CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

DOI 10.35381/cm.v8i4.877

La gestión de seguridad de la información para una empresa

Information security management for a company

Víctor Iván Capa-Sanmartín
ps.victorics64@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Santo Domingo, Santo Domingo de los Tsáchilas
https://orcid.org/0000-0002-9287-3006

Ariel José Romero-Fernández
ua.arielromero@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-1464-2587

Fredy Pablo Cañizares-Galarza
da.fredypcg62@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0003-4854-6996

Silvio Amable Machuca-Vivar
us.silviomachuca@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Santo Domingo, Santo Domingo de los Tsáchilas
Ecuador
https://orcid.org/0000-0002-4681-3045

Recibido: 01 de mayo 2022
Revisado: 25 de junio 2022
Aprobado: 01 de agosto 2022
Publicado: 15 de agosto 2022

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Víctor Iván Capa-Sanmartín; Ariel José Romero-Fernández; Fredy Pablo Cañizares-Galarza;
Silvio Amable Machuca-Vivar

RESUMEN

El objetivo de la presente investigación es analizar la gestión de seguridad de la Información para la empresa GD-PLAST, tomando como referencia la norma ISO 27001, con lo cual se recomendará a la empresa el implementar las políticas planteadas en el documento a ser entregado finalizada la investigación. Se trabajó con una investigación descriptiva observacional. Para la empresa GD-PLAST la información es un activo fundamental, el cual debe ser protegido adecuadamente, debido a que la información está cada vez más expuesta a factores externos que afectan la integridad y la forma de manejo de los datos, por lo cual para obtener seguridad de la información se debe implementa el conjunto de políticas y controles sugeridos, ya que corresponde al proceso investigativo realizado y se desarrolla de forma adecuado para la empresa.

Descriptores: Protección de datos; derecho de la informática; derecho del ciberespacio. (Tesauro UNESCO).

ABSTRACT

The objective of this research is to analyze the information security management for the company GD-PLAST, taking as a reference the ISO 27001 standard, with which it will be recommended to the company to implement the policies set out in the document to be delivered at the end of the research. We worked with a descriptive observational research. For the company GD-PLAST information is a fundamental asset, which must be adequately protected, because the information is increasingly exposed to external factors that affect the integrity and the way of handling data, so to obtain information security, the set of policies and controls suggested should be implemented, as it corresponds to the research process carried out and is developed in an appropriate way for the company.

Descriptors: Data protection; computer law; cyberspace law. (UNESCO Thesaurus).

INTRODUCCIÓN

El mundo moderno exige el manejo de la información como un activo para muchas empresas y organizaciones, y como tal, la información debe ser custodiada y protegida, por el gran valor que representa dentro del mercado globalizado. Las empresas cuentan con sistemas de Tecnología de Información y Comunicación (TIC) que manejan la información de las instituciones y por ende este protegen con gran cuidado estos sistemas (Patiño, et al. 2017).

En Ecuador las redes de computadoras son atacadas y vulneradas, cada año se incrementa la velocidad de propagación, la facilidad de ejecución y el daño que producen estos ataques, por lo tanto, es muy importante para tener una red segura considerar lo que se debe proteger y de quién; luego definir las políticas de seguridad adecuadas en la cual se define las estrategias que permitan la protección, confiabilidad e integridad de la información (Tirado, et al. 2017).

Los sistemas de información, sus datos, estructura pueden ser sujetos a amenazas externas o internas que pueden afectar a la operatividad de los sistemas, para esto se deben identificar los riesgos (Solarte, et al., 2015). La seguridad de la información hace parte de las actividades específicas que se necesitan en las organizaciones para poder garantizar la continuidad del negocio, la privacidad y el uso indebido de los activos de información, los riesgos y las amenazas son de todo tipo y se materializan siempre que no se tienen los controles necesarios para evitarlos. En algunas organizaciones existen controles físicos y acuerdos legales internos como externos, gestión de riesgos, inventario de activos, seguridad en páginas web. (Chaverra, et al. 2015).

La información en la gestión empresarial moderna no puede ser considerada como un mero apoyo o soporte de las actividades operativas de la empresa, sino que debe tratarse como uno de sus principales recursos o activos. La información es un elemento imprescindible para el funcionamiento de las organizaciones, un recurso básico e importante que requiere por lo tanto que se le apliquen las tradicionales técnicas de

gestión de recursos. (Heredero, et al. 2019).

La seguridad de información en una empresa es un tema de vital importancia, ya que se utiliza para proteger la información manteniendo la confidencialidad, disponibilidad e integridad de los datos, tales como la información en la organización, lo cual garantiza reducir los posibles daños causados por la falta de seguridades y evitar riesgos. Las normas, políticas y procedimientos establecidos para la información buscan una protección el cual está encaminado a preservar este activo de vital importancia para el funcionamiento de cualquier empresa, generando grandes beneficios en el desarrollo de las actividades realizadas con el fin de generar ganancias como la agilidad en los procesos para los interesados que serían los clientes (Álvarez, 2016).

La seguridad se debe considerar en una empresa como una medida importante para lograr resguardar los datos y así tener un sistema de información seguro y confiable. La gestión de seguridad de la información debe considerarse como aquella seguridad que, a más de prever cortafuegos, soporte técnico en PC, deba facilitar la gestión de procesos entendida como el recurso humano, jurídico, la protección física y lógica; considerando sus fases de actuación como son el qué hacer, de qué forma verifica y cómo actúa ante los eventos encontrados, para corregir, prevenir e instaurar planes de mejora. (Macas, et al. 2018).

Según (Carpentier, 2016), menciona que la gestión de la seguridad proporciona a la empresa los conceptos y la terminología especifica de manera que el personal pueda entender los objetivos de seguridad y los riesgos potenciales, y de seguir los procedimientos vinculados a los requerimientos exigidos. Según (Aguilera, 2011), menciona que la seguridad informática es considerada como la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable para las empresas. El análisis de riesgos debe realizarse en la empresa de forma continua, ya que es necesario revisar de una manera periódica, por lo que es de vital importancia tener seguridades y permita evitar riesgos de

la empresa.

Mediante el continuo avance de las empresas y que cada vez necesitan resguardar los datos de la organización, se trata de preservar la información para mejorar los procesos, reducir los riesgos y amenazas que se presentan en la organización. Castro, (2014), menciona que los factores como la globalización de las empresas y la competitividad obligan a realizar el cambio en cuanto al manejo de las estructuras de esta era dinámica, la nueva economía se fundamenta sobre áreas del conocimiento, digitalización y la innovación, todo esto encaminado a los clientes ya que ellos son la parte esencial del negocio.

Si una organización desea ser competitiva y permanecer en el tiempo, deberá identificar, crear, almacenar, transmitir y utilizar de forma eficiente la información y el conocimiento individual y colectivo de sus trabajadores, con el fin de resolver problemas, mejorar procesos o servicios y, sobre todo, para aprovechar nuevas oportunidades de negocio (Castillo & Pérez, 2017).

Una empresa debe resguardar de forma segura la información que maneja en la organización, por lo que es de vital importancia llevar los datos de una manera correcta y sin necesidad de que sea propagada, para esto se debe tener el respaldo del personal aplicando políticas y normas de seguridad. Para adoptar e implementar una política de seguridad de la información en una empresa, es necesario partir de una evaluación obtenida de la aplicación de instrumentos como encuesta y entrevistas que nos proporcione información en relación con las diferentes dependencias que participan para garantizar el aseguramiento de la información. (Ramos, et al. 2017).

Los datos son los elementos primordiales del área informática, es por ello que las tecnologías de la información y los procesos innovadores de las empresas consideran esencial la administración y control de estos datos, valiéndose de sistemas de bases de datos que en su conjunto cumplen un fin predeterminado. (Ramírez & Vega, 2015). La gestión de la información en las empresas establece el control sobre uno de los activos

más importantes dentro de la organización, para esto se debe evitar el uso fraudulento de la información minimizando el riesgo que la información sea mal utilizada. (Arévalo, et al., 2015).

La ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Esta norma proporciona una metodología para implementar la gestión de seguridad de la información en una empresa, también permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en cumplimiento con la norma, por lo cual puede ser factible el tomar como referencia para crear políticas de seguridad de la información.

La seguridad de la información en la actualidad es de vital importancia en cualquier ámbito empresarial, al analizar la situación actual de la empresa GD-PLAST se denota que no existe una visión acerca de que tan importante es la seguridad que se debiese manejar en cada uno de los procesos que llevan, permitiendo así en esta investigación poder determinar políticas a desarrollarse y que podrían implementarse para lograr evitar pérdidas económicas y suposición en el mercado de ventas.

La empresa GD-PLAST no cuenta con políticas que le permitan gestionar la seguridad de la información, debido a situaciones que se han presentado sobre la perdida de información y análisis del manejo de los procesos en referencia al área tecnológica, por lo que se establece la necesidad de crear políticas que permitan resguardar la información, lo cual es de gran importancia en una empresa dedicada a las ventas donde se manejan grandes valores diarios y procesos que involucran el manejo de datos importantes para poder lograr alcanzar las metas mensuales planteadas por la empresa.

El objetivo de la presente investigación es analizar la Gestión de Seguridad de la Información para la empresa GD-PLAST, tomando como referencia la norma ISO 27001, con lo cual se recomendará a la empresa el implementar las políticas planteadas en el documento a ser entregado finalizada la investigación.

MÉTODO

Se trabajó con una investigación descriptiva observacional, analizándose los problemas de seguridad informática que existen en la empresa, esta se utiliza para encontrar las soluciones a problemas cotidianos existentes en la organización. Según su alcance se determinó que el tipo de investigación es descriptiva por lo que se analizó de quien, cuando, como y porque existen problemas en cuanto a la seguridad de la información en la organización.

ANÁLISIS DE LOS RESULTADOS.

En la investigación realizada se presenta los resultados obtenidos sobre las seguridades en la empresa GD-PLAST. Se debe tener en cuenta la tecnología que utiliza la empresa para sus procesos diarios y también de todos los dispositivos que se conectan a la red ya que vivimos la era del Internet de las Cosas (IOT), y se debe ver por la seguridad de los equipos informáticos, los dispositivos móviles, los Smart TV existentes, ya que cualquier dispositivo es útil para que se conecte a la red, por tal motivo se debe implementar una red segura y menos vulnerable para los ataques informáticos.

Se analiza la situación en la que maneja la empresa su información y se recalca que es de vital importancia contar con seguridades, por tal motivo los datos pueden verse afectados por ataques informáticos como pueden ser virus, lo cual pueden provocar la pérdida o eliminación de información importante para la organización. Para esto se ven las empresas en la necesidad de invertir en herramientas que mejoren la seguridad de la información, (Dongo, 2016), menciona que los virus son software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Mediante la encuesta realizada al personal de la empresa en cuanto a las seguridades con las que cuentan, se notó que no tienen conocimiento sobre lo que se debe implementar, se analiza y se observa que los equipos informáticos están expuestos a

virus y amenazas ya que los equipos no cuentan con los antivirus actualizados, no cuentan con políticas o restricciones para el ingreso a páginas innecesarias como redes sociales y también mediante el análisis se observa que se realizan descargas de archivos que no tienen nada que ver con el trabajo y esto puede provocar que existe algún ataque informático a la red.

Para resguardar la seguridad de la información se analizó y se tomó en cuenta que exista una persona encargada del área de TIC, ya que debe ser el encargado de proteger la red de las amenazas existentes, para mantener los datos seguros se debe tener en la empresa activado firewall para proteger el hardware y software, esto implica que solo el personal autorizado tenga acceso a la información.

La empresa cuenta con una persona que se encarga de las Tecnologías de la Información, pero también tiene responsabilidades administrativas lo cual se le dificulta realizar un mantenimiento periódico de los equipos y se recomienda que para manejar la seguridad de la información debería existir una persona de planta para el área de TIC de la empresa para que se dé un soporte técnico adecuado a los equipos de la empresa.

Cada empresa debe que tener en cuenta la manera de resguardar su información, para esto se analiza la confidencialidad de los datos ya que es primordial y permite que la información pueda ser revisada por el personal autorizado por la empresa.

Para el ingreso a los equipos informáticos se recomienda establecer un usuario y contraseña para cada empleado y que tenga un acceso limitado a los datos para implementar seguridades en la información, por lo que en la investigación se pudo constatar que no cuentan con contraseñas para el uso de los equipos informáticos, en los equipos se descargan programas que no son importantes para el trabajo diario, lo cual puede provocar que se descarguen virus, la red inalámbrica no posee políticas de seguridad en cuanto a la clave, se debe implementar mediante un formato y debe contener números, letras entre mayúscula y minúsculas y un carácter, tampoco se

realizan copias de seguridad seguidas tal es el motivo que cuando se avería una computadora corren con el riesgo que se pierda información importante para la empresa. Se realiza un análisis al hardware de la empresa para revisar en qué condiciones se encuentra para poder evitar perdida de información y solucionarlas, para esto se debe tomar consideraciones de cuál es el sitio donde están instalados cada uno de los equipos ya que tienen que estar alejados de algún lugar donde pueda existir riesgos o amenazas, como fuego, explosivos, agua, polvo ya que se podría averiar el hardware y se perderá información importante.

La empresa trabaja con conexión a Internet lo cual provoca que varios equipos y dispositivos se conecten a la red, para esto se debe tener en cuenta que las conexiones y los servidores se encuentren en un lugar específico y restringido para el resto del personal, se considera que el encargado de TIC, debe implementar buenas conexiones de equipos y que no estén cables mal ubicados.

Para conectarse a la red de la empresa se debe tener en consideración de la autenticación como primer punto se analiza la clave WIFI que tenga un formato establecido que no sea de fácil acceso, ya que si cualquier persona se logra conectar a la red podría tener acceso a la información que es considerada importante para la organización, lo que podría ocasionarse algún robo o daño de los datos.

La empresa debe realizar una copia de los datos importantes y relevantes, también se debería tener un registro de las novedades o fallas de los equipos informáticos, cuando ocurre algún inconveniente o falla en los servidores, redes o equipos informáticos y realizar respaldos de información.

En lo que es software la empresa trabaja con Fénix Pro, si existe algún inconveniente con el sistema o equipos se debe informar al técnico de TIC, para que se analice cual fue el inconveniente ya que suelen existir falla en los equipos, bloqueos por perdida de contraseñas, para evitar los incidentes existentes ya que suelen existir eventos

inesperados como corto circuito o algún desastre natural y se debe notificar al encargado para que se dé una solución.

Se capacita al personal para informar que todos y cada uno de ellos serán los responsables de proteger la información a la cual tienen acceso para evitar su pérdida, alteración, destrucción o uso indebido. Mediante los resultados en la investigación se constató que la empresa no cuenta con los controles necesarios para proteger la información, esto puede ocasionar que los datos no puedan ser confiables, íntegros y que corran el riesgo de estar disponible a cualquier persona, para esto se analizó cuáles son las vulnerabilidades existentes en la seguridad, con el fin de conocer las amenazas para aplicar políticas de seguridad pertinentes.

De los resultados obtenidos en esta investigación se conoció que los datos que manejan son de vital importancia y son fundamentales, y a la vez cumplen un rol sustancial dentro de la organización, por tal motivo se propone y se considera en implementar políticas de seguridad para poder eliminar, reducir y controlar los riesgos y amenazas que se puede provocar para que no se explote una vulnerabilidad y a desaparecer debido al mal manejo de las seguridades en su información al no implementar políticas de seguridad.

La empresa debe contar con seguridades de su información, para esto no se necesita que la organización sea grande, pequeña, pública o privada para implementarse, todos tienen que resguardar sus datos ya que esto lleva al éxito o fracaso, GD-PLAST está creciendo cada día más pero no cuenta con políticas de seguridad, por tanto, estas políticas ayudan a proteger los datos importantes y guardar sigilo de la información de sus proveedores, lista de precios, clientes que es el pilar fundamental para cualquier empresa.

Para gestionar la seguridad de la información en GD-PLAST, se analiza la necesidad de implementar políticas de seguridad, se investiga las normas y estándares más conocidos como son ITIL, COBIT e ISO 27001, ya que para que la empresa sea beneficiada debe resguardar los datos de los clientes, (Valles & Huamán, 2016), mencionan que ITIL es un

conjunto de librerías que dictan las buenas prácticas en el uso de tecnologías de información. La norma COBIT, se encarga de la guía de mejores prácticas para el manejo de la información (Santacruz, et al., 2017), mencionan como una guía o modelo para realizar auditorías de la gestión y control de los sistemas de información y tecnología.

Para esta investigación no se implementó ITIL y COBIT, solo se tomó en consideración la norma ISO 27001, la cual establece las certificaciones, directrices y técnicas de gestión con el fin de proteger la información mediante la implementación de lineamientos de seguridad para la organización (Chávez, 2016), la define como norma que contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

La empresa GD-PLAST al basarse a los lineamientos de la norma ISO 27001 lograra ser una organización reconocida por sus políticas en cuanto a seguridad de la información, con esto se beneficiara la empresa ya que se incrementará los niveles de confianza en el proceso de manejo de información, se reducirá el riesgo de tener alguna incidencia y se lograra reducir los daños y costos al existir un incidente, por las políticas de seguridad se incrementará el prestigio de la empresa ya que será un indicador de la seriedad con que se maneja la información, los clientes con los que cuentan van a tener la seguridad de sus datos y un excelente servicio, con las seguridades pertinentes se posibilita que la empresa vaya hacia el éxito en el mercado competitivo.

La información con la que cuenta una empresa es algo que se debe resguardar, por lo tanto, se debe aplicar políticas y controles de seguridad, ya que ninguna empresa está a salvo de sufrir algún ataque informático mediante la red o alguna otra técnica de vulnerabilidad de la seguridad de la información, y se debe implementar una serie de medidas que busque mejorar las políticas de seguridad.

Con el presente análisis, se verifico que la empresa está expuesto a ataques por falta de políticas de seguridad de la información, por lo tanto, se analizó realizar una investigación

de la gestión de la seguridad de los datos en la empresa GD-PLAST, para reducir el porcentaje de amenazas informáticas a la empresa.

La organización posee información relevante e importante, sin embargo no existe las debidas precauciones para el manejo de los datos, no hay políticas de seguridad en cuanto al manejo de equipos informáticos, no existe autenticación para el acceso a los equipos y la clave de acceso para las conexiones a la red no mantiene un formato debido, la seguridad que se le debe dar al software de la empresa con herramientas para resguardar la información no está debidamente controlado por alguna persona responsable de planta.

Mediante encuestas al personal y entrevista al gerente, se notó que no existen controles en cuanto al tema de seguridades de información y esto ocasiona problemas en la empresa y facilita para que los delincuentes informáticos tengan acceso a la información importante, por lo cual se ve afectada la información de la organización. La falta de una norma de seguridad en la empresa ocasiona que existan incidentes graves de pérdida de datos. Al aplicar una norma sobre políticas de seguridad se beneficia la empresa como en este caso se tomó como referencia la norma ISO 27001, con el fin de que se implementen reglas para proteger la información mediante lineamientos para mejorar la seguridad de la Información en GD-PLAST.

Al implementar políticas de seguridad rigiéndose en la norma ISO 27001, la empresa reducirá sus riesgos referentes a la seguridad de la información, protegiendo los datos importantes mediante un acceso seguro del personal autorizado para que la información sea confidencial, íntegra y esté disponible, para esto se recomendó tomar emergentes como la implementación de antivirus con licencia, se capacitó al personal de cuán importante es la seguridad de la información en la empresa, se regulo el acceso a los dispositivos que se podrán conectar a la red, se recomendó realizar copias de seguridad con el fin de reducir el riesgo de que los activos de la empresa puedan ser borrados o alterados.

CONCLUSIONES.

Para la empresa GD-PLAST la información es un activo fundamental, el cual debe ser protegido adecuadamente, debido a que la información está cada vez más expuesta a factores externos que afectan la integridad y la forma de manejo de los datos, por lo cual para obtener seguridad de la información se debe implementa el conjunto de políticas y controles sugeridos, ya que corresponde al proceso investigativo realizado y se desarrolla de forma adecuado para la empresa.

Durante el análisis de los datos recolectados se evidenció que todas las áreas que manejan información restringida, el custodio de la información, debe tener el conocimiento necesario de las responsabilidades en el manejo de esta para poder garantizar la debida protección de los datos, en beneficio de responder a los riesgos o amenazas a los que se encuentra expuesta la empresa.

Con la elaboración de políticas de seguridad basadas en la norma ISO 27001, que se ajustan a las necesidades de la empresa, se tendrá un modelo excelente a seguir, con lo cual se manejaría la información mediante normas, con el fin de resguardar la información crítica, la debida aplicación de las políticas dentro de los lineamientos manejados por la empresa, permitirá mantener y mejorar la seguridad de los datos en la organización.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes; por motivar el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Álvarez, J. (2016). Diseño de un Sistema de Gestión de Seguridad de la Información SGSI basado en la norma Iso27001 para el colegio pro colombiano de la ciudad de Bogotá, que incluye: asesoría, planeación [Design of an ISMS Information Security Management System based on the Iso27001 standard for the Pro Colombiano School in the city of Bogota, including: consulting, planning]. Obtenido de https://repository.unad.edu.co/handle/10596/11950

Arévalo, J., Bayona, R., & Bautista, D. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información [Implementation of an information security management system under ISO 27001: Information risk analysis]. *Tecnura, 19*, 123-134.

Carpentier, J. (2016). *La seguridad informática en la PYME situación actual y mejores prácticas* [IT security in SMEs current situation and best practices]. Barcelona: Ediciones ENI.

Castillo, G., & Pérez, E. (2017). Diagnóstico de los sistemas de información en las empresas priorizadas según los requerimientos actuales [Diagnosis of information systems in the prioritized companies according to current requirements]. *Palabra Clave*, 1-11. doi:10.24215/PCe022

Chaverra, J., Restrepo, H., & Pérez, J. (2015). El teletrabajo y la seguridad de la información empresarial [Teleworking and enterprise information security]. *Cintex, 20,* 11. Obtenido de revistas.pascualbravo.edu.co/index.php/cintex/article/view/33/35

Chávez, V. (2016). Desarrollo de un modelo de seguridad de la información en ambientes educativos virtuales [Development of an information security model for virtual educational environments]. *Edu Sup Rev Cient CEPIES, 1*(1).

Dongo, A. (2016). Relación entre los virus informáticos (malware) y ataques en países vulnerables de seguridad en informática utilizando análisis de componentes principales (ACP) [Relationship between computer viruses (malware) and attacks in vulnerable computer security countries using principal component analysis (PCA)]. *Logos, 6*(1), 11.

Heredero, C., López, J., Romo, S., & Medina, S. (2019). Organización y transformación de los sistemas de información en la empresa [Organization and transformation of information systems in the enterprise]. (Cuarta Edición ed.). Madrid: ESIC

Macas, E., Bustamante, W., & Quezada, P. (2018). Gobierno de TI: Elección y Aplicación de Buenas Prácticas en Corporación Nacional de Telecomunicación [IT Governance: Choosing and Applying Best Practices at Corporación Nacional de Telecomunicación]. *Espacios, 39*(03), 19.

Patiño, S., Mosquera, C., Suárez, F., & Nevárez, R. (2017). Evaluación de seguridad informática basada en ICREA e ISO27001 [Computer security assessment based on ICREA and ISO27001]. *Universidad, Ciencia y tecnología, Vol. 21*(85), 129 - 139. Obtenido de http://uct.unexpo.edu.ve/index.php/uct/article/view/805/0

Ramírez, J., & Vega, O. (2015). Sistemas de Información Gerencial e innovación para el desarrollo de las organizaciones [Management information systems and innovation for organizational development]. *TELEMATIQUE, 14*(2), 13.

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca [Adopt an information security policy based on a domain of the NTC ISO/IEC 27002:2013 standard for the Codelcauca Cooperative]. *Revista UPT*, 88-95. Obtenido de https://revistas.utp.ac.pa/index.php/memoutp/article/view/1475

Santacruz, J., Vega, C., Pinos, L., & Cárdenas, O. (2017). Sistema cobit en los procesos de auditorías de los de sistemas informáticos [Cobit system in the IT systems auditing process]. *Ciencia e investigación, 2*(8), 65 - 68.

Solarte, F., Enríquez, E., & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001 [Risk analysis and assessment methodology applied to IT and information security under the ISO/IEC 27001 standard]. *Tecnológica ESPOL – RTE, 28*, 492 - 507.

Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Tirado, N., Ramos, D., Álvarez, E., & Carreño, S. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas [Information Security, a mechanism for safeguarding company information]. Revista *Publicando, 4*(10), 462-473. Obtenido de https://revistapublicando.org/revista/index.php/crv/article/view/367/pdf_3 32

Valles, M., & Huamán, L. (2016). Aplicación de ITIL como herramienta para la gestión de servicios de tecnologías de información de la empresa Palmas del Shanusi – 2015 [Application of ITIL as a tool for the management of information technology services of the company Palmas del Shanusi - 2015]. *Ciencia tecnología y desarrollo, 2*(1), 55 - 65.