UNIVERSIDAD UTE

FACULTAD DE CIENCIAS DE LA INGENIERÍA E INDUSTRIAS

INGENIERÍA EN INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

DESARROLLO DE UNA GUÍA DE PROTECCIÓN DE DATOS PERSONALES PARA UNIDADES EDUCATIVAS DEL ECUADOR BASADO EN LAS MEJORES PRÁCTICAS INTERNACIONALES

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

JUAN CARLOS ROBAYO ZAMORA

DIRECTOR: ING. JÁCOME CANCHIG SEGUNDO BOLÍVAR

2022

FORMULARIO DE REGISTRO BIBLIOGRÁFICO
TRABAJO DE TITULACIÓN

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD:	1714267125
APELLIDO Y NOMBRES:	JUAN CARLOS ROBAYO ZAMORA
DIRECCIÓN:	Serapio Japerabi S11-29 y Lino Curima
EMAIL:	jrobayoz@gmail.com
TELÉFONO FIJO:	(02) 2669461
TELÉFONO MOVIL:	(593) 995620949

DATOS DE LA OBRA	
TÍTULO:	DESARROLLO DE UNA GUÍA DE PROTECCIÓN DE DATOS PERSONALES PARA UNIDADES EDUCATIVAS DEL ECUADOR BASADO EN LAS MEJORES PRÁCTICAS INTERNACIONALES
AUTOR O AUTORES:	JUAN CARLOS ROBAYO ZAMORA
FECHA DE ENTREGA DEL PROYECTO DE TITULACIÓN:	25 de septiembre del 2022
DIRECTOR DEL PROYECTO DE TITULACIÓN:	ING. JÁCOME CANCHIG SEGUNDO BOLÍVAR
PROGRAMA	PREGRADO [x] POSGRADO [ ]
TÍTULO POR EL QUE OPTA:	INGENIERO EN INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN
RESUMEN:	El presente trabajo de titulación tiene como objetivo principal el desarrollo de una guía de protección de datos personales para unidades educativas del Ecuador basado en las mejores prácticas internacionales utilizando como referencia la reciente norma ISO/IEC 27701:2019 que se caracteriza por ser una extensión de la norma ISO/IEC 27001:2013, lo cual permite la

	gestión de la privacidad de la información con sus respectivos requisitos y directrices que son importantes para que las instituciones puedan mantener la ventaja competitiva, el flujo de capital, la rentabilidad, el cumplimiento de las leyes y la imagen institucional. **Con la reciente aprobación de la ley Orgánica de Protección de Datos Personales en mayo del 2021 se tiene ya una base legal que les permita a las empresas realizar el tratamiento de los datos personales, así como también permite a las personas a tener el derecho de solicitar una copia de la información que se conllevan sobre ellas, incluyendo un detalle de como la información es tratada y si terceros tienen acceso a la información.** **La aplicabilidad de la norma ISO 27701 tiene como requisito que las empresas tengan ya establecido un sistema de gestión de seguridad de la información ISO/IEC 27001 ampliando los esfuerzos necesarios para abarcar la gestión de la privacidad proporcionando el marco del sistema de gestión para la protección de la información de identificación personal.** **La ISO 27701 al requerir la existencia de un sistema de gestión de seguridad de la información al cual adherirse, sin embargo, en organizaciones que no disponen de un sistema de gestión de**

	seguridad de la información con la norma ISO 27001, pueden implementar las dos normas ISO 27001 e ISO 27701 en un solo proyecto. **La aplicación de esta norma dentro de las instituciones educativas permite garantizar un correcto manejo de la información de identificación personal ya que ayuda a afrontar los riesgos específicos de privacidad que se puedan enfrentar entre todos los involucrados ya sean internos o externos.**
PALABRAS CLAVES:	**ISO/IEC 27701:2019**
ABSTRACT:	**The main objective of this degree work is to develop a personal data protection guide for educational institutions in Ecuador based on international best practices using as a reference the recent ISO / IEC 27701: 2019 standard, which is characterized as an extension of the ISO / IEC 27001: 2013 standard, which allows the management of information privacy with its requirements and guidelines that are important for institutions to maintain competitive advantage, capital flow, profitability, compliance with laws and institutional image.** **With the recent approval of the Organic Law on Protection of Personal Data in May 2021, there is already a legal basis that allows companies to process personal data, as well as allows people to have the right to request a copy of the information they**

	carry about them, including a detail of how the information is treated and if third parties have access to the information. **The applicability of the ISO 27701 standard as a requirement that companies already have an ISO / IEC 27001 information security management system in place, expanding the necessary efforts to cover privacy management, testing the management system framework for the protection of personally identifiable information.** **ISO 27701 by requiring the existence of an information security management system to adhere to, however, in organizations that do not have an information security management system with the ISO 27001 standard, they can implement the two standards ISO 27001 and ISO 27701 in a single project.** **The application of this standard within educational institutions allows us to guarantee a correct handling of personally identifiable information as it helps to face the specific privacy risks that may be faced by all those involved, whether internal or external.**
KEYWORDS	**ISO/IEC 27701:2019**

Se autoriza la publicación de este Proyecto de Titulación en el Repositorio Digital de la Institución.

JUAN CARLOS ROBAYO ZAMORA
C.I.: 1714267125

DECLARACIÓN Y AUTORIZACIÓN

Yo, **JUAN CARLOS ROBAYO ZAMORA,** C.I.: 1714267125 autor del trabajo de titulación: **Desarrollo de una guía de protección de datos personales para unidades educativas del Ecuador basado en las mejores prácticas internacionales** previo a la obtención del título de **INGENIERO EN INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN** en la Universidad UTE.

1. Declaro tener pleno conocimiento de la obligación que tienen las Instituciones de Educación Superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación de grado para que sea integrado al Sistema Nacional de información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la BIBLIOTECA de la Universidad UTE a tener una copia del referido trabajo de titulación de grado con el propósito de generar un Repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Quito, 25 de sep. de 2022

JUAN CARLOS ROBAYO ZAMORA
C.I.: 1714267125

DECLARACIÓN JURAMENTADA DEL AUTOR

Yo, **JUAN CARLOS ROBAYO ZAMORA**, portador de la cédula de identidad N° 1714267125, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad UTE puede hacer uso de los derechos correspondientes a este trabajo, según los establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

JUAN CARLOS ROBAYO ZAMORA

C.I.: 1714267125

CERTIFICACIÓN DEL TUTOR

En mi calidad de tutor, certifico que el presente trabajo de titulación que lleva por título **Desarrollo de una guía de protección de datos personales para unidades educativas del Ecuador basado en las mejores prácticas internacionales** para aspirar al título de **INGENIERO EN INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN** fue desarrollado por **JUAN CARLOS ROBAYO ZAMORA,** bajo mi dirección y supervisión, en la Facultad de Ciencias de la Ingeniería e Industrias; y que dicho trabajo cumple con las condiciones requeridas para ser sometido a las evaluación respectiva de acuerdo al reglamento de Trabajos de Titulación artículos 19, 27 y 28.

_____

ING. JÁCOME CANCHIG SEGUNDO BOLÍVAR

DIRECTOR DEL TRABAJO

C.I.: 1707004618

DEDICATORIA

A Dios por ser mi guía y brindarme la sabiduría necesaria para culminar esta etapa de mi vida.

A mis padres Miguel y Elizabeth por todo su apoyo y amor incondicional.

A mi esposa Moni por su paciencia, amor, acompañamiento y por tenerme siempre en tus oraciones.

A mis hijas Mia y Valentina para demostrarles el valor de la perseverancia, ya que con sacrificio se puede alcanzar las metas propuestas.

AGRADECIMIENTOS

Doy gracias a Dios, por brindarme la fuerza, salud e inteligencia para culminar mi carrera y alcanzar la meta propuesta, gracias por la vida de mis padres, porque cada día bendice mi vida con esta oportunidad de estar y tenerlos a mi lado.

A mi esposa Moni y a mi hija Mía por su apoyo que ha sido fundamental y que han estado junto a mí, incluso en los momentos más turbulentos de mi vida. Este proyecto no fue sencillo, pero me motivaron y me ayudaron todos los días, por eso y más se los agradezco muchísimo.

A mi hija Valentina, por su tolerancia, paciencia y por ceder su tiempo para culminar mi meta personal.

A mi familiar y amigo el M.Sc., Remigio Chalán, quien con sus consejos me supo guiar, respaldar e impulsar siempre para salir adelante.

A mis suegros Edith y Alan, cuñado Alitan y cuñadas Nicole y Aine por su apoyo, sabios consejos y por estar a mi lado en los buenos y malos momentos. Los quiero mucho.

Gracias a la vida por este nuevo triunfo, a todos mis familiares que me apoyaron y creyeron en la realización de este proyecto.

ÍNDICE DE CONTENIDO

PÁGINA

ÍNDICE DE CONTENIDO 12
RESUMEN 17
ABSTRACT 18
1. INTRODUCCIÓN 19
1. INTRODUCCIÓN 20
DATOS DE CARÁCTER PERSONAL 21
PERTENENCIA DE LOS DATOS DE CARÁCTER PERSONAL 21
TRATAMIENTO DE DATOS PERSONALES 22
RESPONSABLE DEL TRATAMIENTO DE DATOS 22
ENCARGADO DEL TRATAMIENTO DE DATOS 22
TRANSFERENCIA O COMUNICACIÓN DE DATOS 23
LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) 24
LICITUD, LEALTAD Y TRANSPARENCIA 24
LIMITACIÓN DE LA FINALIDAD 24
MINIMIZACIÓN DE LOS DATOS 24
EXACTITUD 25
LIMITACIÓN DEL PLAZO DE CONSERVACIÓN 25
INTEGRIDAD Y CONFIDENCIALIDAD 25
TRANSPARENCIA E INFORMACIÓN 25
MEDIDAS DE SEGURIDAD 25
SEGURIDAD INFORMÁTICA 26
SEGURIDAD DE LA INFORMACIÓN 26
NORMA ISO/IEC 27001:2013 27
ASPECTOS CLAVE DE LA NORMA ISO/IEC 27701:2019 30
PASOS PARA EL PROCESO DE CERTIFICACIÓN 33
2. METODOLOGÍA 34
2. METODOLOGÍA 35
2.1 FASE 1: PLANTEAMIENTO DEL PROBLEMA 35
2.2 FASE 2. FORMULACIÓN DE HIPÓTESIS 36
2.3 FASE 3: LEVANTAMIENTO DE INFORMACIÓN 37
2.4 FASE 4: ANÁLISIS DE DATOS. 37
2.5 FASE 5: COMPROBACIÓN DE LA HIPÓTESIS 38
2.6 FASE 6: CONCLUSIONES 38
3. ANÁLISIS DE RESULTADOS Y DISCUSIÓN 39
3.1 PLANTEAMIENTO DEL PROBLEMA 42
3.2 FORMULACIÓN DE LA HIPÓTESIS 43
3.3 LEVANTAMIENTO DE LA INFORMACIÓN 43

3.3.1 Fase Planificar. 48
3.3.1.1 CONTEXTO DE LA ORGANIZACIÓN: 48
3.3.1.2 LIDERAZGO: 49
3.3.1.3 PLANIFICACIÓN: 49
3.3.1.4 SOPORTE: 50
3.3.2 Fase Hacer 51
3.3.3 Fase Verificar 51
3.3.4 Fase Actuar 52
3.4 PROPUESTA DE LA GUÍA DE PROTECCIÓN DE DATOS PERSONALES PARA INSTITUCIONES EDUCATIVAS 54
4. CONCLUSIONES Y RECOMENDACIONES 55
4.2 CONCLUSIONES 56
4.3 RECOMENDACIONES 56
5 BIBLIOGRAFÍA 58
6 ANEXOS 61
ANEXO 1. GUÍA DE IMPLANTACIÓN ISO/IEC 27701 62

ÍNDICE DE TABLAS

PÁGINA

TABLA 1. CAPÍTULOS QUE COMPRENDE LA NORMA ISO 27001:2013 28

TABLA 2. FASE PDCA. APARTADOS DE LA ISO 27001:2013.....31

TABLA 3. CLÁUSULAS DE LA NORMA ISO 27701:2019 31

TABLA 4. ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA UE CARDENAL SPELLMAN FEMENINO 40

TABLA 5. PROCESOS DEL PDCA DE LA NORMA ISO 27701:2019 47

TABLA 6. ANEXOS ISO 27701:2019 53

ÍNDICE DE FIGURAS

PÁGINA

FIGURA 1. **DIFERENCIAS ENTRE SEGURIDAD DE LA INFORMACIÓN E INFORMÁTICA. 27**

FIGURA 2. **FASES DE MEJORA CONTINUA DEL PDCA 30**

FIGURA 3. **FASES DEL MÉTODO CIENTÍFICO 35**

FIGURA 4. **INICIATIVAS DE CERTIFICACIÓN EN EDUCACIÓN DE LA REGIÓN 44**

ÍNDICE DE ANEXOS

PÁGINA

ANEXO 1. GUÍA DE IMPLANTACIÓN ISO/IEC 27701 62

RESUMEN

El presente trabajo de titulación tiene como objetivo principal el desarrollo de una guía de protección de datos personales para unidades educativas del Ecuador basado en las mejores prácticas internacionales utilizando como referencia la reciente norma ISO/IEC 27701:2019 que se caracteriza por ser una extensión de la norma ISO/IEC 27001:2013, lo cual permite la gestión de la privacidad de la información con sus respectivos requisitos y directrices que son importantes para que las instituciones puedan mantener la ventaja competitiva, el flujo de capital, la rentabilidad, el cumplimiento de las leyes y la imagen institucional.

Con la reciente aprobación de la ley Orgánica de Protección de Datos Personales en mayo del 2021 se tiene ya una base legal que les permita a las empresas realizar el tratamiento de los datos personales, así como también permite a las personas a tener el derecho de solicitar una copia de la información que se conllevan sobre ellas, incluyendo un detalle de como la información es tratada y si terceros tienen acceso a la información.

La aplicabilidad de la norma ISO 27701 tiene como requisito que las empresas tengan ya establecido un sistema de gestión de seguridad de la información ISO/IEC 27001 ampliando los esfuerzos necesarios para abarcar la gestión de la privacidad proporcionando el marco del sistema de gestión para la protección de la información de identificación personal.

La ISO 27701 requiere la existencia de un sistema de gestión de seguridad de la información al cual adherirse, sin embargo, en organizaciones que no disponen de un sistema de gestión de seguridad de la información con la norma ISO 27001, pueden implementar las dos normas ISO 27001 e ISO 27701 en un solo proyecto.

La aplicación de esta norma dentro de las instituciones educativas permite garantizar un correcto manejo de la información de identificación personal ya que ayuda a afrontar los riesgos específicos de privacidad que se puedan enfrentar entre todos los involucrados ya sean internos o externos.

ABSTRACT

The main objective of this degree work is to develop a personal data protection guide for educational institutions in Ecuador based on international best practices using as a reference the recent ISO / IEC 27701: 2019 standard, which is characterized as an extension of the ISO / IEC 27001: 2013 standard, which allows the management of information privacy with its requirements and guidelines that are important for institutions to maintain competitive advantage, capital flow, profitability, compliance with laws and institutional image.

With the recent approval of the Organic Law on Protection of Personal Data in May 2021, there is already a legal basis that allows companies to process personal data, as well as allows people to have the right to request a copy of the information they carry about them, including a detail of how the information is treated and if third parties have access to the information.

The applicability of the ISO 27701 standard as a requirement that companies already have an ISO / IEC 27001 information security management system in place, expanding the necessary efforts to cover privacy management, testing the management system framework for the protection of personally identifiable information.

ISO 27701 by requiring the existence of an information security management system to adhere to, however, in organizations that do not have an information security management system with the ISO 27001 standard, they can implement the two standards ISO 27001 and ISO 27701 in a single project.

The application of this standard within educational institutions allows us to guarantee a correct handling of personally identifiable information as it helps to face the specific privacy risks that may be faced by all those involved, whether internal or external.

1. INTRODUCCIÓN

1. INTRODUCCIÓN

Las unidades educativas del Ecuador ejercen un papel muy importante en el desarrollo y proceso de la sociedad, por tal razón tienen encomendada la tarea de desarrollar el aprendizaje y dotar de competencias a sus alumnos a través de docentes calificados.

En la actualidad cada vez más las personas tienen la necesidad de tener acceso a la tecnología para conocer más del mundo, mantenerse informados en todo momento, y así mismo el uso de Internet para adquirir nuevos conocimientos dentro del área educativa, uso de redes sociales, entre otros.

En el Ecuador la falta de aplicación de estándares de seguridad de información aplicado a los datos personales sensibles que las unidades educativas gestionan puede dar como resultado la exposición de estos datos, y la falta de herramientas legales que permita asegurar la aplicación de estos estándares podría terminar por fuertes afectaciones a los derechos fundamentales de los titulares de dicha información. La organización ISO mediante encuestas a diferentes paises de latinoamerica muestra quienes tiene aplicado las diferentes normas como una referencia de cual es el estado en base a la protección y privacidad de la información.

Los avances tecnológicos que existen en la actualidad y los mecanismos que se dispone para comunicarse, exponen la información de nuestra vida personal privada, la cual podemos encontrar en diferentes partes si no se toman las medidas de control y seguridad adecuadas.

Diferenciando los distintos conceptos existentes se puede decir que los datos personales son la información confidencial e íntima de una persona, los cuales si no son bien manejadas pueden ser filtradas y ser mal utilizadas por personas mal intencionadas.

En materia de los centros educativos privados del sector Belisario Quevedo del distrito metropolitano de la ciudad de Quito, cuyo fin es el de ejecutar el derecho fundamental a la educación, deben proteger la información personal a pesar de que no constituye como su actividad principal, por lo que se generan dudas de cómo aplicar las diferentes regulaciones existentes, además de que estas tienen a cargo la información en sus bases de datos y pueden manipularlas sin mayores restricciones que sus intereses.

Por lo antes indicado, el alto riesgo del mal uso o posible filtración de los datos personales correspondientes a los estudiantes, padres de familia, empleados o proveedores de las unidades educativas es latente ya que están sujetas al

mal uso como la exposición, estafa, lucro ilícito e ilegítimo sin el debido consentimiento.

Por lo tanto, para poder elaborar una guía de protección de datos personales para unidades educativas, es importante hacer una revisión del documento de la ley orgánica de protección de datos personales, aprobada el 9 de noviembre de 2020.

Datos de carácter personal

Los datos de carácter personal son toda información correspondiente a una persona física que sea identificada o identificable; toda persona cuya identidad se pueda determinar, ya sea directa o indirectamente, mediante un identificador como lo es sus nombres y apellidos del alumno y la de sus padres, cédulas de identidad, números telefónicos o correo electrónico, y también lo son las imágenes de los alumnos.

Existen categorías especiales de los datos que en las unidades educativas suelen ser solicitados que sean especialmente sensibles ya que pueden revelar o informar sobre su entorno más íntimo y personal. Por tal razón se les debe prestar especial atención.

Dentro de esta categoría de datos especiales son aquellos que:

- Revelen información ideológica, religiosa o de creencias
- Tengan referencia a la salud y a la vida sexual
- Sean datos genéticos y biométricos.

En el sector educativo es muy frecuente que la información sobre la salud física y mental de los alumnos se incluya para que se puedan prestar servicios de atención médica. Dicha información incluye datos relacionados con lesiones o enfermedades que pudieran sufrir los alumnos durante su permanencia en el centro educativo.

Pertenencia de los datos de carácter personal

Los datos de carácter personal corresponden a la persona física que es la titular de los datos, tales como:

- Alumnos
- Padres de familia
- Tutores
- Personal administrativo

- Docentes
- Personal de servicios

Tratamiento de datos personales

Al momento de realizar el proceso de matriculación al inicio del periodo escolar en una institución educativa sea o no automatizado se realiza la recogida de los datos de los padres de familia y del alumno el cual es un ejemplo claro del tratamiento de datos de carácter personal. Así mismo se considera dentro del tratamiento de los datos personales lo que comprende al mantenimiento y actualización de las fichas o expedientes de los alumnos.

Otras actividades en las que se considera dentro del tratamiento de datos:

- Recogida
- Registro
- Organización
- Estructuración
- Conservación
- Adaptación o modificación
- Extracción
- Consulta
- Utilización
- Difusión
- Supresión o destrucción

Responsable del tratamiento de datos

La ley orgánica de protección de datos personales menciona …*"**Responsable del tratamiento de datos personales:** Persona natural o jurídica, pública o privada, que decide sobre la finalidad y tratamiento de datos personales"…* (LOPD, 2020).

Dependiendo del tipo de unidad educativa la designación del responsable se define en caso de ser fiscal o pública por parte de la administración pública correspondiente. En caso de privadas los responsables de los datos se encargan de designar en la misma unidad educativa.

Encargado del tratamiento de datos

De acuerdo con lo establecido en la ley orgánica de protección de datos personales ecuatoriano menciona que …*"**Encargado del tratamiento de***

datos personales: *Persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales."…* (LOPD, 2020)

Las unidades educativas dentro de sus actividades cuentan también con los siguientes servicios:

- Servicio de comedor
- Servicio médico
- Transporte
- Otras

Estas actividades adicionales que ofrecen las unidades educativas necesitan contar con la colaboración de personas o entidades que no forman parte de esta organización.

Estas entidades o personas externas para poder brindar de manera correcta sus servicios también deben tratar los datos de carácter personal ya bien sea de los alumnos o inclusive de los padres de familia o sus tutores; actividad que debe ser llevada por encargo del responsable del tratamiento de datos, es decir de la unidad educativa o de la administración de educación pública del país.

Para que la prestación de servicios en donde será necesario el tratamiento de los datos implica que debe regirse por un contrato en que se especifiquen las garantías correspondientes y adecuadas como, por ejemplo:

- La obligación de que el encargado del tratamiento de los datos sea únicamente en conformidad a las instrucciones de la unidad educativa o el responsable del tratamiento de los datos.
- Las medidas adecuadas de seguridad que se vayan a implementar por el encargado del tratamiento de los datos.
- Los datos personales que se vayan a tratar por parte del encargado no los utilicen para otras finalidades distintas a las que se estipulan en el contrato.
- Una vez finalizado el contrato de servicios se deberá realizar la devolución de los datos al responsable designado del tratamiento, o también una vez finalizado se proceda a su destrucción. (Rodríguez, 2011)

Transferencia o comunicación de datos

*"**Transferencia o comunicación:** Manifestación, declaración, publicación, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que han de comunicarse deben ser exactos, completos y actualizados"* (LOPD, 2020).

Quienes reciben los datos están entre autoridades públicas, personas físicas o jurídicas, en este caso la unidad educativa por motivo de que el alumno cambia de una unidad educativa a otra, al momento de su matrícula se produce la comunicación de datos.

No se considera comunicaciones o transferencias de datos cuando estas son a empresas que mediante un contrato prestan servicios a la unidad educativa como, por ejemplo, transporte, alimentación en comedores dentro de la institución o servicios médicos. (Bittemple, 1999)

Ley Orgánica de Protección de Datos Personales (LOPDP)

La ley orgánica de protección de datos personales entró en vigor el 11 de mayo del 2021 aprobado por la asamblea nacional del Ecuador en donde se menciona que los responsables del tratamiento de los datos deben realizarse respetando en todo momento los principios establecidos los cuales se revisará para la aplicación en el entorno educativo. (LOPD, 2020)

Licitud, lealtad y transparencia

Al hablar de datos personales en relación con el titular estos deben ser tratados con licitud, leales y transparentes.

> Al momento de recoger los datos personales estos deben ser los estrictamente necesarios para la finalidad legítima y que sean requeridos para cada caso en específico como por ejemplo la educación y orientación de los alumnos de la unidad educativa y no se pueden recoger de manera fraudulenta. (García-Valdecasas, 2018)

Limitación de la finalidad

Toda información recogida por la unidad educativa debe ser informada y de conocimiento de sus titulares. Si los datos personales que sea recogidos para el proceso de matriculación, no se podrán utilizar para otras finalidades que sean diferentes , como la publicación de fotografías de los alumnos en la página web de institución, o el compartir la información de los datos en momento de realizar visitas a museos o empresas que organizan visitas a entidades externas, salvo que tras haber informado con anterioridad y se haya recabado el consentimiento de los tutores, padres de familia o de los alumnos. (García-Valdecasas, 2018)

Minimización de los datos

La minimización de los datos consiste en que toda la información de los datos personales recogidos debe mantenerse al mínimo, es decir que, cuando una unidad educativa recopile información deben recabar lo estrictamente

necesario y específicamente, deben estar relacionados con el fin para los que se requieran. (LOPD, 2020)

Exactitud

Los datos recogidos deben ser precisos y actualizados. Esto quiere decir que también la información debe mantenerse constantemente actualizados, por lo que regularmente el responsable de los datos debe revisar y actualizar esta información ya que puede afectar a la gestión académica o podría sufrir de una revelación indebida de datos a terceras personas. Todos aquellos datos que sean inexactos el responsable debe eliminarlos inmediatamente. (Botín, 2020)

Limitación del plazo de conservación

Al almacenar los datos, el responsable debe determinar el tiempo por el cual se van a guardar para los fines de tratamiento de datos personales, caso contrario se deben eliminar los datos innecesarios.

Integridad y confidencialidad

El responsable del tratamiento de los datos debe brindar todas las medidas de seguridad técnicamente hablando para evitar la pérdida o robo de los datos sea este de manera interna o externa.

Transparencia e información

Durante cualquier proceso que realice la unidad educativa al momento de recabar información de datos personales de los interesados, inclusive cuando no sea necesario su consentimiento, deben brindar la siguiente información:

- Existencia de un tratamiento de los datos personales
- El motivo por el cual se obtiene la información de los datos y su licitud.
- La obligatoriedad o no de facilitar la información de los datos y de las consecuencias que conlleva a no entregarlas.
- El destino de los datos
- Los derechos de la parte interesada y donde ejercitarlos.
- La identificación del responsable del tratamiento de los datos quien sería la unidad educativa o la administración de esta.

Medidas de seguridad

En el artículo 18 del proyecto de ley orgánica de protección de datos personales del Ecuador menciona que *"**Articulo 18. Seguridad de datos personales:** Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas*

y necesarias, sean estas técnicas, organizativas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, perdidas, alteraciones, destrucción o comunicación accidental o ilícita, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto." (LOPD, 2020)

Este trabajo tiene como objetivo, elaborar una guía de protección de datos personales aplicado a las unidades educativas primarias particulares, basado en las mejores prácticas internacionales para el correcto tratamiento de los datos en conjunto con recomendaciones de la RGPD en políticas de control de acceso en donde se indicará el cómo administrar el acceso a los sistemas y la información, así como también políticas de cómo administrar y asegurar la red.

Seguridad Informática

Es una disciplina cuyo fin es el de enfocarse en establecer políticas de seguridad de los dispositivos informáticos por medio de herramientas de seguridad como los firewalls, antimalware, o software de control basado en usuarios.

Seguridad de la Información

Es una ciencia que se encarga de brindar resguardo y protección de la información juntamente con el correcto tratamiento de los datos que se encuentran alojados en un sistema y que son utilizados por una organización mediante los correspondientes niveles de seguridad al crear, usar, almacenar, transmitir, recuperar y disposición final de la misma.

La Figura 1 hablando de ciberseguridad se muestra las diferencias entre los términos de seguridad de la información y la seguridad informática para comprender las diferencias entre los medios que nos permiten asegurar la información respecto a con que medios físicos y tecnológicos podemos realizarlos.

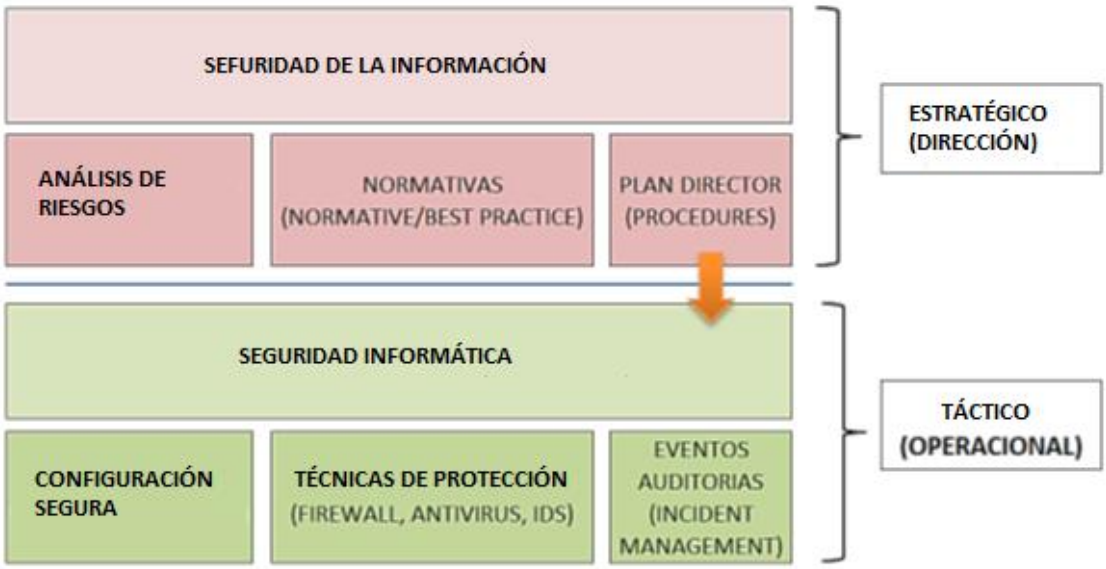

Figura 1. Diferencias entre seguridad de la Información e Informática.

Fuente: Tomado de www.seguridadparatodos.es/seguridad informática o seguridad

Las normas ISO son desarrolladas por la Organización Internacional de Normalización (ISO – por sus siglas en inglés), la cual es una secuencia de patrones, y que se pueden aglomerar por familias según varios aspectos relacionados con calidad y orientado a ordenar la gestión de una empresa.

Existen varias normas publicadas por la ISO pero dentro de las que vamos a considerar para la siguiente guía es la normativa que está relacionada con la gestión de la seguridad.

En el sector TIC (tecnologías de la información y comunicación) la norma ISO que vamos a tratar es la ISO 27001:2013 la cual corresponde a un estándar internacional que se encarga de la gestión de la seguridad de la información de una empresa o una organización. En esta se determinan los requerimientos que deben cumplirse tanto organizaciones privadas, publicas, ya sean grandes o pequeñas, para que la seguridad tanto lógica como física se mejore continuamente de un Sistema de Gestión de Seguridad de la Información (SGSI).

Norma ISO/IEC 27001:2013

La norma de estándar internacional ISO/IEC 27001:2013, gestiona el tratamiento de la seguridad de la información de una empresa u organización.

Con esta norma se podrá determinar los requerimientos necesarios que deberán cumplir cualquier tipo de empresa ya sea privada, publica, grande o

pequeña, con el fin de mejorar continuamente la seguridad tanto física como lógica de la información de un SGSI.

La referencia 2013 menciona que esta corresponde al año de publicación de la revisión más actual y por tal razón se muestra como ISO/IEC 27001:2013. Esta norma está compuesta por varios objetivos de seguridad que recogen aquellos que son fundamentales de analizar para la prevención, detección y mitigación de amenazas que puedan afectar a la información de las empresas.

La norma ISO/IEC 27001:2013 se divide en 11 capítulos, además del Anexo "A", las secciones 0 a 3 son introductorias y opcionales en la implementación, 4 a 10 son obligatorias para la implementación en una organización.

En la Tabla 1 se muestra las características de cada uno de los capítulos de la última edición de la norma ISO 27001:2013. El objetivo principal de tener los capítulos dentro de la norma es la de facilitar la integración de las unidades educativas o de las empresas en general a las normas de gestión de la familia ISO. La norma se apoya sobre el modelo PDCA y se considera como un sistema de gestión de seguridad de la información.

Tabla 1. Capítulos que comprende la norma ISO 27001:2013

Capítulo 0	**Introducción**	**El modelo PDCA (Planificar, hacer, verificar, actuar) es considerado como un SGSI.**
Capítulo 1	Alcance	Es necesario y de obligación el cumplir con los requisitos establecidos entre los capítulos cuatro al diez para que se pueda obtener una aprobación de cumplimiento y así poder certificarse.
Capítulo 2	Referencias Normativas	Se incluye todos los nuevos términos y definiciones necesarios como referencia normativa.
Capítulo 3	Términos y definiciones	Este capítulo contiene la guía de términos y definiciones.
Capítulo 4	Contexto de la organización	Se podrá identificar todos los problemas internos y externos de la organización.
Capítulo 5	Liderazgo	Liderazgo y el compromiso de las altas direcciones de la organización.
Capítulo 6	Planeación	Se organiza los roles, se abordan riesgos y oportunidades. Lograr la mejora continua

Capítulo 7	Soporte	Como con esta mejora continua se implementa a través de recursos, personal competente, comunicación y conciencia de las partes interesadas.
Capítulo 8	Operación	Se realiza la evaluación de los riesgos
Capítulo 9	Evaluación del desempeño	Se realiza el seguimiento, medición, análisis y evaluación por medio de auditorías internas.
Capítulo 10	Mejora	Cuando durante el ejercicio exista no conformidad, se deben aplicar acciones correctivas para evitar que estas se repitan.

Ante la continua actividad a través de la red e Internet en las unidades educativas se están entregando regularmente información de nuestros datos personales y en algunos casos esta información se expone sin tener conocimiento de ello. Debido a esto se han desarrollado nuevas normas y leyes que tiene como objetivo regular el tratamiento de los datos personales para poder garantizar la protección de estos.

Debido a la necesidad de las organizaciones de certificar la gestión de la privacidad de la información y como extensión de las normas ISO 27001 y ISO 27002 nace la norma ISO/IEC 27701:2019 la cual especifica mediante una mejora continua el establecer, implementar, mantener y mejorar el PIMS (Sistema de Gestión de Información de Privacidad).

La norma ISO/IEC 27701:2019 ayuda a reducir los riesgos de privacidad al momento de tratar los datos personales o información de identificación personal. La norma diseñada para ser de uso por el responsable y encargado del tratamiento de los datos personales.

En esta guía vamos a tratar en cómo abordar el cumplimiento de la norma ISO/IEC 27701:2019 siempre que una organización, o en este caso la unidad educativa haya cumplido correctamente la ISO/IEC 27001:2013

Como finalidad de la certificación es importante conocer que este es un mecanismo que permite formalizar la demostración del cumplimiento de la seguridad y privacidad de la información, cuyo funcionamiento se orienta a los resultados y el cumplimiento de objetivos.

Para tener una aproximación a la ISO/IEC 27701:2019 se requiere una certificación inicial o también puede ser conjunta con la ISO 27001.

Aspectos clave de la norma ISO/IEC 27701:2019

Previamente a trabajar en el desarrollo del proceso de implantación de la norma ISO/IEC 27701:2019 debemos partir de las siguientes premisas básicas:

- Las normas ISO no son una regulación, sino más bien una guía de mejores prácticas.
- Los sistemas de gestión de seguridad de la información requieren de un compromiso con la mejora continua.
- Se debe validar su cumplimiento cuando se trata de cláusulas y controles que son catalogados como requisitos.
- La ISO 27001 indica como implementar un sistema de gestión y contiene un anexo A de tipo normativo que indica la descripción de los controles de seguridad referenciado a la ISO 27002.
- La ISO 27002 tiene la descripción de controles y dispone de la guía de implementación para ayudarlo aponer en marcha.

Para entender la ruta de un Sistema de Gestión de Seguridad de la Información SGSI la norma ISO/IEC 27001:2013 describe cómo construir el proceso de mejora continua, así como se muestra en la siguiente gráfica en la que se observa la ejecución constante de acciones que ayudan a mejorar los procesos de cualquier organización y cuyo objetivo es minimizar al máximo los márgenes de error y de perdidas.

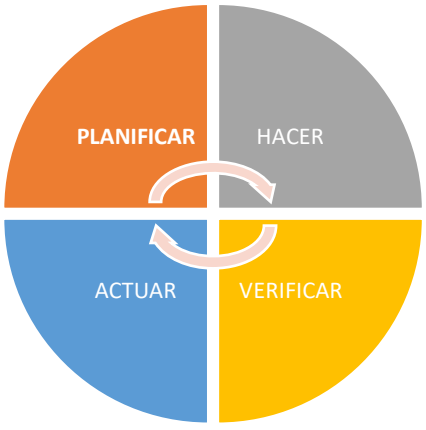

Figura 2. Fases de mejora continua del PDCA

En la tabla 2 se detalla en base al proceso de mejora continua PDCA del ciclo de Deming a los capítulos o apartados de la norma ISO 27001 que se asocian a cada una de las fases.

Tabla 2. Fase PDCA. Apartados de la ISO 27001:2013

FASE PDCA	Apartados de la ISO 27001:2013
Planear	4. Contexto
	5. Liderazgo
	6. Planeación
	7. Soporte
Hacer	8. Operación
Verificar	9. Evaluación del Desempeño
Actuar	10. Mejora

En la norma ISO/IEC 27701:2019 existen cláusulas que son extendidas de la norma ISO/IEC 27001:2013 como se muestran a continuación

La Tabla 3 se muestra las cláusulas de la norma ISO 27701:2019 con la descripción que suman requisitos en las normas ISO 27001 y ISO 27002. El objetivo de la extensión de la ISO27001 con la ISO 27701 es la de incorporar consideraciones relativas a la información de identificación personal necesarios para poder cubrir la ley orgánica de protección de datos personales ecuatoriano.

Tabla 3. Cláusulas de la norma ISO 27701:2019

Cláusula	Cláusulas de la norma ISO 27701
1	Alcance
2	Normativas de referencia
3	Términos, definiciones y abreviaturas
4	General
5	Requisitos específicos de los SGPD relativos a ISO27001
6	Requisitos específicos de los SGPD relativos a ISO27002
7	Medidas adicionales a los responsables de tratamiento
8	Medidas adicionales a los encargados de tratamiento
Anexo A (Normativo)	Objetivos de control y controles específicos para los responsables de tratamiento
Anexo B (Normativo)	Objetivos de control y controles específicos para los encargados de tratamiento
Resto Anexos	Anexos C a F (Informativos): Mapeos de ISO27701 con ISO 29100, el RGPD, la ISO 27018 e ISO 29151

Para implementar de manera adecuada la norma ISO/IEC 27701:2019 las unidades educativas privadas deben tener claro el escenario previo para su implementación para la privacidad de la información. Para ello se dispone de tres opciones:

- **Opción A:** La unidad educativa dispone ya de un SGSI certificado con ISO 27001.

  En este escenario la situación inicial es la más beneficiosa ya que la norma ISO 27701 se la entiende como una extensión de la norma ISO 27001, y por lo tanto esta norma requiere de su existencia previa y así mismo se deben incorporar únicamente los nuevos requisitos para que se pueda construir el sistema de gestión de información de privacidad (PIMS) ISO/IEC 27701:2019

- **Opción B:** La unidad educativa dispone de un sistema de gestión previo de otras normas (ISO9001, ISO14001; ISO20001)

  En este escenario las unidades educativas ya disponen de experiencia en el manejo de los sistemas de gestión y conocen el modelo de mejora continua PDCA

  Las unidades educativas deben contemplar los ajustes necesarios que correspondan en los procesos generales de gestión como son: Control de documentación, auditoria y revisión por dirección.

  Para aplicar esta reciente norma ISO/IEC 27701:2019 debe primeramente construir el SGSI bajo la norma ISO/IEC 27001:2013 e ir añadiendo de manera simultánea los requisitos que se establecen en la norma ISO 27701.

- **Opción C:** No dispone ningún sistema de gestión previo.

  Si la unidad educativa no dispone de un sistema de gestión previo o parte de cero, debe implantar un proceso de gestión basado en mejora continua y construir el SGSI bajo la norma ISO/IEC 27001:2013 las cuales ya existen guías practicas e ir añadiendo de manera simultánea los requisitos que se establecen en la norma ISO 27701.

Pasos para el proceso de certificación

- **Análisis de la ISO 27701:** La unidad educativa debe prepararse para una auditoria final la cual llevara un análisis diferenciado donde se verificarán si los procesos y controles necesarios se han desarrollado de la ISO/IEC 27701:2019

- **Auditoría formal de certificación:** El auditor verificará los procedimientos y controles dentro de la unidad educativa para asegurarse de que funciones de manera adecuada y efectiva en base a los requisitos establecidos por la ISO/IEC 27701:2019 para que se pueda obtener la certificación.

- **Obtención del certificado:** El momento en que la organización obtiene su certificación de la ISO/IEC 27701:2019 el cual tiene valides de tres años la unidad educativa puede usar esta marca de certificación para demostrar que esta se encuentra certificada.

Por lo antes expuesto, el objetivo de este trabajo es la de elaborar una guía de protección de datos personales para unidades educativas del Ecuador basado en las mejores prácticas internacionales, para lo cual es importante primeramente el aplicar una metodología de investigación adecuada para apoyar a las unidades educativas al cumplimiento de las normativas de seguridad y privacidad de la información en apoyo con la ley orgánica de protección de datos personales.

Se realizará una investigación de levantamiento de información por medio de diferentes técnicas como la observación, consultas y revisión basado en las mejores prácticas.

2. METODOLOGÍA

2. METODOLOGÍA

Como se indica en la Figura 3, para el desarrollo de este trabajo se aplicó el método científico, el mismo que consta de las siguientes fases:

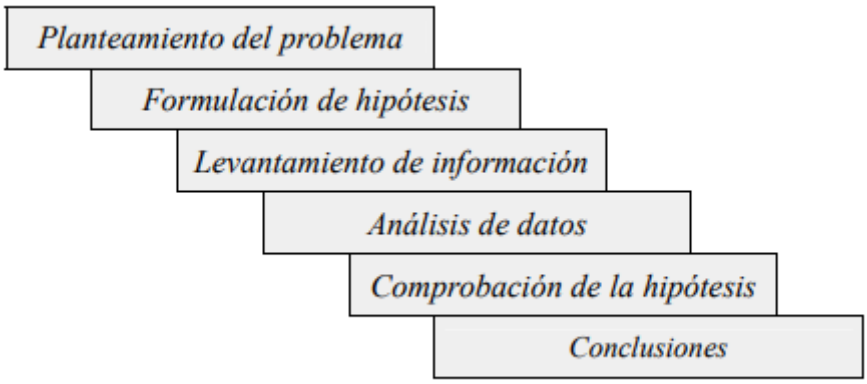

Figura 3. Fases del método científico

Fuente: (Bunce, 1996 y Muñoz 1998)

2.1 Fase 1: Planteamiento del problema

La ley orgánica de protección de datos personales del Ecuador fue aprobada en mayo del 2021 por lo que en lo que se refiere a unidades educativas al tratar información de carácter personal deben tener la capacidad de poder demostrar el cumplimiento de la ley cuando el ente regulador lo requiera, lo cual implica cambios en los procesos de manejo de la información personal tanto en el ámbito legal como en lo tecnológico.

Todas las empresas del sector tanto público y privado en el campo de la tecnología de la información enfrentan diversos riesgos que amenazan su información crítica para el negocio, estos riesgos están respaldados por hardware, software, personal y redes. La protección y la privacidad de la información en sus tres aspectos: confidencialidad, integridad y disponibilidad son muy importantes para mantener la ventaja competitiva, el flujo de capital, la rentabilidad, el cumplimiento de las leyes y la imagen empresarial.

Con la LOPD actualmente aprobada ¿Cuáles serían los beneficios de contar con un sistema de gestión de seguridad de la información?

En la organización: la certificación le permite tener un control para asegurar que la información del cliente está protegida, reducir el impacto de los riesgos

relacionados con los activos de información e implementar medidas de emergencia para asegurar la continuidad del negocio, obteniendo así un plan de ventaja empresarial superior a la competencia en el mercado.

En lo legal: En la actualidad ya se encuentra aprobada al LOPD en el Ecuador por lo que habrá más requerimientos asociados con la seguridad y privacidad de la información. Lo positivo es que ya existen las guías y metodologías para implementar una ISO 27001 que ayudara al tema de seguridad. Hablando de privacidad de la información la reciente ISO 27701 nos permitirá con base a una certificación ISO 27001 a reducir los riesgos de privacidad al momento de tratar los datos personales o información de identificación personal.

En lo económico: La filosofía de la ISO 27701 es la de evitar que se produzcan incidentes sobre la seguridad y privacidad de la información, ya sean estos pequeños o grandes ya que al final involucran un valor económico.

En lo tecnológico: Permitirá la adopción de nuevas tecnologías.

En los empleados: Proporciona a los empleados una constante capacitación lo que conlleva a crecimiento, mejoras en el salario y continuidad laboral.

Para poder cumplir con la LODPDP la norma ISO 27701 permitirá a las unidades educativas y empresas en general a cubrir la ley de la mejor manera. Previamente es necesario conocer el estado actual de como mantienen la confidencialidad, integridad y disponibilidad de los sistemas de información.

2.2 Fase 2. Formulación de hipótesis

Mediante una investigación bibliográfica acudiendo a sitios web como la organización internacional de estandarización ISO por sus siglas en inglés se pudo determinar que en las unidades educativas la falta de implementación de las normas de seguridad y privacidad de la información pueden provocar riesgos de pérdidas de información que conlleven a pérdidas económicas.

La falta de normas trae como consecuencia que todos los riesgos asociados a los activos de información puedan causar daños o paralizar operaciones de las empresas.

2.3 Fase 3: Levantamiento de información

Para la obtención de la información nos basaremos en la técnica de revisión de información:

- Documentación legislativa
- Documentación de la norma ISO 27001
- Documentación de la norma ISO 27701
- Ley orgánica de protección de datos aprobada en el Ecuador
- Investigación exploratoria mediante el levantamiento de información sobre el tratamiento de datos personales en las unidades educativas tomando como referencia las que se encuentran en el sector Belisario Quevedo del distrito metropolitano de Quito y poder determinar las condiciones actuales de la seguridad de la información.

2.4 Fase 4: Análisis de datos.

El análisis de los resultados nos permitirá interpretar de manera adecuada basada en el marco teórico como están las unidades educativas respecto a si están preparadas para estar acorde a lo que exige la LODPDP y a la ISO27701.

Hoy en día la amenaza más cercana está dentro de la misma empresa ya sea por medio de accesos no autorizados o indebidos a la información o que también no tenga los parámetros correctos de privacidad de esta, y que sumado a ataques de tipo informático que pueden ser explotados intencionalmente o por desconocimiento de los propios empleados, puedan ser objeto de robo, manipulación o perdida de la información personal.

La norma ISO 27701 al ser aplicable para todo tipo de empresa proporciona orientación para las organizaciones que sean responsables del procesamiento de la información de identificación personal dentro de un sistema de gestión de seguridad de la información.

Con la información de la norma ISO 27701 obtenemos los siguientes beneficios:

- Generar confianza en la gestión de la información personal
- Cumplimiento de las normas de privacidad de la información
- Facilita acuerdos comerciales
- Los roles y responsabilidades son correctamente definidos
- Se proporciona transparencia entre todas las partes interesadas.

2.5 Fase 5: Comprobación de la hipótesis

Al disponer de una guía basada en la norma ISO 27701 se podrá garantizar los niveles de integridad, disponibilidad y confidencialidad de la información acorde a los requisitos de la empresa.

Los mecanismos de control y procedimientos de seguridad logran que todos los procesos de seguridad y privacidad de la información se realicen de manera segura.

2.6 Fase 6: Conclusiones

Con el apoyo de la guía de implantación de la norma ISO27701 la cual brinda transparencia y confianza al mercado los cuales son dos aspectos que son fundamentales en la actualidad ya que aporta:

- Ventajas competitivas al brindar la seguridad de que los datos van a ser gestionados de manera correcta
- Anticipación de errores por medio de la detección que la norma aporta tanto a oportunidades como amenazas externas, así como las debilidades y fortalezas.
- Mejora continua para garantizar la supervivencia de las empresas en el mercado.
- Se minimiza la perdida de la información ya que estos son uno de los activos más valiosos de las organizaciones en la actualidad.

Además, como se indicó en la introducción, se utilizó la norma ISO/IEC 27701 la misma que ayudo a facilitar la implementación de buenas prácticas en la creación y gestión de datos de información personal en las empresas ya que se trata de una normativa con controles de seguridad más adecuados para las unidades educativas y empresas en general.

3. ANÁLISIS DE RESULTADOS Y DISCUSIÓN

3. ANALISIS DE RESULTADOS Y DISCUSIÓN

Las unidades educativas que se encuentran distribuidas en el sector de Belisario Quevedo del Distrito Metropolitano de Quito, al ser establecimientos educativos que manejan información de carácter personal tanto externos como internos, cuentan con departamentos de sistemas que dan soporte a los sistemas de información y comunicación y a los usuarios.

Ante la llegada de la LODPDP se debe buscar las mejoras para los sistemas de información y comunicación para brindar el descubrimiento, protección y gobierno de la información personal para estar acorde a lo que nos exige la ley.

En la tabla 4 en el establecimiento educativo Cardenal Spellman Femenino mediante el levantamiento de información por medio de diferentes técnicas como la observación, consultas y revisión se pudo verificar que existen procedimientos respecto a temas de seguridad de la información y seguridad informática, basado en los siguientes controles de la ISO 27001

Tabla 4. Estado actual de la seguridad de la información en la UE Cardenal Spellman Femenino

Controles de la norma ISO 27001	**Gestión de la información encontrado en las unidades educativas del sector Belisario Quevedo del DMQ UE Cardenal Spellman Femenino**
Política de Seguridad	• No se posee un manual de políticas de seguridad de la información, pero si tiene controles por medio de software que limita los accesos no autorizados a la información. • Las áreas de caja, compras y cobranzas manejan procedimientos de manera formal.
Organización de seguridad de la información	• Existe la predisposición de la autoridad principal con lo relacionado a la aplicación de la ley orgánica de protección de datos personales. • No se tiene designado y nombrado el comité de gestión de seguridad de la información • No se tiene definidas las herramientas que permitan cubrir lo que exige la ley orgánica de protección de datos personales. • No se ha realizado socialización respecto a los términos de seguridad de la información y la ley orgánica de protección de datos personales a las áreas involucradas de las unidades educativas
Seguridad de los recursos humanos	• Los empleados no han recibido formalmente capacitaciones respecto al

	tratamiento y gestión de la seguridad de la información. • No se tiene definido procedimientos en la gestión de la información personal de los empleados, alumnos, padres de familia, etc., con los diferentes proveedores que ofrecen servicios o productos a las unidades educativas.
Gestión de activos	• No se tiene definido delegado y responsable que se exigirán para el cumplimiento de la ley. El área técnica o de sistemas son quienes tiene asignado responsabilidades con los activos informáticos. • No se tiene definido criterios para la clasificación y gestión de la información.
Control de acceso	• No se dispone de procedimientos de gestión de la seguridad de la información enfocado en accesos seguros. • No se tiene políticas de cambio de credenciales sobre todo en las áreas financieras para sus distintos aplicativos. • No se manejan segmentación de la red para separar la red interna de la red Wireless.
Criptografía	• Las unidades educativas no disponen de aplicaciones que permitan proteger mediante técnicas de anonimización, pseudo anonimización, tokenización o cifrado de los datos personales o sensibles.
Seguridad física ambiental	• El área de informática o técnica realiza dos veces al año el mantenimiento preventivo de los dispositivos.
Gestión de las operaciones y comunicaciones	• Disponen de software para detección de amenazas informáticas antimalwae en todos los dispositivos del área administrativa de las unidades educativas, pero no tienen las habilidades necesarias o herramientas que permitan responder rápida y automáticamente a incidentes activos. • No existe controles definidos de seguridad de la información personal en el intercambio como por correo electrónico. • No se han realizado auditorias en lo que se refiere a seguridad de la información y comunicación.
Adquisición, desarrollo y	• Debido a presupuestos no ha sido posible obtener herramientas de monitoreo y

mantenimiento de los sistemas de información	control ante posibles vulnerabilidades técnicas de los sistemas.
Relación con los proveedores	• Existe información de carácter personal que es compartida con los diferentes proveedores que prestan servicio a las unidades educativas. • No existen políticas para el tratamiento de los datos personales entre las unidades educativas con los diferentes proveedores.
Gestión de incidentes de seguridad de la información	• En algunos casos los usuarios se saltan el proceso de manejo de incidentes reportando directamente a su inmediato superior en lugar de gestionar una solicitud de soporte con el área asignada. • Algunos colaboradores solicitan atención verbalmente saltando el proceso de registro de incidencias.
Gestión de continuidad de negocio	• Se tiene considerada la inclusión de la seguridad de la información en la continuidad del negocio, pero no se tiene presupuesto asignado para realizar estas actividades.
Cumplimiento con requerimientos legales y contractuales	• Aún no se dispone de lineamientos de seguridad y privacidad de la información de carácter personal que evite el uso indebido, reproducción, copia o alteración de esta, sobre la cual no tiene el consentimiento explícito del dueño del dato.

3.1 PLANTEAMIENTO DEL PROBLEMA

De acuerdo con la metodología indicada, y en base a la información recopilada, se puede decir que el problema principal en la institucion educativa es que existe riesgo del mal uso o posible filtración de los datos personales correspondientes a los estudiantes, padres de familia, empleados o proveedores, ya que están sujetas a la posible exposición, estafa, lucro ilícito e ilegítimo sin el debido consentimiento por parte del dueño del dato para los procesos de negocio, usuarios y aplicaciones que tienen acceso a estos y de los controles de quienes con la autorización del duaño del dato puede ver los datos en claro.

3.2 FORMULACIÓN DE LA HIPÓTESIS

A través de la información recopilada se puede notar que se tiene conocimiento sobre la existencia de la ley orgánica de protección de datos personales, así como también las normas que apoyan, proporcionan la orientación necesaria para que ayude a resolver eficazmente los problemas de privacidad de los datos y garantice que se reduzca la brecha entre los requisitos del sistema de gestión existente y la legislación global de privacidad de datos.

El desconocimiento sobre lo que implica tanto en realizar las actividades que conllevan a cumplir con lo que solicita la ley orgánica de protección de datos personales realizándolo mediante tareas de descubrimiento, protección y gobierno de los datos, como en el tiempo ya que en el año 2023 cuando exista el ente regulador puede exigir el cumplimiento de la ley.

3.3 LEVANTAMIENTO DE LA INFORMACIÓN

La Organización Internacional de Estandarización realiza una encuesta cada año, cuyo propósito es comprender el desarrollo global del sistema de gestión ISO. Estos datos se publican en Internet, donde se pueden visualizar todos los datos estadísticos de cada estándar en cada país / región.

En todos los ámbitos, esta regla es básica, pero nos centraremos en explicar su importancia en las instituciones educativas.

En las organizaciones dedicadas a la educación, hoy en día utilizan cada vez más sistemas informáticos para el desarrollo de sus actividades, por lo que es necesario asegurar que su información y sistemas informáticos estén protegidos de cualquier tipo de amenazas, como accesos no autorizados, malware, etc.

Para llevar a cabo esta protección, el enfoque ideal y deseable es adoptar un sistema de gestión de seguridad basado en la norma ISO-27001 e ISO-27701 para la gestión de la privacidad de la información. El departamento de tecnología de la información de la unidad educativa está obligado a aprobar el correcto uso de la información y contener los riesgos que enfrenta la información en su trabajo diario. Debemos tener en cuenta que cualquier ataque o accidente puede provocar el cese de las actividades del centro, la pérdida de material o el acceso a información confidencial.

La norma ISO27001 tiene una amplia gama de aplicaciones porque se puede utilizar en cualquier empresa. Especialmente en los centros

educativos, generalmente no cuentan con departamentos de TI muy complejos, por lo que la adopción y control de sistemas de gestión de seguridad de la información basados en ISO-27001 y su ISO-27701 adicional no incrementará significativamente la inversión económica ni trabajará duro para obtenerlo. Todo centro educativo debe evitar la exposición a riesgos o ataques que pongan en peligro su información para asegurar y brindar servicios educativos de calidad. En el sitio web oficial de la organización ISO, se publican los datos estadísticos de las organizaciones que han pasado la certificación de la norma ISO 27001.

La figura 4 se observa el resultado de la encuesta que organiza la ISO en que en correspondencia para la región de Latinoamérica y sobre todo en Ecuador las iniciativas de certificación en unidades educativas son nulas. Cabe resaltar que no todas las unidades educativas tienen la obligación de responder a las encuestas realizadas por la ISO.

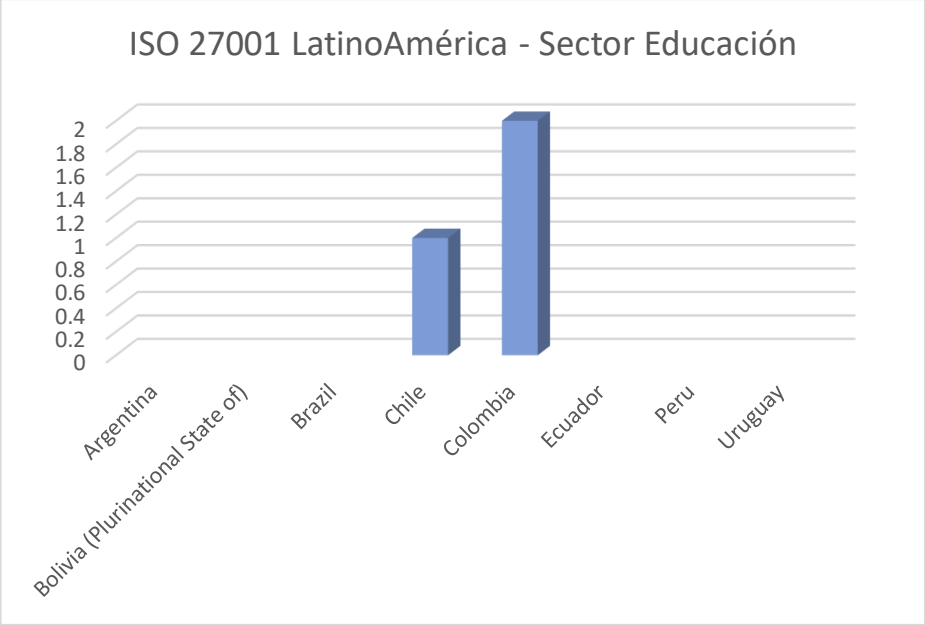

Figura 4. Iniciativas de certificación en educación de la región

Fuente: (ISO.ORG, 2013)

(LOPD) La Ley Orgánica de Protección de Datos Personales de Ecuador

El 26 de mayo de 2021 se promulgó la " La Ley Orgánica de Protección de Datos de Ecuador" luego del correspondiente debate en la Asamblea Nacional y la aprobación del presidente de la República. Cabe destacar que, desde entonces, la empresa cuenta con un periodo de adaptación de

dos años para poder adecuar todos los procesos a los requerimientos de la nueva normativa.

Entre las leyes mencionadas, cabe destacar la evidente influencia de la normativa europea existente y el claro espíritu de garantía a los titulares, porque aboga por la protección de los derechos individuales como derechos de los ciudadanos más que de la empresa y el principio básico de Reconocimiento Aplicaciones que benefician al titular de los datos en caso de duda.

Ámbito de aplicación. ¿A quién afecta?

En cuanto al alcance geográfico de la ley, cabe señalar que debido al domicilio del responsable o del responsable en el Ecuador, todo tratamiento de datos personales en cualquier parte del territorio nacional debe cumplir con sus disposiciones legales.

Sin embargo, cabe señalar que luego del segundo debate en la Asamblea Nacional, los derechos extraterritoriales se introdujeron como una novedad. Esto significa que "cuando un responsable o administrador no establecido en Ecuador procese los datos personales de los titulares residentes en Ecuador, se aplicará la ley cuando las actividades de procesamiento estén relacionadas con lo siguiente: Brindar bienes o servicios a los referidos titulares, independientemente de que necesiten pagar o controlar sus acciones, siempre que se produzca en Ecuador "

Asimismo, este nuevo marco regulatorio viene con un conjunto de principios que deben aplicarse en cualquier tratamiento de datos personales:

La licitud, lealtad, transparencia, finalidad, idoneidad y mitigación de los datos personales, así como la adecuación del procesamiento, consentimiento, confidencialidad, calidad, preservación y seguridad, en la que mejoran la redacción en la segunda parte del debate.

Responsabilidad proactiva

Sin duda, el principio de iniciativa y responsabilidad constituyen el eje central de la organización. Es un principio que no solo obliga a las organizaciones a ser diligentes a la hora de cumplir con la normativa, sino también a poder demostrar siempre la implantación de los mecanismos efectivos de protección de datos personales que les sean encomendados.

Las disposiciones antes mencionadas requieren una evaluación y revisión periódicas de los procesos implementados para respetar el principio de rendición de cuentas de manera permanente a fin de mejorar su efectividad.

La figura del DPO

Además, de que el garante respeta todas las disposiciones de la ley, un nuevo personaje entró en escena; “El Delegado de Protección de Datos” que será, entre sus funciones, el encargado de informar e instruir al responsable de los requisitos normativos, vigilar su adecuado cumplimiento y colaborar con la Autoridad de Protección de Datos Personales, que actúa como punto de contacto entre éste y las entidades que atención.

Nuevos derechos

Por otro lado, para garantizar la aplicación efectiva de la ley, las partes involucradas tienen un conjunto de derechos.

- Derecho de acceso
- Derecho de rectificación y actualización
- Derecho de oposición
- Derecho de portabilidad
- Derecho a la limitación de tratamiento
- Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas
- Derecho a la educación digital
- Derecho de consulta
- Derecho de eliminación

En cuanto a los derechos, cabe señalar que, si bien los derechos de revocación y borrado digital también se consideraron inicialmente, fueron rechazados en la segunda sesión del Congreso.

Asimismo, es importante destacar la introducción de una prohibición general a los prestadores de servicios del sistema de telecomunicaciones compartido, quienes no deben utilizar los datos personales de los usuarios para publicitar sus servicios o productos comerciales sin su consentimiento expreso.

Medidas de seguridad

En cuanto a los procedimientos y controles de seguridad para garantizar la confidencialidad de los datos personales, cabe señalar que son necesariamente el resultado de un análisis de riesgos y una evaluación de impacto. En este sentido, la metodología utilizada para ello debe tener en cuenta la privacidad del procesamiento, la privacidad de las partes interesadas y el tipo y volumen de datos personales que se procesan.

Como se indica en el párrafo anterior, cabe señalar que, en la modificación final de la ley, como nuevo método, será necesario realizar una evaluación de impacto de la protección de datos en el caso de que

- Evaluación exhaustiva y sistemática
- Procesamiento extenso de categorías de datos privados o datos personales relacionados con condenas y delitos penales
- Amplio seguimiento sistemático de las zonas de acceso público.

Además, en caso de incumplimiento de seguridad, se establece un plazo de tres días desde el descubrimiento del incumplimiento para notificar a la Autoridad de Protección de Datos Personales, así como a la Autoridad Reguladora de Telecomunicaciones.

Asimismo, en algunos casos, el aviso también debe enviarse al propietario lo antes posible y en un plazo máximo de 5 días.

Sanciones

Las multas por violar la normativa en materia de protección de datos podrían ascender a la cuantía entre el 0,7% y el 1% Calculada sobre el volumen de negocios, Correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Dada la gran cantidad de nuevos requisitos que trae esta nueva normativa, es necesario abordar un proyecto que asegure el cumplimiento honesto de la ley, así como las medidas de seguridad tomadas para garantizar la confidencialidad de los datos personales.

Norma ISO27701:2019

Como se indica en la Tabla 5, la implantación de la norma ISO27701:2019 pasa primeramente por la construcción del PDCA en donde se detallan los procesos que conllevan a adherirse a los parámetros que establece la norma.

Tabla 5. Procesos del PDCA de la norma ISO 27701:2019

FASE PDCA	PROCESO	
Planear	4. Contexto de la unidad educativa	Compresión de la UE y de su contexto.
		Comprender las necesidades y expectativas de las partes interesadas
		Determinar el alcance del SGPI
		SGPI
	5. Liderazgo	Liderazgo y compromiso
		Política
		Roles, responsabilidades y autoridades

	6. Planeación	Acciones para tratar riesgos y oportunidades
		Objetivos
	7. Soporte	Recursos
		Competencia
		Concienciación
		Comunicación
		Información documentada
Hacer	8. Operación	Planificación y control operacional
		Apreciación de riesgos
		Tratamiento de riesgos
Verificar	9. Evaluación del Desempeño	Seguimiento, medición, análisis y evaluación
		Auditoría interna
		Revisión por dirección.
Actuar	10. Mejora	No conformidad y acciones correctivas
		Mejora continua

El SGIP solo se podrá certificar cuando se tengan todas las evidencias suficientes y de la misma manera cuando al menos se haya ejecutado todos los procedimientos generales una vez, es decir que se haya completado el ciclo del PDCA.

3.3.1 Fase Planificar.

3.3.1.1 Contexto de la Organización:

En el contexto de la Unidad Educativa se deben considerar los roles de la organización tales como:

- El responsable del tratamiento
- El encargado del tratamiento

Se debe entender las necesidades de las partes interesadas, así como definir y documentar el alcance el SGIP.

Dentro de las evidencias documentadas que llevan esta fase está el del alcance del SGIP el cual en su contenido debe contemplar lo siguiente:

- Contexto de la unidad educativa
- Identificación de las partes interesadas: los usuarios/clientes del sistema de gestión
- Identificación de los entornos y servicios incluidos y que no estén incluidos en el alcance.

- Descripción de los sistemas y tratamientos afectados por el sistema de gestión.
- La identificación de la legislación que afectará al sistema de gestión.
- Relación e identificación de los terceros tanto en seguridad como en el tratamiento de los datos.

3.3.1.2 Liderazgo:

Se debe definir la política de seguridad de la información y de la privacidad, así como también los roles y responsabilidades que son parte del SGIP.
Se requieren evidencias de los compromisos de la dirección con el sistema de gestión.

Las evidencias documentadas respecto al liderazgo se tienen las siguientes:

Documento de seguridad y privacidad el cual debe contemplar lo siguiente:

- Extender el alcance para incluir los datos personales.
- Declaración avalada por la dirección del sistema de gestión.
- Definición de los objetivos del sistema de gestión
- Demostrar el compromiso con la mejora continua.

Documento de roles y responsabilidades el cual debe contemplar:

- Quién es quién en el sistema de gestión
- Roles definidos relacionados con la gestión y la seguridad:
    - Dirección
    - Comité de seguridad y privacidad
    - Auditores
    - Resto de los actores

3.3.1.3 Planificación:

En esta fase se implementa el proceso de gestión de riesgos del SGIP, se debe realizar un análisis de riesgo sobre los métodos de tratamiento dentro del alcance del SGIP, definiendo un plan de tratamiento de riesgos y finalmente preparar una declaración de idoneidad o aplicabilidad.

La evidencia documental del plan es:

- Informe de análisis de riesgos
    - Determinar el plan de riesgos que afecta a la unidad educativa.

    - El riesgo debe tener en cuenta la seguridad de los sistemas
    - Aumento de los riesgos legales y organizativos que afectan el tratamiento de los datos personales.
- Plan de tratamiento de riesgos
    - Desarrolla el plan de acción para gestionar los riesgos relacionados que se abordarán.
- Declaración de aplicabilidad
    - Identificar un conjunto de controles que deben ser considerados, extendiendo los controles existentes en el Anexo A-ISO 27001 a los proporcionados por ISO 27701 en los Artículos 7 y 8.

3.3.1.4 Soporte:

La viabilidad de SGIP debe garantizarse asegurando que se logren las capacidades requeridas. Se deben establecer requisitos de capacitación, definir planes de comunicación SGIP y establecer procedimientos de control de documentos.

Las evidencias documentadas para esta fase son:

- Plan de formación
    - Definir las capacidades necesarias del personal en términos de seguridad y privacidad.
    - Diseñar programas de capacitación, formación y sensibilización.
    - Evaluar la efectividad de las acciones.
    - La información documentada del proceso debe estar debidamente acreditada.
- Plan de comunicación
    - Definir las comunicaciones internas y externas de SGPI internamente en la empresa.
    - Quién debe comunicar a qué hora, qué canal y qué partes interesadas.

Para efectuar un control de los registros y la documentación se debe seguir lo siguiente:

- Los requerimientos deben ser idénticos a los ya establecidos a los de la ISO27001.
- En lo que corresponde a la creación de la documentación, controles de cambios, conservación, distribución, etc., se debe definir un proceso adecuado.
- Se debe identificar y controlar toda documentación externa.

3.3.2 Fase Hacer

Operación:

Se deben implementar las disposiciones del plan de tratamiento de riesgos, así como también el realizar la evaluación de riesgos que debe actualizarse periódicamente y también debe revisarse plan de tratamiento. Finalmente debe asegurarse de que se logren los objetivos.

En la fase "DO", también se ha completa el proceso normal de apoyo al sistema de gestión.

- Procedimiento general del SGPI:
    - Control de los registros y la documentación.
    - Procedimiento de auditoría.
    - Procedimiento de gestión de mejora continua.
    - Procedimiento de la revisión por parte de la dirección.

3.3.3 Fase Verificar

Evaluación del desempeño:

La unidad educativa debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema. Gestión de la seguridad de la información estableciendo un proceso de medición, monitorización y gestión del desempeño. Se debe determinar el proceso de auditoría interna para proporcionar información sobre si el sistema de gestión de seguridad de la información cumple, se implementa y mantiene de manera efectiva, y finalmente los altos directivos deben revisar el SGSI en intervalos planificados donde valorarán el funcionamiento, objetivos y eficacia del sistema de gestión.

Las evidencias documentadas son:

- Procedimiento de gestión de objetivos.
    - Los requisitos son idénticos a los establecidos por la ISO 27001 pero se debe extender el alcance a lo que refiere a datos personales.
    - Se debe definir los objetivos, los responsables y los criterios de medición.
    - Se debe definir el proceso de valoración y evaluación de resultados y de desempeño.

- Procedimiento de auditoría interna.
    - Los requisitos son idénticos a los establecidos por la ISO 27001 pero se debe extender el alcance a lo que se refiere a datos personales.
    - Se tiene que considerar los requisitos del proceso de auditoría interna los cuales son: metodología, periodicidad, cualificación de los auditores, los requisitos de los informes y el traslado de resultados.
- Procedimiento de revisión por dirección.
    - Los requisitos son idénticos a los establecidos por la ISO 27001.
    - Debe estar los procesos de valoración del SGSI, así como los cambios, tendencias, cumplimiento de objetivos, etc.

3.3.4 Fase Actuar

Mejora:

La unidad educativa debe mejorar continuamente la aplicabilidad y eficacia del SGSI mediante un proceso de mejora continua, así también el cómo debe determinar la identificación de no conformidades y el establecimiento de cómo se definirán las acciones correctivas.

La evidencia documentada en la fase de mejora es:

- Procedimiento de mejora continua.
    - Los requisitos son idénticos a los establecidos por la ISO 27001 pero se debe extender el alcance a lo que se refiere a los datos
    - Se debe definir el proceso para la creación de no conformidad, analizando las causas, haciendo frente a las consecuencias y estableciendo las acciones correctivas.

Los anexos correspondientes a la ISO 27701 contiene información optimizada para fomentar la certificación ya que facilita la integración de los sistemas de gestión. En la tabla 5 las cláusulas 6, 7 y 9 tendremos resultados que deben ser documentados los cuales se detallan a continuación:

Tabla 6. Anexos ISO 27701:2019

CLÁUSULAS	OBJETIVOS	DOCUMENTO DE RESULTADO
Cláusula 6 – Controles del anexo A ISO 27001	Áreas de control del punto 5 al 18	• Marco normativo de seguridad de la información el cual contempla los cambios sobre los controles modificados por la ISO 27701 • Normativas de seguridad para que se pueda cubrir los controles de la ISO 27001 • Procedimientos de seguridad para cubrir los controles de la ISO 27001
Cláusula 7	7.2 Revisiones de la seguridad de la información	• Registro de las actividades del tratamiento de los datos personales. • Informe correspondiente al deber de información y consentimiento el cual trata las cláusulas informativas. • Informe sobre los encargados del tratamiento y accesos sin tratamiento de los datos. • Procedimientos de atención de los derechos correspondientes a acceso, rectificación, cancelación y oposición de la información de datos personales. • Análisis de riesgos y le evaluación del impacto de los datos personales EIPD. • Procedimiento para el tratamiento en acciones comerciales. • Política de protección de datos personales desde el diseño y el por defecto. • Política de archivo y custodia de los datos. • Procedimiento de transmisión de datos. • Nombramiento del DPD.
	7.3 Obligaciones con los interesados	
	7.4 Privacidad por diseño y privacidad por defecto	
	7.5 Intercambio de PII, transferencia y divulgación.	

Cláusula 8	8.2 Revisiones de la seguridad de la información	1. Contratos con los encargados del tratamiento.
	8.3 Obligaciones con los interesados	
	8.4 Privacidad por diseño y privacidad por defecto	
	8.5 Intercambio de PII, transferencia y divulgación.	

3.4 PROPUESTA DE LA GUÍA DE PROTECCIÓN DE DATOS PERSONALES PARA INSTITUCIONES EDUCATIVAS

La propuesta de guía se puede ver en el anexo 1 en la que se detalla como una guía rápida de implementación de la norma ISO 27701 considerando que la empresa ya implantó la norma ISO 27001 oo que también podrá realizarla simultáneamente con la ayuda de las distintas guías de implantación de la norma ISO 27001 ya existentes.

4. CONCLUSIONES Y RECOMENDACIONES

4 CONCLUSIONES Y RECOMENDACIONES

4.2 CONCLUSIONES

- Con base en investigaciones relacionadas con la situación actual de seguridad de la información con la ISO27001: 2013, se desarrolló un modelo de gestión basado en la norma ISO27701: 2019 para proteger la privacidad de la información de los riesgos de los que no está exenta. De acuerdo con la norma ISO / IEC 27701: 2019, se analizan y establecen controles apropiados para optimizar la privacidad de la información de las instituciones educativas. Al momento en que las empresas implementen un sistema de seguridad de la información, es posible garantizar, mantener y asegurar la disponibilidad, integridad, confidencialidad y privacidad de la información, así como también el acceso a los activos informáticos físicos y no físicos administrados por las unidades educativas.
- En la investigación del proyecto, el estudio mostró que el sector de la educación siempre debe garantizar la seguridad de sus activos de información. Esto muestra que incluso la parte más pequeña del sector de la educación debe estar cubierta por procedimientos de seguridad. Esto muestra que, si se descubre o descuida un área determinada, la organización puede convertirse en un punto de entrada para personas malintencionadas
- Dentro del proceso de protección y privacidad de la información está la socialización del alcance de la ley en todas las áreas de la empresa que de alguna manera trabajan con datos personales tanto internos como externos a las unidades educativas con el fin de que puedan tratar los datos personales únicamente quienes tienen el consentimiento explicito por parte del dueño del dato.

4.3 RECOMENDACIONES

- Es necesario que el departamento de sistemas del sector educativo revise sus capacidades para garantizar que los controles y planes de acción se implementen adecuadamente para cerrar las brechas de seguridad.
- Todos los colaboradores del sector educativo deben comprometerse a realizar todas las actividades establecidas en el sistema de gestión e integrar conscientemente la cultura de seguridad de la información por defecto.
- El modelo de seguridad de la información correspondiente a la norma ISO27701 en este proyecto necesita ser actualizado y retroalimentado continuamente, de lo contrario no se acoplará correctamente con

riesgos futuros, ya que no se desarrollará con el crecimiento que tendrán las unidades educativas del país.

- Finalmente, si no se cumple con el claro compromiso de la alta dirección con la seguridad de la información, no se recomienda implementar un sistema de gestión de la seguridad y privacidad de la información como el introducido en este proyecto en el sector educativo.

5 BIBLIOGRAFÍA

5. BIBLIOGRAFIA

Rodríguez, C. B. (28 de 11 de 2011). *CONVELIA Consultores Legales Tecnológicos*. Obtenido de http://convelia.com/responsable-y-encargado-de-tratamiento-de-datos-personales

Bittemple. (1999). *Bittemple.* Obtenido de https://bittemple.es/legislacion/lopd-151999/titulo-ii-principios-proteccion-datos/

LetsLaw. (24 de 03 de 2018). *LetsLaw*. Obtenido de https://letslaw.es/diferencia-rgpd-lopd/

García-Valdecasas, G. (11 de 8 de 2018). *CYSAE*. Obtenido de https://cysae.com/principios-generales-rgpd/

Botín, R. (25 de 9 de 2020). *OBERLO*. Obtenido de https://ar.oberlo.com/blog/reglamento-general-proteccion-datos

Microsoft. (2020). *Microsoft.com*. Obtenido de https://www.microsoft.com/es-ww/security/business/zero-trust

LOPD. (19 de 09 de 2020). *Asamblea Nacional Republica del Ecuador.* Obtenido de https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos

ISO.ORG. (2013). *International Organitation for Standardization: ISO 27001*. Obtenido de https://www.iso.org/isoiec-27001-information-security.html

ISOTOOLS. (16 de 02 de 2016). *Descubre qué es un SGSI y cuáles son sus elementos esenciales*. Obtenido de https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-son-sus-elementos-esenciales/

NQA.COM. (s.f.). *ORGANISMO DE CERTIFICACIÓN GLOBAL*. Obtenido de https://www.nqa.com/es-es/certification/standards/iso-27001

MINTEL. (s.f.). *Ciclo de Deming (PDCA)*. Obtenido de Gobierno Electrónico : https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

UNIR Revista. (s.f.). Obtenido de El Ciclo de Deming: una estrategia de mejora continua de la calidad de las empresas: https://www.unir.net/ingenieria/revista/ciclo-de-deming-pdca/

ORG, I. (s.f.). *ISO/IEC 27701:2019*. Obtenido de Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines: https://www.iso.org/standard/71670.html

Española, U. N. (s.f.). *Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019).* Obtenido

de UNE-EN ISO/IEC 27701:2021: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0067527

España, A. (s.f.). *AENOR*. Obtenido de Seguridad y Privacidad de la Información: ISO 27001 e ISO 27701: https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

School, E. B. (s.f.). *ISO 27701 y el RGPD: Qué aportan en el ámbito de la Ciberseguridad*. Obtenido de EALDE Business School: https://www.ealde.es/iso-27701-rgpd-ciberseguridad/

NORMA ISO 27001. (s.f.). Obtenido de https://normaiso27001.es

Ecuador, C. d. (s.f.). *Consejo de Comunicación del Ecuador*. Obtenido de https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/Ley%20Orgánica%20de%20Protección%20de%20Datos%20Personales.pdf

Bolívar, U. A. (s.f.). *Protección de datos*. Obtenido de https://www.uasb.edu.ec/ciberderechos/proteccion-de-datos/

Institution, T. B. (s.f.). *Implantación ISO/IEC 27701*. Obtenido de https://www.bsigroup.com/es-ES/iso-27701-gestion-de-informacion-sobre-privacidad/implantacion/

6 ANEXOS

6. ANEXOS

ANEXO 1. GUÍA DE IMPLANTACIÓN ISO/IEC 27701

La guía de implantación de la ISO 27701 requiere de un sistema de gestión existente al cual adherirse, así también no es necesario que todos los controles y cláusulas sean aplicables en todos los casos ya que depende del tipo de empresa.

Requisitos previos

Los requisitos previos de la norma se dividen en 4 grupos que se detallan a continuación:

1. Los requisitos del sistema de gestión de la información confidencial relacionados con la ISO 27001 que se describen en la cláusula 5
2. Los requisitos del sistema de gestión de la información confidencial relacionados con la ISO 27002 que se describen en la cláusula 6
3. La guía del sistema de gestión de la información confidencial para controladores de información personal que se describen en la cláusula 7
4. La guía del sistema de gestión de la información confidencial para procesadores de información confidencial que se describe en la cláusula 8

Adicional, los controles aplicables se describen de mejor manera en los anexos de la norma los cuales se puede utilizar como guía los siguientes:

1. Anexo A: lista los controles para los responsables (controladores).
2. Anexo B: lista los controles para los encargados (procesadores).
3. Anexo C: Se esquematiza las disposiciones de la norma ISO 27001 realizando comparaciones con la ISO 29100.
4. Anexo D: Se esquematiza las disposiciones de la norma ISO 27701 realizando comparaciones con la RGPD.
5. Anexo E: Se esquematiza las disposiciones de la norma ISO 27701 realizando comparaciones con la ISO 27018 e ISO 29151
6. Anexo F: Se proporciona las directrices para la aplicabilidad de la norma ISO 27701 a la ISO 27001 y ISO 27002.

En la mayoría de los casos, cualquier empresa con certificación ISO 27001 debe comenzar con el Anexo F para poder comprender como la aplicación del sistema de gestión de la información confidencial encaja en el sistema de gestión de seguridad de la información de la ISO 27001 existente. En este anexo se encuentran tres instancias de aplicación de la norma:

- Aplicación de los estándares de seguridad
- Adiciones a los estándares de seguridad
- Refinamiento de los estándares de seguridad

Las cláusulas 5 a la 8 del sistema de gestión de la información confidencial amplían a la ISO 27001 para incorporar las consideraciones de la información personal. Hablando de la cláusula 5, esta proporciona los lineamientos específicos del sistema de gestión de la información confidencial respecto a los requerimientos que establece la norma ISO 27001 respecto a la seguridad de la información apropiados para las empresas.

La norma ISO 27701 contiene mejoras para los controles sobre el Anexo A como se detalla a continuación:

- Anexo A Cláusula 6: 37 controles mejorados
- Anexo A Cláusula 7: 31 controles para los controladores
- Anexo A Cláusula 8: 18 controles para los procesadores

Consideraciones adicionales para la implantación de la ISO 27701 que se encuentran en la cláusula 5 que pueden observarse como adicionales a los requisitos ya existentes de un sistema de gestión de seguridad de la información:

- Cláusula 5.1: Los requisitos de ISO 27001 deben ampliarse para proteger la privacidad que puede verse afectada por el procesamiento de información personal. El Anexo F proporciona una tabla muy intuitiva.
- Cláusula 5.2.1: Un requisito adicional en la cláusula 4.1 de ISO 27001 es una descripción de que la organización definirá su función como controlador y/o procesador de información personal. Además, debe identificar factores externos e internos contextualmente relevantes que afecten su capacidad para lograr resultados del sistema de gestión de la información confidencial. Esto incluye cualquier cumplimiento legal revisado según el SGSI existente o los requisitos contractuales que se han especificado hasta ahora en las distintas cláusulas o controles del anexo de la norma ISO 27001.

Una vez que la organización ha identificado el rol del controlador y/o procesador de información personal, se deben definir roles separados, cada uno sujeto a un grupo de control diferente.

- Cláusula 5.2.2: Una consideración adicional en la cláusula 4.2 de ISO 27001 es el requisito de incluir a las partes interesadas responsables en relación con el procesamiento de información personal. Esto puede incluir al cliente, que tampoco está cubierto en SGSI ISO 27001. Además, los requisitos relevantes para el procesamiento pueden ser especificados por estatutos, contractuales u objetivos.
- Cláusula 5.2.3: El alcance del SGSI se requiere en la cláusula 4.3 de ISO 27001. Los elementos adicionales del sistema de gestión de la información confidencial del alcance incluyen el procesamiento de la información. La determinación del alcance del SGIC puede requerir una

revisión del SGSI debido a la interpretación de la seguridad de la información en la cláusula 5.1 de la Norma ISO 27701.

- Cláusula 5.2.4: Además de la cláusula 4.4 de ISO 27001, una organización en la nueva norma debe crear, implementar, mantener y mejorar continuamente un sistema de gestión de información confidencial de acuerdo con los requisitos de las cláusulas 4 a la cláusula 10 de la norma. ISO 27001: 2013 que adicional se amplía por los requisitos de la cláusula 5.
- Clausula 5.3: En la ISO 27001, las organizaciones deben demostrar su compromiso con el SGSI a través de iniciativas de liderazgo y el establecimiento de políticas, roles, responsabilidades y pautas. Así mismo, un sistema de gestión de información confidencial requiere aportaciones similares por parte de la dirección, así como explicaciones específicas relevantes, como se establece en el punto 5.1 de la norma ISO 27701, incluyendo todos los aspectos contenidos en la cláusula 5 del SGSI.
- Cláusula 5.4.1: Los requisitos de la ISO 27001 en lo que refiere a abordar riesgos y oportunidades requiere de un aumento con la consideración de la cláusula 5.1 de la ISO 27701.
- Clausula 5.4.2: Los objetivos de seguridad de la información de la organización establecidos en la cláusula 6.2 deben tenerse en cuenta, complementados con la interpretación de la cláusula 5.1 de la Norma ISO 27701.
- Cláusula 5.5: Las consideraciones que respaldan la norma ISO 27001 en la cláusula 7 pueden aplicarse con la interpretación adicional especificada en la cláusula 5.1 de la norma ISO 27701.
- Cláusula 5.6: La parte operativa de la ISO 27001 en la cláusula 8, incluida también la planificación del tratamiento de riesgos, es requerida de manera similar por la norma ISO 27701 junto con información adicional de la cláusula 5.1 de esta última.
- Cláusula 5.7 y 5.8: Las consideraciones de seguimiento o medición y mejora del SGSI existente, requieren un aumento de las consideraciones que son dadas en la cláusula 5.1 de la ISO 27701.