferentes actividades inherentes a sus funciones como lo son efectuar reportes de incidentes, control del estado de protección de los medios informáticos, así como contar con una mejor preparación de los trabajadores en aspectos relacionados con la seguridad informática y la resolución de un conjunto de dificultades en este aspecto, como son los concernientes con la fluidez de la información, la centralización y confiabilidad en sus datos, (Díaz-Ricardo, 2014), considerando los pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad). (Bogantes, 2020, p. 24). Tomando en consideración esto, la Universidad se enfrenta a los siguientes retos y tendencias relacionados con la auditoría de sus sistemas informáticos.

II. DESARROLLO.

La seguridad de la información es, según Roque & Juárez (2018, p. 2), un tema central para todos los usuarios de equipos de cómputo; especialmente, porque el uso del Internet con su masificación y popularización ha traído consigo importantes riesgos de seguridad, convirtiéndose en una rama de la informática que se encuentra en auge actualmente y se ha constituido en motivo de preocupación de grandes entidades a nivel global y local, puesto que cada día los ataques a las infraestructuras tecnológicas de las organizaciones aumentan de la misma manera que los ataques dirigidos a personas en particular, teniendo como objetivo el robo de contraseñas, cuentas de usuario, acceso a información confidencial, secuestro de la información, entre otros.

El Internet y su veloz adopción, los dispositivos móviles y las aplicaciones en la nube han provocado que las empresas encargadas de velar por la seguridad de la información no implementen al mismo ritmo medidas que mejoren la seguridad para enfrentar las amenazas del mundo actual, que hasta ahora ha sido relegada a un segundo plano; por lo que, hay que

promocionar, en todos los usuarios de medios informáticos, el conocimiento de buenas prácticas en el uso de sistemas de información, dispositivos electrónicos y redes sociales. (Bogantes, 2020, p. 24).

Aunque ya se han caracterizado una serie de delitos informáticos, Acurio (2016), todavía hay mucho campo que legislar para distinguir entre "delitos informáticos, criminalidad mediante computadora, delincuencia informática, criminalidad informática" (p. 4), pero hay mucho por hacer, porque cada día surgen más amenazas. Es por ello que el análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad, plantean una serie de retos y la auditoría de sistemas informáticos se ha convertido en una herramienta donde "las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización. De allí la necesidad de identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación" (Solarte, et al, 2015, p. 492). Esto a su vez se ha tornado en una prioridad de cualquier organización, y las universidades no escapan a esta situación, acarreándoles desafíos a la aplicación de esta herramienta a los sistemas informáticos universitarios y entre ellos están:

- **Gestión de la seguridad informática.**

La gestión de la seguridad informática debe ser visualizada como un proceso bien definido, pero siendo capaz de incrementar su mejoramiento de forma continua, y para la verificación de esto, es fundamental evaluar la efectividad de la gestión de la seguridad de la información y los riesgos asociados a su uso, en redes de computadoras de la universidad. (Altamirano, 2019, p. 248), con la finalidad de establecer objetivos y controles que permitan minimizar las vulnerabilidades del sistema de gestión. (Imbaquingo, et. al, 2019, p. 349).

Las instituciones públicas (entre las cuales se cuentan las universidades estatales), según Chicaiza & Díaz (2014, p. 5), muestran un cierto grado de desinterés en temáticas relacionadas con la seguridad de la información y esto se ha podido establecer a través de indicadores como el poco presupuesto que las autoridades administrativas le asignan a este aspecto, a pesar de que las leyes y normativas universitarias, las obligan a implementar controles de seguridad para el resguardo de la información que ellas manejan, constituyendo a los controles y a los procesos de gestión, en algo prioritario desde un enfoque de automatización, de integración y para disminuir la complejidad de la gestión y aumentar así

la efectividad de los controles de seguridad de la información en redes de computación universitarias. (Benavides & Blandón, 2018, p. 87)

En términos generales, se ha hecho evidente la necesidad de implementar modelos de verificación que vayan de acuerdo con los principales estándares, recomendaciones y regulaciones existentes, tanto a nivel internacional como nacional, sobre gestión de la seguridad de la información, y ofreciendo una visión integral de controles de seguridad de la información, en la que se consideren todos los controles automatizables y no automatizables y se definan acciones por realizar en cada uno de los casos. (Enríquez, 2018, p. 18).

- **Establecimiento de políticas de seguridad informática.**

Dussan (2006), sostiene que en la actualidad todas las organizaciones, al igual que las universitarias, deben preocuparse por la creación de políticas claras, concisas, contextualizadas a una realidad, enfocadas en las personas, los procesos y los recursos. Según las cifras presentadas por este autor sobre estudios relacionados con seguridad informática en las empresas, más de un 60% de las compañías no cuenta con programas y políticas establecidas de seguridad informática, lo que debe ser un reflejo de lo que también ocurre en las universidades. En un momento en donde la globalización, no solo ha influido en la economía sino también en otras áreas sociales/científicas, la universidad debe hacer un gran esfuerzo en fortalecer su plataforma tecnológica e invertir en programas de seguridad. (Díaz-Ricardo, et. al, 2014, p. 1). Por lo que, se considera que es responsabilidad de los rectores liderar proyectos que permitan entrar a una educación soportada en un mundo digital, dado que la información es "uno de los activos más importantes y valiosos de las organizaciones" (Dávalos, 2013, p. 19).

Al respecto, Viteri (2014), señala que en la actualidad, la Universidad se enfrenta a retos, como por ejemplo los relacionados con la definición de políticas de seguridad informática. El diseño de estas políticas redundará en beneficio de la Universidad y su implementación conllevará un mejor uso de los activos tecnológicos y de la información. Con definición de políticas y de estándares de seguridad informática se busca establecer en el interior de la institución una cultura de calidad, pues con ello se facilitarán los procesos de creación, registro y mantenimiento de las mismas políticas. (Martelo, et al, 2018, p. 3).

- **Aplicación de estándares**

Niño & Silega (2018, p. 205), señalan que el aseguramiento de la información y de los sistemas que la procesan es, por tanto, un objetivo crucial para las organizaciones. La gestión de la seguridad informática minimiza las vulnerabilidades que un sistema pueda presentar, mejorando los mismos mecanismos de seguridad, bajando los costos y el tiempo requerido para solucionar un problema. Sin embargo, un dilema común que encuentran los especialistas en seguridad es que se evidencia la falta de estándares establecidos que protejan el entorno informático.

Los objetivos de control que buscan garantizar los requisitos de seguridad de la información en cualquier sistema de gestión de seguridad de la información se aseguran a través de la aplicación de estándares, que facilitan la evaluación del estado actual de un proceso o un conjunto de procesos en la organización (Salgado, et al, 2017).

Es necesario aclarar que la normalización o estandarización tiene como objetivo fundamental la elaboración de una serie de especificaciones técnicas (normas), que deben ser utilizadas por las universidades, para la seguridad de la información y para la seguridad informática y que deben ser aprobadas por un organismo reconocido. Con relación a esto Bodero (et al, 2022), menciona los siguientes estándares. (Ver Figura 1)

Figura 1

Estándares establecidos por diversos organismos para evaluar la seguridad informática y la seguridad de la información en las universidades. Según Bodero (et al, 2022).

Estándar	**Descripción**
UNE-ISO 14721.	Estándar de alto nivel que proporciona un marco para la definición de una estrategia para auditar todo tipo de soporte digital. Esta norma presenta un plan de preservación de contenido asociado a paquetes de información, bases de conocimiento, sistemas de almacenamiento y disponibilidad. Describe tres modelos para la realización de auditorías: el funcional, el de información y las transformaciones del empaquetado de la información.

ISO 16363	Este estándar es una herramienta para auditar, evaluar, potenciar y certificar repositorios digitales. Proporciona un marco de calidad para el análisis de la consistencia de un repositorio con respecto a la integridad de datos. Además, está íntimamente relacionado con la preservación a largo plazo y su accesibilidad. Los gestores de un repositorio pueden usarlo también como una herramienta de diagnóstico del estado del sistema, así como para planificar acciones que deben ser aplicadas en la gestión. Tres dimensiones son las que están presentes en este estándar: 1) infraestructura organizacional, 2) gestión de objetos digitales y 3) gestión de riesgos de infraestructura y de seguridad. Cada una de estas dimensiones poseen diferentes métricas para validar los requisitos que debe cumplir un repositorio digital para su preservación a largo plazo, además de políticas y procedimientos sobre acceso, diseminación y autenticidad de los objetos digitales
ISO 15489	Estándar que es aplicado a los documentos en cualquier formato o soporte; proporciona una metodología de implementación, describiendo principios y conceptos relativos a la gestión de documentos, los sistemas de gestión, el análisis recurrente del contexto de la organización y la identificación de los requisitos. Además, se enfoca en el cumplimiento de un marco legal y reglamentario. Desde el punto de vista estratégico describe las políticas y responsabilidades de los involucrados en el proceso de auditoría. La norma trata de los beneficios de la gestión de documentos, marco reglamentario, política y responsabilidades, requisitos, diseño e implementación de un sistema de gestión, procesos, controles, supervisión, auditoría y formación.
	Estándar que tiene una parte que está referida a especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital. En esta norma se encuentra un conjunto de especificaciones técnicas, pero además políticas organizativas para la implementación, el almacenamiento y el acceso a

UNE-ISO 14641-1	los documentos electrónicos. Está destinado a usuarios como organizaciones que implementan sistemas de información, servicios de tecnología y de archivo de documentos de terceros. Propone en general tres temas: 1) optimizar el sistema para asegurar la preservación, 2) facilitar la búsqueda de información y 3) asegurar la accesibilidad y el uso de documentos electrónicos. En relación con aspectos de planificación, se pueden observar procedimientos, técnicas y un sistema de gestión del cambio y migración.
UNE ISO 30300, 30301, 30302	Estándar que contempla un conjunto de elementos que interactúan para llevar a cabo la política de gestión documental; en él se encuentran involucrados personas, roles y responsabilidades; los procesos y controles; y la infraestructura. Además, es un aporte a la consecución de una estrategia, en la cual se encuentran incluidos los fines, la misión y las metas de la organización mediante políticas y planteamiento de objetivos. Con esto se busca una adecuada planificación con respecto a acciones, procesos y mejora continua.
UNE-ISO/TR 18492	Conservación de documentos electrónicos a largo plazo. El informe técnico declara la publicación de un marco amplio para el desarrollo homogéneo de políticas y estrategias de conservación. El objetivo de este estándar radica en preservar la información digital auténtica y asegurar exactitud, fiabilidad e integridad a lo largo del tiempo. Diseña una estrategia organizacional de transferencia de información a un sistema de almacenamiento, soporte estable contra la obsolescencia tecnológica, entre otras características enfocadas a la seguridad de la información. Incluye además, el diseño de una estrategia en la organización, tomando en cuenta los cambios tecnológicos, compatibilidad en software y hardware para asegurar la preservación a largo plazo y los objetos digitales.

SO/TR 18128	Este estándar está referido a la información y a la documentación. Evalúa el riesgo en procesos y sistemas de gestión documental. Procura ayudar a las organizaciones a evaluar los riesgos para los procesos y sistemas de registros durante el tiempo. Puede ser utilizado por cualquier organización independiente del tamaño. Permite la identificación de riesgos, los cuales han sido propuestos por la Association of Records Managers and Administrators (ARMA), que es la comunidad de profesionales de gestión de registros, gestión de información y gobierno de la información. Además, permite la evaluación de los riesgos administrativos, de control de documentos, legales o normativos y tecnológicos. Incluye el diseño de una estrategia en la organización, tomando en cuenta los cambios tecnológicos, compatibilidad en software y hardware.
ISO 16919	Estándar que especifica los requisitos para los organismos que realizan auditorías y certificaciones de repositorios digitales confiables candidatos. Está destinado principalmente a aquellos que crean y administran la organización, que realizan la auditoría y certificación de repositorios digitales. Está diseñado para seguir el proceso de mejora continua, que es indispensable en una correcta planificación estratégica y tiene un mecanismo de verificación probado en cada etapa siguiendo una jerarquía de estándares. Los requisitos que propone la norma son generales, estructurales, de información, del proceso y del sistema de gestión.

- **Establecimiento de marcos jurídicos acordes.**

La creciente importancia económica de los datos (para las empresas y para los ciudadanos comunes), conlleva la necesidad de incrementar la adopción de medidas dirigidas a garantizar la seguridad y la privacidad; por lo tanto, resulta indispensable el desarrollo de regulaciones

y de legislaciones (Velasco, 2008), que vayan a la par y poder diferenciar conceptos íntimamente relacionados como: derecho informático empresarial, economía digital, sociedad digital, ciberseguridad, sistemas de información, cómputo en la nube e Internet de las Cosas (Internet of Things) (Becerril & Ortigosa, 2018).

Acurio (2016), manifiesta que actualmente se está viviendo la era de la informática, por lo que cuesta abordar tanto las implicaciones de la información en el fenómeno delictivo o las implicaciones del delito a través de la informática; por lo que, hay que analizar y plantear la insuficiencia de los sistemas jurídicos actuales para regular todos los posibles escenarios donde la actividad informática es usada para cometer delitos informáticos.

A pesar de todos los adelantos que se han hecho en el escenario jurídico aún queda mucho por hacer, ya que no existe una adecuada política de seguridad de la información o una legislación interna (en la mayoría de los países latinoamericanos, (Velasco, 2008); sobre el tema, lo que se haga para garantizar la seguridad y privacidad de los datos, dentro de las organizaciones, debe basarse en estándares internacionales, el derecho comparado y autonomía de la voluntad

En la Universidad, la era de la información y cómo asegurar sus datos y encargada de la ejecución de diferentes proyectos, la actividad legal adquiere una vital importancia, por cuanto, esta:

> […] sirve de soporte a sus procesos de negociación, ejecución y cierre, estando presente, por tanto, en todo momento del ciclo de vida de los proyectos. El desarrollo de estos obliga y da la conveniencia de contar con una adecuada gestión legal para el cumplimiento del régimen jurídico establecido en los países e internacionalmente. Esto permitiría, con el uso correcto de las normas y regulaciones, lograr minimizar incumplimientos o violaciones de la legalidad que puedan darse lugar como parte de la actividad propia de la universidad. (Rodríguez y Ciudad, 2019, p. 421).

La actividad universitaria (docencia, investigación y extensión), es sustentada por las tecnologías digitales y permiten la transmisión y utilización de todos los materiales protegidos por el derecho de autor y a propiedad intelectual (Suñé, 2016), para la transmisión de textos, sonidos, imágenes y programas informáticos por y a través de

Internet, esto se ha convertido en moneda corriente, eliminando las barreras del espacio y el tiempo (Martínez & Pocelli, 2015). Esta facilidad para dar y recibir información y para la comunicación, hace necesario avanzar en un marco regulatorio consistente y coherente con la legislación vigente y que incluya normas y procedimientos que protejan, promocionen y difundan la producción intelectual de miembros de la comunidad universitaria, no solo para su reconocimiento, sino también para su utilización. (Amador, 2018).

Si no se establecen normas jurídicas apropiadas, la tecnología digital podría utilizarse para socavar los principios básicos del derecho de autor (Martínez y Pocelli, 2016). En consecuencia, es necesario un marco jurídico adecuado que establezca una competencia equilibrada que proporcione incentivos a los creadores y productores de conocimiento, (Amador, 2018).

Otra cuestión que llama la atención sobre el uso de la informática, en el proceso enseñanza/aprendizaje es que en este ámbito, debe ocuparse de la evolución de la ley y los principios jurídicos y cómo se aplica la tecnología de la información en los campos relacionados con la academia. Según Domínguez-Bernita, et al (2017), en este escenario, la auditoría informática se debe ocupar de la vida privada, la ética y las cuestiones operacionales que invariablemente surgen cuando los instrumentos electrónicos, la información y los medios de comunicación se utilizan en la prestación de un servicio educativo (Viecco & Pinedo, 2018). Entonces, se deben contemplar aspectos vinculados con la ética y la seguridad informática en la esfera de la educación.

- **Gobierno universitario de tecnología informática**

Al constituirse la información como uno de los activos más valiosos intrínsecamente, las organizaciones deben desarrollar estrategias que permitan certificar la disponibilidad, integridad y confidencialidad en el manejo de la misma que puede estar sujeta a robo, violación y amenazas externas e internas; existe la tendencia, de que esto se puede ir solventado con la creación de un gobierno de tecnología informática y con el uso de buenas prácticas del mismo (Macas, et al, 2017).

Cada día cobra mayor interés la institucionalización de las buenas prácticas (Macas, et al, 2021, García, 2018), que deben ir relacionadas con la prestación de servicios a los usuarios, con el desarrollo de softwares, con la seguridad, entre otras (Martínez & Porcelli, 2016), y con la creación de un gobierno que gestione y que alinee las tecnologías de la información con las estrategias, los recursos y las políticas institucionales, a través de un enfoque integrado, global e imprescindible, ya que de él depende el buen funcionamiento y la evolución de todos los procesos que ocurren en una institución y de la información que necesita la gerencia para tomar decisiones operacionales, tácticas y estratégicas (Martínez & Porcelli, 2015).

Esto se ha convertido en una tendencia y debe orientar e impactar la estructura orgánica universitaria, institución que debe adoptar estrategias que promuevan la activa y efectiva participación (Parra, 2019), de las tecnologías de la información en los procesos de gestión para encarar con éxito los procesos de acreditación, tanto institucional como de carreras y programas y así conquistar la gestión de excelencia a través de la evaluación de los servicios (identificación, análisis, determinación, descripción, documentación, evaluación de la calidad y madurez) (Pasini, et al, 2016).

Viecco & Pinedo (2018), sostienen que la actual tendencia de crear un órgano universitario de tecnología, se ha enfocado en que este debe surgir de un modelo planteado de acuerdo a las necesidades de la universidad para aplicar marcos de referencia de la seguridad de la información y de la gestión de riesgo, permitiendo dirigir y controlar, además, las inversiones que se realicen en tecnología de la información y la comunicación y que estas inversiones, aporten al cumplimiento de las metas institucionales, apoyando la toma de decisiones (Gonzáles, 2016).

- **Actualización de los sistemas operativos.**

En la actualidad, los conceptos de innovación, tecnología y gestión universitaria son palabras clave en el eje central de las diferentes buenas prácticas que deben existir en el quehacer educativo universitario. Ejemplo de estas prácticas es la gestión universitaria, que está siendo modificada desde hace algunas décadas como resultado del impacto de las TICs. Sin duda, el uso adecuado de estas, en la universidad, debe ser producto de una planificación estratégica determinada. Así concebida, coadyuvará en la introducción de cambios en la

gestión, conllevando una mejora de la eficacia y de la eficiencia de determinados procesos básicos de esta dentro de las instituciones (Rodríguez, 2018).

Sin embargo, tal y como lo señala Espinoza (et al, 2018), se hace necesario acotar que en la mayoría de los centros universitarios han existido algunas dificultades para la incorporación de las tecnologías, entre las que se puede destacar: la insuficiencia de equipos por falta de presupuesto, la ausencia de un personal especializado que pueda solucionar los problemas técnicos que se pueden presentar con los equipos y la falta de proyectos dirigidos a la formación y actualización del equipo de colaboradores; son estos los aspectos en los que se pueden resumir los retos a los que se enfrenta la seguridad de los sistemas informáticos. (Quiroz & Macías, 2017)

A partir de esto, es necesario apuntalar que la Universidad debe gerenciar una serie de acciones para trabajar con las fortalezas y superar las limitaciones (Martínez & González, 2019), ya que los sistemas informáticos "constituyen una herramienta que, en el ámbito organizacional, son importantes para el desarrollo de las actividades y la toma de decisiones gerenciales". (Antúnez & Valero, 2022, p. 163). El objetivo de una buena gestión universitaria en tecnología es mejorar la calidad de estos sistemas, a través de sus funciones, elementos y clasificación, ya que se ha logrado determinar que en un sistema de información actualizado es necesario combinar hardware y software adecuados para garantizar su desempeño, pero también, la información disponible en las universidades debe cumplir con: contenido apropiado, actualización, exactitud y accesibilidad. (Sobrevilla, et al, 2017).

Se ha podido comprobar que en la medida que las universidades alcanzan un mayor nivel de informatización en sus procesos y se hacen más dependientes de la tecnología, también se hace evidente que carecen de equipos que les permitan reconocer rápidamente a nuevas amenazas. De allí la necesidad de que puedan responder a través de la reconfiguración de las aplicaciones o instalación de parches, que disminuyan el número de vulnerabilidades que son descubiertas constantemente y utilizadas por los atacantes. (Quiroz & Macías, 2017). Los parches de seguridad deben ir dirigidos a minimizar el tiempo de exposición a amenazas concretas y la universidad debe incluirlos en el presupuesto de mantenimiento para disminuir el riesgo y mejorar la seguridad de su infraestructura. (Zaidman, 2017).

La universidad necesita automatizar un inventario de actualizaciones y parches de seguridad del sistema operativo para poder gestionar mejor sus recursos de hardware y software, la descripción de las funcionalidades, y los artefactos deben estar asociados al servicio que presta como institución educativa. (Quiroz & Macías, 2017). Para ello, necesita crear una herramienta de apoyo en la administración que lleve el control y soporte de los equipos que posee y que a la vez le permita capturar y mostrar los datos de las actualizaciones y parches de seguridad instalados y pendientes de su sistema operativo. (Esguerra, et al, 2004). Lo que además facilitará la automatización de la captura, análisis y consulta de la información sobre las actualizaciones y parches de seguridad contribuyendo al control en el cumplimiento de las políticas de seguridad y a la reducción de riesgos (Torres, 2019).

Otra de las cuestiones que atañe a la Universidad es la seguridad de la información, que es concebida por Bonilla (2019), como uno de los activos más importantes con los que cuentan las diferentes organizaciones en todo el mundo; por esto es necesario velar por su integridad y buen uso. Este activo se ve afectado por diversos problemas, tecnológicamente hablando se debe actuar en pro de la seguridad de la información que garantiza que independientemente del formato en el que se encuentre esta deberá ser íntegra. (Zaidman. 2017). Adicionalmente, las organizaciones se pueden ver afectadas por las vulnerabilidades presentes en los sistemas informáticos e infraestructura implementada, de aquí nacen los cuidados y las medidas que deben tomarse para garantizar que la seguridad informática y de la información dentro de las instituciones de educación superior, hagan uso de la implementación de diversos marcos de referencia adoptados mundialmente. (Maucaylle, 2019).

- **Formación o capacitación de los colaboradores**

Se ha podido comprobar que en la actualidad con el avance exponencial que se ha visualizado en el ámbito tecnológico y con la vinculación de estas innovaciones a los distintos aspectos de la vida cotidiana, ha cambiado la vida de las personas, facilitando el intercambio de datos e información para agilizar, no solo la productividad, sino también la comunicación entre las personas. (Castillo, 2015). Con respecto a lo expresado, Guerrero (2020), afirma que lo anterior se ve evidenciado en el desarrollo personal así como en el empresarial, ámbitos donde el manejo de la información sea cual sea su uso tiene un gran valor.

Normalmente se cree que la información manejada si no son contraseñas, datos financieros o cuentas electrónicas no tiene valor alguno, pero eso depende de cómo se use; el más pequeño dato puede revelar una gran cantidad de información.

En consecuencia, Guerrero (2020), afirma que con las nuevas tecnologías van apareciendo nuevos riesgos que buscan lo más valioso de las personas y de las empresas; por lo que es necesario que la información, los equipos que la contienen, los equipos que la manejan, deben ser protegidos, (Gutiérrez, et al, 2018). Pero en realidad, la Universidad debe ser una institución preocupada por la adopción de nuevos controles para proteger los recursos de información que posee y que son importantes (Hernández, 2010).

La Universidad se ha convertido en una organización que debe estar constantemente actualizando las medidas para salvaguardar la información que maneja (Imbaquingo, et al, 2019), y buscando de esta manera brindar una protección adecuada para las nuevas tecnologías con herramientas de virtualización, realizando la identificación de los equipos y el escaneo de las vulnerabilidades presentes en ellos (Igarza, et al, 2018), para tomar acciones correctivas que contribuyan a la protección de sus sistemas, entendiendo que la seguridad informática no es un todo si no la suma de un conjunto de partes (Imbaquigo, et al, 2019), formada por los controles de seguridad, las políticas de seguridad de la información, los equipos de gestión y atención de incidentes, entre muchos otros, que actúan conjuntamente protegiendo los activos de información y respaldando los servicios que ofrece, sus aplicaciones, la red y los equipos de una organización.

En este contexto, la formación y capacitación de los colaboradores en forma constante es de suma importancia dado el cambio acelerado de los recursos y herramientas tecnológicas (Espinosa, et al, 2018). Finalmente, los sistemas de información no solo funcionan de acuerdo con los avances tecnológicos, sino con el uso y capacitación de sus usuarios, pero también, de los colaboradores de una organización. Estos, están debidamente capacitados y actualizados, cuando evitan situaciones donde estén comprometidos los equipos de software y hardware, así como siendo capaces de diseñar e implementar un Plan de Seguridad Informática en la Universidad, que garantice que la información está siendo gestionada por los colaboradores de forma segura y que los riesgos son identificados, gestionados y mitigados de forma proactiva para prevenir que las amenazas se materialicen. Finalmente,

se espera que la Universidad cuente con un proceso de seguridad informática maduro que brinde tranquilidad y que apalanque de forma óptima y segura los proyectos actuales y futuros dando valor esta organización en todos sus procesos misionales. (Duque, 2022).

- **Análisis de vulnerabilidades de seguridad informática**

Morales, et al (2020), hace hincapié que las organizaciones se deben preocupar por la implementación de un sistema de seguridad, por la evolución de la tecnología y la constante demanda que tienen estas para proteger su información y poder así, mantener su prestigio e imagen. La adopción de medidas de seguridad ha facilitado que los sistemas informáticos puedan mantenerse íntegros, estén disponibles, tengan privacidad, control y que la información que es manejada por ellos sea auténtica. (Tapia, 2019). Al hablar de seguridad informática es fundamental distinguir algunas de las tipologías que existen, siendo los principales elementos para dar protección el software, la red y el hardware.

Según Tapia (2019), la seguridad de hardware está relacionada con la protección de dispositivos que se usan para proteger sistemas y redes, como ejemplo, aplicaciones y programas de amenazas exterior. Esta seguridad también se refiere a la protección de equipos físicos frente a cualquier daño físico.

Por otra parte, la seguridad de software, de acuerdo con Navarrete (2019), es usado para salvaguardar los sistemas frente a ataques malintencionados de hackers y otros riesgos relacionados con las vulnerabilidades que pueden presentar los softwares, ya que, a través de estas vulnerabilidades, los intrusos pueden entrar en los sistemas, por lo que se requiere de soluciones que aporten, entre otros, modelos de autenticación. (Tejena-Macías, 2018).

Principalmente, la seguridad de red está relacionada con el diseño de actividades para proteger los datos que sean accesibles por medio de la red y que existe la posibilidad de que sean modificados, robados o mal usados. (Solarte, et al, 2015). Las principales amenazas en esta área son: virus, troyanos, phishing, programas espía, robo de datos y suplantación de identidad. La seguridad perimetral en redes debe evolucionar para ofrecer una mayor confiabilidad a los usuarios sobre la transparencia y protección de su información en cuanto al acceso a diferentes servicios; por ello se torna necesario rastrear y evaluar las

vulnerabilidades de los sistemas informáticos institucionales (Serrato, 2016), especialmente, porque hoy existen muchas personas que usan sus conocimientos y ética profesional de una forma incorrecta al ingresar a redes informáticas restringidas ocasionando pérdidas multimillonarias alrededor del mundo. Díaz (et al, 2021), hace hincapié en la necesidad que tiene la Universidad de reconocer el estado actual de la seguridad informática y perimetral identificando los riesgos y las vulnerabilidades a los que puede estar expuesta por el desconocimiento de controles y políticas que se deben establecer e implementar para la correcta gestión y aseguramiento de la información que ella tiene, produce, genera o utiliza en el ejercicio de sus actividades misionales.

Los mecanismos de seguridad pueden involucrar desde la implementación de guías y/o protocolos para el control de brechas de seguridad en los servicios de internet la cual garantiza una mejor seguridad para todas las aplicaciones y conexiones que utilizan los servicios de Internet, hasta el análisis de vulnerabilidades. Mifsud (s/f, como se citó en Serrato, 2016), define vulnerabilidad como:

> […] una debilidad de cualquier tipo que compromete la seguridad del sistema informático; se pueden agrupar en: Diseño: a) debilidad en el diseño de protocolos utilizados en las redes, b) políticas de seguridad deficientes o inexistentes; implementación: i) errores de programación, ii) existencia de "puertas traseras" en los sistemas informáticos, c) descuido de los fabricantes; uso: i) mala configuración de los sistemas informáticos, ii) desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática, iii) disponibilidad de herramientas que facilitan los ataques, d) limitación gubernamental de tecnologías de seguridad; vulnerabilidad del día cero: i) se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución conocida, pero se sabe cómo explotarla. (p. 21).

La Universidad debe ser modelo de gestión de la calidad de no solo sus procesos sino también de la seguridad, integridad, disponibilidad, confidencialidad, autenticación y confiabilidad de la información y de sus sistemas informáticos. (Avilés, 2010).

- **Realización de auditorías externas de la seguridad informática.**

Bailon (2019), afirma que para una organización es fundamental realizar auditorías de la seguridad informática con la finalidad de evaluar el control y mantenimiento de la infraestructura tecnológica que involucra a:

- Redes. El objetivo es evaluar el funcionamiento y la seguridad de las redes empresariales, como VPN, wifi, firewalls, antivirus, etc.
- Control de acceso. Son auditorías centradas en los controles de acceso y que están vinculadas a dispositivos tecnológicos físicos como cámaras de seguridad, mecanismos de apertura de barreras y puertas y software específico para el control de accesos.
- Hacking ético. Son auditorías que se realizan para medir el nivel de seguridad de una empresa, realizando una simulación de ataque externo (como si se tratase de un ataque real) para evaluar los sistemas y medidas de protección, identificando sus vulnerabilidades y debilidades.

La finalidad de la auditoría informática es verificar las normas de control interno y evidenciar los protocolos para la protección de la información digital (Urquizo, 2021, p. 10), pero lo que es verdaderamente importante es que no solo lo realice el departamento, secretaría, coordinación de Tecnologías de la Información, sino que la organización también solicite esta a empresas especialmente dedicadas a ello, y debe ser realizada en función de fases.

Noguera & Sánchez (2012), sostienen que la auditoria informática en el área de los sistemas de tecnología y comunicación se realiza con el fin de evaluar la eficiencia y eficacia del hardware, del software y de las redes de comunicaciones

> […] los servidores e indicadores de funcionamiento, teniendo en cuenta que la administración de estos recursos es factor clave para el desempeño y funcionamiento de las diferentes actividades que se desarrollan dentro de los procesos pertenecientes a esta área, identificando vulnerabilidades que permitan obtener un diagnóstico para que, por medio de este, la entidad defina planes de mejoramiento a nivel de procesos y por ende a nivel empresarial. para el

> desarrollo de la auditoría se toma como punto de referencia algún modelo, seleccionando y aplicando los procesos de cada dominio relativo a los objetivos de la auditoría. (p. 10).

Con referencia a lo anterior, Urquizo (2021), establece que la auditoría informática identifica el nivel de **"**exposición" de un sistema, por la falta de controles, mientras el análisis de riesgos facilita la evaluación de los riesgos y recomienda acciones con base al costo-beneficio de la misma. Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen la productividad de una organización y de que las amenazas que se materialicen en hechos sea lo más baja posible. Es por ello, que la auditoría informática se ha convertido en mecanismo más adecuado para mejorar los niveles de seguridad en un sistema o de las redes institucionales.

Este mecanismo da paso a técnicas de control de funcionamiento, medidas de protección y análisis de riesgo. Autores como León (2017), Tejena-Macías (2018), han acotado que generalmente la infraestructura de la red interna de las universidades cuenta con el equipamiento para brindar seguridad; el problema está en no tener políticas y procesos de seguridad que garanticen la integridad de la información y de los equipos. Las universidades han reportado y/o han registrado innumerables ataques a la red interna y sus aplicaciones, esto lo realizan personas sin ética que buscan vulnerabilidades en la red para realizar malas acciones queriendo indisponer los servicios informáticos. El portal Web de estas instituciones es el principal objetivo de los atacantes, ya que es la aplicación con mayor cantidad de usuarios y cantidad de información en su base de datos. (Solarte, et al, 2015).

III. CONCLUSIONES.

- En la actualidad, las organizaciones deben comprender la importancia de invertir en la seguridad informática, no solo como una medida de prevención, sino como una forma de salvaguardar los datos y la información que genera o contiene, identificando virus y riesgos de sus sistemas informáticos, mediante el desarrollo de modelos que permitan evaluar su nivel óptimo de seguridad, y teniendo en cuenta aspectos relacionados con la reducción del riesgo, así como con la

finalidad de controlar y servir de herramienta para brindar información en la toma de decisiones y adopción de medidas que le faciliten la mejora de sus propios procesos.

- La Universidad debe convertirse en una organización preocupada no solo por evitar aquellas situaciones que pueden afectar la disponibilidad, integridad y confidencialidad de la información que se manipula, que son el resultado del ejercicio de funciones como son la docencia, la investigación y la extensión, sino que a la vez reconozca la importancia de saber ejercer diferentes formas de control y ser capaz de aplicar diversas herramientas para la evaluación de controles que garanticen la seguridad de la información de su sistema informático.
- La Universidad es una institución que al desarrollar sus funciones sustantivas de extensión, investigación y docencia, genera una serie de datos, información y conocimiento que no solo deben ser procesados y clasificados, sino también controlados, y que los equipos donde se guardan, se deben conservar, mantener y auditar, con la finalidad de conocer el estado de su seguridad actual y eliminar vulnerabilidades, minimizar riesgos y poder así elevar el nivel de protección de sus recursos informáticos.
- Es fundamental un compromiso de autoridades y de toda su comunidad, asegurar una cultura que sea consciente de que es necesaria la prevención y detección del acceso y uso malicioso de sus sistemas informáticos y de sus recursos para evitar estar expuestos a hackers informáticos y/o a delitos informáticos.
- Los retos que presenta la seguridad de los sistemas informáticos están enfocados en los procesos que la Universidad realiza, en la ausencia de controles y de mantenimiento de los sistemas existentes, así como en la verificación de la calidad de la información que generan y en los monitoreos periódicos que se deben realizar a los mismos controles; de allí que deben adoptarse medidas como: establecimiento de políticas sobre seguridad informática, aplicación de estándares para evaluar riesgos, establecimiento de marcos jurídicos que aseguren la seguridad informática, la necesidad de crear un gobierno universitario de tecnología informática y finalmente, la necesidad de formar y actualizar a sus

colaboradores en seguridad de la información para poder realizar auditorías internas y externas a sus sistemas informáticos.

REFERENCIAS BIBLIOGRÁFICAS

Acurio Del Pino, S. (2016). Delitos informáticos: generalidades. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Altamirano Di Luca, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Revista Avances, 21*(2), 248-263.

Amador Lesmes, B. H. (2018). Producción de conocimiento en las universidades. Revista Trilogía, 10(19), 27-43). DOI: https://doi.org/10.22430/21457778.1013

Antúnez, Y., & Valero, J. (2022). Calidad de los sistemas de información en los Centros de Investigación de la Universidad del Zulia. *Revista Espacios Públicos, 18*(44), 163-175.

Arcentales-Fernández, D. y Caycedo-Casas, X. (2017). Auditaría Informática: un enfoque efectivo. *Revista Dominio de las Ciencias, 3*(mon). 157-73. URL:http://dominiodelasciencias.com/ojs/index.php/es/index

Avilés Chacón, H. D. (2010). *Desarrollo de una guía para el control de brechas de seguridad en servicios de internet aplicada a Petroproducción.* (tesis de fin de grado). Escuela Superior Politécnica de Chimborazo. Riobamba, Ecuador.

Bailon Lourido, W. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. *Revista CIENCIAMATRIA, 5*(1), 73-87. https://doi.org/10.35381/cm.v5i1.248

Becerril Gil, A. A., & Ortigoza Limón, S. (2018). Habilitadores tecnológicos y realidades del derecho informático empresarial. *Revista IUS, 12*(41), 11-41. http://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-11.pdf

Benavides Sepúlveda, A. & Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Revista Scientia Et Technica*, *23*(1), 85-92.

Bodero Poveda, E., De Giusti, M., Morales, C. (2022). Preservación digital a largo plazo: estándares, auditoría, madurez y planificación estratégica. *Revista Interamericana de Bibliotecología*, *45*(2), 1-14. https://doi.org/10.17533/udea.rib.v45n2e344178

Bogantes, A. (2020). El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados. *Revista Sistemas, Cibernética e Informática, 17*(1), 24-29.

Bonilla Bonilla, E. V. (2019). *Propuesta de mejoramiento continuo de la seguridad informática y de la seguridad de la información de las instituciones de educación superior*. (trabajo monográfico). Universidad Santo Tomás. Bogotá, D.C., Colombia.

Bracho-Ortega, C., Cuzme-Rodríguez, F., Puniales-Yepez, C., Suárez-Zambrano, L., Peluffo-Ordoñez, D. y Moreira-Zambrano, C. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3; caso de estudio. MASKANA, CEDIA, 307-19. https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1471/1144

Castillo Plata, A. R. (2015). *Actualización Norma ISO/IEC 27001:2005 para la versión 2013 en Caracol Televisión.* (Tesis de fin de grado). Fundación Universitaria Los Libertadores. Bogotá, Colombia.

Chicaiza Jami, P. E., & Díaz Villafuerte, A. V. (2014). *Diseño de un plan de gestión de seguridades de la información para instituciones públicas ecuatorianas.* (trabajo de fin de grado). Escuela Politécnica Nacional. Quito, Ecuador.

Dávalos Suñagua, A. F. (2013). Auditoría de seguridad de la información. *Revista FIDES ET RATIO*, 6(6), 19-30. http://www.scielo.org.bo/pdf/rfer/v6n6/v6n6_a04.pdf

Díaz-Ricardo, Y., Pérez del Cerro, Y., & Proenza-Pupo, D. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. *Revista Ciencias Holguín, 20*(2), 1-14. http://www.redalyc.org/articulo.oa?id=181531232002

Díaz Soto, D. J., Peña Bohórquez, F. M., & Silva Ucar, H. J. (2021). *Análisis del estado actual de la seguridad informática de una PYME del sector de construcción de obras civiles.* (Tesis de fin de grado). Universidad El Bosque. Bogotá, Colombia.

Domínguez-Bernita, E. I., Paladines-Zapata, N. C., & Flores-Balseca, C. H. (2017). Ética y seguridad informática en el sector de salud pública en el siglo XXI. *Revista Dominio de las Ciencias*, *3*(num. esp.), 403-413.

Duque Agudelo, D. A. (2022). *Plan de Seguridad Informática.* (Tesis de fin de grado). Universidad de Antioquía. Medellín, Antioquía, Colombia.

Dussan Clavijo, C. A. (2006). Políticas de seguridad informática. *Revista Entremado*, *2*(1), 86-92. https://www.redalyc.org/pdf/2654/265420388008.pdf

Enríquez Collaguazo, A. A. (2018). *Modelo de gestión de seguridad de la información para instituciones de salud, basado en las normas ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013 aplicada a la clínica médica fértil*. (trabajo de fin de grado). Universidad Técnica del Norte. Ibarra, Ecuador.

Escobar-Rivera, D., Moreno-Pino, M, y Cuevas-Rodríguez, L. (2016). La calidad de la auditoría en Sistemas de Gestión. Software AUDIT_INTEGRATED. *Revista Ciencias de Hoguín*, *22*(2), 1-18. http://www.redalyc.org/articulo.oa?id=181545579007

Esguerra Suárez, M., Robles Hernández, R., & Sierra Mariño, L. D. (2004). *Control de inventario de software y hardware de la Contaduría General de la Nación, CONISH.* (tesis de fin de grado). Universidad Abierta y a Distancia. Bogotá D. C., Colombia.

Espinoza Freire, W. E., Toscano Ruíz, D. F., & Torres Ortiz, S. E. (2018). Gestión de las tecnologías de la información; un desafío en el ámbito académico universitario del Siglo XXI. *Revista Dilemas Contemporáneos: Educación, Políticas y Valores*, *6*(27), 1-22.

García Peñalvo, F. J. (2018). Gobierno de Tecnologías de la Información. En Proyecto Docente e Investigador (Documento de trabajo). 389-449. Universidad de Salamanca, Salamanca, España. https://repositorio.grial.eu/bitstream/grial/1229/3/08-rep.pdf

Gonzáles Cotera, B. (2016). *Uso de las herramientas ETHICAL HACKING con KALI para el diagnóstico de vulnerabilidades de la seguridad de la información en la red de la*

sede central de la Universidad de Huánuco. (Trabajo de grado). Universidad de Huánuco. Huánuco, Perú.

Guerrero Caro, A. (2020). *Capacidades técnicas, legales y de gestión para equipos de Blue Team y Red Team.* (tesis de fin de grado). Universidad Abierta y a Distancia. Bogotá D. C., Colombia.

Gutiérrez Pórtela, F., Álvarez Porras, J. A. y López Guzmán, U. M. (2018). Presente y futuro de la evidencia informática: análisis frente a las competencias del auditor. *Revista Sinergia*, (4), 108-29. http://sinergia.colmayor.edu.co/ojs/index.php/Revistasinergia/article/view/60/38

Hernández Mechate, E. J. (2020). *Vulnerabilidades informáticas en el portal web de la Universidad Andina del Cusco*. (Tesis de fin de grado). Universidad Andina del Cusco. Cusco, Perú.

Igarza, A. S., Gioia, C. V., & Eterovic, J. (2018). Análisis del Marco Normativo Legal para el ciclo de vida de la evidencia digital. *RedUNCI-UNNE*, 1043-1046. http://sedici.unlp.edu.ar/bitstream/handle/10915/68349/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Imbaquingo, D. E., Herrera-Granda, E. P., Herrera-Granda, I. D., Arciniega, S. R., Guamán, V. L., & Ortega-Bustamante, M. C. (2019). Evaluación de los sistemas de seguridad informáticos universitarios. Caso de estudios: sistema de evaluación docente. *Revista RISTI*, (E22), 349-362.

Infante-Moro, A., Infante-Moro, J. C., Martínez-López, F. J. y García-Ordaz, M. (2016). La informática en España: el caso de los hoteles. *International Journal of World of Tourism*, *3*(5), 56-69.

León Gudiño, M. V. (2017). *Auditoría de seguridad informática en la red interna de la Universidad Técnica del Norte según la metodología "Ofensive Security Professional Training and Tools for Security Specialists y planteamiento de políticas de seguridad basadas en la Norma ISO/IEC 27001.* (Tesis de fin de grado). Universidad Técnica del Norte. Ibarra, Ecuador.

Macas Granda, C. J., Granda Asencio, L. Y., & Carbay Cajamarca, W. A. (2021). Rol del docente en la alfabetización digital en el siglo XXI. *Revista Sociedad & Tecnología*, *4*(S2), 350–363. https://doi.org/10.51247/st.v4iS2.156

Macas Ruiz, E. M., Bustamante Granda, W. X., & Quezada Sarmiento, P. A. (2017). Gobierno de TI: elección y aplicación de buenas prácticas en Corporación Nacional de Telecomunicación. *Revista Espacios*, *39*(3), 29-48. https://www.revistaespacios.com/a18v39n03/a18v39n03p29.pdf

Martelo, R. J., Tovar, L. C., & Maza, D. A. (2018). Modelo Básico de Seguridad Lógica. Caso de estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Revista de Información Tecnológica*, *29*(3), 3-10. http://dx.doi.org/10.4067/S0718-07642018000100003

Martínez Cardero, D., & González Arencibia, M. (2019): Habilidades creativas en equipos de desarrollo de software. *Revista Atlante: Cuadernos de Educación y Desarrollo*. En línea: https://www.eumed.net/rev/atlante/2019/09/habilidades-creativas-software.html

Martínez, A. N. y Porcelli, A. M. (2015). La nueva economía del siglo XXI: análisis de los impactos de la informática en el ambiente. Tendencias actuales en tecnologías informáticas verdes, un compromiso de sustentabilidad. *Revista Quaestio luris*, *4*(4), 2174-208.

Martínez, A. N., & Porcelli, A. M. (2015). Análisis de la efectividad de la protección jurídica desl software en las modernas legislaciones. Tendencias actuales. *Revista Electrónica del Instituto de Investigaciones "Ambrosio L. Gioja"*, *9*(14), 125-54. http://www.derecho.uba.ar/revistas-digitales/index.php/revista-electronica-gioja/article/view/29/18

Martínez, A. N., & Porcelli, A. M. (2015). Impactos de la tecnología en el ambiente y nuevas tendencias de la computación verde. *Diario DPI*, (11), 1-2. http://dpicuantico.com/sitio/wp-content/uploads/2015/12/Tecnologia-Doctrina-2015-12-30.pdf

Martínez, A. N., & Porcelli, A. M. (2016). La informática en la Agenda 2030. Reflexiones sobre la tecnología informática en las Cumbres Internacionales del 2015. (DES) Ventajas de la denominada computación verde. *Revista Lex, 14*(17), 301-344. http://dx.doi.org/10.21503/lex.v14i17.945

Martínez, A. N., & Porcelli, A. M. (2016). Las nuevas tecnologías de la informática a la luz de la Encíclica Laudato Si. Reflexiones sobre sus ventajas y desventajas. Modernas tendencias en tecnologías verdes. https://www.researchgate.net/profile/Adriana_Porcelli/publication/316460465

Maucaylle Leandre, A. (2019). *Construcción de un modelo de red virtual para aplicar técnicas de hacking ético y poder analizar los eventos relacionados a la seguridad informática sobre una infraestructura virtual.* (tesis de fin de grado). Universidad Nacional José María Arguedas. Andahuaylas, Apurímac, Perú.

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Risti*, (E27), 553-565.

Navarrete Macías, J. F. (2019). *Administración de servidores virtuales, monitoreo de procesos, fortalecimiento de servidores y actualizaciones de seguridad de la empres Internacional Bussines Machines (IBM).* (tesis de fin de grado). Universidad de Santo Tomás, Seccional de Tunja. Tunja, Colombia.

Niño Benítez, Y., & Silega Martínez, N. (2018). Requisitos de seguridad para aplicaciones web. *Revista UCIENCIA,12*(Esp.), 205-221.

Noguera, L., & Sánchez, E. (2012) *Auditoría informática en el área de sistemas e indicadores de funcionamiento del hardware en la empresa solidaria de salud Emssanar E.S.S. del Departamento De Nariño.* (Trabajo monográfico de fin de grado). Universidad de Nariño, San Juan de Pasto. Nariño, Colombia.

Parra Gamboa. M. C. (25, 26, 27 de noviembre de 2019). *De la "representación" a la "participación" en la estructura orgánica universitaria.* [sesión conferencia]. XIX Coloquio de Gestión Universitaria. Florianópolis, Santa Catarina, Brasil.

Pasini, A., Estévez, E., Pesado, P. y Boracchia, M. (2016). Una metodología para evaluar la madurez de los servicios universitarios. *XXII Congreso Argentino de Ciencias de la Computación (CACIC 2016),* Conferencia en el congreso organizado por la Red de Universidades con Carreras en Informática (RedUNCI).

Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad informática. *Revista Dominio de las Ciencias, 3*(3), 676-688.

Rodríguez Silva, L. R., & Cuidad Ricardo, F. Á. (2019). El derecho informático en la industria cubana de software: El caso de la universidad de las ciencias informáticas. *Revista CES Derecho, 10*(1), 418-446.

Roque Hernández, R. V., & Juárez Ibarra, C. M. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *Revista Paakat, 8*(14), DOI: http://dx.doi.org/10.32870/Pk.a8n14.318

Salgado Soto, M del C., Osuna Millán, N. del C., Sevilla Caro, M. & Morales Garfias, J. I. (2017). La auditoría informática en las organizaciones. *Revista Electrónica sobre Cuerpos Académicos y Grupos de Investigación en Iberoamérica, 4*(8), 1-14. file:///D:/Downloads/165-813-1-PB.pdf

Serrato, G. A. (2016). Metodología para el análisis de vulnerabilidades. *Revista TIA, 4*(2), 20-27.

Sobrevilla, G., Hernández, J., Velasco-Elizondo, P., & Soriano, S. (2017). Aplicando Scrum y Prácticas de Ingeniería de Software para la Mejora Continua del Desarrollo de un Sistema Ciber-Físico. *Revista ReCIBE, 6*(1), 1-15.

Solarte Solarte, F. N. J., Enríquez Rosero, E. R. & Benavides Ruano, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista ESPOL-RTE, 28*(5). 492-507.

Suñé Linás, E. (2016). Derecho informático de las cosas o de segunda generación El Derecho de la Informática en la 4ª Revolución Industrial o de la Productividad. *Revista Ambiente Jurídico*, (19), 163-210.

Tapia Ayala, C. H. (2019). *Mejores prácticas de seguridad en ambientes virtuales.* (tesis de maestría). Universidad de Buenos Aires. Buenos Aires, Argentina.

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Revista Polo del Conocimiento, 3*(4), 230-244. DOI: 10.23857/pc.v3i4.809

Téllez Barrientos, O., Ramírez Hernández, M. y Díaz Alva, A. (2016). Auditaría de sistema TI como medio de aseguramiento de control en empresas del Siglo XXI. *Revista Iberoamericana de las Ciencias Computacionales e Informática, 5*(10), 1-18. Downloads/54-Texto%20del%20artículo-600-3-10-20170328.pdf

Torres Lage, E. (2019). *Módulo de inventario de actualizaciones y parches de seguridad del sistema operativo Windows en XILEMA GRHS.* (Tesis de fin de grado). Universidad de las Ciencias Informática. La Habana, Cuba.

Urquizo Córdova, A. P. (2021). *Auditoría informática para la protección de la información digital a la COAC Acción y Desarrollo LTDA. Ciudad de Riobamba, período 2018.* (Tesis de fin de grado). Universidad Nacional de Chimborazo. Riobamba, Ecuador.

Velasco Melo, A. H. (2008). El derecho informático y la gestión de la seguridad de la información: una perspectiva en base a la Norma ISO 27 001. *Revista de Derecho,* (29), 334-66. http://www.scielo.org.co/pdf/dere/n29/n29a13.pdf

Viecco Rivadeneira, L., & Pinedo Martínez, V. (2018). *Modelo de gobierno de tecnología de la información, basado en gestión del riesgo y seguridad de la información para las universidades públicas: caso de estudio Universidad de La Guajira*. (Tesis de maestría). Fundación Universidad del Norte, Barranquilla, Colombia.

Viteri Jiménez, M. J. (2020). *Políticas de seguridad informática en el departamento de Tecnologías de la Información y la Comunicación en beneficio de la Universidad Técnica Estatal de Quevedo. Manual de procedimientos 2014.* (Tesis de fin de grado). Universidad Técnica Estatal de Quevedo. Los Ríos, Ecuador.

Zaidman, E. (2017). Seguridad Informática. ¿Vulnerabilidades técnicas o errores humanos? *Revista ECONO,* (14). https://revistas.unlp.edu.ar/econo/article/view/3638/3438