EVALUACIÓN DE LAS INCIDENCIAS Y RIESGOS PRESENTES EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ-ECUADOR

Yanina Alexandra Viteri Alcívar[1], María Teresa Cano Montesdeoca[2], Aura Dolores Zambrano Rendón[3], Cristhian Gustavo Minaya Vera[4]
yanina.viteri@uleam.edu.ec[1], mariateresita_83@hotmail.com[2], azambrano@spam.edu.ec[3], cristhian.minaya@uleam.edu.ec[4]
https://orcid.org/0000-0003-0143-6810[4]
Universidad Laica Eloy Alfaro de Manabí[1],[4], Escuela Superior Politécnica Agropecuaria De Manabí Manuel Félix López[3]

Recibido (15/07/19), Aceptado (12/08/19)

Resumen: Se analizaron las vulnerabilidades de la infraestructura tecnológica de la Universidad Laica Eloy Alfaro de Manabí. Para ello se utilizó la metodología por niveles. Inicialmente se determinó la situación actual de la Unidad Central de Coordinación Informática y se identificaron las principales incidencias en el sitio, las cuales fueron valoradas considerando el nivel de sensibilidad de los mismos. Con la metodología Análisis Modal de Fallos y Efectos se alcanzaron los niveles de probabilidad e impacto de los riesgos también se utilizó la metodología MAGERIT para identificar los activos de la unidad y las amenazas a las que pueden estar expuestos. Finalmente se elaboró el Modelo de Gestión de Continuidad, fundamentado en las siguientes fases: Alcance del Plan de Continuidad de Negocio, Evaluación de Riesgos, Análisis de Impactos de Negocios, Estrategias de Recuperación y Desarrollo del Plan. Finalmente se concluye que la unidad de informática está expuesta al 59% de riesgos críticos causados por amenazas de acuerdo al análisis realizado con un nivel alto de criticidad, por lo que el modelo propuesto permitirá responder significativamente ante posibles incidentes con la finalidad de dar continuidad a las operaciones en beneficios de la comunidad universitaria.

Palabras Claves: Modelo de gestión, análisis modal de fallos, unidad informática, evaluación de indicadores, NORMA 22301.

EVALUATION OF CURRENT INCIDENTS AND RISKS IN THE TECHNOLOGICAL INFRASTRUCTURE OF LAICA ELOY ALFARO UNIVERSITY IN MANABÍ-ECUADOR

Abstract: The vulnerabilities of the technological infrastructure of the Lay University Eloy Alfaro de Manabí were analyzed. For this, the methodology was used by levels. Initially, the current situation of the Central Computer Coordination Unit was determined and the main incidents on the site were identified, which were assessed considering their level of sensitivity. With the methodology Modal Analysis of Faults and Effects, the levels of probability and impact of the risks were reached, the MAGERIT methodology was also used to identify the assets of the unit and the threats to which they may be exposed. Finally, the Continuity Management Model was developed, based on the following phases: Scope of the Business Continuity Plan, Risk Assessment, Business Impact Analysis, Recovery Strategies and Plan Development. Finally, it is concluded that the computer unit is exposed to 59% of critical risks caused by threats according to the analysis carried out with a high level of criticality, so the proposed model will allow to respond significantly to possible incidents in order to give continuity to operations for the benefit of the university community.

Keywords: Management model, modal failure analysis, computer unit, indicator evaluation. STANDARD 22301

I.INTRODUCCIÓN

El Estándar Internacional ISO [1], establece que la continuidad de negocio es el término para referirse a las estrategias y planificación, mediante las cuales las organizaciones se preparan para dar respuesta a eventos catastróficos tales como incendios, inundaciones, ataques cibernéticos, accidentes o errores humanos. Por esta razón es importante adoptar medidas y planes que mitiguen el impacto ante cualquier incidente o riesgo. La continuidad de negocio reafirma claramente que se debe hacer en el antes, durante y después de un evento de crisis.

Toda organización establece los requisitos para la continuidad del negocio, la norma [1] determina como tratar y desarrollar los procedimientos para la gestión de un evento disruptivo. Así pues, en este trabajo se ha considerado la evaluación de la unidad informática de la Universidad Laica Eloy Alfaro de Manabí, Ecuador. En ella se han considerado los aspectos que exige la organización para que la unidad mencionada sea óptima y ofrezca los servicios para los que fue creada. Además se espera mejorar la disponibilidad de los servicios, activos y recursos de información al momento de ocurrir alguna eventualidad o incidencia.

EL aumento en el uso de tecnología puede desencadenar puntos de quiebre, o de rendijas en los aspectos relacionados con la seguridad, por tanto es indispensable mantener una infraestructura física segura y controlada, así como medidas apropiadas dentro de la organización y las seguridades oportunas en el sistema informático y de software [2].

En los trabajos de tecnologías se ha demostrado que las situaciones eventuales son inevitables, una reparación sencilla puede convertirse en un problema serio y dejar a la organización sin plataforma tecnológica, lo que ocasionaría un conjunto de situaciones que ponen en riesgo la estabilidad de la estructura informática y de la empresa [3].

Este trabajo está compuesto por cuatro secciones, la primera comprende los aspectos que contextualizan el problema, la segunda sección está constituida por el desarrollo del trabajo de investigación, sus lineamientos teóricos. Luego se encuentra la sección tres con la metodología y la descripción de los procedimientos. Luego se exponen los resultados encontrados y finalmente se presentan las conclusiones.

II.DESARROLLO

Un modelo de gestión es un sistema por el cual se llevan a cabo distintas funciones de una organización, según [4] testifican que en un modelo de gestión debe tomarse en cuenta medidas que contemplen aspectos económicos, logística, talento humano y marketing, además que es vital considerar los servicios institucionales, con el fin de involucrar estos conceptos en el marco del modelo de gestión. Es indispensable añadir que los nuevos tiempos requieren empresas más competitivas, que ofrezcan mejores servicios y estén en constante innovación, lo que hace necesario la realización y ajustes de sistemas de gestión adaptados a los nuevos productos y servicios tal como lo afirma la referencia [5].

Así mismo [6] declaran que las organizaciones están permanentemente en competitividad con el entorno, razón por la que es necesario aplicar los grandes beneficios que brindan los modelos de gestión y eso obliga a mejorar la disciplina y el enfoque para contribuir a la elevación del nivel de vida social. Adicionalmente [7] puntualizan que para enfrentar los desafíos de productividad y competitividad, las organizaciones consideran la implementación de modelos de gestión, que estimulen la mejora sistemática y continua.

Es sustancial resaltar que un modelo de gestión eficiente debe estar asociado a una Infraestructura Tecnológica, que fortalezca los procesos a través de aplicaciones informáticas, y a la vez permita el desarrollo de las actividades con más rapidez y menor posibilidad de errores, además es preciso argumentar que hoy en día la Infraestructura se convierte en la base fundamental de toda organización, debido a que cuentan con la integración de equipos para desarrollar su negocio.

En relación a lo expuesto en el párrafo anterior [8] coinciden que las infraestructuras tecnológicas tienen como objetivo indispensable satisfacer las necesidades de una organización, de tal forma que los procesos se vuelvan más eficientes; complementando la investigación [9] narra que la utilización de una infraestructura adecuada garantiza el desarrollo regular de funciones tecnológicas de las instituciones.

Es evidente entonces que la Norma ISO 22301 [10] ha evolucionado en base a la norma BS25999-2, siendo la primera norma internacional para la Gestión de la Continuidad de Negocio (GCN), desarrollada a contribuir con las organizaciones tanto Públicas como Privadas, permitiendo implementar las normas de acuerdo a los requerimientos Castro (2013). Consecuentemente [11] comentan sobre los nuevos conceptos introducidos en la Norma ISO 22301, y hacen énfasis en el liderazgo de la alta dirección para dar secuencia al aseguramiento de la compatibilidad del SGCN. De igual forma [12] diserta que la verdadera visión dentro de la Norma Internacional de Gestión de Continuidad del Negocio se establece en principios y terminología.

La Norma ISO 22301 ofrece una base de conoci-

ISSN 2542-3401/ 1316-4821 UNIVERSIDAD, CIENCIA y TECNOLOGÍA Vol. 23, Nº 94 Octubre 2019 (pp. 62-68)

mientos relacionados con la instauración de la Continuidad de Negocio en las instituciones, cabe recalcar que contiene elementos para continuar trabajando aun en situaciones imprevistas, sin perder la calidad del producto ni la reputación del negocio. Así mismo pretende evitar los contratiempos producidos por posibles desastres, que vienen asociados a la gestión administrativa, igualmente evitan la pérdida de tiempo causada por incidencias y situaciones inesperadas que podrían ocasionar el retraso en la prestación de servicios y calidad del producto, como aquellos eventos inesperados que afectan la continuidad del proceso de negocios

Como se puede inferir [13] aseveran que el SGCN es un proceso efectuado por el personal, que implementan respuestas efectivas para que la operatividad del negocio continúe de una manera razonable. Así mismo coincidiendo con el criterio de otros autores [14] difunde que la Continuidad del Negocio es considerable dentro de los planes, puesto que al no contar con estos preceptos hace que las organizaciones sean vulnerables. Por consiguiente es esencial tener presente lo que enaltece [15] en cuanto a la implementación de un plan de Continuidad del Negocio, deben existir dos factores inevitable: Compromiso y Conocimiento de las personas encargadas del desarrollo.

Es necesario destacar que toda Institución tanto Pública como Privada, al momento que quiera ser certificada por estos estándares, deben ser avalados por Instituciones especializadas en el tema de Continuidad de Negocio, los mismos que se hallan bajo el enfoque de la Norma ISO 22301 [16].

En contexto general la Norma ISO 22301 sostiene las fases PHVA que permite elaborar el Plan de Continuidad de Negocios (BCP), de acuerdo a lo mencionado por [17] un plan emergente permite equilibrar la estabilidad del negocio ante situaciones de contingencia o adversidad, apropiándose de las prevenciones y los procedimientos para la restauración del sistema de continuidad.

En este trabajo se ha considerado la evaluación de ítems e indicadores en la Unidad de Informática, para evaluar la posibilidad de un modelo de continuidad de negocio. Para esto existen diferentes metodologías que permiten efectuar un estudio del nivel de confiabilidad y seguridad dentro de un sistema de información, entre ellas la MAGERIT (Metodología de Análisis y Gestión de Riesgo) y la AMFE (Análisis Modal de Fallos y Efectos).

MAGERIT, ésta metodología fue elaborada por el Consejo Superior de Administración Electrónica (CSAE), respondiendo a la percepción de la Administración Pública, cuyo objetivo final es apreciar las vulnerabilidades a las cuáles están comprometidos, teniendo en cuenta las diferentes dimensiones de la seguridad tales como: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

MAGERIT atribuye a todo ente que trabaja con información digital y sistemas informáticos, ya que les permitirá conocer cuánto valor está en juego y por ende les ayudará a resguardar los servicios e información que se prestan. Así mismo percibe el riesgo al que están sometidos los elementos de labores, es loable establecer los elementos para el análisis de riesgo.

III.METODOLOGÍA

Para este trabajo se empleó el método descriptivo, permitiendo identificar características y aspectos que son relevantes en las áreas de Infraestructura y Redes, Desarrollo, Mantenimiento y Soporte a Usuarios y Operaciones, lo cual se obtuvo a través de la aplicación de la entrevista y checklist, que fueron utilizados para la recolección de datos. Así mismo se recurrió al método exploratorio, permitiendo aportar todo lo referente a características, observaciones, comportamientos y elementos que fueron de gran importancia para la elaboración del Plan de Continuidad. En una primera etapa se estudió la norma [1], para verificar lo esencial de cada uno de los requisitos que exige la institución y la normativa. En la segunda etapa se utilizó la metodología AMFE, para la identificación, evaluación y análisis de los riesgos encontrados con respecto a vulnerabilidades y amenazas, de forma que, se proporcionan medidas como acciones de mitigación y criterios de aceptación de acuerdo a los niveles de riesgos establecidos.

IV.RESULTADOS

Una vez realizada la investigación, se pudo observar que las principales carencias en la unidad, es que no tienen un plan de continuidad para casos de eventualidades o incidentes, solo se efectúan controles de riesgos pero no se documentan los procesos de identificación, análisis, evaluación y mitigación de los mismos, por lo tanto, no hay un relevamiento formal de los posibles riesgos. La configuración segura de equipos no se realiza uniformemente a toda la institución porque no hay implementados dominios que le permita a la unidad distribuir políticas y reglas para este proceso. No existe un control riguroso de los bienes, en algunos casos está a cargo de los guardias y en otros casos está a cargo del departamento de bienes, pero tampoco existe un acta de entrega-recepción de los guardias actuales ni información actualizada del estado y ubicación de los equipos.

Se tienen implementadas políticas de seguridad de información que les permita mantener la confidencia-

ISSN 2542-3401/ 1316-4821 UNIVERSIDAD, CIENCIA y TECNOLOGÍA Vol. 23, Nº 94 Octubre 2019 (pp. 62-68)

lidad, integridad, autenticación y disponibilidad de la información. Cuenta con equipos auxiliares para continuar brindando los servicios en caso de que alguno interrumpa sus funciones, además tienen prioridad para reanudar los servicios. A partir del terremoto del año 2016 la Universidad ha sufrido eventualidades de desastre y de incidentes en Ciberseguridad. El tiempo estimado que tienen para restaurar un servicio en caso de desastre natural es de 5 días y los incidentes de Ciberseguridad están en un promedio de 4 horas en contenerlos y recuperar los servicios.

Actualmente la institución tiene 23000 estudiantes y 13000 docentes, por lo que si el servicio sufre una eventualidad, el mayor impacto que tendría sería en el proceso de enseñanza aprendizaje debido a la utilización del sistema de gestión académica y plataforma virtual. Las redes LAN, WAN tienen 25000 usuarios aproximadamente.

Los procesos principales se llevan a cabo en el área de Desarrollo son la Gestión de proyectos y la organización de la metodología de desarrollo. Esta área se maneja de acuerdo a lineamientos establecidos en la unidad como Lenguaje de programación PHP y JAVA SCRIPT, diseño HTML y CC y de consulta SQL, para lo que se refiere a una aplicación (programa) nueva, de este modo se puede determinar si este se desarrolla de forma integrada, semi-integrada o aislada.

La universidad utiliza metodologías formales y ágiles como: XP, HAS, CMI; como marco de trabajo el estándar MBC en el lado del servidor, MVVM en el lado del cliente de manera técnica y en los servicios web, el estándar REST para las comunicaciones entre sistemas.

Otra de las carencias que tiene la unidad son los procedimientos operacionales en TIC, ya que no están definidos en su totalidad. Los equipos críticos son monitorizados frecuentemente al igual que los sistemas de información son comprobados en funcionalidad de acuerdo a los estándares aplicados. Los cambios que se efectúan en los sistemas o aplicaciones son autorizados por el director de área, los registros de auditoría cuando tienen cambios se revisan y coordinan frecuentemente.

Tabla I. Identificación de vulnerabilidades según la secciones de la normas.

SECCIÓN	IDENTIFICACIÓN	CANTIDAD
Directrices de gestión de la seguridad de la Información.	Muy sensible	6
	Sensible	0
	Poco sensible	0
	No sensible	0
Roles y responsabilidades en seguridad de la información.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	6
Segregación de tareas.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	3
Propiedad de los activos.	Muy sensible	1
	Sensible	2
	Poco sensible	0
	No sensible	8
Uso aceptable de los activos y Devolución de activos.	Muy sensible	1
	Sensible	2
	Poco sensible	0
	No sensible	8
Áreas seguras.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	2
Seguridad de los equipos.	Muy sensible	8
	Sensible	5
	Poco sensible	1
	No sensible	21
Documentación de procedimientos de la operación.	Muy sensible	3
	Sensible	5
	Poco sensible	1
	No sensible	32
Gestión de cambios.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	1
Gestión de capacidades.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	9

Uso aceptable de los activos y Devolución de activos.	**Muy sensible**	**1**
	Sensible	2
	Poco sensible	0
	No sensible	8
Áreas seguras.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	2
Seguridad de los equipos.	Muy sensible	8
	Sensible	5
	Poco sensible	1
	No sensible	21
Documentación de procedimientos de la operación.	Muy sensible	3
	Sensible	5
	Poco sensible	1
	No sensible	32
Gestión de cambios.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	1
Gestión de capacidades.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	9
Separación de los recursos de desarrollo, prueba y operación.	Muy sensible	1
	Sensible	4
	Poco sensible	0
	No sensible	1
Copias de Seguridad de la Información.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	8
Registro de eventos.	Muy sensible	3
	Sensible	1
	Poco sensible	0
	No sensible	11
Protección de la información de registro.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	3
Gestión de las vulnerabilidades técnicas.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	4

ISSN 2542-3401/ 1316-4821 UNIVERSIDAD, CIENCIA y TECNOLOGÍA Vol. 23, Nº 94 Octubre 2019 (pp. 62-68)

Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	**Muy sensible**	**3**
	Sensible	0
	Poco sensible	2
	No sensible	3
TOTAL		**210**

Una vez obtenida esta información se pudo concluir que han existido vulnerabilidades de tipo severas (muy sensibles y sensibles) y leves (poco sensibles) que se detectaron por áreas según la situación actual de la infraestructura.

La clasificación de las amenazas a las cuales puede estar propensa las áreas activas de la UCCI según la metodología MAGERIT son: [N] Desastres Naturales, [I] De Origen Industrial, [E] Errores y Fallos y no Intencionados y [A] Ataques Intencionados en referencia a los activos y recursos de la información, en la cual se observa mayor relevancia en el área general de la UCCI (Figura 1)

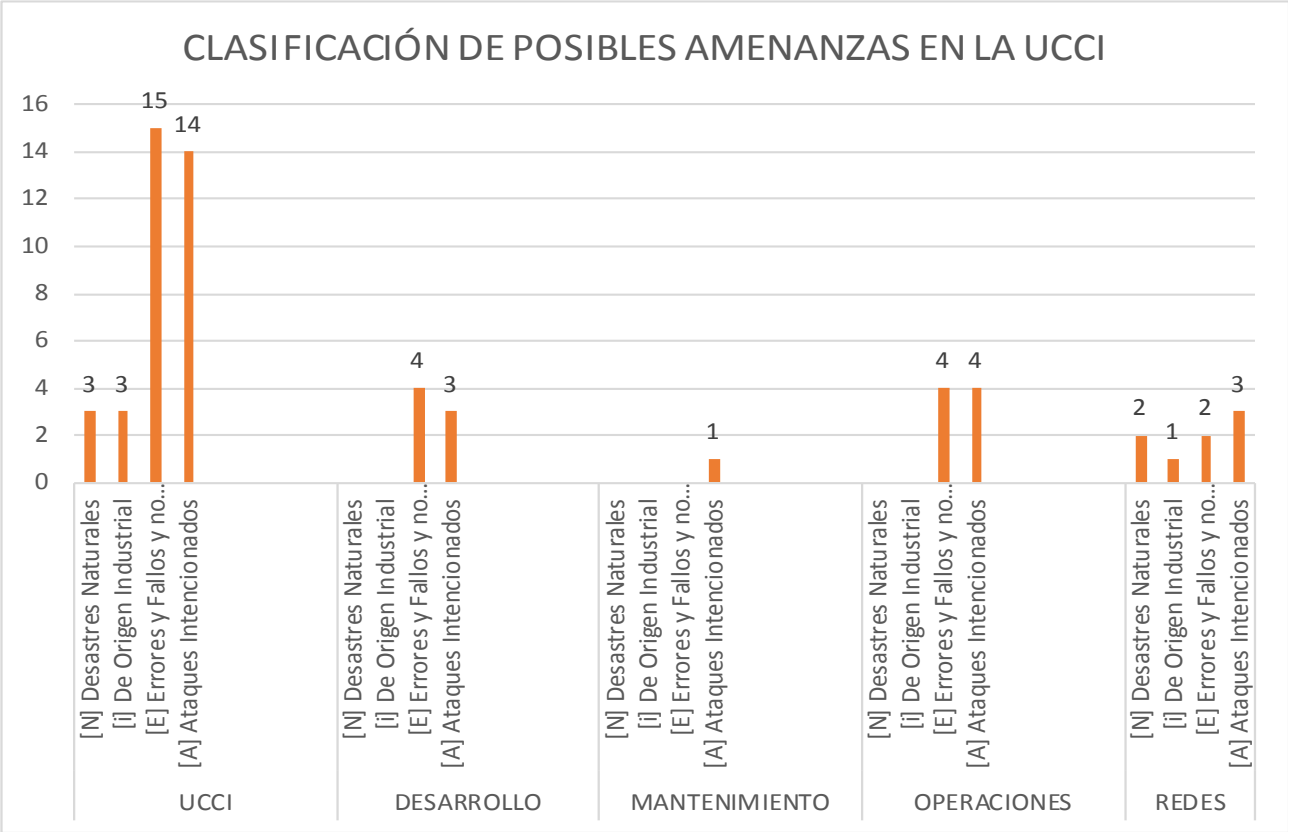

Figura 1. Clasificación de las posibles amenazas en la UCCI.

Es importante hacer énfasis en los criterios por área, dando por resultado lo siguiente: Que el área que tuvo mayor impacto en cuanto a criticidad fue la del área General de la UCCI con un 59% equivalente a 35 criterios, Redes con el 14% equivalente a 8, seguidamente de operaciones correspondiente a 14% equivalente a 8, desarrollo con 11% equivalente a 7 y por ultimo mantenimiento 2% equivalente a 1, mismos que fueron influencias críticas en algunos de los procesos de la infraestructura tecnológica.

CONCLUSIONES

•La Infraestructura Tecnológica de la ULEAM posee medidas de seguridad, pero no se encuentran guiadas ni documentadas, por lo tanto no son efectivamente utilizadas al momento de ocurrir un incidente.

•La metodología AMFE y como complemento la metodología MAGERIT aportan gran ayuda al momento del análisis y gestión de riesgo, además como resultado de esta investigación se concluye que la Unidad Central de Coordinación Informática está expuesta a riesgos críticos causados por amenazas

•Para poner en marcha un plan de negocios apropiado, es necesario que la unidad responsable ajuste los criterios y los indicadores para mejorar el servicio, la seguridad y la confiabilidad de los datos.

REFERENCIAS

[1]ISO, «ISO,» [En línea]. Disponible: https://www.iso-tools.org/normas/ [Último acceso: marzo 2019].

[2] A. R. Castro y Z. O. Bayona, «Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios,» Dialnet, vol. 16, nº 2, pp. 56-66, 2011.

[3] M. Bautista, «Marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio.,» Rev. Técnica de energía, pp. 200-207, 2014.

[4]J. Aguirre y J. Iñiguez, «Implementación de un modelo de gestión por procesos para el área operativa del taller automotriz La ´France en función de la mejora de la productividad,» UIDE, Quito-Ecuador, 2018.

[5]AHPC, «Ayuda Humanitaria y Protección Civil,» 2015. [En línea]. Disponible: https://reliefweb.int/sites/reliefweb.int/files/resources/Guia_Operativa_CEPRE-DENAC_ECHO.pdf. [Último acceso: 11 septiembre 2019].

[6]M. Lopes, «Los modelos de gestión en los centros educativos de Iberoamérica. Retos y posibilidades,» Rev. Iberoamericana de Educación, nº 67, pp. 11-14, 2014.

[7]F. J. G. ColinaI, S. C. J. Hernández y L. Salgado, «Gestión escolar y calidad educativa,» Rev. cuabana de Educación Superior, vol. 2, pp. 206-2016, 2018.

[8]F. Proaño, «Modelo de gestión de TICs para la gerencia de división de informática de la Corporación Financiera Nacional, basado en gerencia estratégica de procesos.,» Escuela Politécnica Nacional, Quito-Ecuador, 2012.

[9]J. Moreno y N. L. Sierna, «Modelo de Calidad para la Gestión de las TIC en el Proceso de Enseñanza para Instituciones Educativas Peruanas del Nivel Secundario,» Rev. de la facultad de ingeniería industrial, vol. 17, nº 1, pp. 110-119, 2014.

[10]ISO, «ISOTools,» [En línea]. Disponible: https://-www.isotools.org/normas/riesgos-y-seguridad/iso-22301/. [Último acceso: marzo 2019].

[11]F. Bolaños, N. Angulo y J. Cárdenas, «La continuidad de negocio en las instituciones de educación superior del ecuador. Caso de estudio,» Universidad Espíritu Santo, Guayaquil-Ecuador, 2019.

[12]K. Bonilla, «Materialización del riesgo y gestión de la continuidad del negocio,» Universidad Piloto de Colombia, pp. 1-7, 2018.

[13]C. María, V. Alcívar y Z. Aura, «Modelo de gestión de continuidad en la infraestructura tecnológica de la Universidad Laica Eloy Alfaro de Manabí, basada en la norma ISO 22301,» Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Manabí-Ecuador, 2019.

[14]A. Y. H. Seminario, «Diseño de un Plan de Recuperación de Desastres de TI (DRP TI) para el Centro de Cómputo de la sede principal de una entidad educativa superior del sector privado basado en la norma NIST SP 800-34,» Universidad Peruana de Ciencias Aplicadas, Lima-Perú, 2019.

[15]H. Figueroa y M. Salamanca, «Guías para la implementación y auditoría de planes de continuidad de negocio desde la perspectiva de las normas ISO 22302, BS 25999, NTC 5722 y las prácticas profesionales del SRII y de ISACA,» Universidad Piloto de Colombia, Bogotá-Colombia, 2013.

[16]M. Raba y A. López., «Metodología de auditoría de sistemas de información de gestión documental SIGD para entidades estatales,» Universidad Católica de Colombia, Bogotá-Colombia, 2018.

[17]J. Blanco, L. Martínez, C. Quintero y J. Rincón, «Plan de continuidad para el centro de desarrollo e innovación tecnológica de la universidad francisco de paula santander ocaña,» Universidad Francisco De Paula Santander Ocaña, Ocaña, 2015.