Revista de investigación de sistemas e informática
15(1): 113-126 (2022)
DOI: https://doi.org/10.15381/risi.v15i1.23362

ISSN: 1815-0268 (Impreso) / ISSN: 1816-3823 (Electrónico)
Facultad de Ingeniería de Sistemas e Informática - UNMSM

Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001

Importance of information security management in educational institutions with ITIL and ISO 27001

Evellyn Milles Duval Guevara Vega
https://orcid.org/0000-0002-0879-5819
emguevarav@unitru.edu.pe

José Ricardo Delgado Deza
https://orcid.org/0000-0003-0777-0107
jrdelgadod@unitru.edu.pe

Alberto Carlos Mendoza de los Santos
https://orcid.org/0000-0002-0469-915X
amendozad@unitru.edu.pe

Universidad Nacional de Trujillo. Trujillo, Perú

Recibido: 09/08/2022 - Aceptado: 28/08/2022 - Publicado: 20/09/2022

RESUMEN

La educación es uno de los factores fundamentales para el desarrollo humano, aportando conocimientos que ayudan en el desarrollo de la persona, así como también en la sociedad. Con el avance del tiempo, las instituciones educativas han ido implementando nuevas metodologías y procesos en la enseñanza, donde se encuentra un factor muy importante como lo es la tecnología. La educación, luego de la pandemia COVID-19 se vio afectada por los ciberataques e incluso, mediante el estudio virtual, donde la información se podría perder si no se fija correctamente una gestión de seguridad. Esta gestión de seguridad se tiene que guiar de acuerdo a las normas establecidas por lo que se realiza esta revisión sistemática que tiene como pregunta: ¿Es importante la gestión de seguridad de información en las distintas instituciones educativas aplicando ITIL y la norma ISO 27001? Por ende, nuestro objetivo de investigación es identificar los beneficios que ofrece tener una gestión de seguridad en una institución educativa eligiendo como marco a ITIL e ISO 27001. Esta búsqueda se logró gracias a las revisiones de artículos publicados en base de datos como Scielo, Google Academy, Scopus y Redalyc comprendida entre los años 2017 al 2021.

Palabras clave: Seguridad de información; instituciones educativas; ITIL; ISO 27001; educación.

ABSTRACT

Education is one of the fundamental factors for human development, providing knowledge that helps in the development of the person as well as in society. As time has progressed, educational institutions have been implementing new methodologies and processes in teaching, where technology is a very important factor. Education, after the COVID-19 pandemic, was affected by cyber-attacks and even through virtual study, where information could be lost if security management is not correctly established. This security management has to be guided according to the established standards so this systematic review is carried out with the question: Is information security management important in different educational institutions by applying ITIL and ISO 27001? Therefore, our research objective is to identify the benefits of having security management in an educational institution by choosing ITIL and ISO 27001 as a framework. This search was achieved through reviews of articles published in databases such as Scielo, Google Academy, Scopus and Redalyc from 2017 to 2021.

Keywords: Information security; educational institutions; ITIL; ISO 27001; education.

I. INTRODUCCIÓN

Las instituciones educativas, con el paso del tiempo, han ido implementando nuevas metodologías y procesos en la enseñanza, donde se encuentra un factor muy importante como lo es la tecnología. Valencia Morocho, C.A. (2021), afirma que se han dado saltos exponenciales en las diversas actividades humanas gracias al avance de la tecnología, como la educación, siendo uno de los pilares fundamentales para la formación profesional y personal no ha sido la excepción a este avance tecnológico.

Debido a su importancia y evolución, se busca mejorar la calidad del servicio en toda la institución, Álvarez Tay, R. C (2021) rectifica que la calidad en las instituciones de educación superior siempre será uno de los aspectos más significativos para crear conocimientos, desarrollo de recursos humanos y la fuerza social de todo país.

Dentro de todos estos aspectos, uno de los más relevantes y que siempre debe estar actualizado es la seguridad de la información, definido como el grupo de medidas correctivas y preventivas que una organización usa para proteger y preservar toda la información manteniendo la confidencialidad, disponibilidad e integridad de la misma (Carlos Bladimir Moreano Guerra, 2019), de esta manera se evita que la información pueda ser borrada, extraída o manipulada ya sea por personas de la institución, así como también alguien externo a ello.

Para poder fortalecer la seguridad de la información, aparece ITIL y la ISO 27001 para tener una óptima gestión. Algunos autores como Garzón Cruz, G. F., Merchan Carrillo, J. F., & Morea Vergara, K. J. (2020) definen a ITIL como un marco de referencia que cubre a toda la organización respecto al gestionamiento para la entrega y ejecución de productos y servicios autorizados por TI; esto quiere decir que, no se encarga de autentificar a las organizaciones. El objetivo de ITIL es que las organizaciones logren la adaptación y con ello producir mejores resultados para sus procesos. ITIL viene a ser de gran utilidad para todos los procesos en una organización, cubriendo numerosas áreas, pero para este caso se enfocará en la seguridad de la información.

Carlos Bladimir Moreano Guerra, (2019) nos cuenta que las normas ISO son una cadena de organismos de normalización que cuenta con más de 160 países donde finalmente las conclusiones dadas por ISO son publicadas como una norma internacional, de esa manera las normas ISO indican un estándar a seguir para tener una gestión adecuada, para esta investigación, se hace uso de la ISO 27001, enfocada en los sistemas de gestión de la seguridad de la información.

Aparte, un Sistema de Gestión de Seguridad de la Información brinda un modelo que permitirá establecer, implementar, operar, monitorear, y/o mejorar el resguardo de los activos de información. En este caso se hace mención a la norma ISO 27001.

Por ello, con la importancia de la educación y los cambios en tecnología que afecta a este servicio tiene que haber una mejora y revisión constante en términos de seguridad de información, por lo que en este contexto se responderá a la siguiente pregunta: ¿Es importante la gestión de seguridad de información en las distintas instituciones educativas aplicando ITIL y la norma ISO 27001?

II. MATERIAL Y MÉTODOS

Para esta revisión sistemática se tuvo que revisar la literatura científica en base a la metodología PRISMA, definida por Urrutia & Bonfill (2010): Preferred Reporting Items for Systematic Reviews and Meta-Analyses. La pregunta de investigación establecida para dirigir este estudio fue la siguiente: ¿Es importante la gestión de seguridad de información en las distintas escuelas aplicando ITIL y la norma ISO 27001?

Esta metodología promueve según Urrútia & Bonfill, 2010 que un sistema fundamentado en la evaluación de los distintos componentes del diseño y ejecución de los estudios nos revelará evidencias precisas y empíricas acerca de la relación entre ellos.

Por lo que es necesario realizar este estudio con un método que sea de manera explícita, buscando el indagar para satisfacer los resultados del estudio.

Este método comienza con la búsqueda de registros o citas en las distintas bases de datos, continuando con la eliminación de los duplicados y terminamos con aquellos estudios implicados en síntesis cualitativa y cuantitativa (revisión sistemática y metaanálisis respectivamente) , referenciado por Urrútia & Bonfill, (2010).

Para poder empezar el proceso de búsqueda se van a emplear descriptores como términos a partir de la pregunta de investigación: “seguridad de información”,” institución educativa”,” ITIL”,” ISO 27001”,” educación”,” ciberseguridad”, “information security”, “educational institutions”, “ITIL”, “ISO 27001”, “education”.

Siguiendo con el proceso de búsqueda, se clasificará y para eso se realizó un manejo de los términos ya dados junto con operadores booleanos: ("sistema educativo" OR "ciberseguridad" AND "ISO 27001" AND "seguridad de información")

Las bases de datos seleccionadas para esta revisión sistemática fueron SCIELO, GOOGLE ACADEMY, SCOPUS y REDALYC.

Scielo

("seguridad de información" OR "institución educativa" OR "ITIL" OR "ISO 27001" OR "educación" OR "ciberseguridad" OR "information security" OR "educational institutions" OR "ISO 27001" OR "education")

Google Academy

("gestion" AND "seguridad de información" AND "institución educativa" AND "ITIL" AND "ISO 27001" OR "ciberseguridad" OR "information security" OR "educational institutions" OR "ISO 27001" OR "education")

Scopus

(TITLE-ABS-KEY (information AND security) AND TITLE-ABS-KEY (educational AND institutions) AND TITLE-ABS-KEY (iso 27001)) AND PUBYEAR > 2016 AND PUBYEAR < 2023 AND PUBYEAR > 2016 AND PUBYEAR < 2023 OR (TITLE-ABS-KEY (information AND security) AND TITLE-ABS-KEY (educational AND institutions) OR TITLE-ABS-KEY (itil)) AND PUBYEAR > 2016 AND PUBYEAR < 2023 AND PUBYEAR > 2016 AND PUBYEAR < 2023

Redalyc

("seguridad de información" AND "institución educativa" AND "itil")

Para realizar este estudio, se presentan artículos publicados en bases de datos científicas, en los idiomas inglés y español, comprendidos entre los años 2017 al año 2022 (últimos 5 años).

Con respecto al criterio de inclusión son: contexto de la seguridad de información en la educación de estudios secundarios y universitarios, el efecto de la pandemia en la seguridad de la información en la educación, y el uso exclusivo de ITIL y norma ISO 27001.

Con respecto al criterio de exclusión se dispuso no abordar las publicaciones que tienen como temas de seguridad de información en empresas que no abarquen el ámbito educativo, seguridad de información sin ITIL y las normas ISO 27001 y las distintas aplicaciones que se utilizan para la educación.

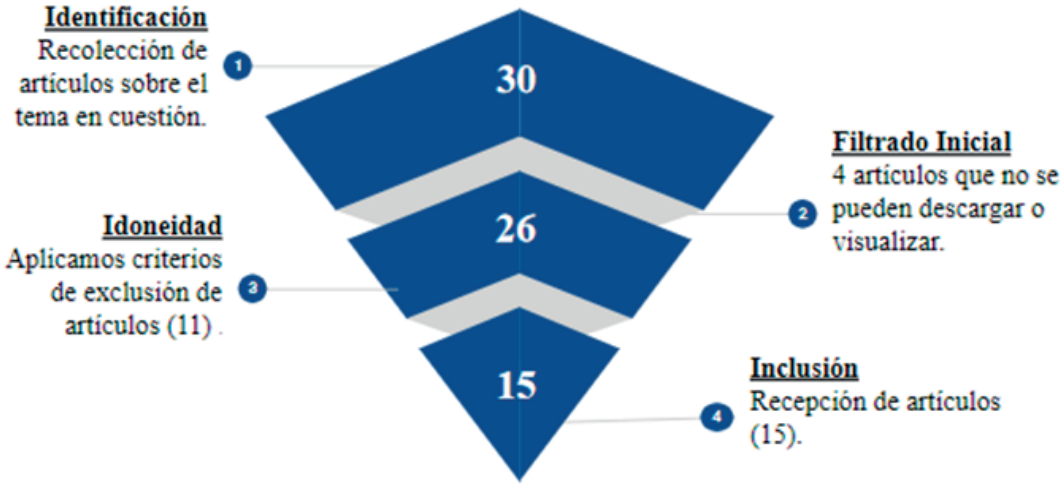
El registro de búsqueda y de extracción de información fue tratado por los colaboradores del estudio de manera independiente, donde las desigualdades fueron observadas y resueltas en consenso por los mismos para poder realizar una revisión sistemática. Tal y como se muestra en la Figura 1.

III. RESULTADOS

Por la búsqueda de artículos en las bases de datos y motores de búsqueda se determinaron un total de, aproximadamente, 30 artículos publicados entre el

Figura 1

Flujograma sobre el Proceso de Selección de Artículos



Fuente: Elaboración Propia

periodo de tiempo de 2017 a 2022; ordenados así: Google Academy 15 artículos, seguida de Scielo con 11 artículos, Scopus 3 artículos y por último Redalyc con 1 artículo.

A partir de este número total, se aplicaron criterios de inclusión y de exclusión, explicados anteriormente, hasta obtener 15 artículos, donde nos basaremos para los resultados del tema.

Tomando en cuenta estos artículos seleccionados, se procedió a precisar las definiciones sobre seguridad de información o ciberseguridad de acuerdo a las normas ITIL e ISO 27001 para la educación, así también como los beneficios de aplicar una gestión de seguridad que se muestran en la siguiente Tabla 1.

Con respecto a los países que lideran las publicaciones, se demuestra que es importante para todos los países el tema de gestión de la seguridad de información en las instituciones educativas; principalmente Ecuador que cuenta con 5 publicaciones, seguida de Perú y Colombia con 4 artículos cada uno y otros con 1 artículo, tal y como se muestra en la Figura 2.

La educación se tuvo que adaptar a medidas sanitarias de seguridad como el encierro en sus propias viviendas recibiendo clases virtuales, donde la seguridad de información en aquellas plataformas: zoom, Moodle, meet; se puede afectar fácilmente y directamente al computador al hacer un clic. Olmedo, M. R. M., & Chaves, V. E. J. (2020) citando a Santiso, Koller, & Bisaro nos dice que si deseamos enfrentar eficientemente la problemática se requerirá un proceso de gestión de la seguridad de la información teniendo como una perspectiva global los riesgos, lo cuál permitirá obtener un equilibrio entre la usabilidad y el control, incluyendo exitosamente las nuevas tecnologías de seguridad, ayudando a reducir las amenazas importantes y conservando la facilidad de uso.

Entonces, debido a la pandemia tanto estudiantes, docentes y personal administrativo hacen uso de un computador para realizar sus actividades. Di Luca,

Tabla 1

Lista de artículos incluidos en la revisión sistemática en los últimos 5 años.

INSTITUCIÓN EDUCATIVA/ UNIVERSIDAD	AÑO	PAÍS	TÍTULO
Universidad Nacional Mayor de San Marcos	2021	Perú	Evaluación del nivel de satisfacción del estudiante respecto al servicio educativo bajo el enfoque del modelo HEdPERF en las universidades públicas que integran la Alianza Estratégica de la Universidad Peruana y que implementaron el mecanismo de licenciamiento.
Universidad Cesar Vallejo	2021	Perú	La educación virtual en el pensamiento crítico de los estudiantes universitarios.
Escuela Superior Politécnica de Chimborazo	2019	Ecuador	Propuesta de mejores prácticas: ITIL para la gestión de las TIC en apoyo a la actividad docente
Universidad Cooperativa de Colombia	2020	Colombia	IMPLEMENTACIÓN DE BUENAS PRÁCTICAS BASADAS EN ITIL 4 E ISO 20000 PARA LA GESTIÓN DE INCIDENTES Y REDUCCIÓN DE RIESGOS DEL SERVICE DESK DE LA EMPRESA INGEAL S.A.
Universidad Tecnológica Empresarial de Guayaquil	2019	Ecuador	Seguridad de la Información para Instituciones Educativas a tercer nivel basado en la ISO/IE27001
Universidad Cesar Vallejo	2018	Perú	ITIL V3 para la calidad de los servicios de los usuarios de las instituciones educativas JEC-UGEL-05, 2017
Universidad Nacional de San Agustin de Arequipa	2019	Perú	Modelo de análisis para la implantación de un SGSI basado en ISO 27001 y COBIT para una empresa del Sector Educación
Escuela Superior Politécnica de Chimborazo	2018	Ecuador	Estudio de las normativas de seguridad de la información de instituciones públicas: propuesta de una normativa en una institución de educación superior.
Universidad Autónoma de Manizales	2017	Colombia	Modelo de Sistema de Gestión de Seguridad de la Información Basado en la Norma NTC ISO/IEC 27001 para Instituciones Públicas de Educación Básica de la Comuna Universidad de la Ciudad de Pereira
Technical University of Moldova	2021	Republic of Moldova	Cyber security strategies for higher education institutions
Universidad de Cuenca	2020	Ecuador	Information security management frameworks and strategies in higher education institutions: a systematic review
Universidad del Valle	2021	Colombia	Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá
Universidad De La Costa	2021	Colombia	Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias
Universidad de la Integración de las Américas	2021	Paraguay	SEGURIDAD DE LA INFORMACIÓN EN PLATAFORMAS DE E-LEARNING EN TIEMPOS DE PANDEMIA COVID-19
Universidad Estatal Península de Santa Elena	2019	Ecuador	Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso

Fuente: Elaboración Propia

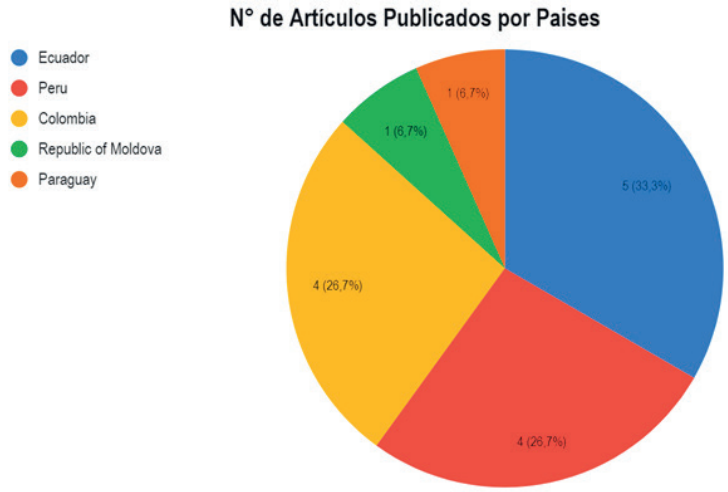
M.A. (2019) nos ofrece un modelo de gestión de la seguridad de la información junto con los riesgos en las redes de computadoras, tal y como se muestra en la Figura 3.

Para poder dar un mayor enfoque sobre cómo se ha visto afectada la seguridad de información en la pandemia, Estrada Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E. (2021) citando a Castellanos Vega dio a conocer en el país de Bogotá que durante la pandemia las modalidades de ciberataques se incrementaron de 33 a 41.

Aparte se realizó una encuesta en la Universidad del Valle, sede Tuluá (Colombia) donde se encontraron con resultados inquietantes con respecto a

Figura 2

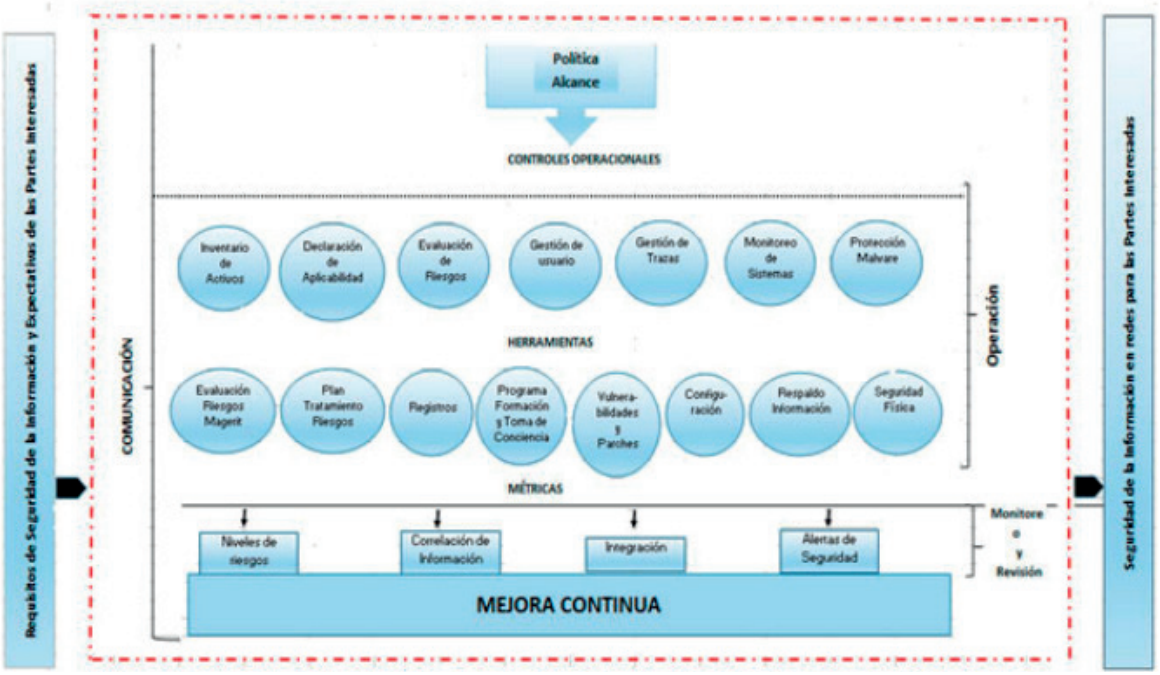
Distribución del número de artículos publicados según cada país.



Fuente: Elaboración Propia.

Figura 3

Modelo de gestión de la seguridad de la información.



Fuente: Elaborada por Di Luca, M. A., 2019.

los estudiantes y/o docentes y su comportamiento con la seguridad de información, donde se refieren que durante la pandemia un 47,8% de los encuestados no recibió alguna información falsa y un 43,3% recibió noticias falsas. (Estrada Esponda, R. D. y otros, 2021), véase Tabla 2.

En relación a la actualización de seguridad de manera automática, un 59,1% lo realizó exitosamente, un 23,1% desconoce la frecuencia de actualización (mensual, semanal o diaria) y por último un 17,8% desconoce totalmente este proceso, véase Figura 4 (Estrada Esponda, R. D. y otros , 2021).

Por lo tanto, se puede comprobar que esta pandemia resurgió incidentes en la seguridad de la información aumentando a una gran escala y para poder darle fin a los ataques que afectan a nuestra información es

Tabla 2

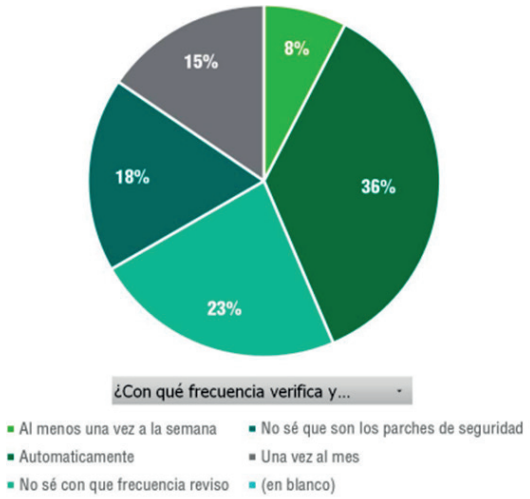
Encuesta a estudiantes y docentes sobre seguridad informática en pandemia.

Pregunta	Respuesta	Mensaje
¿Ha recibido recientemente informacion falsa (fake news) o informacion conspirativa sobre la pandemia?	No	47.8%
	No sabe / No responde	8.9%
	Si	43.3%
¿Fue victima de robo de informacion por software maliciosos que parecian o aparentaban ser archivos que contenian medidas para prevenir el COVID-19?	No	94.5%
	No sabe / No responde	3.1%
	Si	2.4%
¿Ha visitado o visito dominios de internet asociados con la palabra COVID-19 o coronavirus, que resultaron ser faltos y su unico proposito tenia que ver con actividades malintencionadas?	No	81.1%
	No sabe / No responde	4.7%
	Si	14.2%
¿Fue suplantado en plataformas virtuales de conectividad sincronica, como Zoom, Google Meet u otra?	No	92.7%
	No sabe / No responde	3.9%
	Si	3.4%
¿Fue suplantado en plataformas e-learning ofrecidas por su universidad en relacion con actividades academicas no sincronicas?	No	94.0%
	No sabe / No responde	4.7%
	Si	1.3%
¿Fue testigo de ingresos no autorizados a sesiones de trabajo sincronicas que afectaron el desarollo de dichas sesiones?	No	88.2%
	No sabe / No responde	3.7%
	Si	8.1%
A raiz de la pandemia del COVID-19, ¿ha tenido que realizar teletrabajo a traves de una VPN?	No	68.5%
	No sabe / No responde	11.5%
	Si	19.9%

Fuente: Elaborada por Estrada Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E., 2021.

Figura 4

Encuesta a estudiantes y docente sobre la aplicación de actualizaciones de seguridad.



Fuente: Elaborada por Estrada Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E., 2021.

importante tener una buena gestión de seguridad; de lo contrario, nuestra información se podría filtrar para usos maliciosos.

Dentro de los temas que abarca Melgarejo Terán, R. (2018), habla de la aplicación de ITIL en una institución educativa JEC (Jornada Escolar Completa) para mejorar la calidad de servicio, nos encontraremos con las siguientes variables:

Esta investigación se centrará en el análisis de la segunda y tercera dimensión, esto debido a que son las dimensiones que más tienen relación con la seguridad de información, siendo la capacidad de respuesta muy importante ante cualquier incidente con la información, así como también la capacitación del personal para evitar estos incidentes.

La aplicación de ITIL fue mediante un GLPI que contiene las dimensiones anteriormente mencionadas en la Tabla 3 y Figura 5.

Según Melgarejo Terán, R. (2018) para la medición de resultados de esta investigación se realizó un

Tabla 3

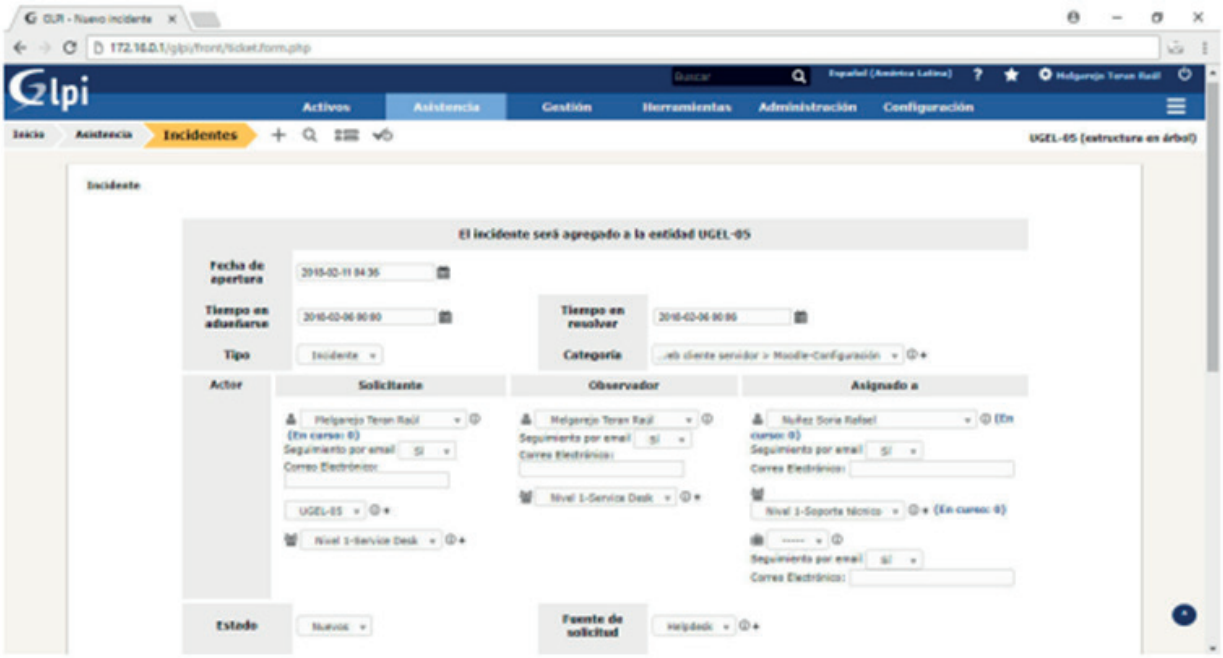
Operacionalización de variables

DIMENSIONES	INDICADORES	ITEMS	ESCALA DE VALORES	NIVEL Y RANGO
Fiabilidad	Necesidades satisfechas del usuario por el servicio prestado	P1,P2,P3,P4	Ordinal 1. Totalmente en desacuerdo 2. Bastante en desacuerdo 3. Ni de acuerdo ni en desacuerdo 4. Bastante de acuerdo 5. Totalmente de acuerdo	Deficiente [7;16> Regular [16;26> Eficiente [26;35>
	Requerimiento concluido en tiempos establecidos	P5,P6,P7		
Capacidad de respuesta	Atencion brindada al usuario	P8,P9,P10		Deficiente [3;7> Regular [7;11> Eficiente [11;15>
Capacitacion del personal	Disposicion de atencion mostrada al usuario	P11,P12		Deficiente [3;7> Regular [7;11> Eficiente [11;15>
	Conocimiento suficiente mostrada al usuario	P13		
Atencion al cliente	Atencion individual al usuario	P14,P15		Deficiente [2;5> Regular [5;7> Eficiente [7;10>
Imagen	Apariencia mostrada al usuario	P16,P17		Deficiente [2;5> Regular [5;7> Eficiente [7;10>

Fuente: Elaborado por Melgarejo Terán, R., 2018

Figura 5

Glpi aplicado a la institución educativa (registro de incidentes)



Fuente: Elaborado por Melgarejo Terán, R., 2018

cuestionario y el análisis de estos datos de pre-test y post-test por medio de la prueba estadística de Wilcoxon (ver Figuras 6 y 7).

De estos resultados Melgarejo Terán, R. (2018) concluye que:

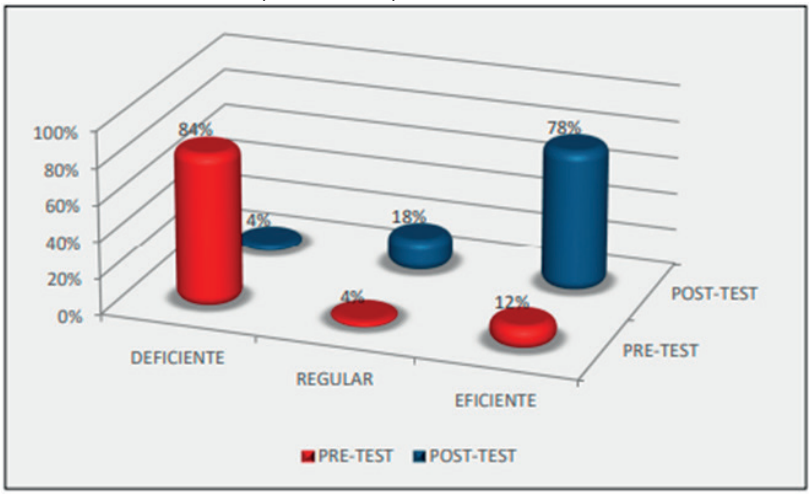
- Con ITIL V3 se logra mejorar la capacidad de respuesta en la calidad de los servicios que brindan los centros educativos JEC-UGEL-05, 2017.
- Con ITIL V3 se logra mejorar la credibilidad y confianza por medio de las capacitaciones a los trabajadores de los centros educativos JEC-UGEL-05, 2017.

Como ya se ha mencionado, la ISO 27001 tiene como su pilar principal al SGSI (Sistema de Gestión de Seguridad de la Información) debido a su activo que es la información, el autor Ríos, B., & Milton, W. (2019) muestra los requisitos de un SGSI (ver Figura 8).

Estos pilares permiten una correcta gestión de la seguridad de la información, de manera que es posible gestionar un riesgo existente y lograr solucionar con un mínimo impacto para la organización. Es por esto que estos pilares son fundamentales para el sistema de gestión de la información y parte también de la ISO 27001.

Figura 6

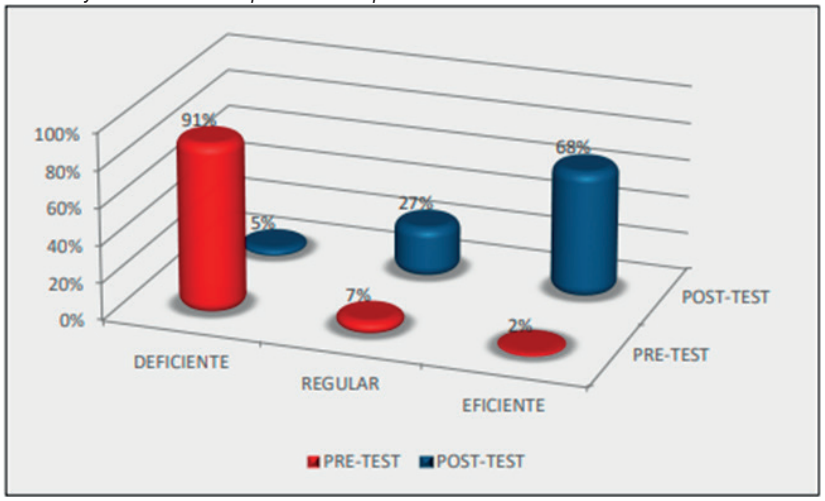
Pre-Test vs Post-test de la capacidad de respuesta.



Fuente: Elaborado por Melgarejo Terán, R., 2018

Figura 7

Pre-test y Post-test de la capacitación de personal.



Fuente: Elaborado por Melgarejo Terán, R., 2018

Para Carlos Bladimir Moreano Guerra (2019) la norma ISO 27001:2013 se orienta al concepto de seguridad como un todo, definiendo objetivos claros que se puedan conseguir con planes específicos, teniendo en cuenta las posibles alteraciones en los procesos de evaluación de riesgos. Dentro del soporte se detalla los recursos, personal y comunicación.

Esta tabla 4 contiene algunos activos que cuenta la institución educativa que son importantes para la seguridad de la información, logrando identificar la probabilidad de riesgo de cada uno de ellos, y conforme a esto, se aplicará el control según la ISO, de manera que se pueda comprobar si la institución cumple o no con la ISO 27001.

Figura 8

Pilares de la Seguridad de la Información

Fuente: Elaborado por Ríos, B., & Milton, W. (2019)

Tabla 4

Establecimiento de activos de la institución educativa

TIPO	ACTIVO	NOMBRE ACTIVO	CLASIFICACION DE LA INFORMACION	IMPACTO	PROBABILIDAD	RIESGO
DATOS INFORMACION	COPIAS RESPALDOS	ARCHIVOS DE NOTAS	CONFIDENCIAL	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
		ARCHIVOS DE CONTABILIDAD	USO INTERNO	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
		ARCHIVOS DE ACTAS Y RESOLUCIONES	PUBLICO	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
		COPIAS DE SEGURIDAD DE LA INFORMACION DEL INSTITUTO	SECRETA	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
	DATOS DE CONFIGURACION	DATOS DE CONFIGURACION DE COMPUTADORAS Y SERVIDORES	CONFIDENCIAL	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
	CONTRASEÑAS	CONTRASEÑAS DE COMPUTADORES	RESERVADO USO INTERNO	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
SERVICIOS	PAGINA WEB	SERVICIO QUE OFRECEN LOS INSTITUTOS A LA COMUNIDAD EDUCATIVA	PUBLICA	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
	INTERCAMBIO DE DATOS	INTERCAMBIO DE DATOS QUE OFRECEN LOS INSTITUTOS	PUBLICA	MUY ALTA	PRACTICAMENTE SEGURO	CRITICO
SOFTWARE APLICACIONES INFORMATICAS	SISTEMAS OPERATIVOS	VERSIONES DE WINDOWS	PUBLICA	BAJO	POCO PROBABLE	BAJO
	SERVIDOR DE CORREO	SERVIDOR DE CORREO ELECTRONICO	CONFIDENCIAL	MEDIO	POSIBLE	APRECIABLE
	SIGBD	GBD ALMACENA DATOS DE ESTUDIANTES	CONFIDENCIAL	MEDIO	POSIBLE	APRECIABLE
	GESTOR DE MAQUINAS VIRTUALES	VIRTUAL BOX	PUBLICA	BAJO	POCO PROBABLE	BAJO
	SERVIDOR DE APLICACIONES	XAMPP APACHE	PUBLICA	BAJO	POCO PROBABLE	BAJO
EQUIPAMIENTO INFORMATICO	PC PORTATILES	EQUIPOS DE COMPUTO	PUBLICA	MEDIO	POSIBLE	APRECIABLE
REDES	WIFI	RED INALAMBRICA	RESERVADO USO INTERNO	BAJO	POCO PROBABLE	BAJO
	INTERNET	INTERNET	RESERVADO USO INTERNO	BAJO	POCO PROBABLE	BAJO

Fuente: Elaborado por Carlos Bladimir Moreano Guerra, 2019

Por último, con la tabla 5 se ha podido contrastar el cumplimiento de la ISO 27001 con respecto a los activos de la institución educativa donde se llegó a la conclusión que no se contaba con políticas de seguridad adecuadas para proteger su información.

Tabla 5

Control de ISO en la institución educativa

CONTROL ISO	CONTROLES	CUMPLE SI	CUMPLE NO	CONTROL DESCRIPCION
5.1	5.1.1. Politicas para la seguridad de la informacion		X	Se deberia definir un conjunto de politicas para la seguridad de la informacion, aprobada por la direccion, publicada y comunicada a los empleados y partes externas pertinentes.
	5.1.2. Revision de la politica de seguridad de la informacion		X	Las politicas para seguridad de la informacion se deberian revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuacion y eficacia continuas.
6.1	6.1.1. Roles y responsabilidades para la seguridad de informacion.		X	Se deberian definir y asignar todas las responsabilidades de la seguridad de la informacion.
7.1	7.1.1. Investigacion de antecedentes	X		Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberian llevar a cabo de acuerdo con las leyes, reglamentos y etica pertinentes, y deberian ser proporcionales a los requisitos de negocio, a la clasificacion de la informacion a la que se va a tener acceso, y a los riesgos percibidos
	7.2.1. Responsabilidades de la direccion		X	La direccion deberia exigir a todos los empleados y contratistas a la aplicacion de la seguridad de la informacion de acuerdo con las politicas y procedimientos establecidos por la organizacion.
8.2	8.2.1. Clasificacion de la informacion	X		La informacio se deberia clasificar en funcion de los requisitos legales, valor, criticidad y susceptibilidad a divulgacion o a modificacion no autorizada.
	8.2.3. Manejo de activos		X	Se deberian desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificacion de informacion adoptado por la organizacion.
9.1	9.1.1. Politica de control de acceso		X	Se deberia establecer, documentar y revisar una politica de control de acceso con base en los requisitos del negocio de seguridad de la informacion.
	9.1.2. Politica sobre el uso de los servicios de red		X	Solo se deberia permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados especificamente.
	9.2.3. Gestion de derechos de acceso privilegiado		X	Se debera restringir y controlar la asignacion y uso de derechos de acceso privilegiado.
9.4	9.4.1. Restriccion de acceso Informacion	X		El acceso a la informacion y a las funciones de los sistemas de las aplicaciones se deberia restringir de acuerdo con la politica de control de acceso.
	9.4.2. Procedimiento de ingreso seguro		X	Cuando lo requiere la politica de control de acceso, el acceso a sistemas y aplicaciones se deberia controlar mediante un proceso de ingreso seguro.
	9.4.3. Sistema de gestion de contraseñas		X	Los sistemas de gestion de contraseñas deberian ser interactivas y deberian asegurar la calidad de las contraseñas.
	9.4.4. Uso de programas utilitarios privilegiados.		X	Se deberia restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
11	11.1.3. Seguridad de oficinas, recintos e instalaciones.	X		Se deberia diseñar y aplicar seguridad fisica a oficinas, recintos e instalaciones.
	11.1.4. Proteccion contra amenazas externas y ambientales	X		Se deberia diseñar y aplicar proteccion fisica contra desastes naturales, ataques maliciosos o accidentes.
	11.2.2. Servicios de suministro	X		Los equipos se deberian protger contra fallas de energia y otras interrupciones causadas por fallas en los servicios de suministro.
	11.2.4. Mantenimiento de equipos	X		Los equipos se deberian mantener correctamente para asegurar su disponibilidad e integridad continuas.
12	12.1.1. Controles contra codigos maliciosos		X	Se deberian implementar controles de deteccion, de prevencion y de recuperacion, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra codigos maliciosos.
	12.3.1 Respaldo de informacion	X		Se deberian hacer copias de respaldo de la informacion, del software e imagenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una politica de copias de respaldo aceptada.
	12.4.1. Registro de eventos		X	Se deberian elaborar, conservar y revisar regularmente los registros y acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la informacion.
	12.4.2. Proteccion de la informacion de registro	X		Las instalaciones y la informacion de registro se deberian proteger contra alteracion y acceso no autorizado.
	12.5.1. Instalacion de software en sistemas operativos		X	Se deberian implementar procedimientos para controlar la instalacion de software en sistemas operativos.
	12.6.2. Restricciones sobre la instalacion de software		X	Se deberian establecer e implementar las reglas para la instalacion de software por parte de los usuarios.
13	13.1.1. Controles de redes	X		Las redes se deberian gestionar y controlar para proteger la informacion en sistemas y aplicaciones.
	13.2.3. Mensajeria electronica	X		Se deberia proteger adecuadamente la informacion incluida en la mensajeria electronica.
16	16.1.3. Reporte de debilidades de seguridad de la informacion	X		Se deberia exigir a todos los empleados y contratistas que usan los servicios y sistemas de informacion de la organizacion, que observene e informen cualquier debilidad de seguridad de la informacion observada o sospechada en los sistemas o servicios.
17	17.1.2. Implementacion de la continuidad de la seguridad de la informacion	X		La organizacion deberia establecer, documentar, implementar y mantener procesos, procedimientos y controles para segurar el nivel de continuidad requerido para la seguridad de la informacion durante una situacion adversa.
18	18.2.2. Cumplimiento con las politicas y normas de seguridad.		X	Los directores deberian revisar con regularidad el cumplimiento del procesamiento y procedimientos de informacion dentro de su area de responsabilidad, con las politicas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

Fuente: Elaborado por Carlos Bladimir Moreano Guerra, 2019

Al final la aplicación de la ISO 27001 resultó de gran ayuda porque permitió identificar si la información es segura, pudiendo analizar qué controles cumple y cuáles no, y por último en qué grado se encuentra.

ITIL, en forma general, nos ofrece los siguientes beneficios: (Hidalgo Ponce, B. F., Layedra Larrea, N. P., & Ramos Valencia, M. V., 2019)

En el Departamento de TI:

- Tener una clara perspectiva de las capacidades de TI en la realidad con la finalidad de mejorarlas.
- Aumentar los beneficios de los recursos de TI.
- Implantar mecanismos para aprender de experiencias pasadas.

El objetivo de ITIL es que las organizaciones logren la adaptación y con ello producir mejores resultados para sus procesos; al igual, ISO permite obtener servicios que sean bien gestionados, planificados y entregados.

La norma ISO 27001 se puede relacionar con otras normas como COBIT e ITIL, las cuales presentan procesos comunes y se basan en los procesos de las aplicaciones, sistemas de TI y servicios, es por esto que al aplicar COBIT e ISO 27001 se enfocan específicamente en la seguridad de la información (Carlos Bladimir Moreano Guerra, 2019).

Espinosa, G., & Verónica, L., (2018) discrimina que la norma ISO 27001 a comparación de ITIL comprende una perspectiva hacia la gestión de seguridad por medio del mejoramiento o realización de una normativa, pero estos marcos consideran la importancia de los riesgos a la hora de cumplir los objetivos propuestos.

Por lo tanto, al aplicar un Sistema de Gestión de la Seguridad de la Información (SGSI) en instituciones educativas tendrán los siguientes beneficios: (Benavides Sepúlveda, Alejandra & Blandón Jaramillo, Carlos,2018)

- Mejora continua.
- Reducción en los costos de incidentes.
- Mayor confiabilidad.
- Mejoramiento de la imagen institucional.
- Aplicar una metodología de riesgos logrará la identificación y priorización de amenazas y riesgos del sector educación.
- Identificar y establecer cargos con respecto a cada actividad relacionada a la seguridad de la información.

Según una encuesta realizada en la Universidad Nacional de Pereira, se busca ver que tanto la universidad hace el respectivo cumplimiento con los requisitos establecidos en la ISO 27001 y diagnosticar el grado de madurez de los SGSI establecidos actualmente, véase Tabla 6 y Figura 9. (Benavides Sepúlveda, Alejandra & Blandón Jaramillo, Carlos,2018)

Conforme a lo presentado, se evidencia la nula existencia de los sujetos de estudio con respecto a la mejora activa de acciones para dar cumplimiento a la seguridad de información, por lo que es necesario intervenir en este tema para que de esta manera la información se resguarde.

En contraparte, en otros países, en educación, ha habido un aumento constante en el número de instituciones certificadas en ISO 27001, de manera que en 2018 certificadas internacionalmente fueron 137 instituciones, en 2019, su número

Tabla 6

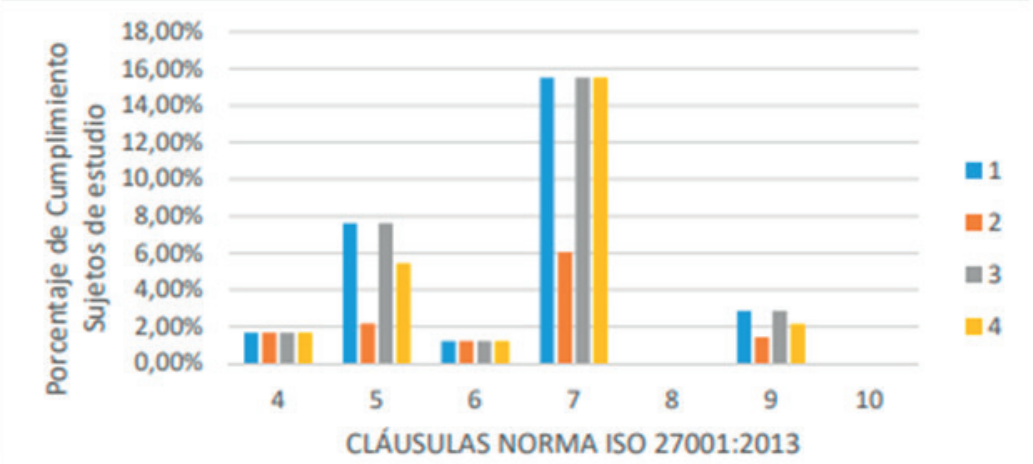
Porcentaje de cumplimiento de los requisitos de la ISO 27001.

CLAUSULAS	SUJETOS DE ESTUDIO COMUNA UNIVERSIDAD			
	1	2	3	4
4. Contexto de la organizacion	1.67%	1.67%	1.67%	1.67%
5. Liderazgo	7.67%	2.17%	7.61%	5.43%
6. Planificacion	1.22%	1.22%	1.22%	1.22%
7. Soporte	15.52%	6.03%	15.52%	15.52%
8. Operacion	0.00%	0.00%	0.00%	0.00%
9. Evaluacion del desempeño	2.86%	1.43%	2.86%	2.14%
10. Mejora	0.00%	0.00%	0.00%	0.00%

Fuente: Elaborado por Benavides Sepúlveda, Alejandra & Blandón Jaramillo, Carlos,2018

Figura 9

Porcentaje de cumplimiento de los requisitos de la ISO 27001.



Fuente: Elaborado por Benavides Sepúlveda, Alejandra & Blandón Jaramillo, Carlos,2018

fue de 176 instituciones certificadas. La mayoría ISO 27001 las instituciones certificadas están en Japón (26), Grecia (30), Italia (11), Polonia (12), la República Checa (11). (Alexei, A., & Technical University of Moldova, 2021); aparte los investigadores recomiendan la creación de un marco de seguridad cibernética que soporte ISO Certificación 27001, para tener valor internacional.

IV. DISCUSIÓN

La revisión sistemática realizada nos permite identificar los beneficios de tener una gestión del sistema de seguridad de información en las instituciones educativas basándose en ITIL e ISO 27001, controlando de mejor manera la gestión de riesgos en la información para mitigar pérdidas, robos y/o alteraciones, recordando así que la seguridad de la información no se trata solo de TI, el estándar ISO 27001 también contiene controles específicos para la gestión de recursos humanos, restricciones legales y organizativas de gestión; declarado por Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sánchez, F., López-Fonseca, G., & Quiroz, D., (2021).

A través del marco de referencia de ITIL y de la mano de la norma ISO 27001, se busca generar la iniciativa para las instituciones educativas para aplicar una gestión del sistema de información, consiguiendo como resultado correctas ayudas para el usuario y la organización, desarrollando una mejora en sus procesos y resguardando su información.

La investigación se realizó en base a las revisiones de los artículos publicados en base de datos Scielo y Google Academy de los últimos cinco años, en donde se observa que el país de Ecuador que cuenta con el mayor número de publicaciones, tal y como se muestra en la Figura 2.

V. CONCLUSIONES

Debido al contexto de la pandemia COVID-19, los docentes y alumnos se vieron obligados a realizar y/o tener clases virtuales, además del personal administrativo que tuvo que realizar sus labores virtualmente, es aquí donde la seguridad de información se vio más afectada, este cambio brusco en los labores diarios a llevado a cierto desconocimiento y vulnerabilidad en la información así como también cambios en los procesos dentro de estas instituciones, por lo que las instituciones educativas debe estar más conscientes de sus necesidades y de los usuarios, es aquí donde más se necesita de ITIL e ISO 27001.

ITIL e ISO 27001 permiten el gestionar de una manera más óptima un sistema de gestión de seguridad de información brindándonos pautas para mejorar la calidad del servicio, mejorando así la imagen institucional, vigilando que la información del estudiante, docente y administrativo permanezca solo dentro de la institución, protegiéndola de ataques cibernéticos mediante la gestión de riesgos aplicando políticas de control de acceso, como se muestra en la Tabla 5.

Además, la norma ISO 27001, nos ayuda a identificar de mejor manera el sistema de seguridad de la información donde los roles y responsabilidades del personal administrativo es de vital importancia para su óptimo funcionamiento, esto nos ayuda a controlar la información que se genera a diario y quién puede acceder a cada parte de esta información; demostrando la importancia de tener una buena gestión de un sistema de seguridad de información con la aplicación de ISO 27001 e ITIL, lo cual conlleva a una mejor calidad de servicio de la institución educativa.

VI. REFERENCIAS BIBLIOGRÁFICAS

[1] Urrútia, G., & Bonfill, X. (2010). Declaración PRISMA: una propuesta para mejorar la publicación de revisiones sistemáticas y metaanálisis. Medicina clínica, 135(11), 507–511. https://doi.org/10.1016/j.medcli.2010.01.015

[2] Álvarez Tay, R. C**.** (2021). Evaluación del nivel de satisfacción del estudiante respecto al servicio educativo bajo el enfoque del modelo HEdPERF en las universidades públicas que integran la Alianza Estratégica de la Universidad Peruana y que implementaron el mecanismo de licenciamiento. Industrial Data, 24(1), 23–47. https://doi.org/10.15381/idata.v24i1.17749

[3] Valencia Morocho, C. A. (2021). La Educación virtual en el pensamiento crítico de los estudiantes universitarios. Desde El Sur Revista de Ciencias Humanas y Sociales de La Universidad Científica Del Sur, 13(2), e0018. https://doi.org/10.21142/des-1302-2021-0018

[4] Hidalgo Ponce, B. F., Layedra Larrea, N. P., & Ramos Valencia, M. V. (2019). Propuesta de mejores prácticas: ITIL para la gestión de las TIC en apoyo a la actividad docente. Ciencia Digital, 3(3.4.), 167–179. https://doi.org/10.33262/cienciadigital.v3i3.4..844

[5] Garzón Cruz, G. F., Merchan Carrillo, J. F., & Morea Vergara, K. J. (2020). Implementación de buenas prácticas basadas en itil 4 e iso 20000 para la gestión de incidentes y reducción de riesgos del service desk de la empresa Ingeal s.a. https://repository.ucc.edu.co/handle/20.500.12494/20122

[6] Carlos Bladimir Moreano Guerra (2019): "Seguridad de la información para instituciones educativas a tercer nivel basado en la ISO/IE27001", Revista Caribeña de Ciencias Sociales (julio 2019). En línea https://www.eumed.net/rev/caribe/2019/07/seguridad-informacion.html

[7] Melgarejo Terán, R. (2018). ITIL V3 para la calidad de los servicios de los usuarios de las instituciones educativas JEC-UGEL-05, 2017. Universidad César Vallejo.

[8] Ríos, B., & Milton, W. (2019). Modelo de análisis para la implantación de un SGSI basado en ISO 27001 y COBIT para una empresa del Sector Educación. Universidad Nacional de San Agustín de Arequipa.

[9] Espinosa, G., & Verónica, L. (2018). Estudio de las normativas de seguridad de la información de instituciones públicas: propuesta de una normativa en una institución de educación superior. Escuela Superior Politécnica de Chimborazo.

[10] Benavides Sepúlveda, Alejandra M., & Blandón Jaramillo, Carlos A. (2017). Modelo de Sistema de Gestión de Seguridad de la Información Basado en la Norma NTC. ISO/IEC 27001 para Instituciones Públicas de Educación Básica de la Comuna. Universidad de la Ciudad de Pereira. https://core.ac.uk/download/pdf/344935889.pdf

[11] Alexei, A., & Technical University of Moldova. (2021). Cyber security strategies for Higher Education Institutions. Journal of Engineering Science, XXVIII (4), 74–92. https://doi.org/10.52326/jes.utm.2021.28(4).07

[12] Merchán-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sánchez, F., López-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: a systematic review. Annals of Telecommunications - Annales Des Télécommunications, 76(3–4), 255–270. https://doi.org/10.1007/s12243-020-00783-2

[13] Estrada Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos Ciencia & Tecnología, 13(3), 98–110. https://doi.org/10.22335/rlct.v13i3.1446

[14] Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. CIT Información

Tecnológica, 32(5), 145–156. https://doi.org/10.4067/s0718-07642021000500145

[15] Olmedo, M. R. M., & Chaves, V. E. J. (2020). Seguridad de la información en plataformas e-learning en tiempos de pandemia COVID-19. Revista UNIDA Científica, 4(1). http://revistacientifica.unida.edu.py/publicaciones/index.php/cientifica/article/view/9

[16] Di Luca, M. A. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. Avances, 21(2), 248–263. https://dialnet.unirioja.es/servlet/articulo?codigo=6989568

Fuentes de financiamiento:

Propia.

Conflictos de interés:

Los autores declaran no tener conflictos de interés.

Contribución de los Autores

Los autores en mención han contribuido conjuntamente en la elaboración del manuscrito, J.Delgado tuvo participación activa en la búsqueda de información y recolección de datos junto con la redacción. E. Guevara llevó a cabo la redacción y el traslado de tablas de la información obtenida. A. Mendoza participó siendo el supervisor y revisor crítico del contenido.