Dom. Cien., ISSN: 2477-8818
Vol. 5, núm. 3, julio, 2019, pp. 132-158

DOI: 10.23857/dc.v5i3.929

Ciencias económicas y empresariales

Artículo de investigación

Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001, centro de datos diseñado con el estándar ANSI/TIA 942

Information security management policies, based on the ISO / IEC 27001 standard, data center designed with the ANSI / TIA 942 standard

Políticas de gerenciamento de segurança da informação, baseadas no padrão ISO / IEC 27001, data center projetado com o padrão ANSI / TIA 942

César Wilfrido Astudillo-García [I]
ing.cesar.astudillo@hotrmail.com

Augusto Enrique Cabrera-Duffaut [II]
acabrerad@ucacue.edu.ec

Recibido: 23 de febrero de 2019 ***Aceptado:** 10 de mayo de 2019 * **Publicado:** 05 de julio de 2019

I. Ingeniero en Sistemas, Jefatura de Posgrados. Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Ingeniero en Sistemas, Jefatura de Posgrados, Docente de la Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

Es muy usual que las empresas o instituciones construyan o implementen sus centros de datos fundamentándose en normas de diseño de construcción, con el objetivo de alcanzar algún nivel de certificación basándose en la disponibilidad de los mismos. Sin embargo, al momento de tratar de implementar políticas de seguridad de la información se evidencian los inconvenientes que no fueron tomados en cuenta en la construcción, afectando a la financiación del proceso e incrementando e tiempo de la ejecución del proyecto. Cabe mencionar que la información se ha vuelto un pilar muy importante dentro de los activos de las empresas, la forma eficaz de gestionar estas áreas es fundamental para lograr contrarrestar amenazas, e incrementar controles. Los llamados Centros de Datos, tiene la responsabilidad de vigilar y garantizar los procesos de almacenamiento de la información, por lo que es necesario que se cuente con políticas de seguridad de la información que garanticen la disponibilidad de los servicios que los sistemas consumen.

Este trabajo expone una propuesta de gestión de seguridad de la información, fundamentado en la generación de Políticas en este aspecto, usando como referencia la norma ISO/IEC 27001:2013 para el Centro de Datos diseñado con el estándar ANSI/TIA-942, garantizando la confidencialidad, integridad y disponibilidad de la información.

Palabras clave: Seguridad de la información; confidencialidad; integridad; disponibilidad.

Abstract

It is very common for companies or institutions to build or implement their data centers based on construction design standards, with the aim of achieving some level of certification based on the availability of them. However, when trying to implement information security policies, the disadvantages that were not taken into account in the construction are evident, affecting the financing of the process and increasing the time of the execution of the project. It is worth mentioning that information has become a very important pillar within the assets of companies, the effective way to manage these areas is fundamental to achieve counteracting threats, and increase controls. The so-called Data Centers have the responsibility to monitor and guarantee the storage processes of information, so it is necessary to have information security policies that guarantee the availability of the services that the systems consume.

This work exposes a proposal of management of information security, based on the generation of Policies in this aspect, using as reference the ISO / IEC 27001: 2013 standard for the Data Center designed with the ANSI / TIA-942 standard, guaranteeing the confidentiality, integrity and availability of the information.

Key words: Security of the information; confidentiality; integrity; availability.

Resumo

É muito comum que empresas ou instituições construam ou implementem seus centros de dados com base em padrões de projeto de construção, com o objetivo de alcançar algum nível de certificação com base na disponibilidade dos mesmos. No entanto, ao tentar implementar políticas de segurança da informação, as desvantagens que não foram levadas em conta na construção são evidentes, afetando o financiamento do processo e aumentando o tempo de execução do projeto. Vale ressaltar que a informação tornou-se um pilar muito importante dentro dos ativos das empresas, o modo efetivo de gerenciar essas áreas é fundamental para se contrapor às ameaças e aumentar os controles. Os chamados Data Centers têm a responsabilidade de monitorar e garantir os processos de armazenamento de informações, por isso é necessário ter políticas de segurança da informação que garantam a disponibilidade dos serviços que o sistema consome.

Este trabalho expõe uma proposta de gerenciamento de segurança da informação, baseada na geração de Políticas neste aspecto, utilizando como referência a norma ISO / IEC 27001: 2013 para o Data Center projetado com o padrão ANSI / TIA-942, garantindo a confidencialidade, integridade e disponibilidade das informações.

Palavras-chave: Segurança da informação; confidencialidade; integridade; disponibilidade.

Introducción

En la actualidad las empresas consideran a la información como el activo más importante, es un recurso vital que puede significar el éxito o el fracaso de una organización; resguardar los datos de una institución se ha convertido en una labor muy importante. Los dispositivos o equipos digitales son los medios más usados para almacenar la información, por lo tanto, la tecnología se ha convertido en un aliado muy importante de las organizaciones. La tecnología a su vez, está sujeta

a continuos cambios, la evolución de este campo es muy acelerada, la infraestructura de los lugares donde la tecnología ha sido implementada debe tener la capacidad de adaptabilidad para brindar servicios que los sistemas consumen. Estas circunstancias, han sido los ejes principales a la hora de decidir el sitio donde almacenar la información, pues se toman en cuenta muchos parámetros de seguridad y se evalúan de manera minuciosa el o los Centros de Datos con los que se dispondrá para este propósito.

Se considera de vital importancia el cumplimiento de conceptos de: seguridad, disponibilidad y redundancia dentro de los Centro de Datos. Estos conceptos se fundamentan en políticas y normas para la protección de la información, mismos que contribuyen al desarrollo fundamental de la empresa u organización.

Las instituciones, organizaciones y empresas, poseen un gran volumen de información, y los sitios en donde se almacena esta información deben contar con los diseños apropiados para Centro de Datos con un nivel de disponibilidad aceptable, por tal motivo se usará como referencia la norma internacional establecida por American National Standards Institute con colaboración de Telecommunications Industry Association (ANSI/TIA-942), la cual expresa requisitos de diseño y construcción para un Centro de Datos. Esta norma contempla recomendaciones para infraestructura de obra civil, infraestructura de cableado estructurado, infraestructura del sistema eléctrico y sus servicios auxiliares, entre otros.

Sin embargo, no existe un estándar o norma que complete tanto los requisitos de diseño de un Centro de Datos (norma ANSI / TIA-942) y las políticas de seguridad de la información (norma International Standards Organization /International Electrotechnical Comisión en sus siglas ISO/IEC 27001:2013); lo cual implica un análisis posterior a la construcción del Centro de Datos, afectando directamente a los recursos de la empresa: tiempo, costo y riesgo de la información.

El objetivo de este proyecto se basó en proponer una alternativa de gestión de políticas de seguridad de la información, fundamentada en la norma ISO/IEC 27001:2013 y los requisitos de la norma ANSI / TIA-942; con el fin de establecer políticas y controles, para la gestión de la información dentro de un Centro de Datos.

El alcance del presente trabajo de investigación, está fundamentado en una propuesta de gestión de políticas de seguridad de la información, la misma que está destinada a un Centro de Datos. Esta propuesta está apalancada sobre la norma ISO/IEC 27001:2013 y los requisitos de la norma ANSI / TIA-942; que se convierten en la base para establecer políticas y controles, para la gestión de la información dentro de un Centro de Datos, contribuyendo con la continuidad del negocio de las empresas que consumen servicios de este tipo.

La información es considerada uno de los activos más importantes de las empresas, su gestión está en manos de funcionarios o empleados designados para esta responsabilidad; es así, que las organizaciones tienen la responsabilidad de crear políticas de seguridad de la información, establecidas en normas internacionales. Estas normas han sido reconocidas como los métodos más efectivos para el control de la información, ya que permiten establecer niveles de acceso a los procesos críticos de alto nivel.

En este sentido y apoyados en las leyes y reglamentos del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) del Ecuador, en su Acuerdo Ministerial No.5 de Registro Oficial No. 755 del 16 de Mayo de 2016, (MINTEL (2016) establece que “el marco de referencia a través del cual el Ministerio de Telecomunicaciones y de la Sociedad de la Información, implementará el Sistema de Gestión de Seguridad de la Información (SGSI) Ministerial, fijando así los estándares de seguridad de la información a aplicar para proteger adecuadamente sus activos de información. De conformidad a lo establecido en el Acuerdo Ministerial No. 166, del 19 de septiembre de 2013 y las normas ISO 27000, se consideran los siguientes elementos centrales:

- La disponibilidad, integridad y confidencialidad de la información.
- La implementación, mantención, monitoreo y mejoramiento continuo de la aplicación de la presente política.
- El levantamiento y categorización de los activos de información, y sus responsables.
- La gestión de riesgos que afecten a los activos de información, frente a amenazas internas o externas, deliberadas o accidentales.

- La operación correcta y segura de las instalaciones de procesamiento de información.
- La seguridad física y del entorno donde se encuentran y operan los activos de información.
- La relación con los proveedores y usuarios externos.
- La legislación vigente en lo referente a la definición de la información pública, confidencial y reservada."

Considerando que no existe un estándar o norma que complete tanto los requisitos de diseño de un Centro de Datos y las políticas de seguridad de la información, el presente trabajo de investigación propone políticas de seguridad de la información para un Centro de Datos, aplicados a los requisitos de la norma ANSI/TIA-942.

Desarrollo

En la actualidad no existe una norma o estándar internacional que permita a las organizaciones diseñar o construir sus Centro de Datos, considerando políticas se seguridad de la información, en cada uno de los requisitos de la norma ANSI / TIA-942. Por ejemplo, la norma ANSI / TIA-942 nos proporciona recomendaciones para infraestructura de obra civil, infraestructura de cableado estructurado, infraestructura del sistema eléctrico y sus servicios auxiliares, entre otros, sin embargo, esta norma no contempla políticas de seguridad de la información.

Conociendo la importancia que tiene la implementación de la norma ISO 27001 en las empresas, se ha realizado una investigación sobre los países en donde las empresas se encuentran certificadas. A nivel global los estudios demuestran que hay un crecimiento de un 45%, en una comparación de los años 2015 al 2017, según el artículo (ISOTools Excellence, 2017), en la que se detalla un número de certificaciones ISO por región y país. Sin embargo, estos datos están sujetos a cambios, ya que algunas empresas prefieren no participar en las encuestas propuestas. Esta información puede acercarse a la realidad, empezando en países a nivel mundial como podemos observar en el gráfico 1.

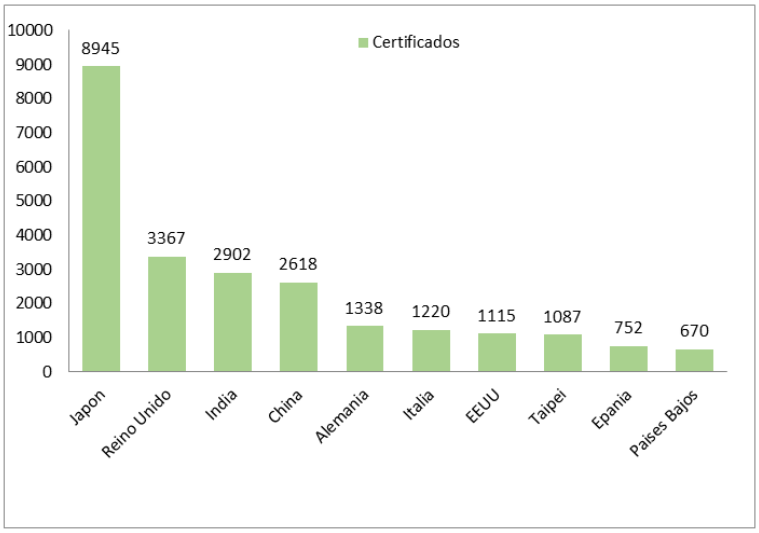

Gráfico 1. Países con certificaciones a nivel mundial.

A nivel de centro y sur américa el número de certificaciones desciende notablemente, como se demuestra en el gráfico 2.

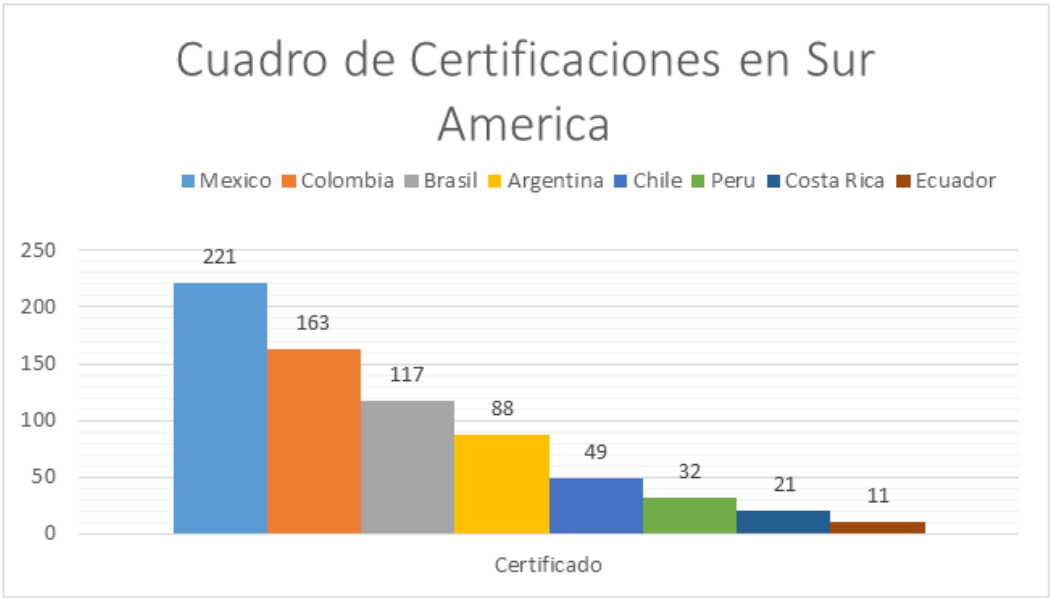

Gráfico 2. Certificadas en ISO 27001 en América latina.

Como se puede notar aún no se cuenta con una cultura que resguarde la información de manera formal en las empresas que residen en latino américa. Actualmente, en Ecuador, se encuentran certificadas 11 empresas con la norma ISO/IEC 27001, de esta cantidad se pudo constatar que empresas como CNT, Telconet, Movistar, Banco de Guayaquil, se encuentran certificadas, mientras que el resto de empresas, como se observa en la gráfico 2, prefieren guardar esta información en secreto por motivo de políticas internas (ISOTools Excellence, 2017).

La norma ANSI/TIA-942 establece requisito para el diseño de Centro de Datos, considerando cuatro aspectos:

- Arquitectura: El diseño de un centro de datos debe basarse en la seguridad, ubicación física, accesos y la necesidad de ajustarse a las especificaciones de la norma del centro de datos.
- Sistema eléctrico: El diseño eléctrico tales como la energía, la energía de reserva y puesta a tierra; cumplirá con las normas establecidas. Considerando PDU dedicados y paneles de energía alimentada por UPS. La cantidad de circuitos eléctricos depende de los requisitos de los equipos que se ubicarán en las salas. Las habitaciones deberán contar con sistemas de respaldo (UPS eléctricos y generadores) que son utilizados para la sala de ordenadores, el grado de redundancia para sistemas mecánicos y eléctricos será la misma en todo el centro de datos.
- Sistema mecánico: El sistema de climatización de una instalación incluye unidades individuales o múltiples de aire acondicionado, con la capacidad de refrigeración combinado para mantener la temperatura y la humedad relativa en condiciones óptimas. Si estas unidades de aire acondicionado son atendidas por un sistema de agua o de condensador de agua fría, los componentes de estos sistemas están igualmente dimensionadas para mantener las condiciones de diseño.
- Telecomunicaciones: Por su naturaleza, los centros de datos consumen grandes cantidades de energía, la mayoría de los cuales se convierte en calor, lo que requiere una seria consideración la eficiencia de enfriamiento. No existe una arquitectura única de gestión térmica eficiente para todas las instalaciones. Los factores físicos, la aplicación

y el medio ambiente deben ser cuidadosamente evaluados en el análisis de puesta en marcha, junto con el análisis operativo.

La norma ISO/IEC-27001:2013 establece políticas de seguridad de la información para el diseño de Centro de Datos.

Metodología

El presente trabajo de investigación se desarrolló a través de los métodos analítico y científico, los mismos que permitieron alcanzar los objetivos planteados en el mismo:

- Método analítico: este método analiza cada uno de los requisitos establecidos en la norma ANSI / TIA-942, en los cuales se propone políticas de seguridad de la información fundamentadas en la norma ISO/IEC 27001:2013.

- Método científico: a través de la observación del autor se plantea un problema científico, el mismo que se pretende mitigar a través de una hipótesis, consiguiendo como resultado una propuesta fundamentada en normas internacionales.

- Instrumentos de investigación: las encuestas son consideradas los procedimientos que se pueden diseñar para realizar una investigación descriptiva, en la cual la persona que investiga o el llamado investigador, recopila información mediante un cuestionario que ha sido elaborado previamente. Se recopila los datos mediante un tríptico, gráfico o tablas donde el entrevistado es el encargado de entregar la información.

En el caso de una posible implementación de este método, se deberán tomar en cuenta algunas etapas para el desarrollo de la misma, la gestión que abarca estas etapas van de la mano con los procesos de maduración de la empresa.

La primera etapa en el desarrollo de este proceso, es saber el estado situacional de la empresa o el proyecto en el que se va a implementar. Para este proceso se utilizan herramientas que la misma norma ISO/IEC 27001:2013 las describe como controles. Estos controles se especifican en la ISO/IEC 27002, las cuales especifican el estado actual de la empresa o el proyecto a ejecutarse.

La segunda etapa se focaliza en planificar y analizar las alternativas para el proceso de integración de la norma ISO/IEC 27001:2013, tomando en cuenta que se puede optar por una autogestión o la contratación de un consultor externo o también una opción mixta. Las ventajas y desventajas de cualquiera de estas opciones radican en el nivel de experticia que tengan las personas que manejan el proyecto. Al utilizar matrices como herramientas, en las que definen parámetros como gastos generales, inversión de tiempo, integridad de la documentación, trasferencia de conocimiento; el alcance del proyecto estará mucho mejor definido.

La tercera etapa se fundamenta en la documentación, la organización y la puesta en marcha del proyecto como tal. Se debe mencionar que en este punto la presentación del proyecto está en mesa de los patrocinadores, lo cuales tomaran la decisión definitiva del avance del miso. Lo que implica que el apoyo económico también está inmerso en esta etapa de la panificación. De esta manera las políticas y controles llegaran a formar parte de las labores cotidianas de la organización.

Resultados

Las políticas expresadas en el presente trabajo de investigación, son una propuesta para un Centro de Datos, fundamentadas en la norma establecida ISO/IEC 27001:2013; la misma que se aplica en cada uno de los requisitos establecidos en la norma internacional ANSI / TIA-942. La elaboración de las políticas de seguridad de la información, se realizó considerando las mismas áreas establecidas por la norma ANSI / TIA-942: área de telecomunicaciones, área de arquitectura, área de sistemas eléctricos, y área de sistemas mecánicos.

Políticas de seguridad de la información para el área de Telecomunicaciones

En este ítem se identificaron políticas de seguridad de la información para la infraestructura de telecomunicaciones en un centro de datos: equipos, cableado, salas, áreas, proveedor y accesos.

Se deberá etiquetar los paneles, el sistema de cableado, armarios y bastidores en concordancia al esquema de clasificación de la organización; los mismos que deberán contar con mecanismos de seguridad contra daños, interferencias e interceptaciones garantizando la continuidad del servicio ya la protección de la información.

Los proveedores deberán sujetarse las políticas de seguridad de la información establecidas por la organización, establecidos en los acuerdos de nivel de servicio.

Los accesos a las diferentes áreas, salas y equipos del centro de datos; deberán contar con mecanismos de seguridad, protecciones contra fallos, alteraciones en el suministro eléctrico y seguridad contra daños físicos y ambientales, garantizando la continuidad del servicio ya la protección de la información.

Además, se realizó la propuesta de los controles para la gestión de seguridad para el área de Telecomunicaciones.

Políticas de seguridad de la información para el área de Arquitectura

Aquí, se propuso políticas de seguridad de la información para el área de arquitectura en un centro de datos:

La ubicación y construcción del centro de datos deberá estar exenta de riesgos naturales (inundaciones, incendios, sismos), vía navegables, carreteras, líneas de ferrocarril, aeropuertos, muelles; con el fin de precautelar accidentes y ataques maliciosos y aplicar políticas de acceso al personal autorizado.

Las áreas de estacionamiento, muelles de carga, visitantes deberán ser claramente identificadas y separadas del edificio principal del centro de datos; para precautelar accidentes y ataques maliciosos, e impartir políticas de acceso solo a personal autorizado.

El centro de datos deberá contar con resistencia al fuego, protección contra amanezcas externas y ambientales en su diseño arquitectónico: muros, marco estructural, paredes, tabiques, corredores, recintos, suelos, puertas, ventanas, techos, tumbados, área de generadores y almacenamiento de combustible; para precautelar accidentes, ataques maliciosos y garantizar áreas seguras para laborar.

El centro de datos deberá contar con sistema de monitoreo y control dogmatizado en todas sus áreas, para precautelar accidentes, ataques maliciosos y garantizar áreas seguras para laborar.

Además, se propusieron los controles de gestión de seguridad para el área de Arquitectura.

Políticas de seguridad de la información para el área del Sistema Eléctrico

En este apartado, se propusieron políticas de seguridad de la información para el sistema eléctrico de un centro de datos:

- El sistema eléctrico del centro de datos deberá tener redundancia, permitir el mantenimiento concurrente, evitar puntos de fallo, analizar la potencia del sistema, garantizar la alimentación continua y adecuada de los equipos; además del adecuado funcionamiento en caso de algún desastre natural.
- El centro de datos deberá contar con un sistema de monitoreo de la vida útil de baterías y UPS, así como su tiempo de respaldo; para garantizar la alimentación continua y adecuada de los equipos y su adecuado funcionamiento en caso de algún desastre natural.
- El sistema eléctrico del centro de datos y todos sus elementos deberán estar protegidos de sobrecargas de energía, protección contra rayos, fallos a tierra; para garantizar la alimentación continua y adecuada de los equipos y su adecuado funcionamiento.

Los controles de gestión de seguridad, se proponen para el área del Sistema Eléctrico.

Políticas de seguridad de la información para el área del Sistema Mecánico

En esta sección se proponen políticas de seguridad de la información para el sistema mecánico de un centro de datos:

- El sistema de tuberías deberá tener la capacidad de rechazar el calor y controlar los niveles de humedad, su enrutamiento no debe estar asociado con los equipos; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo.
- El sistema de climatización deberá ser redundante, tener presión positiva, contar con sistemas mecánicos de reserva, unidades aire acondicionado, sistemas de control; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo.
- El sistema mecánico del centro de datos deberá contar con sistemas de detección de fuego, rociadores contra incendios, supresión gaseosa, detecciones de humo de alerta temprana y

detección de fugas de gas; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo.

Se determinan y proponen controles de gestión de seguridad para el área del Sistema Mecánico.

Valoración de la propuesta de las políticas de seguridad de la información.

Las políticas de seguridad de la información propuesta como resultado del presente trabajo de investigación, fueron valoradas por expertos profesionales que laboran actualmente en el área de Tecnologías de la Información y en la Administración de Centros de Datos con altos estándares de disponibilidad.

Para la valoración de las políticas, se aplicó una encuesta que contó de respuestas en una escala de valoración.

Resultado general de la encuesta

El resultado obtenido a nivel general, posterior a la aplicación de las encuestas; reflejaron un 88% de total acuerdo a las políticas propuestas y un 12% de acuerdo, tal como se evidencia en la tabla 1 y gráfico 3.

Tabla 1. Resultados generales de la encuesta

Totalmente en desacuerdo	En desacuerdo	Neutral	De acuerdo	Totalmente de acuerdo
0%	0%	0%	12%	88%

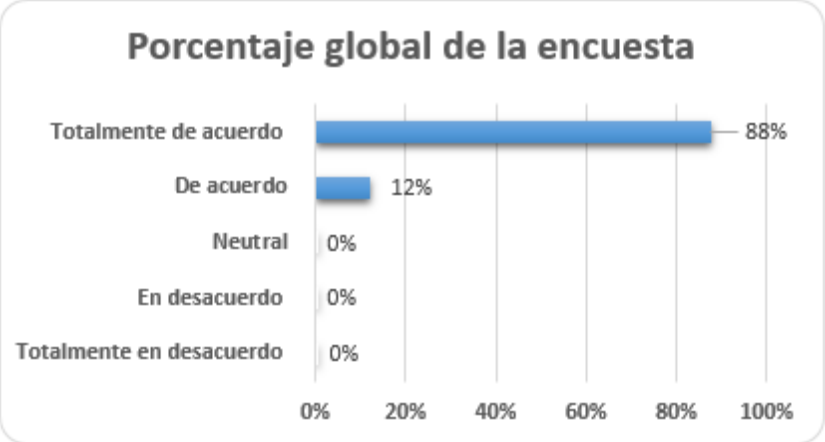

Gráfico 3. Porcentaje general de la encuesta

Resultado parcial de la encuesta

El resultado obtenido a nivel parcial, posterior a la aplicación de las encuestas, reflejan un acuerdo a las políticas propuestas, tal como se evidencia en el gráfico 4; los encuestados afirman estar de acuerdo con las políticas de seguridad de la información propuestas para un centro de datos.

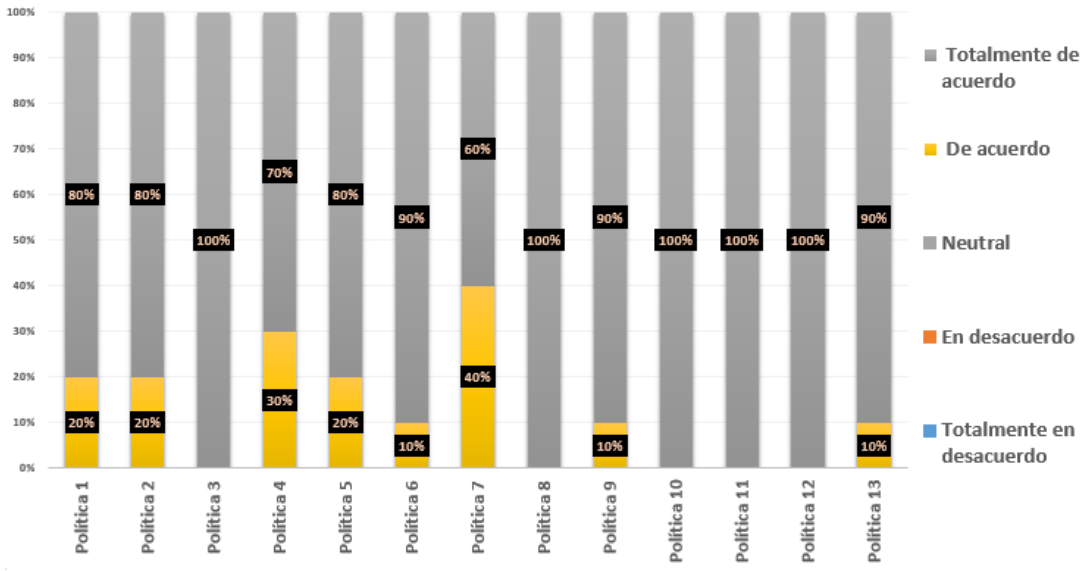

Gráfico 4.Valoración parcial de políticas propuestas. Autoría propia

Política propuesta #1

En esta política se propone que se deberá etiquetar los paneles, el sistema de cableado, armarios y bastidores en concordancia al esquema de clasificación de la organización; los mismos que deberán contar con mecanismos de seguridad contra daños, interferencias e interceptaciones garantizando la continuidad del servicio y la protección de la información. A lo cual, los encuestados respondieron en un porcentaje del 80% estar totalmente de acuerdo, como se observa en el gráfico 5.

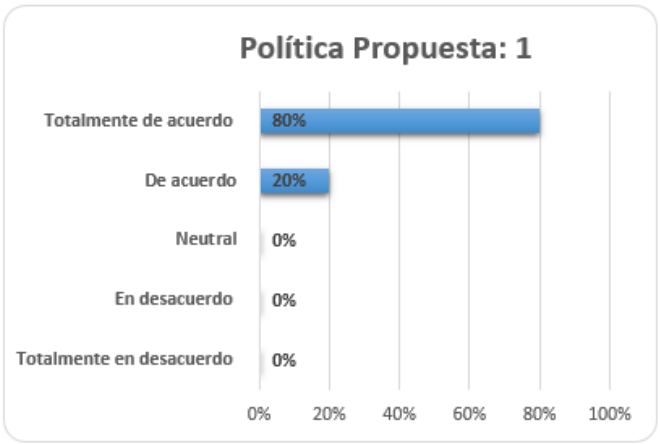

Gráfico 5. Resultado de la encuesta, política propuesta 1

Política propuesta #2

En esta política se propone que los proveedores deberán sujetarse a las políticas de seguridad de la información establecidas por la organización, de acuerdo al nivel de servicio. A lo cual, los encuestados respondieron en un porcentaje del 80% estar totalmente de acuerdo, como se observa en gráfico 6.

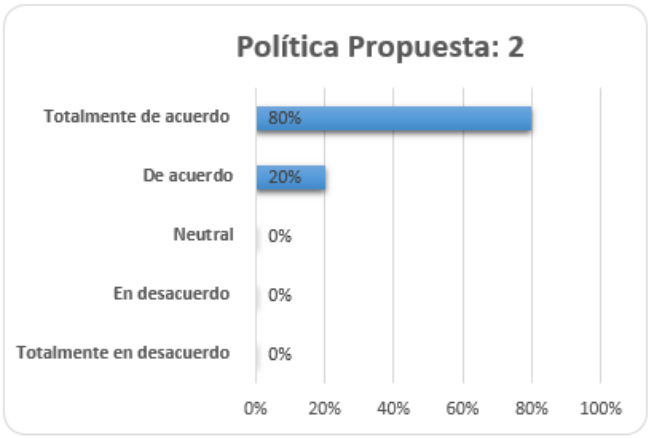

Gráfico 6. Resultado de la encuesta, política propuesta 2

Política propuesta #3

En esta política se propone que los accesos a las diferentes áreas, salas y equipos del centro de datos; deberán contar con mecanismos de seguridad, protecciones contra fallos, alteraciones en el suministro eléctrico y seguridad contra daños físicos y ambientales, garantizando la continuidad del servicio y la protección de la información. A lo cual, los encuestados respondieron en un porcentaje del 100% estar totalmente de acuerdo, como se observa en gráfico 7.

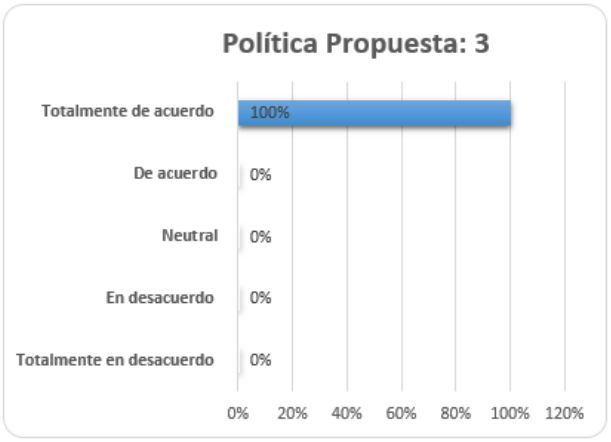

Gráfico 7. Resultado de la encuesta, política propuesta 3

Política propuesta #4

En esta política se propone que la ubicación y construcción del centro de datos deberá estar exenta de riesgos naturales (inundaciones, incendios, sismos), vía navegables, carreteras, líneas de ferrocarril, aeropuertos, muelles, etc.; con el fin de precautelar accidentes y ataques maliciosos y aplicar políticas de acceso para el personal autorizado. A lo cual, los encuestados respondieron en un porcentaje del 70% estar totalmente de acuerdo, como se observa en gráfico 8.

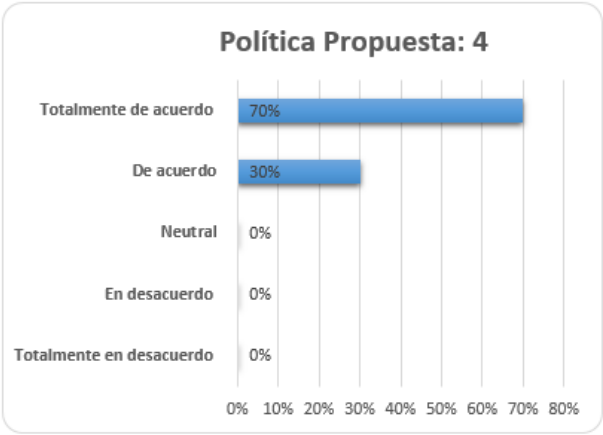

Gráfico 8. Resultado de la encuesta, política propuesta 4

Política propuesta #5

En esta política se propone que las áreas de estacionamiento, muelles de carga y visitantes; deberán ser claramente identificadas y separadas del edificio principal del centro de datos, para precautelar accidentes y ataques maliciosos, e impartir políticas de acceso solo a personal autorizado. A lo cual, los encuestados respondieron en un porcentaje del 80% estar totalmente de acuerdo, como se observa en gráfico 9.

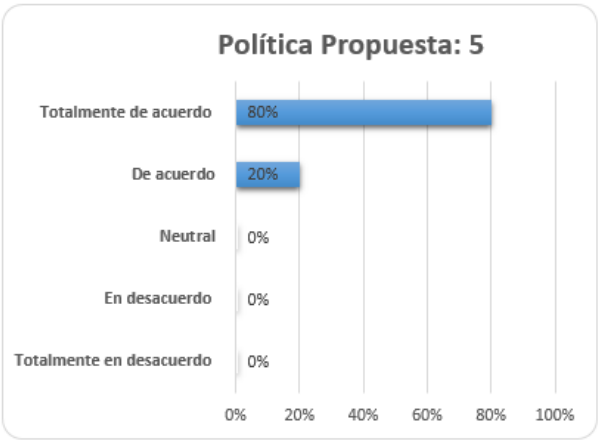

Gráfico 9. Resultado de la encuesta, política propuesta 5

Política propuesta #6

En esta política se propone que el centro de datos deberá contar con resistencia al fuego, protección contra amenazas externas y ambientales en su diseño arquitectónico (muros, marcos estructurales, paredes, tabiques, corredores, recintos, suelos, puertas, ventanas, techos, tumbados), área de generadores y almacenamiento de combustible; para precautelar accidentes, ataques maliciosos y garantizar áreas seguras para laborar. A lo cual, los encuestados respondieron en un porcentaje del 90% estar totalmente de acuerdo, como se observa en gráfico 10.

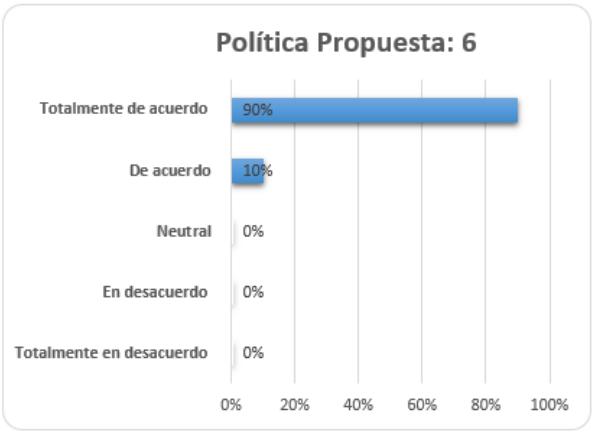

Gráfico 10. Resultado de la encuesta, política propuesta 6

Política propuesta #7

En esta política se propone que: El centro de datos deberá contar con sistema de monitoreo y control de domótica en todas sus áreas para precautelar accidentes, ataques maliciosos y garantizar áreas seguras para laborar. A lo cual, los encuestados respondieron en un porcentaje del 60% estar totalmente de acuerdo, como se observa en gráfico 11.

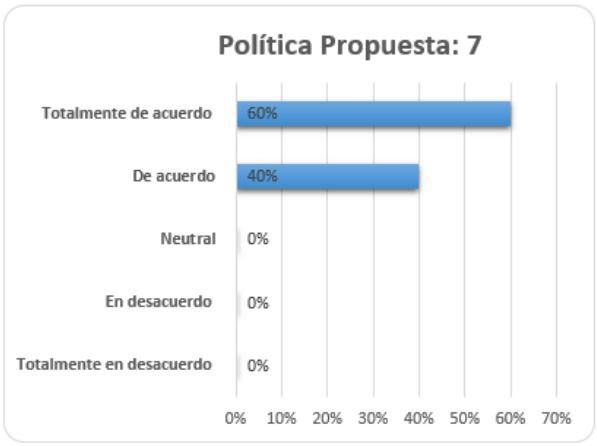

Gráfico 11. Resultado de la encuesta, política propuesta 7

Política propuesta #8

En esta política se propone que el sistema eléctrico del centro de datos deberá tener redundancia, permitir el mantenimiento concurrente, evitar puntos de fallo, analizar la potencia del sistema, garantizar la alimentación continua y adecuada de los equipos; además, del adecuado funcionamiento en caso de algún desastre natural. A lo cual, los encuestados respondieron en un porcentaje del 100% estar totalmente de acuerdo, como se observa en gráfico 12.

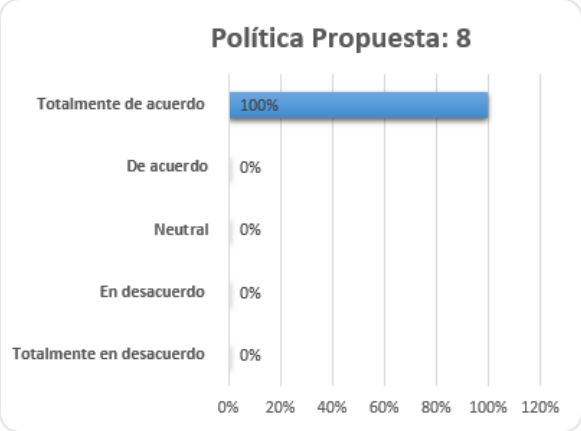

Gráfico 12. Resultado de la encuesta, política propuesta 8

Política propuesta #9

En esta política se propone que el centro de datos deberá contar con un sistema de monitoreo de la vida útil de baterías y UPS, así como su tiempo de respaldo; para garantizar la alimentación continua y adecuada de los equipos y su adecuado funcionamiento en caso de algún desastre natural. A lo cual, los encuestados respondieron en un porcentaje del 90% estar totalmente de acuerdo, como se observa en gráfico 13.

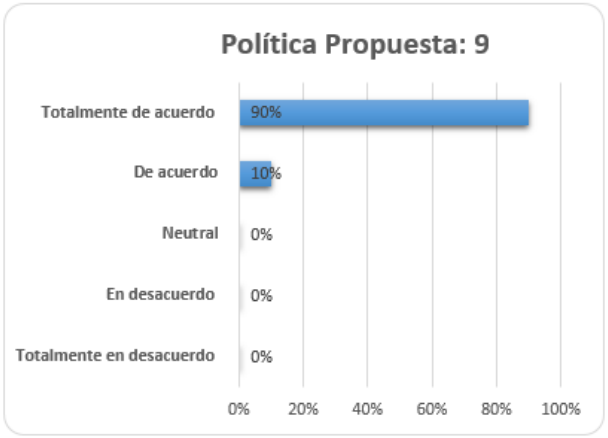

Gráfico 13. Resultado de la encuesta, política propuesta 9

Política propuesta #10

En esta política se propone que el sistema eléctrico del centro de datos y todos sus elementos deberán estar protegidos de sobrecargas de energía, protección contra rayos, fallos a tierra; para garantizar la alimentación continua y adecuada de los equipos y su adecuado funcionamiento. A lo cual, los encuestados respondieron en un porcentaje del 100% estar totalmente de acuerdo, como se observa en gráfico 14.

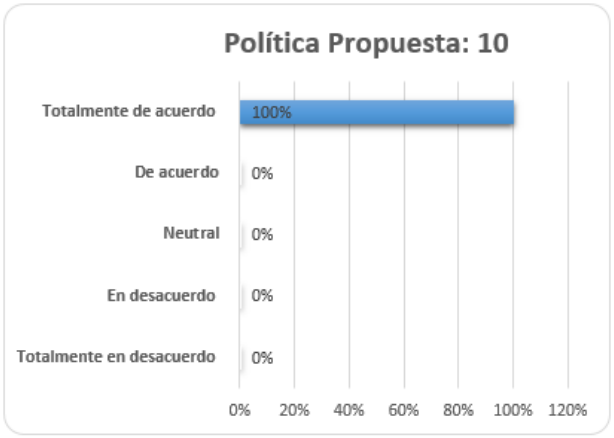

Gráfico 14. Resultado de la encuesta, política propuesta 10

Política propuesta #11

En esta política se propone que el sistema de tuberías deberá tener la capacidad de rechazar el calor y controlar los niveles de humedad, su enrutamiento no debe estar asociado con los equipos; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo. A lo cual, los encuestados respondieron en un porcentaje del 100% estar totalmente de acuerdo, como se observa en gráfico 15.

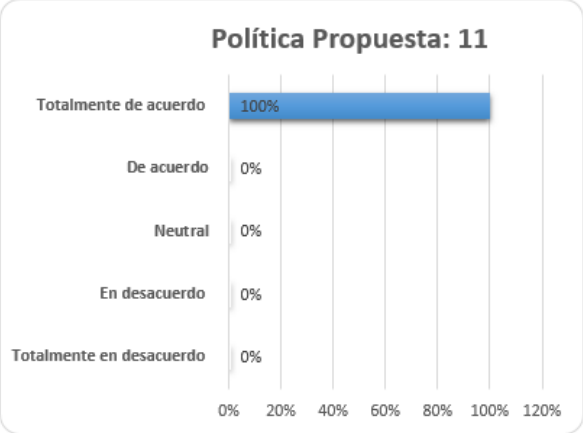

Gráfico 15. Resultado de la encuesta, política propuesta 11

Política propuesta #12

En esta política se propone que el sistema de climatización deberá ser redundante, tener presión positiva, contar con sistemas mecánicos de reserva, unidades de aire acondicionado, sistemas de control; para brindar seguridad y evitar incidentes que pueden ocasionarse por fallas en el mismo. A lo cual, los encuestados respondieron en un porcentaje del 100% estar totalmente de acuerdo, como se observa en gráfico 16.

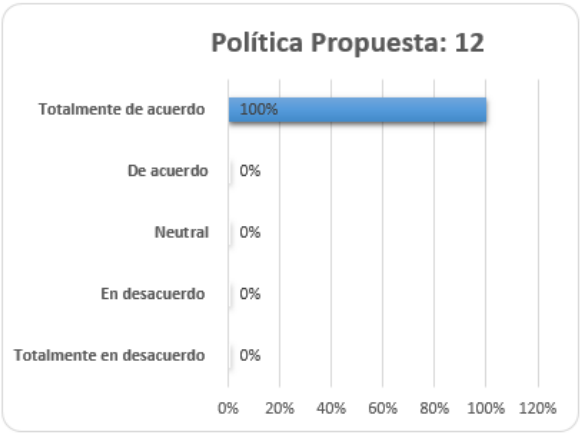

Gráfico 16. Resultado de la encuesta, política propuesta 12

Política propuesta #13

En esta política se propone que el sistema mecánico del centro de datos deberá contar con sistemas de detección de fuego, rociadores contra incendios, supresión gaseosa, detecciones de humo de alerta temprana y detección de fugas de gas; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo. A lo cual, los encuestados respondieron en un porcentaje del 90% estar totalmente de acuerdo, como se observa en gráfico 17.

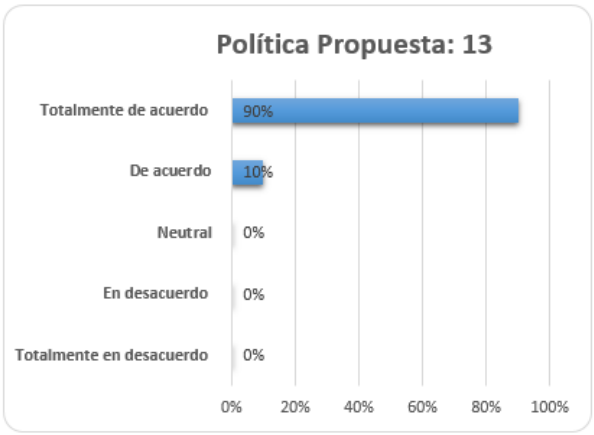

Gráfico 17. Resultado de la encuesta, política propuesta 13

Conclusiones

En la actualidad, la información en las empresas u organizaciones es el activo intangible más valioso pues sin ella la organización no podría ejecutar sus procesos de negocio. Es tan importante, pues el análisis de la misma permite mejorar los procesos de negocio de acuerdo a los objetivos estratégicos establecidos por la empresa u organización. La información al ser un activo valioso, debe estar sujeta a ciertos parámetros que garanticen la seguridad de la misma; evitando así los riesgos de divulgación no autorizada, acceso no autorizado, entre otros.

La ISO 27001:2013 es una norma internacional que proporciona políticas para garantizar la seguridad de la información, esta norma se puede aplicar a cualquier empresa u organización que

tenga como prioridad proteger su información. En Ecuador, la cultura de proteger la información no se encuentra muy fortalecida, pues el número de empresas ecuatorianas que tienen una certificación ISO 27001:2013, es el más bajo en comparación con los demás países latinoamericanos.

Los centros de datos al ser los lugares donde muchas empresas alojan su información, es fundamental que estos dispongan de políticas que garanticen la seguridad de la información, tanto la información de la organización como la de sus clientes. Sin embargo, como se indicó anteriormente, no existe una estar o normativa que implique parámetros de seguridad de información previo a su diseño y/o construcción.

Las políticas de seguridad elaboradas y propuestas, tienen como objetivo que al momento de analizar o diseñar un centro de datos, se garantice la seguridad de la información; esto permitirá a la empresa optimizar costos y recursos, pues de lo contrario se tendría que diseñar/construir el centro de datos y posteriormente aplicar políticas que garanticen la seguridad de la información.

Las políticas de seguridad de la información propuestas, están enfocadas en las cuatro áreas que contempla la norma ANSI/TIA-942 y cotejadas con controles establecidos en la ISO 27001:2013; teniendo así, un marco referencial de 13 políticas de seguridad desarrolladas para un centro de datos, garantizando la confidencialidad, integridad y disponibilidad de la información.

Referencias Bibliográficas

Aceco TI. (s.f.). CONOZCA LOS TIPOS DE DATA CENTER Y SUS APLICACIONES. Recuperado de http://www.acecoti.com/es/blog/conozca-los-tipos-de-data-centers-y-sus-aplicaciones

Devoto, C. y Raquel, L. (2011). Diseño de la infraestructura de telecomunicaciones para una data center. Pontificia Universidad Católica del Perú, Lima.

Díaz, B. y Roberto, C. (2017). Decisiones gerenciales para la optimización energética de una data center. Universidad Militar Nueva Granada, Bogotá.

Fernández, C. y Piattini, M. (2013). Modelo para el gobierno de las TIC basado en las normas ISO. Madrid, España: AENOR Ediciones (Asociación Española de Normalización)

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. Recuperado de https://www.iso.org/standard/54534.html

ISOTools Excelente. (2017). ¿Cuál es la situación de la norma ISO 27001 en Sudamérica? Recuperado de https://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/

ISOTools Excelente. (2018). Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. Recuperado de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Kordel, Luc. (2004). IT governance hands-on: Using CobiT to implement IT governance. Information Systems Control Journal. 2. 39-46. Recuperado de http://www.qualified-audit-partners.be/user_files/ITforBoards/GVIT_ISACA-Kordel_Luc_IT_Governance_Hands-on_-_Using_Cobit_To_Implement_IT_Governance_2004.pdf

Ladino M., Villa P. y López A. (2011). FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. Scientia Et Technica, XVII (47), 334-339.

MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACION (2016). Acuerdo Ministerial 5 del 16 de mayo de 2016 mediante el cual se emite la POLITICA DE SEGURIDAD DE INFORMACION EN EL MIN. DE TELECOMUNICACIONES. Ecuador: MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACION

Pacio, G. (2014). DATA CENTERS HOY: PROTECCION Y ADMINISTRACION DE DATOS EN LA EMPRESA. España: S.A. MARCOMBO.

Pizarro, G., Urvina, R., Plaza, A., Bojorque, R. y Pauta, L. (2017). Sistemas de información en ciencias de la computación. Quito, Ecuador: Editorial Universitaria Abya-Yala.

Quinteros, J. y Ponce, D. (2017). Elaboración de las políticas de seguridad de la información para el Consejo Nacional Electoral del Ecuador. UNIVERSIDAD DE CUENCA, Cuenca.

TIA-942. (s.f.). Welcome to TIA-942.org. Recuperado de http://www.tia-942.org/.

International Organization for Standardization. (1997). Friendship Among Equals. Geneve, Switzerland: ISO. Recuperado el 1 de abril de 2016, de International Organization for Standardization: http://www.iso.org/iso/2012_friendship_among_equals.pdf

International Organization for Standardization. (2013). ISO 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.

International Organization for Standardization. (2016). The Benefits of International Standards - ISO. Recuperado el 07 de 04 de 2016, de http://www.iso.org/iso/home/standards/benefitsofstandards.htm

International Organization for Standardization. (04 de julio de 2016). www.iso.org. Obtenido de http://www.iso.org/iso/catalogue_detail?csnumber=65034

Norma Técnica Peruana NTP-ISO/IEC 27001. (20 de noviembre de 2014 2ª Edición). Obtenido de:https://canvas.utp.edu.pe/courses/8870/files/42244/download?download_frd=1.

ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls (Tecnología de la información – Técnicas de seguridad – Código de práctica para controles de seguridad de la información)

ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance (Tecnología de la información – Técnicas de seguridad – Guía de implementación del sistema de gestión de seguridad de la información)

ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement (Tecnología de la información – Técnicas de seguridad – Gestión de seguridad de la información – Medición)

ISO/IEC 27005, Information technology — Security techniques — Information security risk management (Tecnología de la información – Técnicas de seguridad Gestión de riesgos de seguridad de la información)

ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012 (Directivas, Parte 1, Suplemento Consolidado de ISO – Procedimientos específicos a ISO, 2012)