Revista de Administración Pública

INAP

Seguridad de la información en instituciones de educación superior de México

Rafael Espinosa García, Guillermo Morales Luna.

Resumen: Hacemos una investigación bibliográfica de la ciberseguridad en ambientes universitarios y centros de investigación gubernamentales de México. Planteamos la importancia de la seguridad informática en cuanto a la seguridad nacional y su normatividad actual. Las características principales de la seguridad de la información y la gobernanza de los datos y su valor agregado, en el ambiente propiamente universitario y científico para salvaguardarlos para la toma de decisiones de la entidad universitaria. Presentamos un caso de estudio para ilustrar la efectividad de las medidas que proponemos para resguardar los datos obtenidos en el laboratorio de investigación.

Palabras clave: Ciberseguridad, Gobernanza, Información, Acceso, Transparencia

Information security in Mexico's higher education institutions

Abstract: A bibliographical research is performed related to cybersecurity in academic and government scientific centers in Mexico. We analyze the relevance of information security with respect to national security and legal and technical standards. The main features of information

security and data governance are described in order to advice the academic and scientific authorities in decision making. A case of study is discussed with the purpose to illustrate the proposed measures to keep in protection the collected data in a scientific laboratory.

Keywords: Cybersecurity, Governance, Information, Access, Transparency

Fecha de recepción: 10 de enero de 2019
Fecha de aceptación: 28 de enero de 2019

Revista de Administración Pública

INAP

Seguridad de la información en instituciones de educación superior de México

Rafael Espinosa García*
Guillermo Morales Luna**

1. Introducción

La seguridad informática a nivel nacional es de tanta importancia que ha de ser motivo de atención de la seguridad y la defensa nacional, y a nivel universitario es igualmente de gran relevancia. El conocimiento es poder, proclama el dicho popular, y las universidades y los centros de investigación son generadores de conocimiento. Tan sólo por este punto, la seguridad informática de los centros universitarios y de investigación es un tema de

* Licenciatura en Sistemas de Computación Administrativa por la UVM, Maestría en Ingeniería en Sistemas por la UVM. Perito Certificado en Cómputo Forense. Certificación CISCO CCNA. Iniciador del dominio cinvestav.mx, y administrador del mismo por 7 años. Intereses de investigación: Seguridad Informática, Protocolos de comunicación TCP/IP, Seguridad en Big Data y Programación de Sistemas IOT. Actualmente Auxiliar de Investigación en la Sección de Electrónica del Estado Sólido del Departamento de Ingeniería Eléctrica en Cinvestav-IPN.

** Investigador Titular en el Departamento de Computación del Cinvestav-IPN, Licenciatura en Física y Matemáticas por la ESFM-IPN, Maestro en Ciencias con especialidad en Matemáticas por el Cinvestav-IPN, y Doctor en Ciencias Matemáticas por el Instituto de Matemáticas de la Academia Polaca de Ciencias. Áreas de interés: Fundamentos Matemáticos de Computación, Lógica, Criptografía y Teoría de la Complejidad. Ha sido profesor en el IPN y en la B. Universidad Autónoma de Puebla. Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y le fue concedida la ciudadanía polaca.

interés nacional. De manera global, nos referiremos a las instituciones de educación superior, a las universidades, y a los centros de investigación básica y de tecnología como centros académicos.

Dichos centros requieren manejar procesos administrativos (tanto de control de personal como de control escolar), educativos (en cuanto a cursos en línea, herramientas de auxilio a profesores, experimentos de laboratorio, accesos a bibliotecas digitales, o cualesquiera otros servicios digitales), de desarrollo tecnológico (tales como el diseño de dispositivos, vinculación universidad-empresa, resguardo de productos tecnológicos y biotecnológicos, realización de pruebas de calidad, calibración de equipos, certificación de componentes, etc.) y de investigación científica (control de experimentos, avances de investigaciones, publicación, diseminación, resguardo, seguimiento y validación de resultados, etc.) Todos estos procesos involucran el uso y la explotación de información sensible desde varios puntos de vista, tales como los de tipo social, institucional, organizativo y, también, comercial y económico. Pero ciertamente, los centros académicos han de esmerarse en el cuidado de su prestigio y de su buen nombre institucional.

Las vulnerabilidades de las que se pueda adolecer impactarían gravemente en los centros académicos. Pretendemos enfatizar en el presente texto la importancia que tiene la seguridad informática en los centros académicos a la luz de los más recientes recursos tecnológicos.

En una primera sección nos referimos al acceso a la red de redes en México y a los esfuerzos y estrategias gubernamentales en preservar la ciberseguridad a nivel nacional. Después nos referimos, de manera general y conceptual, a la seguridad informática. La tercera sección trata específicamente de la seguridad informática en centros académicos. Describimos los riesgos principales y bosquejamos una organización corporativa universitaria para afrontarlos, disminuirlos y acaso evitarlos y presentamos finalmente un caso de estudio concreto.

2. La carretera de la información a nivel nacional

2.1 Seguridad en la carretera de la información

México se clasifica como el segundo país de América Latina con más ataques cibernéticos. Hubo aproximadamente 10 millones de víctimas en 2014, y un incremento del 40% entre 2013 y 2014. Dado que el 57.4% de los 127 millones de habitantes en la República Mexicana son usuarios de Internet, cerrar las brechas en su entorno de seguridad cibernética es una tarea importante con implicaciones para una parte grande y creciente de su población. El gobierno, el sector privado y la sociedad civil deben mantenerse al día con la innovación constante en el sector de la tecnología de la información (TI), como usuarios y como posibles objetivos de ataques. México ocupa el segundo lugar después de Brasil entre los países que envían correos no deseados por medio de la red. Brasil, México y Colombia reciben o emiten el 75% del correo basura en Latinoamérica.[1]

En la Era del Conocimiento, el acceso a Internet se encuentra asociado de manera importante con el nivel de estudios. En particular, en México se ha encontrado que nueve de cada diez personas con nivel superior de estudios (licenciatura y posgrado), cuatro de cada cinco con nivel medio superior (preparatoria o equivalente), y poco menos de la mitad (48.7%) con nivel básico (primaria o secundaria) han incorporado en sus actividades diarias el uso de Internet.[2]

Actualmente las amenazas de ciberseguridad plantean un problema de riesgo creciente cada vez más común para colegios, universidades y centros de investigación, públicos

1 Parraguez K. L., The State of Cybersecurity un Mexico: An Overview, Wilson Center. Mexico Center, Woodrow Wilson Center. January 2017. Recuperado el 7 de julio de 2018. https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf

2 INEGI, Estadísticas a propósito del día mundial del Internet (17 de mayo). 15 de mayo de 2017. Recuperado el 7 de julio de 2018. http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf

y privados.[3] La continuidad del avance tecnológico y académico requiere la protección de la información personal e intelectual de investigadores, profesores, administradores y estudiantes. Además, en cualquier institución académica es imprescindible mantener un ancho de banda para cubrir sus necesidades de comunicación, procesamiento y almacenamiento, mientras se bloquean las amenazas e intromisiones que afecten el funcionamiento y el prestigio de la institución.[4]

2.2 Ciberseguridad y estrategia de seguridad nacional

A fines de 2012, el Presidente de la República, Enrique Peña Nieto, presentó el Plan de Desarrollo 2013-2018, en donde se establece la estrategia del Programa de Seguridad Nacional 2014-2018, y enfoca los intereses estratégicos y los objetivos nacionales de México.[5] Se creó el Comité Especializado de Seguridad de la Información, encargado de la redacción de la Estrategia Nacional para la Seguridad de la Información, basándose en una idea de seguridad multidimensional que abarque amenazas antiguas y nuevas, y se planteó que tal estrategia es un elemento importante en la preservación de la paz y la estabilidad no sólo del país, sino de todo el Continente Americano. En cuanto a las políticas específicas de ciberseguridad para proteger y promover los intereses nacionales, los principales compromisos que se detallan son: promover acciones para prevenir y combatir los ataques cibernéticos; fortalecer los mecanismos para prevenir incidentes en los sitios ejecutivos federales; defender el cumplimiento y el desarrollo de procedimientos para evaluar y fortalecer el

3 Dovey F. T., Clark C. and Lyn G. J., Elevating cybersecurity on the higher education leadership agenda: Increasing executive fluency and engagement in cyber risk. Deloitte Insights, February 2018. https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

4 Palo Alto Networks, Next Generation Security for Higher Education Institutions. 2017. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/higher-education-institutions-solution-brief

5 Gobierno de México, Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI. Publicado en el Diario Oficial de la Federación de México, el 30 de Abril de 2014. Recuperado el 4 de octubre de 2018. http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

desempeño de los equipos de respuesta ante incidentes de seguridad cibernética en los poderes federales; mejorar las capacidades de capital humano y la infraestructura tecnológica para abordar los incidentes de seguridad cibernética; establecer una cooperación internacional sobre seguridad cibernética y defensa cibernética, en particular con los países de América del Norte para prevenir y abordar los ataques a los sistemas informáticos del país.

Aunque en México el terrorismo no representa un riesgo alto, es necesario adoptar medidas preventivas para identificar vulnerabilidades y protegerse de amenazas y riesgos externos. El Gobierno de México estableció una serie de medidas y acciones en el Programa de Seguridad Nacional 2014-2018 para identificar posibles ataques contra la seguridad nacional. Expertos mexicanos mantienen colaboración estrecha y constante con más de 300 equipos de 69 países para prevenir y combatir estos delitos. México es miembro del Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST), una agrupación de 369 equipos en 78 países, y participa con cuatro agrupaciones.[6] La seguridad de la información en la red se ha vuelto cada vez más importante con la amenaza creciente en el ciberespacio. Sólo algunos ciberdelitos son punibles, ellos no siempre se encuentran explícitamente tipificados y el entorno legal está disperso en diversos ordenamientos de diversas índoles en los planos federal y local. El Gobierno Federal se ha centrado en fortalecer la seguridad cibernética y promover la legislación pertinente para garantizar la seguridad nacional y reducir el nivel de violencia. Reconoce los desafíos globales que conllevan problemas tecnológicos, energéticos, demográficos y ambientales, y describe las vulnerabilidades del Estado.

2.3 Regulación gubernamental de la información en México

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es un organismo autónomo en México.[7] El organismo, antes

6 CERT-MX, Mnemo-CERT, Scitum-CSIR and UNAM-CERT FIRST (2016). https://www.first.org/members/map#mexico

7 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. http://inicio.ifai.org.mx/SitePages/ifai.aspx

conocido como Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), cambió de nombre en mayo de 2015 tras la aprobación de la Ley General de Transparencia y Acceso a la Información.

El organismo tiene la función, principalmente, de:

- Garantizar el derecho de acceso de las personas a la información pública gubernamental.
- Proteger los datos personales que están en manos tanto del gobierno federal, como de los particulares.
- Resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.

A partir de la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el 12 de junio de 2003, más de 240 dependencias y entidades del gobierno federal tienen la obligación de responder a solicitudes de información bajo la vigilancia del IFAI. El IFAI promovió la recepción de estas solicitudes a través de internet, mediante el sistema INFOMEX.[8]

Los centros académicos en nuestro país con base en sus Reglamentos de Transparencia y Acceso a la Información Pública establecen el catálogo de datos personales a proteger y su alcance, considerados en lo general como información confidencial. Estos reglamentos definen las reglas de cómo se identificarán y consultarán los documentos que se publicarán en la Plataforma de Transparencia y Obligaciones de cada entidad universitaria. Los reglamentos serán utilizados por las áreas universitarias para la elaboración de versiones públicas que deriven de solicitudes de información y aquéllas que sean necesarias para el cumplimiento de las obligaciones comunes de transparencia.

El año pasado el INAI publicó un estudio acerca de los alcances del derecho de acceso a la información, sin embargo, sólo se considera la rendición de cuentas y la

8 Plataforma Nacional de Transparencia.
http://www.infomex.org.mx/gobiernofederal/home.action

transparencia en las entidades universitarias.[9] No hay una reglamentación en lo que respecta a los datos obtenidos en las investigaciones desarrolladas por los investigadores en los centros académicos.

El incremento en la adopción de procesos basados en Internet, el hecho de que la información fundamental se genera a partir de datos que se obtienen del consumidor, incrementan el riesgo en forma importante.

El establecimiento de una regulación gubernamental de la información, tanto en manos del gobierno como en la de particulares, es un avance importante en México, sin embargo, *el cumplimiento regulatorio no elimina el riesgo*.[10]

Es de suma importancia el desarrollo de estándares y procedimientos de seguridad adecuados a la realidad operativa de cada nivel escolar existente en el país, que permitan el aseguramiento de la información que se encuentra almacenada en los sistemas de cómputo y redes de los planteles del sector educativo nacional.

El desarrollo de una normatividad nacional de ciberseguridad orientada al sector educativo de México, podría ser encabezada por el INAI o establecer un organismo nacional dedicado al desarrollo, certificación y el establecimiento de estándares y procedimientos de innovación tecnológica en el área de seguridad de la información para el sector público o privado.

2.4 Agencia de Ciberseguridad Nacional

En 2017 se desarrolló un estudio por la CANIETI, la Asociación Mexicana de Tecnologías de la Información y la

9 Islas, J, Estudio sobre los alcances del derecho de acceso a la información en Universidades e Instituciones de Educación Superior públicas dotadas de autonomía, derivado de la Reforma Constitucional en materia de transparencia. INAI, Diciembre 2017. http://inicio.inai.org.mx/Estudios/AlcancesUniversidadesWeb.pdf

10 Kravchenko, S. and Riley, M., The American Fugitive From the JPMorgan Hack Turns Up in a Russian Cell. https://www.bloomberg.com/news/articles/2016-10-10/jpmorgan-hack-fugitive-said-to-seek-u-s-deal-from-russian-cell

Asociación de Internet MX, que mostró algunos hallazgos importantes.[11]

Dentro de los principales resultados y recomendaciones destacan:

- La necesidad de contar con una Agencia de Ciberseguridad Nacional que coordine la estrategia que se está definiendo y genere la ruta crítica de la gobernanza en Internet, y que además coadyuve a generar certeza y confianza en el nuevo ecosistema digital.
- La importancia de redefinir el marco jurídico para la ciberseguridad, armonizando las legislaciones federales y estatales, garantizando la protección a datos personales y estimulando la compartición de información. Un marco que dote a los cuerpos policiacos de herramientas adecuadas.
- Garantizar la protección de infraestructura crítica, sobre todo la ciberresiliencia bajo un enfoque de gestión de riesgo para que se tengan mecanismos y protocolos claros para la recuperación de los sistemas.
- El desarrollo de habilidades y competencias para el nuevo ecosistema digital, definiendo claramente las nuevas habilidades que serán necesarias ampliando, desarrollando y reclutando el mejor talento posible.

Por otra parte, de acuerdo al mismo estudio del sector privado, las brechas más importantes de las organizaciones mexicanas se encuentran: "en cuanto a clasificación de información, métricas de ciberseguridad, capacitación en continuidad de negocio o ciberresiliencia; así como pruebas de vulnerabilidades por terceros".

11 Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), Asociación Mexicana de Tecnologías de la Información (AMITI) y la Asociación de Internet MX, Evaluación de la Ciberseguridad en México: brechas y recomendaciones en un mundo hiper-conectado, Octubre 2017. Recuperado el 26 de enero de 2019. https://docplayer.es/65552142-Evaluacion-de-la-ciberseguridad-en-mexico-brechas-y-recomendaciones-en-un-mundo-hiper-conectado.html

3. Seguridad de la información

Las amenazas cibernéticas en México contra la seguridad en los sistemas de tecnologías de la información (TI), y en los datos incluyen los llamados *malware, spyware, keystroke loggers* (registradores de teclas), los accesos de *puertas traseras* a sistemas de TI, la suplantación de identidades y las estafas *dirigidas*, las cuales son diseñadas para robar partículas de identidad de usuarios, el mal uso intencional por usuarios con accesos legítimos, y los ataques de denegación de servicios. Quienes manejen los sistemas de TI y los datos contenidos en ellos deben protegerse de eventos fortuitos: desastres naturales, cortes de energía y recursos de TI perdidos o extraviados (p. ej., aspectos minúsculos como memorias USB perdidas que contengan datos confidenciales). También, se debe proteger a datos y a sistemas de acciones descuidadas realizadas por usuarios legítimos, como la eliminación accidental de datos importantes, la publicación accidental de datos confidenciales en un recurso público (una página *web*) o enviando información (digamos por correo electrónico) a personas indebidas.

La seguridad de la información se refiere a mecanismos que protegen datos. Con frecuencia, aquellos menos familiarizados con la seguridad de la información la consideran como meros procedimientos de control técnico en los sistemas de TI. Sin embargo, la seguridad de la información es más que eso y debe entenderse como el estudio y la práctica de protección de datos en todas sus formas (por ejemplo, almacenada en sistemas de TI o colocada en papel u otro medio físico). Los datos deben ser protegidos de cualquier tipo de amenazas, sean estas últimas perpetradas por personas externas o personas con acceso legítimo. La práctica de proteger datos incluye tres conceptos distintos de seguridad de la información, descritos a continuación.[12]

12 Lyn J. G., Understanding Information Security and Privacy in Postsecondary Education Data Systems. EDUCAUSE, May 2016. Recuperado el 22 de mayo de 2018.
http://www.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/information_security_and_privacy-executive_summary.pdf

Confidencialidad. Su propósito es proteger datos contra todas las formas de acceso no autorizado a lo largo de sus ciclos de vida (desde la creación de datos hasta la destrucción de ellos), impidiendo el acceso a individuos no afiliados a la organización que almacena datos (delincuentes, espías o *hackers*). También incluye el acceso de individuos dentro de una organización que exceden deliberadamente sus privilegios al acceder la información (por ejemplo, individuos que buscan los registros de celebridades u otras personas específicas cuando no tienen una razón profesionalmente legítima para hacerlo, o empleados desleales que usurpan funciones o alcances de superiores).[13] La confidencialidad es el concepto de seguridad de la información mayormente implicada cuando una organización sufre una violación de datos.

Integridad. Su propósito es garantizar que los datos dentro de los sistemas de TI sean correctos y completos al ser grabados o reproducidos en medios físicos. Los responsables de TI han de implantar controles dentro del sistema bajo su responsabilidad para garantizar que los usuarios ingresen y procesen los datos correctamente y que se identifiquen y resuelvan los elementos de datos conflictivos. Para la integridad se requiere que sólo usuarios autorizados puedan tener la capacidad de agregar, cambiar, mover o eliminar ciertos tipos de datos de los archivos. Cuando estos datos poseen integridad, se les considera precisos y se puede confiar en ellos para la toma de decisiones.

Disponibilidad. Esta propiedad garantiza que los datos estén al alcance de la mano cuando sea necesario y que los sistemas de TI funcionen confiablemente. Los llamados *stakeholders* pueden garantizar la disponibilidad de datos diseñando sistemas "redundantes" y robustos a ataques, asegurando que los usuarios hagan copias de seguridad de los datos regularmente.

Privacidad. Esta propiedad se refiere a conceptos que se aplican tanto a individuos como a la sociedad en general.

13 Gorman, A., and Sewell, A. (2015, July 12). Six people fired from Cedars-Sinai over patient privacy breaches. Los Angeles Times, July 12, 2013. http://articles.latimes.com/2013/jul/12/local/la-me-hospital-security-breach-20130713

Para los individuos, la privacidad entraña el derecho que tiene un individuo a controlar sus propios datos y para especificar cómo se recopilan, se usan y se comparten. La privacidad debería ser esencial en cualquier política de seguridad de la información. Es posible sin embargo imaginar una situación donde los datos son seguros pero no son privados. Los datos podrían almacenarse en un sistema de TI de una manera segura, pero si esos datos fueron recolectados sin el consentimiento de la persona propietaria u originaria, o sin la debida autoridad legal, entonces la privacidad de esos datos, en lo que se refiere a un individuo, puede estar comprometida. Por lo contrario, los datos pueden ser privados pero no seguros, por ejemplo, si los datos son recolectados con el consentimiento de una persona o de conformidad con una ley que permita la recopilación de datos, y éstos son almacenados en un sistema de TI que carece de la seguridad suficiente para protegerlos de quienes buscan robarlos, la seguridad de los datos está comprometida.

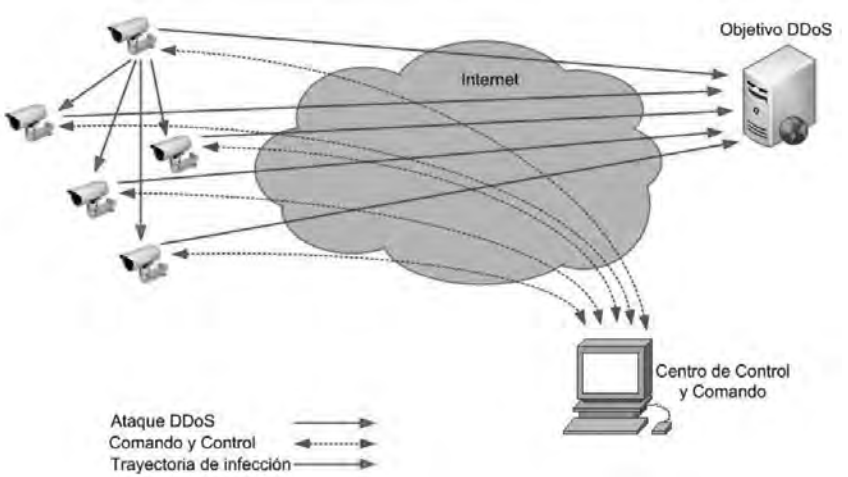
Los conceptos de seguridad de la información y privacidad deben considerarse en forma integral para proteger datos recopilados, almacenados, transmitidos y analizados dentro del ecosistema informático de cualquier institución de educación superior. Las medidas de privacidad y seguridad de la información deben ser utilizadas para proteger la confidencialidad, integridad y disponibilidad de cualquier información recolectada. En la actualidad existe una gran cantidad de dispositivos de IoT (*Internet of Things*) inseguros (*routers* domésticos, cámaras habilitadas para redes y grabadoras de vídeo digital), con un alto poder de cómputo, lo que los convierte en objetivos muy atractivos para los *hackers*, ya que los buscan para comprometerlos y usarlos en la construcción de *botnets* en gran escala, como se muestra en la figura 1. Un *botnet* (apócope de *bot network*, y éste a su vez de *web robot network*) es una red de máquinas infectadas llamados *bots* o *zombies* que forman una infraestructura de control y comando, la cual es utilizada para diversas actividades maliciosas tales como el lanzamiento de ataques distribuidos DDoS (*Distributed Denial of Service*).[14]

14 Bertino, E., and Islam, N., Botnet and Internet of Things Security. Computer, Vol. 50, Issue 2, Feb. 2017, pp. 76-79.

Entre los investigadores y estudiantes de nuestro país, es usual que para desarrollar sus actividades de investigación se apoyen en la tecnología BYOD (*Bring YOur Device*), lo que les permite una movilidad sin restricciones. Sin embargo, estos dispositivos incrementan la posibilidad de que puedan ser usados en ataques distribuidos en base a dispositivos de Internet de las Cosas (IoT), como son los ataques de negación de servicios (DDoS) o *malware*, o su combinación, si no se cumple con una política de seguridad institucional.[15]

De acuerdo a la investigación dirigida por *Markets and Markets*, hubo un crecimiento de 50% a finales del 2017 de los dispositivos móviles (laptops, teléfonos celulares y tabletas personales). Un estudio de Cisco Systems en 2017, concluyó que el 69% de las decisiones de tecnologías de la información favorecieron a BYOD.[16]

Figura 1
Plataforma distribuida para dispersión de malware o ransomware usando infraestructura de IOT para generación de ataques DDoS17



15 Aenugu, N.R., Butakov S., Zavarsky P., Aghili S. (2018) Security Perspective in Comparative Study of Platform-Based and Platform-Less BYOD Systems. In: Kim K., Kim H., Baek N. (eds) IT Convergence and Security 2017. Lecture Notes in Electrical Engineering, Vol. 450. Springer, Singapore.

16 Bouk, J., Top BYOD Trends for 2018. 14 november 2017, Cass Telecom Systems. https://www.casstelecom.com/blog/top-byod-trends-for-2018

17 Hinden, B., The Internet of Insecure Things. The Internet Protocol Journal, Volume 20, Number 1, March 2017.

3.1 Gobernanza de los datos

El término "gobernanza", en general, se refiere a la forma en que una organización asegura que las estrategias se establecen, se monitorean y se logran.[18] Como las Tecnologías de Información son torales en cada organización gubernamental o empresarial, por definición, el gobierno de TI se convierte en una parte integral de cualquier estrategia comercial, y cae bajo el gobierno corporativo.[19] Históricamente, los datos surgieron de sistemas transaccionales heredados dispares. Entonces, fueron vistos como un subproducto de la gestión del negocio, y tenían poco valor más allá de la transacción y la aplicación que los procesó, por lo tanto, los datos no se trataron como un activo valioso; esto continuó hasta principios de la década de los 90, cuando el valor de los datos comenzó a tomar otra tendencia más allá de las meras transacciones. Las decisiones y los procesos empresariales comenzaron a ser impulsados por los datos y sus correspondientes análisis. Una mayor inversión en la gestión de datos fue el enfoque adoptado al aumentar el volumen, la velocidad y la variedad de datos, como repositorios de datos complejos, almacenes de datos, *Enterprise Resource Planning* (ERP) y *Customer Relationship Management* (CRM).[20] Los enlaces de datos se volvieron muy complejos y compartidos entre sistemas múltiples, además de contar con la necesidad de proporcionar un solo punto de referencia para simplificar las funciones diarias, lo que se volvió crucial, dando origen a los datos maestros de gestión.[21]

18 Weber, K.; Otto, B.; Osterle, H. One Size Does Not Fit All—A Contingency Approach to Data Governance. ACM Journal of Data Information Quality, Vol. 1 Issue 1 June 2009 Article No. 4.

19 Salami, O.L.; Johl, S.K.; Ibrahim, M.Y. Holistic Approach to Corporate Governance: A Conceptual Framework. Global Business Management Research: An International Journal, vol. 6, No. 3, 2014.

20 Begg, C.; Caira, T. Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. The Electronic Journal Information Systems Evaluation 2012, Vol. 15, pp 3–13.

21 Buffenoir, E.; Bourdon, I. Managing Extended Organizations and Data Governance. Advances in Intelligent Systems and Computing. 2013, Vol. 205, (pp 135–145), Springer, Berlin, Heildelberg.

Un primer esfuerzo para crear un marco de referencia de gobernanza de datos se publicó en 2007.[22], [23] Para lograr un gobierno de datos exitoso, las organizaciones requieren un marco estratégico que pueda ser fácil de implementar de acuerdo con las necesidades y los recursos de la información.[24], [25] Una buena información en el marco de la gobernanza también puede ayudar a las organizaciones a crear una misión clara, lograr transparencia, aumentar la confianza en el uso de los datos de la organización, establecer responsabilidades, mantener el alcance y el enfoque, así como definir éxitos medibles.[26] Para facilitar el gobierno de los datos, las organizaciones deben diseñar un modelo de gobierno de datos donde las responsabilidades de las funciones sirvan para identificar a las personas que tienen un nivel de responsabilidad para definir, producir y usar datos en la organización[27]. En líneas similares, se ha argumentado que las organizaciones deben obtener la responsabilidad de los datos del departamento de tecnologías de la información con la participación y el compromiso del personal de TI, la gestión empresarial y el patrocinio ejecutivo de alto nivel en la organización.[28] Los expertos en este campo hablan de que el caos no es tan obvio dentro de las organizaciones que no implementen la gobernanza de datos, pero los indicadores son elocuentes, y esas organizaciones conllevan datos sucios, redundantes e inconsistentes, incapacidad para integrarse, bajo rendimiento, escasa disponibilidad, poca responsabilidad, usuarios que están cada vez más insatisfechos con el

22 Wende, K., A Model for Data Governance - Organizing Accountabilities for Data Quality Management. In Proceedings of the 18th Australasian Conference on Information Systems; University of Southern Queensland: Toowoomba, Australia, 5-7 Dec 2007; pp. 417–425.

23 Poor, M. Applying Aspects of Data Governance from the Private Sector to Public Higher Education; University of Oregon: Eugene, OR, USA, July 2011.

24 Fu, X.; Wojak, A.; Neagu, D.; Ridley, M.; Kim, T. Data governance in predictive toxicology: A review. Journal of Cheminformatics. 2001, 3, 24.

25 Prasetyo, H.N.; Surendro, K., Designing a Data Governance Model Based on Soft System Methodology (SSM) in Organization. Journal of Theoretical and Applied Information Technology,10 August 2015, Vol. 78, pp. 46–52.

26 Panian, Z., Some Practical Experiences in Data Governance. World Academy of Science, Engineering and Technology, Vol. 62, 2010, pp. 939–946.

27 Seiner, R.S., Non-Invasive Data Governance. 1st ed.; Technics Publications: New York, NY, USA, 2014.

28 Russom, P., Data Governance Strategies: Helping Your Organization Comply, Transform, and Integrate; The Data Warehousing Institute: Los Angeles, CA, USA, 2008.
http://download.101com.com/pub/tdwi/Files/TDWI_BPR_DG_Q208.pdf

rendimiento de TI, y una sensación general de que las cosas están fuera de control.[29]

El cómputo en la nube es un desarrollo relativamente nuevo de la tecnología. El *National Institute of Standards and Technology* (NIST) de los Estados Unidos[30] definió al cómputo en la nube como "un modelo para permitir acceso a la red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios". El modelo de cómputo en la nube mejora la disponibilidad y se compone de cinco características esenciales, cuatro modelos de implementación y tres modelos de servicio.[31] Las características esenciales incluyen autoservicio bajo demanda, amplio acceso a la red, agrupación de recursos, elasticidad rápida y servicio medido.[32] Los modelos de implementación de la nube son el privado, el público, el híbrido y el comunitario.[33] Los modelos de prestación de servicios, son: Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como servicio (IaaS).[34] El cómputo en la nube ofrece beneficios potenciales para el público y organizaciones privadas al poner a

29 Kamioka, T.; Luo, X.; Tapanainen, T., An Empirical Investigation of Data Governance: The Role of Accountabilities. In Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, Summer 6-27-2016. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1028&context=pacis2016

30 Mell, P.; Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145; Gaithersburg, MD, USA, 2011.

31 Almarabeh, T.; Majdalawi, Y.K.; Mohammad, H., Cloud Computing of E-Government. Communications and Network, Scientific Research Publishing, 2016, 8, 1–8.

32 Kshetri, N., Cloud computing in developing economies. IEEE Computer 2010, No. 10, Vol. 43, pp. 47–55.

33 Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., Current State of Cloud Computing Adoption - An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA). Procedia Computer Science Vol. 110, 2017, pp. 378–385.

34 Bojanova, I.; Samba, A., Analysis of Cloud Computing Delivery Architecture Models. Proceedings of the 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), Singapore, 22–25 March 2011; pp. 453–458.

disposición los servicios de TI como un producto básico.[35],[36] En general, los beneficios del cómputo en la nube incluyen: eficiencia de costos, almacenamiento ilimitado, respaldo y recuperación, integración automática de software, fácil acceso a la información, implementación rápida, facilidad para ampliar servicios, y entrega de nuevos servicios;[37] incluye otros beneficios tales como utilización optimizada del servidor, ampliación dinámica y desarrollo del ciclo de vida minimizado de nuevas aplicaciones. Sin embargo, la nube aún no se ha adaptado como debiera a la informática debido a muchos factores, principalmente relacionados con el movimiento de la información administrado por un tercero, donde, además del consumidor y proveedor de la nube, hay otros actores: el auditor, el intermediario y el operador de la nube.[38] Por lo tanto, en la administración de los datos, la pérdida de control, seguridad y privacidad, calidad y seguridad, etc., son citados como preocupaciones reales al adoptar el modelo de cómputo en la nube.[39] El bloqueo de datos es otro riesgo potencial, donde los clientes de la nube pueden enfrentar dificultades para extraer sus datos.[40] Los consumidores de la nube pueden sufrir desafíos operacionales y regulatorios como el de la territorialidad a medida que las organizaciones transfieren sus datos a terceros para su almacenamiento y procesamiento.[41] Además, puede ser difícil para los

35 Forell, T.; Milojicic, D.; Talwar, V., Cloud Management: Challenges and Opportunities. Proceedings of the 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), Shanghai, China, 16–20 May 2011; pp. 881–889.

36 Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science Vol.94, 2016, pp. 160–167.

37 Ko, R.K.L.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Liang, Q.; Lee, B.S., TrustCloud: A Framework for Accountability and Trust in Cloud Computing. Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, 4–9 July 2011; pp. 584–588.

38 Bumpus, W., US Government Cloud Computing Technology Roadmap Volume I Release 1.0 (Draft), NIST Special Publication 500-293, Gaithersburg, MD, USA, 2011.

39 Ramachandra, G.; Iftikhar, M.; Khan, F. A., A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science Vol. 110, 2017, pp. 465–472.

40 Opara-Martins, J. N., A Decision Framework to Mitigate Vendor Lock-in Risks in Cloud (SaaS Category) Migration; Bournemouth University: Poole, UK, 2017.

41 Jennings, B.; Stadler, R., Resource Management in Clouds: Survey and Research Challenges. Journal of Network and Systems Management, July 2015, Vol. 23, No. 3, pp. 567–619.

consumidores la verificación de mejores prácticas de manejo de datos del proveedor de la nube o cualquiera de los otros actores involucrados.[42], [43] El modelo de cómputo en la nube es una tecnología altamente emergente, de tal forma que la adopción de sus servicios requiere estrategias de gobernanza de datos aún más rigurosas y programas más complejos, pero necesarios.

El consenso general es que el gobierno de datos se refiere a la totalidad de la decisión de derechos y responsabilidades relacionados con la gestión de datos como activos en las organizaciones. Sin embargo, no proporciona la misma importancia para la gobernanza de datos dentro de la computación en el contexto tecnológico de la nube, por lo tanto, este déficit requiere una comprensión profunda de la gobernanza de datos y del cómputo en la nube. Esta tendencia, contribuye a los cambios en la estrategia de gobierno de datos en la organización, así como en la estructura y las regulaciones legales, las personas, la tecnología, los procesos, los roles, y responsabilidades Este es uno de los grandes desafíos que enfrentan las organizaciones hoy en día cuando ubican sus datos a entornos de cómputo en la nube, particularmente con respecto a cómo la tecnología de la nube afecta a la gobernanza de los datos. La observación general de los autores revela que el área de gobernanza de datos en general ha sido investigada poco y por lo general no se practica por las organizaciones, y mucho menos la nube informática, donde la investigación está en su infancia y aún lejos de alcanzar su madurez. En la figura 2, se muestran las interrelaciones entre los dominios de gobernanza de datos en la nube.

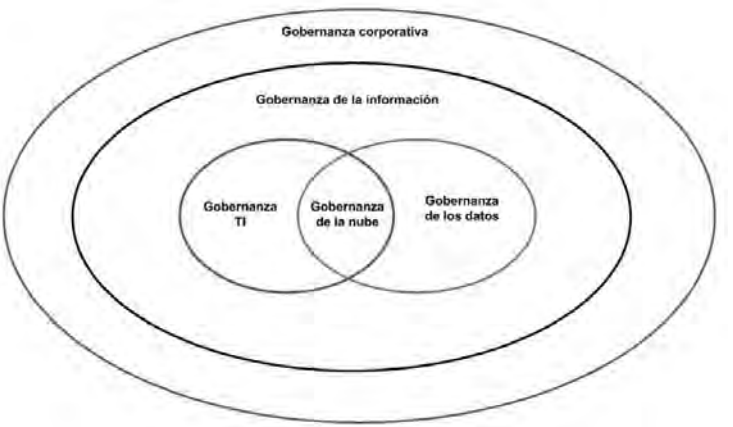
Pero la mayoría de los términos comúnmente utilizados, ya sean de gobierno, gestión o administración, describen

42 Rifaie, M.; Alhajj, R.; Ridley, M., Data Governance Strategy: A Key Issue in Building Enterprise Data Warehouse. Proceedings of the iiWAS '09, 11th International Conference on Information Integration and Web-Based Applications & Services, Kuala Lumpur, Malaysia, 14–16 December 2009; pp. 587–591.

43 Neela, K.L.; Kavitha, V., A Survey on Security Issues and Vulnerabilities on Cloud Computing. International Journal Computer Science & Engineering Technology, Vol 4, No. 7, 2013, pp. 855–860.

diferentes aspectos del mismo objetivo: utilizar datos para "gobernar" mejor la institución.[44]

Figura 2
Las interrelaciones entre los dominios de gobernanza en la nube[45]



En esencia, la gobernanza de datos implica implementar políticas y sistemas para garantizar que las personas tengan acceso a los datos que requieren para tomar decisiones sólidas y para llevar a la institución hacia el éxito. El gobierno de datos tiene esencialmente cuatro componentes básicos:

Propiedad de los datos. Al igual que en cualquier área de la vida, si no hay alguien explícitamente responsable de hacer que suceda algo, es probable que no lo haga. Las instituciones no pueden arriesgarse con los datos. La gobernanza implica asignar en la organización a las

44 Dvries, H., Data Governance. Ellucian, February, 15, 2018. Recuperado 25 de julio de 2018. https://www.ellucian.com/Insights/The-analytics-powered-campus/

45 Al-Ruithe, M., Benkhelifa, E. and Hameed, K., Data governance Taxonomy: Cloud versus Non-Cloud. Sustainability 2018, 10(1), 95. https://doi:10.3390/su10010095

personas adecuadas la responsabilidad de administrar, definir, interpretar y proteger los datos apropiados.

Acceso a los datos. Establecer reglas sobre la jerarquización de los datos, y luego implementar los sistemas para hacer cumplir esas reglas, es una de las metas angulares de la gobernanza. Sin reglas, se corre el riesgo de no cumplir con las regulaciones gubernamentales de privacidad; el personal no compartirá datos por temor a un uso incorrecto; y no estará disponible la información relevante que se necesita para desarrollar el trabajo.

Calidad de los datos. "Datos erróneos" es lo que las personas asocian más a menudo con la falta de gobierno. Esto se debe a que los datos no confiables, faltantes o inexactos tienen el impacto más visible en las operaciones diarias. La gobernanza implica la creación de procesos formales para la entrada cuidadosa de datos, así como la definición, codificación e interpretación de datos en forma consistente en la organización.

Seguridad de los datos. Obviamente hay un gran componente de TI para la seguridad de los datos, la forma en que los usuarios medios manejan los datos es muy importante. La gobernanza implica el establecimiento y la aplicación de reglas sobre cómo se pueden mostrar, compartir y eliminar los datos.

4. Seguridad en ambientes universitarios en México

4.1 Ciberdelincuentes buscan datos de los centros académicos

Las instituciones de educación superior son objetivos atractivos para los cibercriminales por las siguientes razones:

- Se maneja una amplia variedad de datos muy sensibles: las instituciones de educación superior poseen datos confidenciales sobre estudiantes, padres, ex-alumnos, profesores y personal. Los registros se retienen por lo común durante décadas. Por otro lado, los centros académicos, particularmente aquellos que involucran altos volúmenes de investigación, a menudo alojan datos

que pertenecen a una amplia gama de corporaciones y entidades gubernamentales; las instituciones vinculadas con hospitales locales y regionales, en general, almacenan datos médicos confidenciales.

- Se carece de una estructura centralizada: las instituciones tienden a albergar sus datos sensibles en diversas ubicaciones diferentes en lugar de uno centralizado. Los datos de los estudiantes se pueden guardar por separado en cada campus, dentro de una universidad o en diferentes ramas en un sistema universitario estatal. Los mismos datos se pueden guardar en una variedad de lugares, oficinas de exalumnos, administración central, o incluso a nivel departamental para programas de posgrado.
- Los datos sensibles relacionados con las subvenciones corporativas o gubernamentales pueden estar alojados en departamentos que reciben esas subvenciones o incluso en dispositivos individuales de profesores y estudiantes de posgrado que desempeñan funciones claves de investigación. Esta estructura descentralizada puede dar a los ciberdelincuentes diversas rutas para explotar vulnerabilidades en diferentes sistemas que alberguen datos confidenciales.
- Vulnerabilidades organizacionales: La naturaleza descentralizada del almacenamiento de datos en instituciones de educación superior se debe a menudo a cuestiones organizativas y estructurales. La responsabilidad de implementar las medidas de seguridad y determinar los procesos pueden recaer en diferentes instancias interesadas, en la amplia gama de departamentos universitarios. Las instituciones carecen por lo general de una estructura de mando vertical y eso hace que las nuevas medidas sean difíciles de implementar; por lo tanto, departamentos, profesores o estudiantes pueden tardar en adoptar las mejores prácticas necesarias para mejorar la seguridad.
- Uso generalizado de dispositivos personales: los administradores, el profesorado o la planta científica pueden desconocer en qué medida exponen a su institución a riesgos cibernéticos cuando

> descargan en sus dispositivos datos confidenciales provenientes de personal menos protegido. Como resultado, incluso si una institución tiene medidas de seguridad sólidas, cualesquiera personas en la institución pueden, ya sea por descuido, de manera involuntaria, o por falta de conocimiento, exponer o propagar datos confidenciales.

En resumen, el gran volumen de datos potencialmente valiosos, almacenados en la mayoría de las instituciones de educación superior, tiende a convertirlas en objetivos altamente atractivos. Los ejemplos también ilustran que las vulnerabilidades de la seguridad cibernética son causadas por la combinación de elementos técnicos y humanos en un sistema. Los elementos técnicos pueden incluir vulnerabilidades de software que permitan el acceso no autorizado a través de programas particulares. Los usuarios legítimos pueden ser dirigidos por la ingeniería social que los alienta a tomar ciertas acciones o divulgar información que permitan a los atacantes acceder a los sistemas. El acceso remoto persistente también se puede lograr mediante el acceso físico no autorizado a redes, y por medios transportables o extraíbles como computadoras portátiles o dispositivos móviles.

El riesgo principal de las diferentes amenazas cibernéticas es la pérdida de la continuidad del trabajo de una institución, provocado por el robo de información o daño a las redes, es decir, imposibilitan a la universidad y a su comunidad hacer su trabajo. Las instituciones o los investigadores pueden perder acceso a datos esenciales, los datos pueden corromperse, la información puede ser robada, sin considerar los costos de impacto al proyecto o a la institución. Esto puede tener una serie de implicaciones, por ejemplo:

De prestigio. El robo de información y los problemas de integridad pueden dañar gravemente el prestigio de una universidad a los ojos de estudiantes, socios, empresas y gobiernos.
De tipo legal. El robo de información puede dejar en tal situación a las instituciones que infrinjan la legislación o los contratos vigentes y el riesgo de ser enjuiciados,

sancionados y el retiro de fondos de proyectos existentes y futuros.

De tipo económico. El robo de información puede directamente minar a la universidad o la capacidad del investigador para capitalizar el potencial de la propiedad intelectual o en la transferencia de conocimiento.

De tipo operacional. Puede haber daños inmediatos a las redes e infraestructura que dificulta las actividades de una institución y que da como resultado importantes costos de reparación.

Un enfoque institucional para la evaluación de riesgos tendrá que identificar y evaluar los activos de datos y sus riesgos. Un proceso de evaluación de riesgos debe tener en cuenta lo siguiente:

- ¿Qué información se considera crítica por la universidad?
- ¿Qué información puede ser de interés para fines delincuenciales, políticos o económicos?
- ¿Cómo y dónde se puede acceder la información en forma legítima e ilegítima?
- ¿Los controles y políticas que administran acceso y uso de datos son los adecuados?

Es esencial para este proceso de evaluación de riesgos estar integrado en la gobernanza de la información y la investigación para permitir decisiones de gestión de riesgos que permitan establecer un equilibrio apropiado entre:

- El riesgo de ciberseguridad, en donde se incluyen a la probabilidad, naturaleza e impacto potencial
- Prioridades de gestión de datos, incluidos acceso, usuarios y ciclo de vida de la publicación
- Los costos de implementación de controles, incluyendo los recursos y los costos indirectos

4.2 Equilibrio de seguridad cibernética con la apertura

La seguridad y la apertura se pueden abordar como dos temas en una misma administración de datos y proceso de evaluación de riesgos. La evaluación de riesgos efectiva deberá permitir que una universidad identifique el manejo

adecuado y seguro en todo el ciclo de vida de los diferentes tipos de información que son producidos y utilizados. El proceso debe incluir la evaluación de las prioridades de administración, riesgos de seguridad, controles de acceso apropiados y la forma de publicación e infraestructura de almacenamiento. Un enfoque integrado podría permitir a una institución abordar la seguridad cibernética y los datos abiertos, así como la transferencia de conocimiento, con confianza, en el conocimiento que los datos son apropiados para su reutilización por parte de terceros.

4.3 Implementación de seguridad cibernética en la gobernanza de la información

Las universidades deberían considerar quién en la institución 'tiene' o 'controla' los datos para establecer líneas claras de evaluación, rendición de cuentas y monitoreo entre la producción descentralizada y el uso de los datos de la institución que comparte los costos de las fallas de seguridad. Las instituciones universitarias deberán también realizar auditorías internas y externas de sus riesgos, prioridades de administración y sistemas. La identificación y la selección de controles de seguridad en ciertos tipos de datos sólo se pueden lograr con la participación activa de los controladores de datos. Estos grupos están en mejor posición para identificar activos, evaluar cuales tipos de controles serán los más apropiados e implementarlos en última instancia, así como para ser responsables de mantener la integridad de sistemas y datos. El equipo ejecutivo informa al rector, quién por lo general tiene acceso sin límite de los datos corporativos de la institución, aunque los datos también estarán en manos de las instancias académicas y tutores. En el caso de la investigación, los investigadores principales y decanos de las áreas de investigación pueden ser principalmente responsables de controlar los datos. Como resultado, es importante que desempeñen un papel central al decidir las vulnerabilidades de riesgo de una institución y la identificación y evaluación de activos de información.

La seguridad de la red académica es una responsabilidad de toda la institución. Los administradores de red pueden mantener el conocimiento actualizado de amenazas y

contramedidas a través del intercambio de información con compañeros y con agencias de gobierno. Sin embargo, son los usuarios quienes juegan roles cruciales para la seguridad de cualquier red y de la información. Los usuarios deben tener un papel central en la evaluación del riesgo que enfrenta la información, configuración de gestión y las prioridades de la seguridad, en última instancia, como usuarios, son responsables para la implementación de controles. Es esencial que los usuarios de la red, incluso aquellos usuarios que manejan activos más sensibles, sean conscientes de sus responsabilidades y actúen en consecuencia.

4.4 Gobernanza corporativa universitaria

Todas las instituciones de educación superior deben conocer sus responsabilidades con respecto a la protección de datos administrativos, personales y financieros y, por tanto, tener medidas apropiadas para garantizar que cumplan con la Ley de Protección de Datos del INAI. También deben tener diferentes estructuras para la administración de datos e investigación, y contar con los procedimientos apropiados de supervisión; es necesario que las instituciones y los investigadores desarrollen políticas y planes para la administración de datos, teniendo una supervisión corporativa adecuada. Estas características se presentan como desafíos a un gobierno corporativo para entender ambos problemas y los enfoques que se pueden emplear para ayudar a desarrollar la práctica de seguridad cibernética en la universidad. La figura 3 (página siguiente), muestra el proceso de administración de amenazas de seguridad cibernética en una universidad .

La seguridad cibernética corporativa universitaria efectiva debe tener en cuenta la estructura descentralizada de la administración de datos, considerando el riesgo de toda la institución que puede ser asociado con cualquier falla de gestión. La supervisión corporativa de los riesgos inevitablemente depende de la comunicación y la gestión por aquellos con responsabilidad para controlar los datos. Una función de supervisión puede ser integrada en procesos

de aprobación de investigación existentes; no obstante, estos pueden necesitar ser ajustados para tomar en cuenta los riesgos económicos potenciales, los requisitos éticos, legales y contractuales. Cuando se establece la política, el gobierno corporativo debe buscar respuestas claras a las siguientes preguntas:

- ¿Qué información tiene su universidad, que la ley, los donantes o socios consideren sensibles?
- ¿Quién posee o controla los datos dentro de la institución?
- ¿Cómo se deberían establecer las prioridades de administración para los datos?
- ¿Cuáles son los canales para monitorear y administrar los riesgos de seguridad?

Figura 3
Modelo de proceso para la gestión de amenazas de seguridad cibernética en instituciones de educación superior[46]

46 Universities UK, Cyber security and universities: managing the risk. 28 November 2013. Recuperado el 10 de septiembre de 2018. https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf

4.5 Recomendaciones para gobernanza corporativa

- Es importante valorar la implementación de un comité de gobernanza para mantener la supervisión institucional de la administración de datos y riesgos de la seguridad cibernética.
- Considere realizar una evaluación institucional de riesgos de ciberseguridad y gestión de prioridades de los datos de los activos existentes y nuevos.
- Asegurar de que existen canales claros de comunicación y reportes entre controladores de datos y la gobernanza de riesgos y la administración de prioridades.
- Valore la función de auditoría interna e independiente para evaluar el gobierno corporativo y la administración de la ciberseguridad incluidos más allá de las responsabilidades legales.

4.6 Administración de los datos de investigación

Medidas para mejorar la seguridad de los datos dentro de las áreas de investigación de las universidades, que deben trabajar con políticas de administración de datos en evolución y estructuras de apoyo. La política debe enfocarse a que los investigadores puedan administrar eficazmente los datos de investigación de forma tal que puedan ser presentados en repositorios de acceso abierto o tener controles de seguridad apropiados como la administración de prioridades de los datos que evolucionan.

Las universidades deben considerar auditorías de los datos para identificar los datos potencialmente sensibles y evaluar sus riesgos y prioridades de administración. Los objetivos para la auditoria deben hacerse explícitos a todos aquellos involucrados en la identificación y evaluación de riesgos, deben cubrir las consideraciones de seguridad tan amplias como sean posibles, las políticas de administración y prioridades de las mejores prácticas con el fin de apoyar a los investigadores en su trabajo. Los parámetros de cualquier auditoría deberían ser cuidadosamente definidos para asegurar que sólo se incluyen datos relevantes en el proceso. Debido a esto una auditoría puede considerar centrarse en la evaluación de una serie de conjuntos

de datos de investigación significativos y la naturaleza de las mejores prácticas de administración existentes, con una visión para informar una política y una práctica más integrales.

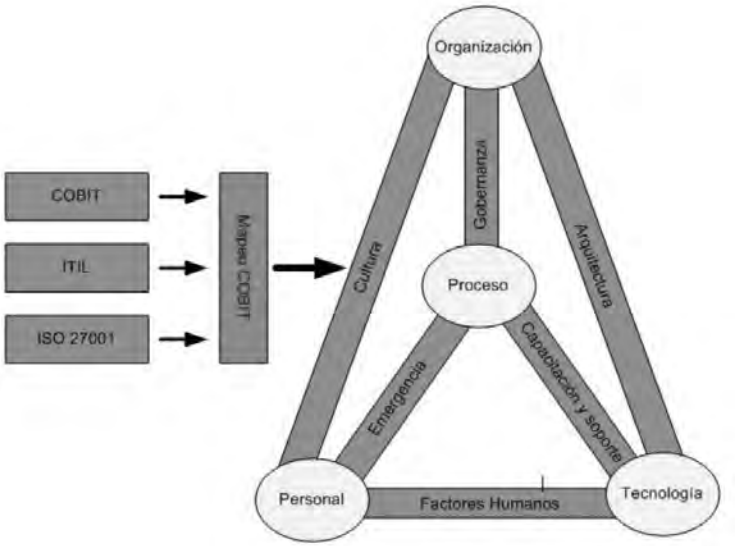
4.7 Recomendaciones para administrar la investigación

- Desarrollar una auditoría y evaluación de enfoque ligero bajo un marco de referencia para evaluar riesgos y administración de medidas a los datos existentes.
- Revisar los planes de manejo de datos como parte de una revisión ética e investigación en curso de procesos de gobierno, para evaluar el potencial de riesgos de seguridad y prioridades de gestión.
- Requerir que las consideraciones de seguridad sean incluidas en los planes de administración de los datos para todas las nuevas propuestas de investigación.

4.8 Modelo de madurez de seguridad de la información

El modelo de madurez de seguridad de la información (ISMM) está pensado como una herramienta para evaluar la capacidad de las organizaciones para cumplir los objetivos de seguridad: confidencialidad, integridad y disponibilidad a la vez que previene los ataques y logra la misión de la organización a pesar de los ataques e infracciones. El modelo define un proceso que administra, mide y controla todos los aspectos de la seguridad. Se basa en cuatro indicadores básicos para la evaluación comparativa y sirve como ayuda para comprender los requerimientos de seguridad de la universidad. Estos indicadores están orientados a la meta de alcanzar las necesidades de seguridad. Muchos de estos modelos son bastante detallados y cumplen los requisitos de seguridad con respecto a los requisitos tecnológicos, generalmente conduce a un programa de trabajo muy costoso para implementar la seguridad que se centra en la tecnología, pero no es orientado a los negocios. La figura 4 muestra la arquitectura del modelo de madurez de seguridad de la información.

Figura 4
Modelo de seguridad de la información[47]



Se han usado otros modelos, incluyendo la restricción del alcance para unidades administrativas individuales o dado su alcance en términos de los procesos de la administración universitaria. Un análisis del desarrollo del modelo de gobierno de TI se muestra en la Figura n para ilustrar los conceptos básicos de los enfoques teóricos.

Este modelo comienza con el modelo de Madurez COBIT 5 utilizando el proceso de control RACI (Responsable, Contable, Consultado e Informado). Una combinación del modelo de madurez de gobierno de TI, COBIT® 5, ISO 27001 e ITIL ® V3 alcanzando en el nivel de estándares y procesos dentro del marco de referencia más que a nivel de control objetivo. El proceso clave de ITIL ® V3 es para la gestión de cambios

47 Suwito M.H., Matsumoto S., Kawamoto J., Gollmann D., Sakurai K. (2016) An Analysis of IT Assessment Security Maturity in Higher Education Institution. In: Kim K., Joukov N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, Vol. 376. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-10-0557-2_69

y modelos de procesos de administración de liberación de aplicaciones mapeadas a ISO 27001 y luego presentado en un programa convencional de estructura de gestión EPM para la elaboración de informes y administración continua. Cada concepto de seguridad, construcción o tipo de dispositivo tiene una dimensión asociada con los cambios que se identifican en este modelo.

El objetivo de la seguridad de la información es proteger adecuadamente este activo y garantizar la continuidad de operación de la institución universitaria, reducir el daño a la universidad y mejorar el rendimiento de inversiones realizadas en la institución. Según lo definido por la norma ISO 27001, la seguridad se describe como preservación,[48] considerando los siguientes principios:

- Confidencialidad: Esto es para asegurar que la información es accesible solo para aquellos que están autorizados y tienen derecho a acceso
- Integridad: esto es para garantizar que la información sea precisa y ahora debe modificar y mantener de forma segura la exactitud e integridad de la información, así como los métodos de procesamiento
- Disponibilidad: esto es para asegurar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

4.9 Combinación de estándares

A medida que un marco de referencia y diferentes estándares evolucionan, crean confusión, especialmente al usar uno de ellos. Al mirarlos más de cerca, es muy claro que se pueden alinear con éxito. Realizar el proceso de prestación de servicios informáticos sin definir realmente las medidas para monitorear el proceso, generará un mayor riesgo y sería menos eficiente. Este es uno de los argumentos para la combinación de COBIT® 5, ITIL ® V3 e ISO / IEC 27001. Por lo tanto, las mejores prácticas deben adaptarse a las necesidades de la universidad e integrarse entre sí con los procedimientos internos. COBIT® 5 se puede utilizar al

48 Daminda, P., ISO/IEC 27001, Information Security Management System, ISO 27001 Family, pp. 2-21 (2008).
https://www.dnvgl.com/services/iso-iec-27001-information-security-management-system-3327

más alto nivel, proporcionando un marco de control general basado en el modelo de proceso de TI que debe adaptarse a cada organización en general. Prácticas y estándares específicos como ITIL ® V3 e ISO/IEC 27002 cubren áreas discretas que pueden ser mapeadas al marco de referencia de COBIT® 5, proporcionando una guía jerárquica de materiales de orientación.

Las instituciones de educación superior enfrentan retos que las hacen competir estratégicamente, como otras organizaciones sin fines de lucro. Para soportar este nuevo enfoque sus sistemas de información y estrategias comerciales deben estar totalmente alineados. El entorno actual de sistemas de información heterogéneos y aplicaciones implementadas en diversas instituciones puede comprometer tal objetivo. Para enfrentar estos retos han surgido las arquitecturas y modelos de referencia como instrumentos adecuados para auxiliar a los tomadores de decisiones de la universidad. Aunque muchos de estos modelos de software ya existen para diversas industrias, hasta ahora se ha hecho poco en la educación superior. Se han construido algunos desarrollos que pueden considerarse como un modelo de referencia de sistemas de información unificados específicamente para instituciones de educación superior.[49]

4.10 Caso de estudio

Se estableció la gobernanza de los datos en un centro de investigación, implementando una solución de seguridad en un laboratorio que es susceptible de ser visitado frecuentemente por *hackers* para intentar extraer información de su servidor principal de diseño. En algún momento, se tuvo un ataque de negación de servicios en una computadora personal de un integrante del laboratorio. Por lo anterior, se establecieron políticas de seguridad más radicales y se establecieron controles para la navegación *web*, así como perfiles de uso por usuario y por computadora.

49 Sánchez-Puchol F., Pastor-Collado J. A., Borrell B., Towards an Unified Information Systems Reference Model for Higher Education Institutions, Procedia Computer Science, Vol. 121, 2017, pp. 542-553. https://doi.org/10.1016/j.procs.2017.11.072.

La infraestructura de red de este laboratorio consta de un enrutador que administra los enlaces de red Ethernet de 1 Gb de ancho banda, un dispositivo de almacenamiento en red con 2 Tb de almacenamiento, una antena inalámbrica de 700 Mhz de ancho de banda, un servidor Blade Intel X64 de 1 Tb de almacenamiento y 8 Gb de RAM, dos impresoras en red y 12 estaciones personales Intel Windows X64. Se cuenta con las herramientas de diseño electrónico de tipo industrial, que permiten diseñar un circuito desde su modelado matemático hasta la generación de los archivos necesarios para su construcción en silicio. Desde cualquier computadora personal es posible acceder al servidor de diseño a través de un software de comunicación que permite tener el ambiente gráfico de las herramientas de diseño electrónico que se tienen en una estación de trabajo de alto desempeño.

Se implantó el software que establece la función de consola que vigila la red de prueba y realiza la función principal de administración del antivirus y del cortafuegos, además de parametrizar los perfiles de seguridad de cada grupo o usuario a vigilar de acuerdo a su jerarquía en la red. La consola interactúa con los sistemas operativos Windows, Mac OS y diversas versiones de Linux. Sin embargo, con el sistema Windows cualquier versión tiene mejor disponibilidad de funciones de monitoreo con respecto a los otros sistemas, inclusive es posible dar mantenimiento al registro y defragmentar el disco duro de cada computadora que tenga Windows, en forma remota. Las estaciones personales se monitorean a través de un agente que se instala en cada una de las computadoras y tiene acceso completo al equipo remoto. El dispositivo de almacenamiento en red tiene su propio sistema de seguridad. El uso de los recursos del laboratorio tiene que mantener la sencillez de siempre al utilizarlos.

La consola de monitoreo se apega a lo dispuesto por el ISO 27001, permite definir políticas de seguridad de acuerdo a los perfiles que se requieran. El posible detectar el polimorfismo de los archivos que se reciben en el correo electrónico, previene los ataques de negación de servicios; además, cada agente que reside en cada una de las computadoras tiene un detector de malware.

Se busca que se pueda generar una red de repositorios de almacenamiento en red que respalden en automático la información de cada computadora que esté conectada a la red, y que tengan políticas de seguridad que limiten el posible hurto de la información generada de las investigaciones en los distintos laboratorios de investigación de la institución.

Por el otro lado, se pretende integrar los dispositivos de almacenamiento masivo en red a través de protocolo LDAP, lo que permitirá unificar el acceso bajo una política de seguridad institucional; al igual que los dispositivos de IoT. Lo anterior es con el fin principal de que los dispositivos de almacenamiento masivo por edificio pueden garantizar que la información no sea robada o alterada, y en caso que se requiera compartir que sea bajo una política de seguridad.

La gobernanza de los datos que se implantó ha protegido los diseños tecnológicos y la propiedad intelectual de este laboratorio. Los usuarios se han apegado a las reglas implantadas para el uso de los recursos computacionales. Aun cuando se implantó una plataforma de bajo costo, los beneficios que se obtuvieron son de alto valor. Se evaluaron soluciones de mayor seguridad, pero por su alto costo y las restricciones del presupuesto no fue posible implantarlas.

Conclusiones

La seguridad informática es una componente esencial de la seguridad nacional. En el ambiente académico, la confidencialidad, la privacidad, la disponibilidad y la integridad de la información ha de preservarse y garantizarse, tanto la de tipo administrativo, como educativo, de desarrollo tecnológico y de investigación básica.

Los centros académicos por sus propias características de plena libertad y consciencia crítica han sido desde siempre blancos predilectos de ciberdelincuentes, los que han tenido éxitos de diverso tipo en sus ataques: ha habido ataques inocuos e infructuosos, algunos que significan incomodidades intrascendentes a la vida académica, pero ha habido también ataques exitosos, como el control de equipo, el robo de información, la suplantación de identidades ola tergiversación de resultados, con lo cual el prestigio institucional se ha visto fuertemente afectado.

Así pues, cada centro académico ha de poner especial atención en su política de seguridad informática. Hemos presentado esquemas convencionales de tipo organizativo que se han implantado en diversas universidades en el mundo, y que ciertamente nos atrevemos a recomendar para el medio universitario mexicano. La adopción de tales políticas la ilustramos con un caso de estudio propio de nuestro centro de investigación.

BIBLIOGRAFÍA

Aenugu, N.R., Butakov S., Zavarsky P., Aghili S. (2018) Security Perspective in Comparative Study of Platform-Based and Platform-Less BYOD Systems. In: Kim K., Kim H., Baek N. (eds) IT Convergence and Security 2017. Lecture Notes in Electrical Engineering, Vol. 450. Springer, Singapore.

Almarabeh, T.; Majdalawi, Y.K.; Mohammad, H., Cloud Computing of E-Government. Communications and Network, Scientific Research Publishing, 2016, 8, 1–8.

Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science Vol.94, 2016, pp. 160–167.

Al-Ruithe, M.; Benkhelifa, E.; Hameed, K., Current State of Cloud Computing Adoption - An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA). Procedia Computer Science Vol. 110, 2017, pp. 378–385.

Al-Ruithe, M., Benkhelifa, E. and Hameed, K., Data governance Taxonomy: Cloud versus Non-Cloud. Sustainability 2018, 10(1), 95. https://doi:10.3390/su10010095

Begg, C.; Caira, T. Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. The Electronic Journal Information Systems Evaluation 2012, Vol. 15, pp 3–13.

Bertino, E., and Islam, N., Botnet and Internet of Things Security. Computer, Vol. 50, Issue 2, Feb. 2017, pp. 76-79.

Bojanova, I.; Samba, A., Analysis of Cloud Computing Delivery Architecture Models. Proceedings of the 2011 IEEE Workshops of International Conference on Advanced In-

formation Networking and Applications (WAINA), Singapore, 22–25 March 2011; pp. 453–458.

Bouk, J., Top BYOD Trends for 2018. 14 november 2017, Cass Telecom Systems. https://www.casstelecom.com/blog/top-byod-trends-for-2018

Buffenoir, E.; Bourdon, I. Managing Extended Organizations and Data Governance. Advances in Intelligent Systems and Computing. 2013, Vol. 205, (pp 135–145), Springer, Berlin, Heildelberg.

Bumpus, W., US Government Cloud Computing Technology Roadmap Volume I Release 1.0 (Draft), NIST Special Publication 500-293, Gaithersburg, MD, USA, 2011.

Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), Asociación Mexicana de Tecnologías de la Información (AMITI) y la Asociación de Internet MX, Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado, Octubre 2017. Recuperado el 26 de enero de 2019. https://docplayer.es/65552142-Evaluacion-de-la-ciberseguridad-en-mexico-brechas-y-recomendaciones-en-un-mundo-hiper-conectado.html

CERT-MX, Mnemo-CERT, Scitum-CSIR and UNAM-CERT FIRST (2016). https://www.first.org/members/map#mexico

Daminda, P., ISO/IEC 27001, Information Security Management System, ISO 27001 Family, pp. 2-21 (2008). https://www.dnvgl.com/services/iso-iec-27001-information-security-management-system-3327

Dovey F. T., Clark C. and Lyn G. J., Elevating cybersecurity on the higher education leadership agenda: Increasing executive fluency and engagement in cyber risk. Deloitte Insights, February 2018. https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

Dvries, H., Data Governance. Ellucian, February, 15, 2018. Recuperado 25 de julio de 2018. https://www.ellucian.com/Insights/The-analytics-powered-campus/

Forell, T.; Milojicic, D.; Talwar, V., Cloud Management: Challenges and Opportunities. Proceedings of the 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), Shanghai, China, 16–20 May 2011; pp. 881–889.

Fu, X.; Wojak, A.; Neagu, D.; Ridley, M.; Kim, T. Data governance in predictive toxicology: A review. Journal of Cheminformatics. 2001, 3, 24.

Gobierno de México, Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI. Publicado en el Diario Oficial de la Federación de México, el 30 de Abril de 2014. Recuperado el 4 de octubre de 2018. http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

Gorman, A., and Sewell, A. (2015, July 12). Six people fired from Cedars-Sinai over patient privacy breaches. Los Angeles Times, July 12, 2013. http://articles.latimes.com/2013/jul/12/local/la-me-hospital-security-breach-20130713

Hinden, B., The Internet of Insecure Things. The Internet Protocol Journal, Volume 20, Number 1, March 2017.

Islas, J, Estudio Sobre Los Alcances del Derecho de Acceso a la Información en Universidades e Instituciones de Educación Superior Públicas Dotadas de Autonomía, Derivado de la Reforma Constitucional en Materia de Transparencia. INAI, Diciembre 2017. http://inicio.inai.org.mx/Estudios/AlcancesUniversidadesWeb.pdf

INEGI, Estadísticas a propósito del día mundial del Internet (17 de mayo). 15 de mayo de 2017. Recuperado el 7 de julio de 2018. http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Na1.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. http://inicio.ifai.org.mx/SitePages/ifai.aspx

Jennings, B.; Stadler, R., Resource Management in Clouds: Survey and Research Challenges. Journal of Network and Systems Management, July 2015, Vol. 23, No. 3, pp. 567–619.

Kamioka, T.; Luo, X.; Tapanainen, T., An Empirical Investigation of Data Governance: The Role of Accountabilities. In Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, Summer 6-27-2016. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1028&context=pacis2016

Ko, R.K.L.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Liang, Q.; Lee, B.S., TrustCloud: A Framework for Accountability and Trust in Cloud Computing. Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, 4–9 July 2011; pp. 584–588.

Kravchenko, S. and Riley, M., The American Fugitive From the JPMorgan Hack Turns Up in a Russian Cell. https://www.bloomberg.com/news/articles/2016-10-10/jpmorgan-hack-fugitive-said-to-seek-u-s-deal-from-russian-cell

Kshetri, N., Cloud computing in developing economies. IEEE Computer 2010, No. 10, Vol. 43, pp. 47–55.

Lyn J. G., Understanding Information Security and Privacy in Postsecondary Education Data Systems. EDUCAUSE, May 2016. Recuperado el 22 de mayo de 2018. http://www.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/information_security_and_privacy-executive_summary.pdf

Mell, P.; Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145; Gaithersburg, MD, USA, 2011.

Neela, K.L.; Kavitha, V., A Survey on Security Issues and Vulnerabilities on Cloud Computing. International Journal Computer Science & Engineering Technology, Vol 4, No. 7, 2013, pp. 855–860.

Opara-Martins, J. N., A Decision Framework to Mitigate Vendor Lock-in Risks in Cloud (SaaS Category) Migration; Bournemouth University: Poole, UK, 2017.

Palo Alto Networks, Next Generation Security for Higher Education Institutions. 2017. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/higher-education-institutions-solution-brief

Panian, Z., Some Practical Experiences in Data Governance. World Academy of Science, Engineering and Technology, Vol. 62, 2010, pp. 939–946.

Parraguez K. L., The State of Cybersecurity un Mexico: An Overview, Wilson Center. Mexico Center, Woodrow Wilson Center. January 2017. Recuperado el 7 de julio de 2018. https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf

Poor, M. Applying Aspects of Data Governance from the Private Sector to Public Higher Education; University of Oregon: Eugene, OR, USA, July 2011.

Prasetyo, H.N.; Surendro, K., Designing a Data Governance Model Based on Soft System Methodology (SSM) in Organization. Journal of Theoretical and Applied Information Technology,10 August 2015, Vol. 78, pp. 46–52.

Ramachandra, G.; Iftikhar, M.; Khan, F. A., A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science Vol. 110, 2017, pp. 465–472.

Rifaie, M.; Alhajj, R.; Ridley, M., Data Governance Strategy: A Key Issue in Building Enterprise Data Warehouse. Proceedings of the iiWAS '09, 11th International Conference on Information Integration and Web-Based Applications & Services, Kuala Lumpur, Malaysia, 14–16 December 2009; pp. 587–591.

Russom, P., Data Governance Strategies: Helping Your Organization Comply, Transform, and Integrate; The Data Warehousing Institute: Los Angeles, CA, USA, 2008. http://download.101com.com/pub/tdwi/Files/TDWI_BPR_DG_Q208.pdf

Salami, O.L.; Johl, S.K.; Ibrahim, M.Y. Holistic Approach to Corporate Governance: A Conceptual Framework. Global Bussiness Management Research: An International Journal, vol. 6, No. 3, 2014.

Sanchez-Puchol F., Pastor-Collado J. A., Borrell B., Towards an Unified Information Systems Reference Model for Higher Education Institutions, Procedia Computer Science, Vol. 121, 2017, pp. 542-553. https://doi.org/10.1016/j.procs.2017.11.072.

Seiner, R.S., Non-Invasive Data Governance. 1st ed.; Technics Publications: New York, NY, USA, 2014.

Suwito M.H., Matsumoto S., Kawamoto J., Gollmann D., Sakurai K. (2016) An Analysis of IT Assessment Security Maturity in Higher Education Institution. In: Kim K., Joukov N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, Vol. 376. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-10-0557-2_69

Universities UK, Cyber security and universities: managing the risk. 28 November 2013. Recuperado el 10 de septiembre de 2018. https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf

Weber, K.; Otto, B.; Osterle, H. One Size Does Not Fit All—A Contingency Approach to Data Governance. ACM Journal of Data Information Quality, Vol. 1 Issue 1 June 2009 Article No. 4.

Wende, K., A Model for Data Governance - Organizing Accountabilities for Data Quality Management. In Proceedings of the 18th Australasian Conference on Information Systems; University of Southern Queensland: Toowoomba, Australia, 5-7 Dec 2007; pp. 417–425.