INNOVA Research Journal, ISSN 2477-9024
(Septiembre-Diciembre 2019). Vol. 4, No.3.2 pp. 144-151
DOI: https://doi.org/10.33890/innova.v4.n3.2.2019.1081
URL: http://revistas.uide.edu.ec/index.php/innova/index
Correo: innova@uide.edu.ec

Propuesta de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en una empresa comercial

Proposal of policies to reduce the risk of loss of information on the Cloud office 365 platform in a commercial company, 2019

Rupay Velazco Merlin Stefanny
https://orcid.org/0000-0002-0982-292X
Correa Rosales César Marcelo
https://orcid.org/0000-0003-0137-7240
Rivas Flores Kiara Alessandra
https://orcid.org/0000-0003-0850-8178
Salvatierra Garamendi Miriam Erica
https://orcid.org/0000-0003-2176-8134
Universidad Norbert Wiener, Perú

Autor para correspondencia: merlinrupayvelazco@gmail.com; cesarcorrearosales@gmail.com; kiararf725@gmail.com; msalvatierragaramendi@gmail.com
Fecha de recepción: 13 de julio del 2019 - Fecha de aceptación: 10 de diciembre del 2019

Resumen
La investigación tuvo como objetivo proponer políticas de seguridad de la información para la protección de datos sensibles de la empresa que utilizan frecuentemente los trabajadores en la plataforma de office 365, segmentando documentos de data sensible por áreas, usuarios determinados y mejorando la seguridad de accesos a sus cuentas de correo, o acceso a dispositivos móviles que no cuentan con limitaciones en el uso de la data organizacional. El estudio se basó en el sintagma holístico, enfoque mixto y en el tipo proyectivo, se aplicaron métodos de recolección cuantitativo y cualitativo. Para ello, se entrevistó a tres usuarios con los cargos respectivos de director, gerente y jefe del área; se extrajeron registros de auditoría con accesos de usuarios desde ambientes externos e internos, el cual nos ayudó a conocer quienes acceden a sus cuentas desde IP's fuera del rango de la oficina. Se evidenció que poseen acceso a sus cuentas y documentos de la empresa, los mismos que pueden ser eliminados y/o descargados porque utilizan los servicios en nube de SharePoint u OneDrive. En conclusión, la información se ve expuesta a ser sustraída y manipulada por usuarios externos, dado que la empresa tiene políticas básicas aplicadas a los usuarios.
Palabras clave: protección de la información; políticas de seguridad; plataforma Cloud office 365

Abstract
The objective of the investigation was to propose information security policies for the protection of sensitive data of the company that workers frequently have in the office 365 platform, segment sensitive data documents by areas, specific users and improve access security to your email accounts, or access to mobile devices that do not have limitations in the use of organizational

information. The study was based on the holistic phrase, mixed approach and projective type, quantitative and qualitative collection methods were applied. For this, three users were interviewed with the specific positions of the director, manager and head of the area; audit records were extracted with user access from external and internal environments, which helps us to know who access their accounts from IP outside the office range. It is evident that they have access to their accounts and company documents, which can be deleted and / or downloaded because they use the services in the SharePoint or OneDrive cloud. In conclusion, the information is exposed to be stolen and manipulated by external users, since the company has basic policies applied to users.
Key words: information protection; security policies; Cloud office 365 platform

Introducción

Actualmente las empresas a nivel nacional cuentan con muchas amenazas tecnológicas por las que podrían perder información, en su mayoría las empresas no tienen la infraestructura correcta de prevención o cómo actuar ante casos como este, generando inconvenientes en su trabajo como pérdidas de información, vulnerabilidad, o casos de retención de información y llamadas de secuestro de datos.

En las tendencias en el ámbito tecnológico empresarial y comercial se puede observar la necesidad de disponibilidad de la información y la colaboración, para esto utilizan sistemas o plataformas que les permitan utilizar estas funcionalidades, los correos y archivos con alta disponibilidad y de edición, aunque con este tipo de disponibilidad, nace la consulta. ¿Cómo protejo la información de la empresa cuando se encuentra fuera del área perimetral? Los encargados de sistemas tienen la tarea de analizar un plan para la implementación de seguridad en los administradores donde se alojan los documentos sensibles y/o vulnerables, ello para mantener la confidencialidad, disponibilidad y la integridad de la información de manera segura entonces cuál sería el plan o proyecto para ejecutar que nos ayude a que los documentos tengan y se encuentren disponibles.

Según datos y estimaciones de la rentabilidad muestran que la adopción de la nube aumentaría de una manera significativa entre 2012 y 2016, en forma particular en México y en Argentina. Se suman, Colombia y Chile que figuran entre los países de rápido crecimiento o evolución hacia los servicios en nube, según lo informado por la Cepal. (Israel, 2016).

En el segmento del mercado cloud y Gartner el software como servicio (SaaS) se refleja en un crecimiento del 22%, este año llegó a los US$73.600 millones. De esta forma, las empresas están invirtiendo el 45% en SaaS para los softwares de aplicaciones para el 2021. (Aetecno, 2018).

No obstante, las actividades que se programaron, para consultoría informática y actividades conexas aumentaron en 5,29% por el mejor desarrollo de empresas relacionadas a gestión de negocios (e-commerce), en la investigación de implementación de un sistema de video vigilancia, cloud (computación en nube), data center, correos electrónicos, inteligencia artificial como chatbots (comunicación automática) y ciberseguridad, que se especializaron para empresas del sector bancario y retail; de la misma forma también el avance de las empresas de ingeniería informática como desarrollo de software, diseños y estructuras de páginas WEB y aplicaciones

informáticas, que se impulsaron por la creciente demanda en transformación digital y agilización de las transacciones comerciales del sector telecomunicaciones, financiero y retail. (Zanabria, Sánchez Aguilar, & Montoya Sánchez, 2019).

Materiales y Métodos

El presente estudio se realizará con una plataforma en nube la cual proporciona servicios de correo electrónico, almacenamiento en nube, gestor documental y centro de comunicaciones; cabe mencionar que las herramientas de dicha plataforma se pueden complementar adquiriendo más servicios de niveles superiores para un mejor rendimiento. La metodología está basada en una investigación de tipo proyectiva, con un nivel comprensivo haciendo uso de la recolección de datos e información para su análisis (Hurtado, 2000). El desarrollo inicia con la determinación de los procesos que realizan los usuarios por medio de la acumulación de los datos, posteriormente son extraídos recolectando información a través de registros de auditoría para finalmente, obtener datos cualitativos de la elaboración de una entrevista que se aplicará a 3 jefes con amplio conocimiento en el rubro de TI. Para procesar la información del resultado de datos cuantitativos, cualitativos y triangulación se hizo uso del software Atlas ti.

Resultados

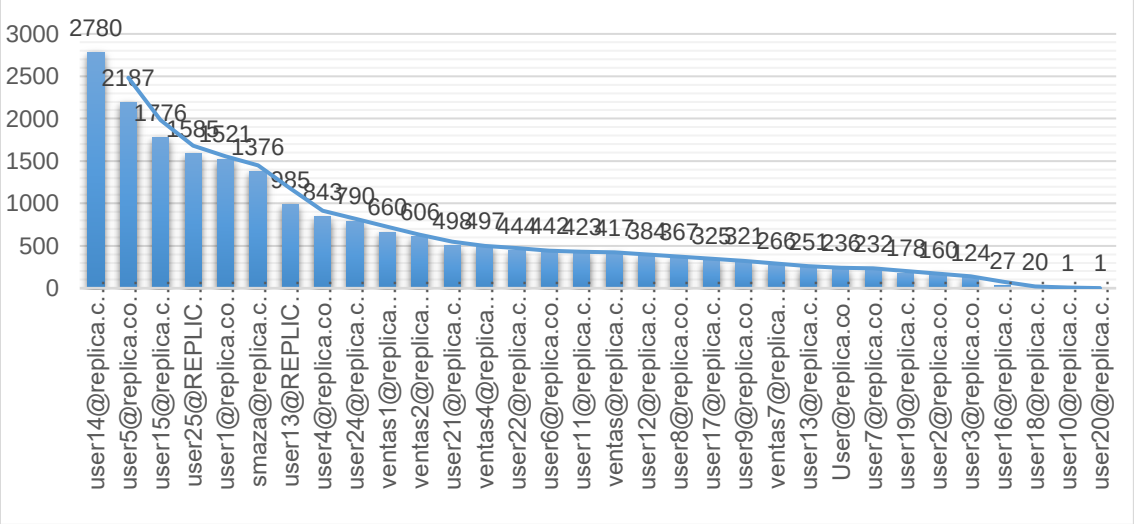

Figura 1. Inicios de sesión por usuario *Fuente*: Elaboración propia.

En este gráfico podemos revisar que 06 usuarios utilizan sus cuentas de correo con mayor afluencia, tanto dentro como fuera de la organización. Indicamos que 05 usuarios son administradores del portal, los cuales identificamos por los accesos cotidianos al sistema. Mientras que 01 usuario accede con mayor continuidad a la información de la organización tanto fuera como dentro de la empresa.

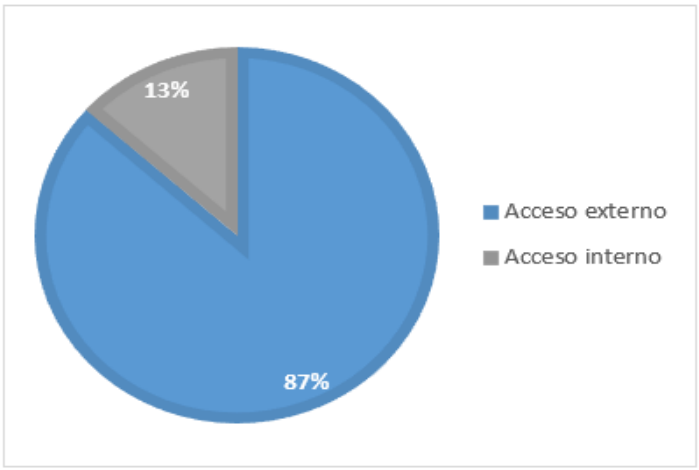

Figura 2. Inicios de sesión por usuario *Fuente:* Elaboración propia.

En el gráfico se muestra que el 87% de los usuarios se conectan externamente porque utilizan las aplicaciones móviles de Office 365 y el correo vía web (OWA), los cuales están fuera de la red de internet de la empresa, mientras el 13% accede dentro de la red de internet de la empresa.

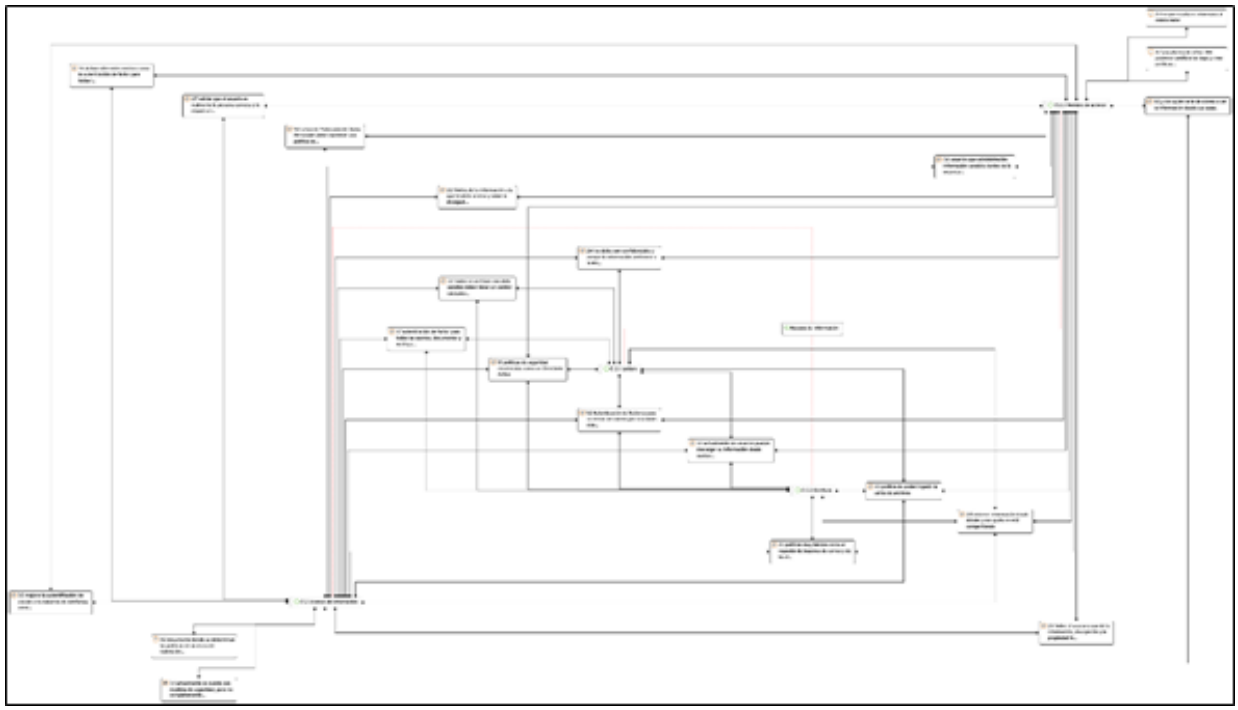

Figura 3. Red de la subcategoría accesos de información. *Fuente:* Elaboración propia.

Según la red de la subcategoría de accesos de información que se realizó por medio del análisis cualitativo, podemos identificar que los permisos de acceso a los usuarios no indica las restricciones, por ello no se tiene una política establecida correctamente(falta de comunicación de las políticas de la empresa), de tal modo que se realiza la auditoría de los accesos externos e internos, la descarga de archivos y registro de archivos eliminados desde la plataforma office

365, ya que hay data sensible a la que el usuario podría tener acceso desde su casa y poder descargarla.

Propuesta

Como primer objetivo: Implementar políticas de seguridad en la plataforma nube. Como parte del desarrollo se plantea una infraestructura desde el análisis de datos, reconocimiento de data sensible y permisos por grupos, áreas y personas. La arquitectura por aplicar será una administración de AIP (Azure Information Protection) y DLP (Data Loss Protection), estos aplicados en el portal de administración en nube, en el que se determina la protección accediendo a OneDrive y SharePoint, permitiendo mantener el control de los documentos pertenecientes a la empresa.

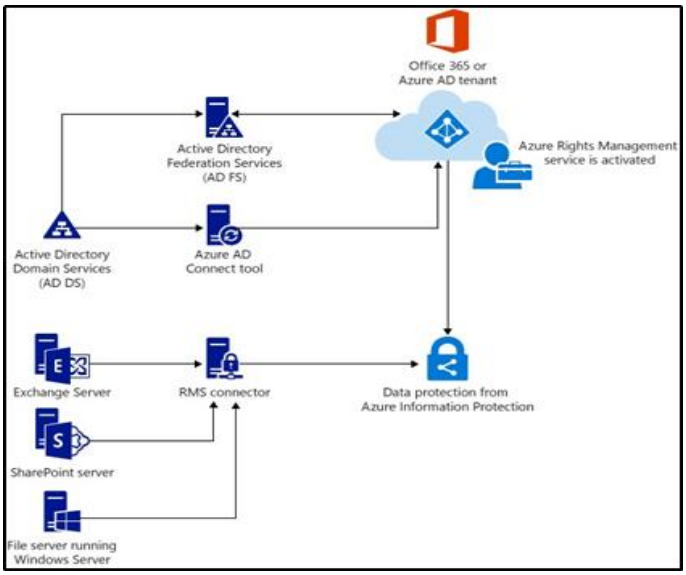

Figura 3. Red de la subcategoría accesos de información. *Fuente:* Elaboración propia.

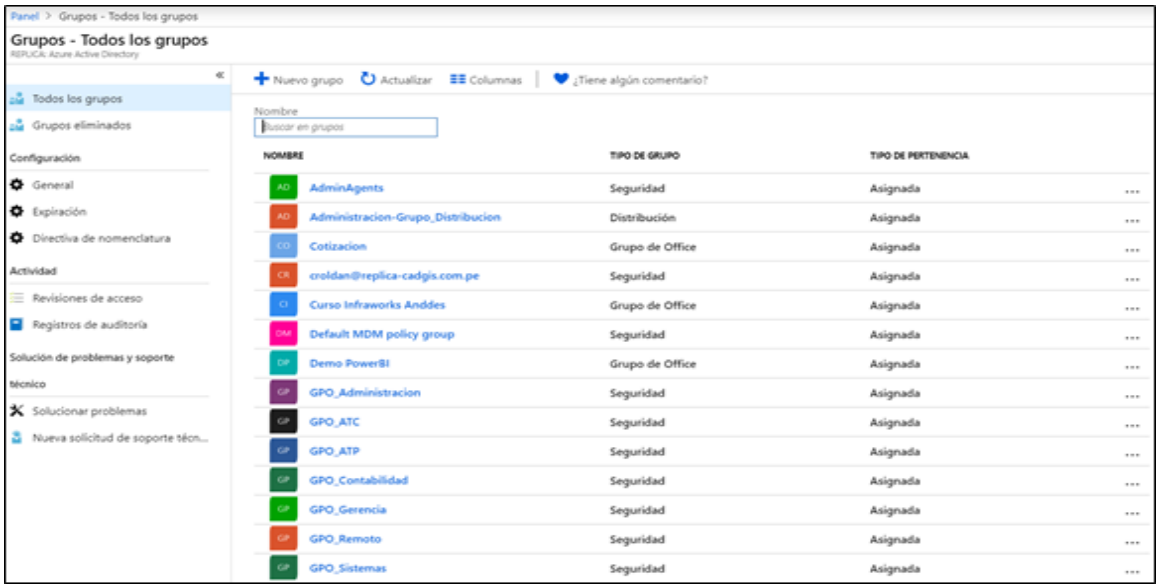

Figura 4. Plataforma de administración de usuarios. *Fuente:* Portal nube.

Como segundo objetivo: Controlar el acceso a las aplicaciones e información de la empresa desde dispositivos móviles. Como parte del desarrollo de la propuesta se plantea una infraestructura desde la administración de dispositivos. La arquitectura para aplicar será un básico MDM que consiste en un agente en nuestro caso será portal empresa de office 365, se instala la aplicación en los dispositivos que se deben administrar, un servidor de en plataforma nube nos ayudara con la configuración necesaria por dispositivo y una base de datos donde se almacén todas las configuraciones realizadas.

Los agentes mantienen una conexión con el servidor a través de USB, Wi-Fi, GPRS, 3G o diferentes medios de transmisión de datos, lo cual le permite al MDM tomar control del dispositivo, en sus algunos casos cubriendo características de lista de aplicaciones no deseadas, el control remoto de la solución y arreglo de los problemas en las máquinas alejadas, podría ser reseteo y o eliminación de cuenta, administración de la información que esté dentro del dispositivo perteneciente a la empresa, gestión de contenido, actualizaciones de OS.

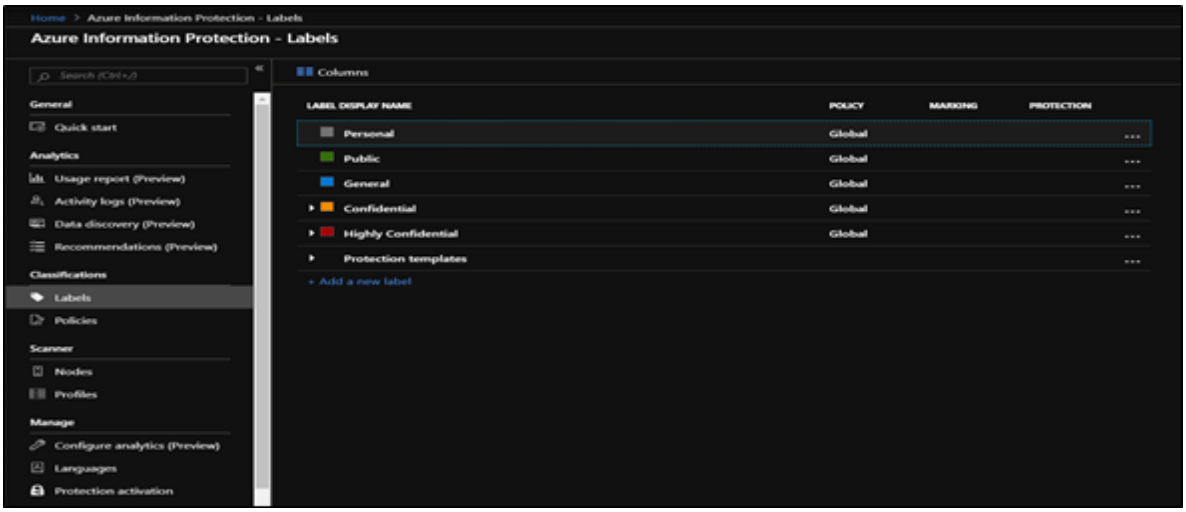

Figura 5. Plataforma de Azure Information Protection. *Fuente:* Portal nube

Como tercer objetivo: Concientizar a los usuarios en el uso y las políticas de seguridad de la información. Como parte del desarrollo de la propuesta se plantea que los usuarios deben estar familiarizados con las actuales mejoras que se llevarán a cabo para la protección de los datos de la empresa, se deberá capacitarlos y orientarlos en el uso de la autenticación por usuario y cómo será el manejo de la data a la que tengan acceso fuera de la empresa.

La empresa comercial requiere la solución planteada la cual consta de la activación de políticas de seguridad de la información, autenticando la información de cada usuario al registrarse en un nuevo equipo, segmentar la información a la que se debe tener acceso.

Determinar la data sensible, la cual se avala con Alcantará (2015) que coincide con el objetivo de contribuir en la mejora del nivel de seguridad de la información. Empleando las políticas de seguridad de la información que se configuran en la plataforma en nube, la cual se segmentara por grupos desde Azure AD.

Realizando estas configuraciones podremos tener relación con el objetivo del estudio de Bermúdez y Bailon (2015) de los cuales su objetivo fue analizar los procesos críticos para respaldar la confidencialidad, integridad y disponibilidad de la información, ya que cada usuario puede tener accesos para una mejor productividad, con relación al estudio de Vasquez (2015), se determinó la prevención de los ataques cibernéticos, para esto tendremos un mejor control por usuario.

Conclusiones

Se propuso la implementación de políticas de seguridad para proteger la información corporativa de tal manera reducir y evitar la salida de datos corporativos y mantener un control de los documentos.

Se basó el diagnóstico en un estudio cuantitativo y cualitativo que se trabajó de la mano con la ayuda con el administrador de Sistemas para la obtención del log de auditoria del cual obtuvimos resultados indicando que la mayoría de los accesos a cuentas era de manera externa.

Se trabajó con categorías, subcategorías e indicadores los cuales se pudo conceptualizar con la ayuda de artículos y tesis encontrados, así mismo nos ayudó a conocer más sobre el tema de investigación percibir que son enriquecedores para poder generar un a propuesta de implementación.

Se planteó una implementación de las políticas de seguridad para mejorar el control de acceso a la data de la empresa, reduciendo así la posibilidad de ataques con el autenticador de usuarios y utilizando un token, para cuando se genere un intento de acceso a data de la empresa, agregando portal de administración para el control de los dispositivos con acceso a la data de la empresa.

Bibliografía

Abreu, J. L. (2014). El Método de la Investigación. Daena: International Journal of Good Conscience, 195-204.

Aetecno. (31 de julio de 2018). Aetecno. americaeconomia, 1-2. Obtenido de Aetecno.

Albarracín, J. (2002). La teoría del riesgo y el manejo del concepto riesgo en las sociedades agropecuarias andinas. *CIDES-UMSA, Posgrado en Ciencias del Desarrollo*, 1-27.

Benito Jaén, A. (1981). *Fundamentos de teoría general de la información.* Madrid: Editorial Piramide.

Bertalanffy, L. (1989). *Teoría general de Sistema.* Distrito Federal: Fondo de cultura económica.

Corral, Y. (2010). Diseño de cuestionarios para recoleccion de datos. *Ciencias de la educación*, 152-168.

Fermín, F. (2012). La Teoría de Control y la Gestión Autónoma de Servidores Web. *COMTEL 2012*, 73-78.

Fernández, L. (2007). Fichas para investigadores. *Butlletí LaRecerca*, 1-9.

Guevara, L. (2012). gestión del riesgo en la seguridad informática: "cultura de la auto-seguridad informática. bogota. obtenido de

https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/parramorenoduveraugusto2012.pdf;jsessionid=17f4bbca76c61725122d03185d6ce6f4?sequence=2

Hurtado de Barrera, J. (2000). *Metodologia de la investigacion holistica.* Caracas: Servicios y proyecciones para America Latina.

Israel, D. (junio de 2016). *Itsitio*. Obtenido de Itsitio: https://www.itsitio.com/ec/todos-los-caminos-llevan-a-la-nube/

Jaime Gutiérrez, J. (2003). *Protocolos criptográficos y seguridad en redes.* Obtenido de https://books.google.com.pe/books?id=cQk_Ms6MUfEC&pg=PA14&dq=proteccion+de+la+informacion&hl=es&sa=X&ved=0ahUKEwiunuK4i-riAhVJK7kGHYlbA3IQ6AEIOjAD#v=onepage&q=proteccion%20de%20la%20informacion&f=false

Lopez, A., Parada, A., & Simonetti, F. (1995). *Teoria de la información.* Santiago.

López, N., & Sandoval, I. (2013). *Métodos y técnicas de investigación cuantitativa y cualitativa.* Guadalajara.

Núñez Vidal, E., Villarroel González, C., & Cuevas Gil, V. (2010). *Suplantación de la identidad.* Universidad Complutense de Madrid.

Ojeda, C. (2017). *Sistema De Gestion De Seguridad Y Salud En El Trabajo.* Magdalena. Obtenido de http://www.infotephvg.edu.co/cienaga/hermesoft/portalIG/home_1/recursos/julio_2017/05072017/manual-sst.pdf

Rayme Serrano, R. (2007). *Gestión de seguridad de la información y los servicios críticos de las universidades : un estudio de tres casos en Lima Metropolitana.* Lima: Universidad Nacional Mayor de San Marcos.

Sarabia, A. (1995). *La teoria general de Sistemas.* Madrid: Editorial Isdefe.

Sistema de Gestión Integrado. (2017). Gestion de Logs y registros de auditoría. *Superintendencia de sociedades*, 1-7.

Tamayo, A. (1998). *Sistemas de Información.* Colombia: Universidad Nacional de Colombia.

UCM. (2019). *Ingeniería de Sistemas y de Control.* Madrid: Universidad complutense.

Valbuena, F. (1997). *Fundamentos de teoría general de la información.* Madrid: Universidad Complutense.

Zanabria, J. G., Sánchez Aguilar, A., & Montoya Sánchez, L. (Mayo de 2019). *informe Tecnico Producto Nacional.* Lima: Producción Nacional. Obtenido de informe Tecnico Producto Nacional.