



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Proyecto De Titulación

Carrera De Tecnologías De La Información

**Desarrollo Y Evaluación de un Sistema Web Para la Verificación de
Cumplimiento de la Norma ISO 27001 en la Unidad Educativa Fe y
Alegría**

Autor: Bedoya Garcia Danny Javier

Tutor: Ing. Pablo Francisco Puentes Ponce

Santo Domingo, 14 de Marzo 2024

REPORTE DE VERIFICACIÓN DE CONTENIDO



Plagiarism and AI Content Detection Report

BEDOYA_DANNY_UIC_V1.4.docx

Scan details

Scan time: March 5th, 2024 at 12:45 UTC Total Pages: 34 Total Words: 8306

Plagiarism Detection



Types of plagiarism		Words
Identical	1.3%	110
Minor Changes	0.1%	5
Paraphrased	3.6%	303
Omitted Words	5.3%	438

AI Content Detection



Text coverage		Words
AI text	1.7%	144
Human text	98.3%	7724

[Learn more](#)

🔍 Plagiarism Results: (29)

🌐 **Texto completo | Argentina.gob.ar** 0.8%
<https://www.argentina.gob.ar/normativa/nacional/resoluci%c3%b3n-549-2022-370136/texto>
Presidencia de la Nación Pasar al contenido principal Campañas Nacionales ...

Firma:



Firmado electrónicamente por:
PABLO FRANCISCO
PUENTE PONCE

.....
Ing. Pablo Francisco Puente Ponce

C.C: 1002771762



Departamento de Ciencias de la Computación

Carrera de Ingeniería en Tecnologías de la Información

Certificación

Certifico que el trabajo de integración curricular: **“Desarrollo y evaluación de un sistema web para la verificación de cumplimiento de la norma ISO 27001 en la Unidad Educativa Fe y Alegría”** fue realizado por **Bedoya Garcia Danny Javier**, el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Santo Domingo, 1 de marzo del 2024



.....
Puente Ponce, Pablo Francisco

C. C: 1002771762



**DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN
CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN**

RESPONSABILIDAD DE AUTORÍA

Yo, **Bedoya Garcia Danny Javier**, con cédula de ciudadanía n° 2300298029, declaro/declaramos que el contenido, ideas y criterios del trabajo de integración curricular: "**Desarrollo y evaluación de un sistema web para la verificación de cumplimiento de la norma ISO 27001 en la Unidad Educativa Fe y Alegría**" es de mi/nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Santo Domingo de los Tsáchilas, 25 de febrero del 2024

Firma:

.....
Bedoya Garcia Danny Javier

C.C.: 2300298029



**DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN
CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN**

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Bedoya Garcia Danny Javier**, con cédula de ciudadanía n° 2300298029, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **"Desarrollo y evaluación de un sistema web para la verificación de cumplimiento de la norma ISO 27001 en la Unidad Educativa Fe y Alegría"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Santo Domingo de los Tsáchilas, 25 de febrero del 2024

Firma:

.....
Bedoya Garcia Danny Javier

C.C.: 2300298029

Dedicatoria

A mis amados padres que siempre me apoyaron durante todo el proceso, me demostraron que siempre confiaron en mis capacidades para llegar hasta este punto; a mi hermana que fue un ejemplo a seguir por su dedicación; a todos esos compañeros que formaron parte del camino y que aportaron su grano de arena, estaré eternamente agradecido. Comparto este logro con todas y cada una de estas personas.

Danny Javier Bedoya Garcia.

Agradecimiento

Quiero expresar mis más sinceros agradecimientos a mis padres, Luis Bedoya y Jessica Garcia, por todo su apoyo y por ser quienes día a día estuvieron ahí a mi lado y fueron una gran motivación durante mi proceso académico.

Agradezco profundamente a cada uno de mis compañeros que entre nosotros nos dimos la mano a lo largo de la carrera universitaria.

Al Ing. Pablo Puente, tutor de tesis, por su conocimiento y confianza durante este proceso.

Danny Javier Bedoya Garcia.

Índice de contenido

Dedicatoria	I
Agradecimiento	II
Resumen	1
Abstract	2
I. Introducción.....	3
Estado del arte:.....	4
Objetivos	5
General.....	5
Específicos.....	5
II. Marco teórico	6
Norma ISO 27001	6
Ventajas de implementar un SGSI bajo la norma ISO 27001	7
Seguridad de la información	8
Sistemas de Gestión de la Seguridad de la Información	8
Node JS	9
MySQL	9
Express JS	10
III. Metodología/Técnicas/Diseño.....	10
Metodología:	10
Técnicas:	15
Controles Tecnológicos y Personas	19
Controles Físicos y Organizacionales.....	21
Controles Tecnológicos y Organizacionales	22

Controles Organizacionales y Personas.....	23
Diseño:	25
Arquitectura de sistema web.....	25
Esquema de interfaz de usuario	26
Base de datos	27
Acceso a la aplicación web.....	28
Consumo de API.....	31
IV. Resultados	41
Cumplimiento de controles	41
Controles Tecnológicos y Personas	41
Controles Físicos y Organizacionales.....	44
Controles Físicos	45
Controles Tecnológicos y Organizacionales	46
Controles Organizacionales	47
Controles Tecnológicos	48
Controles Organizacionales y Personas.....	49
Reporte de evaluación.....	52
Pruebas de funcionalidad del sistema	60
V. Conclusiones y recomendaciones.....	63
Conclusiones	63
Recomendaciones.....	63
VI. Referencias bibliográficas	64

Índice de figuras

Fig. 1. Arquitectura de sitio web.	26
Fig. 2. Esquema de interfaz de usuario.	27
Fig. 3. Base de datos.....	28
Fig. 4. Interfaz de inicio de sesión.....	29
Fig. 5. Interfaz de registro de usuario.....	30
Fig. 6. Validaciones opciones de inicio y registro.	30
Fig. 7. Interfaz de apartado "Perfil".	31
Fig. 8. Interfaz de registro de institución.....	32
Fig. 9. Interfaz de lista de instituciones.....	32
Fig. 10. Confirmación de eliminación de institución.	33
Fig. 11. Vista de editar institución.	34
Fig. 12. Vista de institución.	34
Fig. 13. Vista de proceso de evaluación.....	35
Fig. 14. Ventana emergente de información acerca de los controles.	36
Fig. 15. Vista de evaluaciones registradas.	37
Fig. 16. Reporte PDF de evaluación.	38
Fig. 17. Reporte PDF de evaluación.	39
Fig. 18. Reporte PDF de evaluación.	40
Fig. 19. Gráfica de cumplimiento de controles tecnológicos y personas.	42
Fig. 20. Gráfica de cumplimiento de controles físicos y organizacionales.....	44
Fig. 21. Gráfica de cumplimiento de controles físicos.....	45
Fig. 22. Gráfica de cumplimiento de controles tecnológicos y organizacionales.	46
Fig. 23. Gráfica de cumplimiento de controles organizacionales.	48
Fig. 24. Gráfica de cumplimiento de controles tecnológicos.....	49
Fig. 25. Gráfica de cumplimiento de controles organizacionales y personas.	50
Fig. 26. Primer reporte de evaluación a la institución.....	52
Fig. 27. Primer reporte de evaluación a la institución.....	53
Fig. 28. Primer reporte de evaluación a la institución.....	54
Fig. 29. Gráfica de cumplimiento de controles ISO 27001.....	55
Fig. 30. Reporte final.....	56

Fig. 31.Reporte final.....	57
Fig. 32. Reporte final.....	58
Fig. 33. Reporte final.....	59
Fig. 34. Prueba de funcionalidad P01.	60
Fig. 35. Prueba de funcionalidad P02.	60
Fig. 36. Prueba de funcionalidad P03.	61
Fig. 37. Prueba de funcionalidad P04.	61
Fig. 38. Prueba de funcionalidad P05.	61
Fig. 39. Prueba de funcionalidad P06.	62
Fig. 40. Prueba de funcionalidad P07.	62
Fig. 41. Prueba de funcionalidad P08.	62

Índice de tablas

TABLA I	11
TABLA II	12
TABLA III	13
TABLA IV	14
TABLA V	14
TABLA VI	16
TABLA VII	17
TABLA VIII	18
TABLA IX	19
TABLA X	43
TABLA XI	44
TABLA XII	45
TABLA XIII	47
TABLA XIV	48
TABLA XV	49
TABLA XVI	51

Resumen

En este proyecto de investigación aplicada se abordó el desafío de implementar un sistema web para la evaluación del cumplimiento de la norma ISO 27001, para ello tomando en cuenta el alcance del proyecto se determinaron los diferentes controles para evaluar a la unidad educativa Fe y Alegría, la cual se encuentra ubicada en Ecuador Santo Domingo de los Tsáchilas. Para lograrlo, se utilizó la metodología Scrum como marco de trabajo. Para ello primero se realizó una exhaustiva investigación para así poder determinar los diferentes controles a evaluar. Los controles se encuentran divididos en 4 grupos, los cuales se encargan de gestionar los riesgos de seguridad de la información. De ese conjunto de controles se tomaron los considerados como más relevantes en base a los requerimientos de la unidad educativa para poder realizar el sistema web. Este proyecto representa un gran aporte a la unidad educativa Al proporcionar una plataforma eficiente para la gestión de los controles de seguridad de la información seleccionados, este sistema no solo agiliza el proceso de evaluación, sino que también mejora la transparencia y la eficacia en la identificación y mitigación de riesgos, fortaleciendo así la confianza y el cumplimiento de los estándares de seguridad establecidos por la norma ISO 27001.

Palabras clave: ISO 27001, Sistemas de Gestión de la Seguridad de la Información, sistema web, certificación.

Abstract

In this applied research project, the challenge of implementing a web system for evaluating compliance with the ISO 27001 standard was addressed. Taking into account the project scope, different controls were determined to assess the Fe y Alegria educational unit located in Santo Domingo de los Tsáchilas, Ecuador. The Scrum methodology was used as the framework for this endeavor. An exhaustive investigation was conducted initially to identify the various controls for evaluation. These controls are categorized into 4 groups responsible for managing information security risks. From this set of controls, those deemed most relevant based on the educational unit's requirements were selected to develop the web system. This project represents a significant contribution to the Fe y Alegria educational unit by providing an efficient platform for managing the selected information security controls. This system not only streamlines the evaluation process but also enhances transparency and effectiveness in identifying and mitigating risks, thereby strengthening confidence and compliance with the security standards established by the ISO 27001 standard.

Keywords: *ISO 27001, Information Security Management Systems, web system, certification.*

I. Introducción

En la actualidad, las instituciones educativas implementan sus sistemas de información en entornos digitales, lo que genera un requerimiento incrementado de la aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Por esta razón, en el presente proyecto se abordará esta necesidad por medio del desarrollo de un sistema web que verifique el cumplimiento de controles específicos de la Norma ISO/IEC 27001 en la Unidad Educativa Fe y Alegría.

El objetivo principal de esta aplicación es proporcionar una herramienta eficaz para verificar el cumplimiento de los requisitos y controles esenciales establecidos por la Norma ISO 27001. A través de un conjunto de validaciones en base a una métrica de ponderación especializadas, la aplicación se centrará en garantizar que los sistemas de gestión de la seguridad de la información (SGSI) cumplan con los controles de seguridad necesarios para obtener la certificación ISO 27001.

Este prototipo se muestra como una alternativa para poder simplificar el proceso de certificación, permitiendo a las organizaciones que se enfocan en la educación realizar evaluaciones para poder evaluar los controles planteados. Ofreciendo una interfaz intuitiva con diferentes funciones de análisis detallados, generando reporte y mostrando grafica de cumplimiento de los controles.

Estado del arte:

La norma ISO 27001 es una norma internacional la cual es la encargada de definir los diferentes requisitos y lineamientos para la implementación de sistemas de gestión de la seguridad de la información dentro de una organización. Tiene como enfoque principal lograr una gestión eficaz para poder salvaguardar la confidencialidad que se encarga de garantizar el acceso a la información solo a personal autorizado, integridad que se encarga que los datos se mantengan fiables durante el periodo de procesamiento y almacenamiento, y disponibilidad que el proceso encargado de mantener accesible la información para su uso[1].

Existen diferentes investigaciones y proyectos basados en la norma ISO 27001, los cuales impulsan la información acerca de cómo realizar el manejo adecuado de seguridad de la información en diferentes organizaciones e instituciones. Un ejemplo de ello es el trabajo realizado por Tigse Moposita (2020), proyecto de investigación, titulado "PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA" realizado en la Universidad Técnica de Ambato, el cual aborda la aplicación de la norma ISO 27001 en el ámbito tecnológico [2].

También, existe evidencia de la aplicación e implementación de controles de seguridad informática según la ISO 27001 enfocado en el contexto educativo, en el proyecto realizado por Solís Granda (2018) titulado "DESARROLLO E IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA PARA EL SISTEMA ERP ACADEMIUM DE LA UNIDAD EDUCATIVA JAVIER". Este proyecto muestra de qué manera se puede ejecutar la aplicación de la norma ISO 27001 dentro de entornos educativos e indica como establecer diferentes medidas para la gestión de la seguridad de la información [3].

Objetivos

General

Diseñar, implementar y desarrollar un sistema web que facilite la evaluación del cumplimiento de la norma ISO 27001 en el contexto de sistemas de gestión de seguridad de la información en la unidad educativa Fe y Alegría.

Específicos

- Analizar la Norma ISO 27001 para comprender sus requisitos, principios y enfoques en la gestión de seguridad de la información.
- Identificar y seleccionar los controles a evaluar en la Unidad Educativa en relación con la seguridad de la información.
- Desarrollar un sistema web capaz de evaluar el cumplimiento de los controles de la Norma ISO 27001.
- Llevar a cabo pruebas de funcionalidad del sistema web implementado para verificar su eficacia al momento de evaluar los controles de la norma ISO 27001.
- Validar la aplicación como una herramienta eficaz para facilitar el proceso de evaluación de la norma ISO 27001.

II. Marco teórico

Norma ISO 27001

La norma internacional ISO 27001 ayuda a garantizar la seguridad, confidencialidad e integridad de los datos, la información y los sistemas que los manejan. La versión actualizada, ISO 27001:2022, en el área de Sistemas de Gestión de la Seguridad de la Información, permite a las empresas evaluar riesgos y aplicar medidas necesarias para reducirlos o eliminarlos. Adoptar ISO 27001 supone una diferencia significativa al proporcionar a la empresa una ventaja competitiva y mejorar su reputación [4].

La norma ISO 27001 cuenta con una estructura detallada para los Sistemas de Gestión de Seguridad de la Información. A continuación, se presenta un resumen de su estructura:

- **Alcance:** Establece el ámbito del SGSI y los requisitos obligatorios [5].
- **Introducción:** Proporciona una visión general de la norma, su propósito y su relación que esta atiene con otras normas [1].
- **Contexto de la Organización:** Detalla la comprensión de la organización, se enfoca en su contexto externo e interno, y las partes interesadas relevantes [1].
- **Liderazgo:** Establece roles y responsabilidades de la alta dirección en la implementación y mantenimiento del SGSI [4].
- **Planificación:** Incluye la identificación de riesgos y oportunidades, así como la planificación para abordarlos [5].
- **Soporte:** Cubre recursos, competencia, conciencia y comunicación interna [1].
- **Operación:** Detalla la planificación y control de procesos para tratar los riesgos y oportunidades [6].
- **Evaluación del Desempeño:** Incluye la medición, monitoreo, análisis y evaluación del desempeño del SGSI [7].
- **Mejora:** Establece procesos para la mejora continua del SGSI [4].

Ventajas de implementar un SGSI bajo la norma ISO 27001

Existen varias ventajas al momento de implementar un SGSI, a continuación, se enlistarán algunas de esas ventajas:

- Facilita los procesos de sincronización y equilibrio de los procesos de seguridad [7].
- A pesar de la imposibilidad de eliminar por completo el riesgo, posibilita la creación de metodologías para mitigar y fortalecer la seguridad de la información [7].
- En situaciones de riesgo, minimiza las pérdidas y establece un plan de acción eficiente [7].
- Cumple con los diferentes requisitos legales que establecen las autoridades de control [7].
- La norma ISO 27001 aporta un valor adicional a la empresa, ya que esta certificación aún no es común en muchas organizaciones [7].
- Optimiza la eficiencia de la organización, esto implica una gran mejora en la reducción de costos [7].
- Promueve la confianza entre los diferentes miembros de la entidad, incluidos clientes, proveedores y empleados de la organización [7].
- Habilita la activación de alertas ante actividades sospechosas [7].
- Facilita el seguimiento y monitoreo de los controles de seguridad [7].
- Sirve como herramienta eficaz para la planificación y seguimiento de procesos [7].
- Contribuye de manera exponencial a la reputación y la imagen corporativa [7].
- Proporciona una metodología clara y efectiva [7].
- Minimiza y previene de riesgos de pérdida o robo de información [7].

Seguridad de la información

La seguridad de la información puede describirse como un proceso integral responsable de salvaguardar la identificación, gestión y los riesgos inherentes a la información. El enfoque de la seguridad de la información implica implementar diferentes estrategias y acciones de mitigación para garantizar la confidencialidad de los datos de la organización. Es de gran importancia diferenciar entre seguridad de la información y seguridad informática, ya que la seguridad informática se centra en la seguridad en entornos informáticos, estos pueden ser equipos físicos de la organización, mientras que la seguridad de la información aborda cualquier tipo de información, ya sea digital o impresa. Dentro de los aspectos que abarca la seguridad de la información se puede encontrar la disponibilidad, comunicación, detección de problemas, análisis de riesgos, integridad, confidencialidad y recuperación de riesgos[7].

Dentro de la seguridad de la información se encuentran tres elementos que son considerados claves e indispensables para la implementación de seguridad en cualquier organización:

- **Personas:** Son los responsables de la gestión y manipulación de la información, esto abarca los empleados, directivos, autoridades competentes, clientes, proveedores, contratistas y proveedores de servicios [7].
- **Procesos:** Establece las acciones que se realizan para alcanzar los diferentes objetivos establecidos por las organizaciones, siendo muchas de ellas dependientes de información y, por ende, susceptibles a vulnerabilidades [7].
- **Tecnología:** Vinculada a los servicios y estructuras empresariales, dirige la gestión y desarrollo de la información. Adicionalmente, proporciona la capacidad de almacenar, recuperar, compartir y mantener los datos de valor almacenados [7].

Sistemas de Gestión de la Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información es considerado como el núcleo fundamental de la norma ISO 27001. Es por ello que se define a la seguridad de la información como la protección de la confidencialidad, integridad y disponibilidad. Es mediante estos tres aspectos que se lleva a cabo el análisis y la evaluación de los activos de información [7].

Un SGSI debe estar enfocado en los siguientes fundamentos:

- **Confidencialidad:** Implica que la información no puede ser divulgada ni compartida con personas, entidades o procesos no autorizados por la organización [8].
- **Integridad:** Se centra en preservar la precisión y totalidad de la información de la organización, así como de sus métodos de procesamiento [8].
- **Disponibilidad:** Se centra en el acceso y uso de la información y sus sistemas de procesamiento por individuos, entidades o procesos autorizados, según las necesidades de la organización [8].

Node JS

Node js es un entorno de ejecución de JavaScript, este nos permite realizar ejecuciones de código del lado del servidor, lo cual ayuda para poder ampliar las capacidades del lenguaje más allá del navegador web, posibilitando el desarrollo de aplicaciones de red altamente escalables y de alto rendimiento [9]

Node js se destaca en el desarrollo de aplicaciones web y móviles, APIs RESTful, servicios de mensajería en tiempo real, entre otros. Su ecosistema de paquetes npm es uno de los más grandes del mundo, lo que simplifica la integración de diversas funcionalidades y bibliotecas en las aplicaciones Node.js [10]

MySQL

MySQL es una base de datos utilizada principalmente en la informática. Oracle lo ha desarrollado y soportado. MySQL trabaja mediante el modelo cliente-servidor, los datos se encuentran dentro del servidor y para obtener acceso a ellos es donde se involucra el cliente. Cuenta con una doble licencia que combina código abierto y opciones comerciales, lo cual hace que esta herramienta sea atractiva tanto para los proyectos de código abierto como para empresas que buscan soluciones de base de datos. MySQL se destaca por su confiabilidad, rendimiento y posibilidad de expansión. Ofrece una serie de características, incluyendo una única arquitectura que puede integrarse con diferentes plataformas y lenguajes de programación. [11].

Express JS

Express JS es un framework backend encargado del desarrollo de aplicaciones web basadas en Node.js. Cuenta con una amplia gama de funcionalidades, características, herramientas y diferentes plugins encargados de ayudar a simplificar los procesos de desarrollo destinadas a la creación de aplicaciones tanto para la web como para dispositivos móviles, destacándose por su facilidad de uso y flexibilidad en el proceso de desarrollo. Los desarrolladores tienen la potestad de asignar diferentes funciones específicas a rutas URL, lo que facilita la implementación de APIs y la creación de aplicaciones web dinámicas y escalables. La principal característica de Express radica en la capacidad que tiene para simplificar la creación de aplicaciones del lado del servidor, proporciona una estructura ligera y versátil que permite a los programadores configurar middleware de forma personalizada para gestionar solicitudes y respuestas de manera eficiente [12].

III. Metodología/Técnicas/Diseño

Metodología:

El proyecto de integración curricular fue elaborado mediante una metodología ágil basada en el marco de trabajo Scrum, este marco de trabajo es ampliamente utilizado en el ámbito de desarrollo de proyectos ágiles. En esta metodología en particular se destacan diferentes roles los cuales son clave y cada uno desempeña un papel fundamental para la elaboración y cumplimiento de los requerimientos del proyecto, los roles son: el Scrum Master, el Product Owner y Team Development. Cada uno de estos roles desempeña funciones específicas que son de gran importancia a medida que se van cumpliendo los objetivos planteados, en la tabla 1 se puede observar de qué manera se asignaron los roles para el equipo de trabajo.

TABLA I
ROLES SCRUM

Roles Scrum			
Código	Rol	Integrante	Descripción
01	Scrum Master	Ing. Pablo Francisco Puente Ponce	Líder del equipo Scrum
02	Product Owner	Danny Javier Bedoya Garcia	Representante del equipo de trabajo
03	Team Development	Diego Garcia Flores	Desarrolladores del modelo y aplicativo web

Nota: Asignación de roles scrum.

En la gestión ágil de proyecto, el Backlog del Proyecto desempeña un papel crucial al proporcionar una visión detallada y estructurada de todas las tareas pendientes y objetivos a alcanzar. Este elemento, esencial en metodologías como Scrum, se presenta como una tabla dinámica que evoluciona a lo largo del ciclo de desarrollo. El Backlog captura tanto las funcionalidades prioritarias como los elementos adicionales, permitiendo una planificación flexible y adaptativa. A través de esta herramienta, se logra una comunicación efectiva entre los diferentes roles del equipo, como el Product Owner, el Scrum Master y los miembros del Team Development. En la tabla 2 se puede observar de manera detallada. El tiempo estimado de desarrollo del proyecto es de setenta y ocho días aproximadamente, los cuales se llevarán a cabo en el respectivo periodo 202351.

TABLA II
PRODUCT BACKLOG

Código	Nombre	Tiempo estimado (Días)	Prioridad	Orden
R1	Recolección de datos	10	Alta	1
R2	Planeación de aplicativo web	5	Alta	2
R3	Análisis de base de datos	3	Alta	3
R4	Creación de base de datos	2	Alta	4
R5	Desarrollo de login	8	Alta	5
R6	Implementaciones de seguridad	5	Alta	6
R7	Desarrollo de vistas CRUD para los usuarios	10	Alta	7
R8	Desarrollo de vistas CRUD para los formularios	10	Alta	8
R9	Creación de vista de previsualización de los formularios	10	Alta	9
R10	Desarrollo de front end	3	Alta	10
R11	Elaboración de documentación y entregables	8	Alta	11
R12	Evaluación y corrección	4	Alta	12

Nota: asignación de producto backlog.

En el marco de metodología SCRUM, se estructuraron tres sprints estratégicos para guiar el desarrollo del proyecto. En el primer sprint, con una duración de 20 días, se ha focalizado en la fase inicial del proyecto, priorizando la investigación y la creación de la base de datos. Este enfoque inicial sienta las bases esenciales para el éxito futuro del proyecto, asegurando una comprensión

profunda de los requisitos y estableciendo una robusta infraestructura de datos. Teniendo en cuenta el enfoque del proyecto el cual es de desarrollo de software también durante este sprint se deberá seleccionar las diferentes herramientas y entornos de trabajo que se usarán para cuando se inicie la fase de desarrollo. A través de esta tabla 3, detallaremos la planificación específica de este primer sprint.

TABLA III
SPRINT 1

Sprint 1			
Duración del Sprint		07 Noviembre 2023 al 05 Diciembre 2023	
Días de trabajo		20	
Miembro del equipo	Días hábiles durante el Sprint	Horas hábiles por día	Horas hábiles por Sprint
Danny Bedoya	20	8	160

Nota: detalles de sprint 1.

En el marco del Sprint 2 de la metodología SCRUM del proyecto, fue netamente orientado hacia el desarrollo de la aplicación web. Este sprint, con una duración específica de 33 días, se enfoca en la implementación de las funcionalidades planificadas en el proyecto, avanzando desde la fase de investigación y diseño hasta la fase de ejecución. En el cual se empieza a programar el backend del sistema web, en la tabla 4 se puede observar los detalles del sprint 2.

TABLA IV
SPRINT 2

Sprint 2			
Duración del Sprint		06 Diciembre 2023 al 20 Enero 2024	
Días de trabajo		33	
Miembro del equipo	Días hábiles durante el Sprint	Horas hábiles por día	Horas hábiles por Sprint
Danny Bedoya	33	8	264

Nota: detalles de sprint 2.

En el último sprint de la metodología SCRUM, con una duración de 24 días, estuvo centrado en la fase culminante del proyecto. Durante este período, se llevó a cabo un exhaustivo proceso de refinamiento, donde cada detalle del proyecto fue minuciosamente revisado y perfeccionado. Este sprint final no solo representa el cierre operativo del proyecto, sino también la fase crucial de evaluación y mejora continua. en la tabla 5 se puede observar los detalles del sprint 3.

TABLA V
SPRINT 3

Sprint 3			
Duración del Sprint		21 Enero 2024 al 23 Febrero 2024	
Días de trabajo		24	
Miembro del equipo	Días hábiles durante el Sprint	Horas hábiles por día	Horas hábiles por Sprint
Danny Bedoya	24	8	192

Nota: detalles de sprint 3.

Técnicas:

Para la obtención de datos que puedan aportar a la elaboración del sistema web se realizó un análisis documental, en el cual se buscaba obtener la mayor información para la evaluación del cumplimiento de la norma ISO 27001. En el estudio realizado por Tanía López, nos da a conocer los principales cambios que existen en la versión de la ISO 27001 de la última versión lanzada en 2022. Menciona que existen 93 controles que se encuentran en el Anexo A distribuidos en cuatro dominios. El Anexo A es una tabla la cual brinda controles de seguridad para que las organizaciones puedan seleccionar e implementarlos dependiendo sus necesidades y en función de la evaluación de riesgos y el plan que vayan a implementar para tratar estos mismos, Los controles son los siguientes:

- **Controles Organizacionales:** Incluyen 37 controles relacionados con la gestión de la seguridad de la información a nivel organizacional, como políticas, procedimientos y responsabilidades para garantizar la protección de la información dentro de la empresa [14].
- **Controles Orientados a las Personas:** Se refiere a 8 controles que abordan la seguridad de la información en relación con el personal de la organización, tales como la gestión de recursos humanos, la concienciación sobre seguridad y la capacitación en seguridad de la información [14].
- **Controles Físicos:** Comprende 14 controles diseñados para proteger los recursos físicos de la organización, como las instalaciones, equipos y dispositivos de almacenamiento, a fin de prevenir accesos no autorizados o daños físicos a la información [14].
- **Controles Tecnológicos:** Involucra 34 controles relacionados con la seguridad de los sistemas de información y la tecnología utilizada para procesar, almacenar y transmitir datos, abordando aspectos como el acceso lógico, la gestión de activos y la seguridad de la red [14].

Para seleccionar los controles a evaluar en la unidad educativa se usó como técnica una encuesta, la cual fue realizada a la persona que nos fue designada el cual era el encargado del área

de informática, también contaba con el apoyo del área administrativa para determinar y responder las preguntas, en la siguiente tabla podemos observar los controles que fueron mencionados en base a la importancia de estos mismos dentro del entorno analizado para una organización educativa.

TABLA VI.
RESULTADOS DE ENTREVISTA A LA UNIDAD EDUCATIVA.

Control	Pregunta	SI	NO
Equipo de usuario desatendido	¿Cuenta con equipos que trabajen de manera autónoma sin la intervención de un usuario?	X	
Mensajería electrónica	¿Usa el servicio de mensajería electrónica?	X	
Actividades de seguimiento	¿Se realizan revisiones periódicas de funcionamiento en los sistemas?	X	
Zonas de entrega y carga	¿Cuenta con zonas establecidas para entrega y carga?	X	
Monitoreo de seguridad física	¿Cuenta con un sistema para el monitoreo de la seguridad física?	X	
Protección de la información de registro	¿Cuenta con registros almacenados para la manipulación de la información?	X	
Restricciones en la instalación de software	¿Cuenta con restricciones para la instalación de software?	X	
Protección de servicios de aplicaciones en redes públicas	¿Cuenta con medidas y prácticas diseñadas para garantizar la seguridad de los servicios y aplicaciones que se ejecutan a través de redes públicas?	X	

Nota: detalles de los resultados obtenidos de la encuesta.

TABLA VII
RESULTADOS DE ENTREVISTA A LA UNIDAD EDUCATIVA

Control	Pregunta	SI	NO
Protección de transacciones de servicios de aplicaciones	¿Cuenta con medidas para garantizar la seguridad de las transacciones realizadas?	X	
Seguridad de la información para el uso de servicios en la nube.	¿Usan el servicio en la nube?	X	
Continuidad del negocio	¿Tienen un plan de continuidad del negocio?	X	
Enmascaramiento de datos	¿Usan la técnica de enmascaramiento de datos para datos sensibles?	X	
Políticas de seguridad de la información	¿Tienen políticas para la seguridad de la información?	X	
Uso de activos	¿Tienen clasificados los activos?	X	
Pruebas de aceptación del sistema	¿Realizan pruebas en los sistemas que manejan?	X	
Propiedad de los activos	¿Clasifican las propiedades de todos los activos?	X	
Política de dispositivos móviles	¿Tienen políticas para el manejo de dispositivos móviles?	X	
Eliminación de información	¿Tienen un protocolo para la eliminación de datos?	X	

Nota: detalles de los resultados obtenidos de la encuesta.

Los controles mencionados en la encuesta fueron seleccionados en base a la técnica de observación estructurada del entorno, no obstante, en base a esta misma técnica existen otros controles que deben ser evaluados a pesar que la unidad educativa no cumpla con estos, esto con la finalidad de fortalecer la seguridad de la información y los diferentes procesos que se desempeñan en la organización.

TABLA VIII
RESULTADOS DE TÉCNICA DE OBSERVACIÓN ESTRUCTURADA DEL ENTORNO

Control	Pregunta
Sistemas de gestión de contraseñas	La unidad cuenta con diferentes equipos los cuales son asignados al personal de la institución, es por ello que debe cada uno de estos manejar contraseñas para controlar el acceso no autorizado a usuarios que no corresponden. También debe tener políticas para el manejo de contraseñas seguras y cambios periódicas de estas mismas
Inteligencia de amenazas	La zona donde se encuentra la unidad educativa puede ser considerada de alto riesgo, no solo para los activos tecnológicos, si no para el personal. Implementar políticas y sistemas para evaluar estos es importante para la mejorar las medidas de seguridad.
Codificación segura	La unidad educativa al contar con una carrera técnica, imparte conocimientos acerca de desarrollo de software. Por ello tener políticas para hacer uso de buenas prácticas para codificación segura es importante.
Gestión de la configuración	La unidad educativa cuenta con varios equipos tanto para el área administrativa y el área de laboratorios la cual es enfocada para los estudiantes. Gestionar la configuración de los equipos para supervisarlos y garantizar la integridad de los sistemas.
Filtrado web	Al tener una red de internet las organizaciones suelen ser vulnerables al no tener un control sobre estas mismas. Aplicar filtrado para que los usuarios ingresen y así también mejorar la eficiencia.

Nota: detalles de los resultados obtenidos de la técnica de observación estructurada del entorno.

TABLA IX
RESULTADOS DE TÉCNICA DE OBSERVACIÓN ESTRUCTURADA DEL ENTORNO

Control	Pregunta
Eliminación de activos	Eliminar activos de manera segura es importante para proteger información sensible, al contar con múltiples equipos que contienen información catalogada como sensible es importante tener diferentes procesos para en caso de ser necesario eliminar estas se hagan de manera correcta sin poner en riesgo la información.
Evaluación permanente de debilidades en la seguridad de la información	Tener un encargado que supervise de manera activa y periódica la información de la institución es de gran importancia. Al contar con diferentes en las diferentes áreas, es importante realizar evaluaciones regulares para identificar las debilidades en la seguridad de la información.
Revisión de cumplimiento técnico	La unidad educativa maneja grandes conjuntos de información, tanto por la parte administrativa, así como la parte de estudiantes. Es importante garantizar que esta información este siendo manipulada de manera correcta y que cumpla con las normas y políticas que se deben establecer.

Nota: detalles de los resultados obtenidos de la técnica de observación estructurada del entorno.

Una vez aplicadas las técnicas se determinaron los respectivos controles para realizar el sistema web, esto basándose en el alcance del mismo y en los grupos de controles ya mencionados. Los controles a evaluar son los siguientes:

Controles Tecnológicos y Personas

El grupo de Controles Tecnológicos y Personas se refiere a la combinación de medidas tecnológicas y la participación activa de individuos en la implementación y ejecución de prácticas de seguridad de la información. Este enfoque utiliza diferentes tecnologías como sistemas de seguridad informática, también usa softwares de protección de datos y herramientas de gestión de riesgos con la finalidad de poder salvaguardar la integridad y confidencialidad de la información. Sin embargo, el éxito de estas medidas de controles tecnológicos también depende de la conciencia

y el comportamiento de las personas que se encuentran involucradas en el control de estos sistemas [15].

Para ello se debe capacitar al personal en prácticas seguras, fomentar una cultura de ciberseguridad y alentar al personal para asumir la responsabilidad individual en la protección de datos y sistemas. Además, las personas desempeñan un papel clave en la detección temprana de posibles amenazas, la respuesta rápida a incidentes de seguridad y la colaboración en la mejora continua de los procesos técnicos de seguridad [16]. Los controles son los siguientes:

- **Sistema de Gestión de Contraseñas:** Involucra diferentes tecnologías que se encargan de gestionar contraseñas, este control depende de la intervención y el comportamiento de las personas de la organización al utilizar y mantener las contraseñas seguras.
- **Equipo de usuario desatendido:** Trata de equipos que trabajan de manera independiente sin necesidad de una supervisión continua de un encargado. No obstante, puede requerir de la atención y entrenamiento de usuarios para asegurar que los equipos desatendidos estén protegidos mediante tecnologías y buenas prácticas.
- **Mensajería electrónica:** La mensajería electrónica requiere de buenas prácticas y del manejo apropiado teniendo en cuenta los controles de seguridad pertinentes. Requiere la atención y comportamiento adecuado de las personas al utilizar la mensajería electrónica, así como tecnologías para proteger estas mismas.
- **Inteligencia de amenazas:** Es un proceso de recopilación, análisis y comprensión de amenazas, Este proceso depende de la habilidad y experiencia de personas en la identificación de posibles riesgos.
- **Actividades de seguimiento:** Las personas desempeñan un rol importante dentro de este control en conjunto con las tecnologías que ayudan a detectar comportamientos anormales. Se requiere de la supervisión y registro de actividades.

- **Codificación segura:** Se deben emplear buenas prácticas para el desarrollo de software, esto requiere de la intervención de personas para asegurar la integridad del código.
- **Enmascaramiento de datos:** Se encarga de ocultar o distorsionar datos sensibles durante el procesamiento de estos mismos, esto implica el uso de tecnologías para este proceso.

Controles Físicos y Organizacionales

El grupo de Controles Físicos y Organizacionales se enfoca en implementar diferentes medidas tangibles y en establecer políticas y procedimientos para garantizar la seguridad y el cumplimiento dentro de una organización. Los controles físicos son aquellos que incluyen diferentes aspectos como la seguridad física de las instalaciones, el control de acceso a áreas restringidas y la protección de activos físicos contra daños o intrusos. Por otro lado, los controles organizacionales son aquellos que abarcan la formulación de políticas, la asignación de responsabilidades para las diferentes áreas, la creación de estructuras de gobierno y la implementación de prácticas de gestión de riesgos y cumplimiento dentro de la organización [15].

Estos controles no solo se encargan de prevenir amenazas físicas y mitigar riesgos, sino que también son los responsables de promover la eficiencia operativa, la transparencia y la responsabilidad dentro de la organización. La combinación efectiva de controles físicos y organizacionales es de gran importancia dentro de las organizaciones para garantizar la protección integral de los activos y la información de una empresa, así como para mantener la integridad y la reputación de la organización en su conjunto, los controles son los siguientes:

- **Zonas de entrega y carga:** Se trata de la asignación física de áreas específicas para la entrega y carga,
- **Monitoreo de seguridad física:** Se trata de la implementación de medidas físicas para el monitoreo y la protección de la seguridad física de instalaciones de la organización, así mismo para sus activos.

- **Continuidad del negocio:** Se refiere a la planificación y ejecución de diferentes medidas organizacionales que se encargan de mantener las operaciones críticas bajo situaciones adversas y así poder garantizar la continuidad del negocio.

Controles Tecnológicos y Organizacionales

El grupo de Controles Tecnológicos y Organizacionales se encarga de la gestión efectiva y segura de una organización. Los controles tecnológicos se refieren a las medidas y sistemas que implementa la organización para proteger los activos de información y garantizar la integridad, confidencialidad y disponibilidad de los datos. Comúnmente se incluye la utilización de firewalls, cifrado de datos, sistemas de detección de intrusiones y políticas de seguridad de la información. Los controles organizacionales se enfocan en las políticas, procedimientos y estructuras de gobernanza establecidas para supervisar y regular el comportamiento de los empleados de la organización. [15].

Estos controles abarcan diferentes aspectos como la asignación adecuada de roles y responsabilidades dentro de la organización, la capacitación en cuanto a la seguridad informática del personal, la elaboración de políticas de seguridad y la realización de auditorías internas para controlar y evaluar el cumplimiento y la eficacia de los controles que se encuentren establecidos. Los controles tecnológicos y organizacionales son de gran importancia dentro de las organizaciones para proteger los activos y la reputación de una organización, así como para garantizar su continuidad operativa en un entorno cada vez más digitalizado y complejo, los controles son los siguientes:

- **Protección de la información de registro:** Es el manejo de tecnologías las cuales son las encargadas de proteger la información de registro.
- **Restricciones en la instalación de software:** Son la implementación de tecnologías encargadas de controlar y restringir instalaciones de softwares de terceros no permitidos por la organización, también cuenta con políticas organizacionales.
- **Protección de servicios de aplicaciones en redes públicas:** Implementa tecnologías que se encargan de proteger los servicios de aplicaciones. También cuenta con políticas organizacionales relacionadas al respecto.

- **Protección de transacciones de servicios de aplicaciones:** Es la implementación de tecnologías encargadas de proteger transacciones, estos pueden ser sitios web bancarios o servicios de pagos en línea.
- **Gestión de la configuración:** Se trata de la implementación de políticas y tecnologías para gestionar y controlar los cambios en la configuración de sistemas y software. También se realiza un seguimiento de este control para que los cambios que se realicen a las configuraciones sean controlados.
- **Prevención de fuga de datos:** Se trata de la implementación de políticas organizacionales para evitar la salida no autorizada de información considerada, esto con la finalidad de salvaguardar datos sensibles y prevenir amenazas.
- **Pruebas de aceptación del sistema:** Se trata de la participación de personas en la realización de pruebas y la definición de procesos organizacionales para poder realizar una verificación de cumplimiento del sistema.
- **Seguridad de la información para el uso de servicios en la nube:** Son políticas que se encargan de medir diferentes procesos como autenticación, cifrado de datos y gestión de accesos. Implementa políticas organizacionales para garantizar la seguridad de la información al utilizar servicios en la nube.
- **Filtrado web:** Son políticas organizacionales enfocadas en el control y monitoreo de los sitios web a los que se tiene acceso. Esto sirve para reducir riesgos de la seguridad cibernética, controlando el acceso a sitios maliciosos, contenido web inapropiado o no autorizado.

Controles Organizacionales y Personas

El grupo de Controles Organizacionales y Personas está centrado en las políticas, procedimientos y estructuras dentro de una organización. Sirven para poder regular el comportamiento humano y garantizar la eficiencia operativa dentro de la organización. Estos controles son esenciales para promover la integridad, la transparencia y la responsabilidad en todas las áreas de la organización, desde la toma de decisiones hasta la ejecución de tareas diarias [15]. Los controles son los siguientes:

- **Políticas de seguridad de la información:** Son un conjunto de reglas y directrices organizacionales las cuales están diseñadas con la finalidad de proteger los activos de la organización. Son principalmente para garantizar seguridad y confidencialidad de información considerada como sensible.
- **Uso de activos:** Este control es importante para el funcionamiento eficiente de la organización. La organización debe tener políticas en donde se establezcan procedimientos y reglas para el uso de los activos.
- **Eliminación de activos:** Son diferentes procesos dentro de una organización, debe contar con la participación activa de personas para asegurar la eliminación segura de activos de manera adecuada. Los activos antes de ser eliminados deben estar correctamente identificados y previamente realizado un proceso de eliminación.
- **Pruebas de aceptación del sistema:** Involucra la participación de personas en la realización de pruebas y la definición de los procesos organizacionales para llevarlas a cabo. Deben definirse diferentes procesos que los respalden.
- **Evaluación permanente de debilidades en la seguridad de la información:** Implica la participación de personas en la evaluación continua y la implementación de procesos organizacionales para identificar debilidades y mitigar riesgos existentes con la finalidad de mantener la integridad, confidencialidad y disponibilidad de los datos.
- **Revisión de cumplimiento técnico:** Requiere la revisión de personas para evaluar el cumplimiento técnico y la implementación de procesos organizacionales para esta revisión se realiza una evaluación exhaustiva de los sistemas de la organización.
- **Propiedad de los activos:** Se refiere a la definición de la propiedad de activos y la participación de personas en su gestión adecuada sobre los diferentes recursos de la organización, estos recursos pueden ser tangibles o intangibles.
- **Política de dispositivos móviles:** Involucra la definición de políticas organizacionales para el uso de dispositivos móviles y la colaboración de personas

en su implementación. Son un conjunto de reglas y directrices que establece la organización para el uso responsable de dispositivos móviles.

- **Eliminación de información:** Incluye procedimientos organizacionales y la participación de personas para garantizar la eliminación segura de información, evitando exposiciones no autorizadas.

Diseño:

Arquitectura de sistema web

El sistema web desarrollado para la verificación del cumplimiento de la Norma ISO 27001 en la Unidad Educativa Fe y Alegría se basa en una arquitectura de tres componentes como podemos observar en la Figura 1 en el cual se observa que incluye un usuario, la aplicación web y la base de datos.

- **Usuario:** Representa a los usuarios finales que interactúan con la aplicación web. Pueden ser administradores o los evaluadores que acceden al sistema para realizar diversas acciones, como ingresar información, generar informes o verificar el cumplimiento de las normativas de seguridad informática.
- **Aplicación Web:** Desarrollada utilizando Node js, Express y tecnologías JavaScript, este componente constituye el núcleo funcional del sistema. Se encarga de recibir las solicitudes del usuario, procesarlas y enviar respuestas adecuadas. Utiliza MySQL como gestor de base de datos para almacenar y gestionar la información relacionada con la verificación de cumplimiento de la Norma ISO 27001.
- **Base de Datos:** MySQL se emplea como el motor de almacenamiento de datos para la aplicación. Aquí se guardan todos los registros, configuraciones y datos relevantes para el proceso de verificación de cumplimiento. La base de datos proporciona la capacidad de almacenamiento y recuperación eficiente de la información necesaria para el funcionamiento del sistema.



Fig. 1. Arquitectura de sitio web.

Nota: diseño de la arquitectura del sistema web.

Esquema de interfaz de usuario

El esquema de la interfaz de usuario está diseñado con un enfoque claro en la navegación y la interacción con el contenido a través de la integración de API. En la Figura 2 se puede observar un esquema de cómo está distribuida la interfaz de usuario.

- **Encabezado de navegación:** La interfaz presenta un encabezado que proporciona elementos identificativos y opciones de navegación para los usuarios. Esto incluye enlaces a las diferentes secciones del sistema y opciones de inicio de sesión para acceder a funcionalidades personalizadas.
- **Opciones de sesión de usuario:** Dentro del encabezado de navegación, se incluyen las opciones de inicio de sesión para que los usuarios puedan autenticarse y acceder a sus cuentas personalizadas, lo que les permite interactuar con el sistema de manera segura y acceder a funcionalidades exclusivas.
- **Apartado de contenido con consumo de API:** La interfaz también cuenta con un área de contenido donde se presentan los datos y la información relevante para los usuarios. Este contenido se obtiene a través de la integración con API, lo que permite recuperar datos de fuentes externas y mostrarlos de manera dinámica en la interfaz de usuario. Las API se utilizan para proporcionar actualizaciones en tiempo real y garantizar que la información presentada sea precisa y relevante.



Fig. 2. Esquema de interfaz de usuario.

Nota: boceto realizado para la interfaz de usuario.

Base de datos

En base al funcionamiento de la aplicación, se determinó la base de datos con sus diferentes campos, la base de datos cuenta con cuatro tablas, en la Figura 3 podemos observar las respectivas tablas. La tabla usuario es donde se registrarán cada uno de los datos del usuario que cumple el rol de evaluador. La tabla institución tendrá los registros de la institución. La tabla formulario almacenara los resultados de cada uno de los ítems que se van a evaluar mientras que observacion_formulario almacena las observaciones de los ítems que serán evaluados. La tabla rasci contendrá los valores de fecha de cumplimiento y las respectivas evidencias. Por último, la planificación donde se agregará la tarea asignada y los responsables bajo la matriz RASCI.

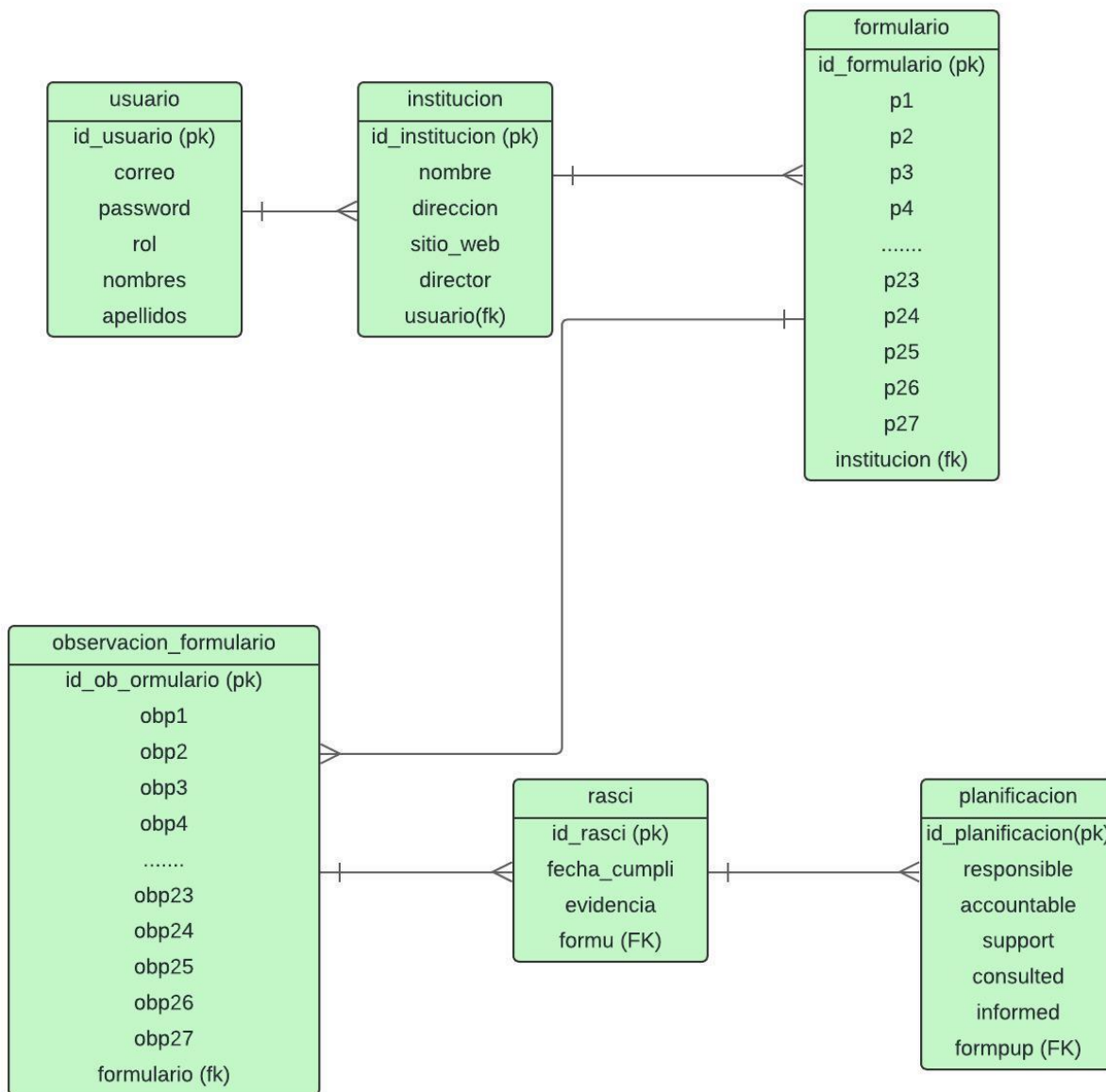


Fig. 3. Base de datos

Nota: esquema de la base de datos.

Acceso a la aplicación web

Para acceder a la funcionalidad completa del sitio web debe realizarse un inicio de sesión previo, este proceso va a garantizar la seguridad y privacidad de usuarios que pueden acceder al sistema. En caso de no tener una cuenta se puede realizar el registro de un usuario nuevo, mediante el cual se debe llenar la información requerida. Para ambos procesos se usan técnicas de

encriptación, asegurando que los datos se almacenen de manera segura en la base de datos. También se usaron las técnicas necesarias para agregar contraseñas que cumplan con los requisitos para ser de alta seguridad. Los resultados obtenidos fueron satisfactorios, en la Figura 4 se puede observar el inicio de sesión, que es donde el usuario final podrá acceder a la aplicación en caso de tener una cuenta. En la Figura 5 se observa el apartado de registro de usuario, únicamente se debe llenar los campos con los datos requeridos y el formulario realizara las respectivas validaciones de estos mismos como podemos observar en la Figura 6.



ISO27001 VALIDATION

Iniciar Sesión Registrarse

INICIAR SESIÓN

Correo*

Ingrese su correo electrónico

Contraseña*

Ingrese su contraseña

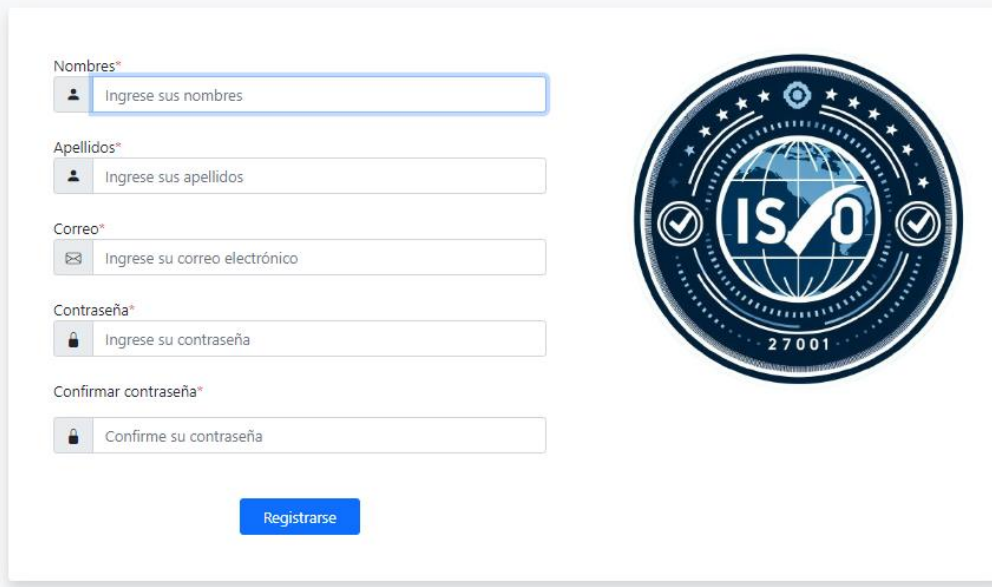
Ingresar



Fig. 4. Interfaz de inicio de sesión.

Nota: interfaz que se muestra al usuario final para que realice el inicio de sesión.

REGISTRARSE



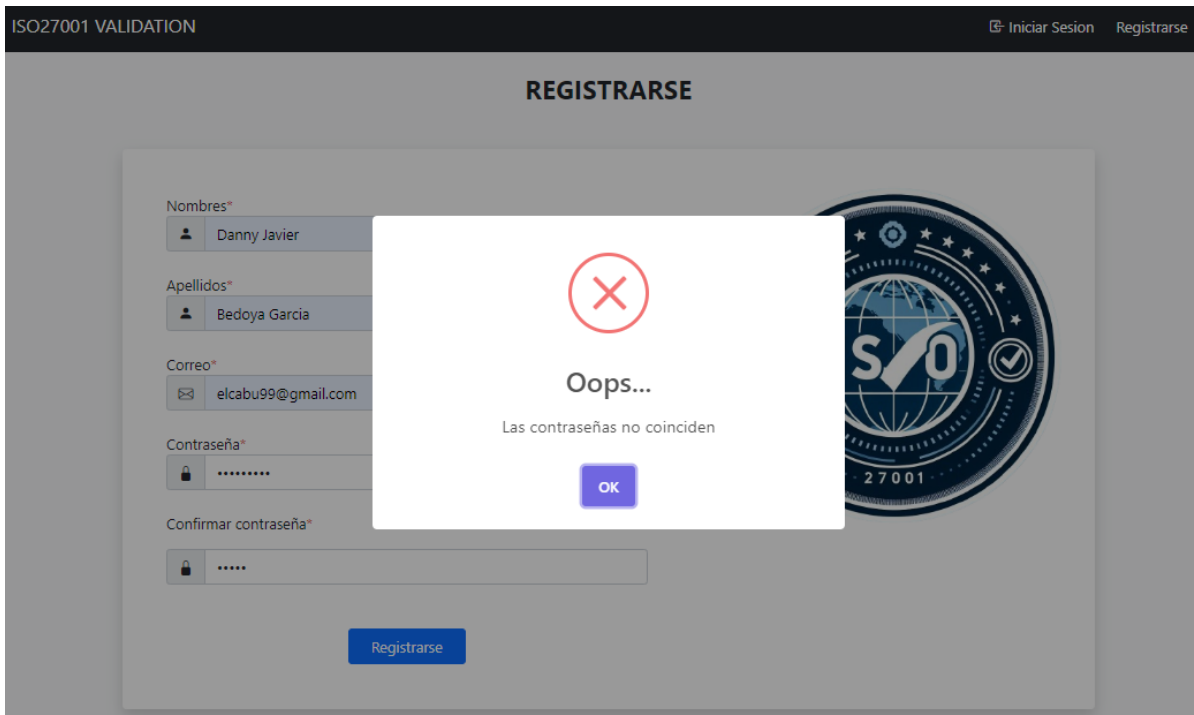
The registration form is titled "REGISTRARSE" and is set against a light gray background. On the right side of the form is a circular logo for ISO 27001, featuring a globe and the text "ISO 27001". The form contains five input fields, each with a small icon and a placeholder text:

- Nombres***: Input field with a person icon and placeholder "Ingrese sus nombres".
- Apellidos***: Input field with a person icon and placeholder "Ingrese sus apellidos".
- Correo***: Input field with an envelope icon and placeholder "Ingrese su correo electrónico".
- Contraseña***: Input field with a lock icon and placeholder "Ingrese su contraseña".
- Confirmar contraseña***: Input field with a lock icon and placeholder "Confirme su contraseña".

At the bottom center of the form is a blue button labeled "Registrarse".

Fig. 5. Interfaz de registro de usuario.

Nota: interfaz que se muestra al usuario final para realizar el registro de un usuario nuevo.



The registration form is shown with a gray background. The form fields are filled with the following data:

- Nombres***: Danny Javier
- Apellidos***: Bedoya Garcia
- Correo***: elcabu99@gmail.com
- Contraseña***: (masked)
- Confirmar contraseña***: (masked)

A white error message box is overlaid on the form, containing a red "X" icon, the text "Oops...", and "Las contraseñas no coinciden". Below the message is a blue "OK" button. At the bottom center of the form is a blue button labeled "Registrarse".

Fig. 6. Validaciones opciones de inicio y registro.

Nota: comprobación de validaciones de campos.

Consumo de API

El consumo de API en el sistema permitió llevar a cabo operaciones CRUD (Crear, Leer, Actualizar y Eliminar) en las tablas "institucion" y "formulario". A través de estas operaciones, los usuarios pudieron interactuar de manera dinámica con los datos almacenados en la base de datos, permitiendo la creación, visualización, actualización y eliminación de registros relacionados con instituciones y formularios. El uso de API facilitó la integración de estas funcionalidades dentro del sistema, proporcionando una forma eficiente y segura de manipular la información almacenada, garantizando la consistencia y la integridad de los datos.

Una vez realizado el proceso de inicio de sesión, se puede acceder al aplicativo web, para lo cual se redireccionará al apartado de "Perfil", donde se mostrarán los datos del usuario que acaba de iniciar sesión, en la Figura 7 podemos observar esta interfaz. También se habilitará en el navegador un nuevo acceso al apartado "Instituciones", en ese apartado nos mostrará las instituciones que el usuario haya registrado, en caso de no haber ninguna institución se debe registrar una, en la Figura 8 se puede observar el apartado donde se registra la institución. Una vez ya registrada la institución ya se puede observar la misma en el apartado "Instituciones" como se observa en la Figura 9.

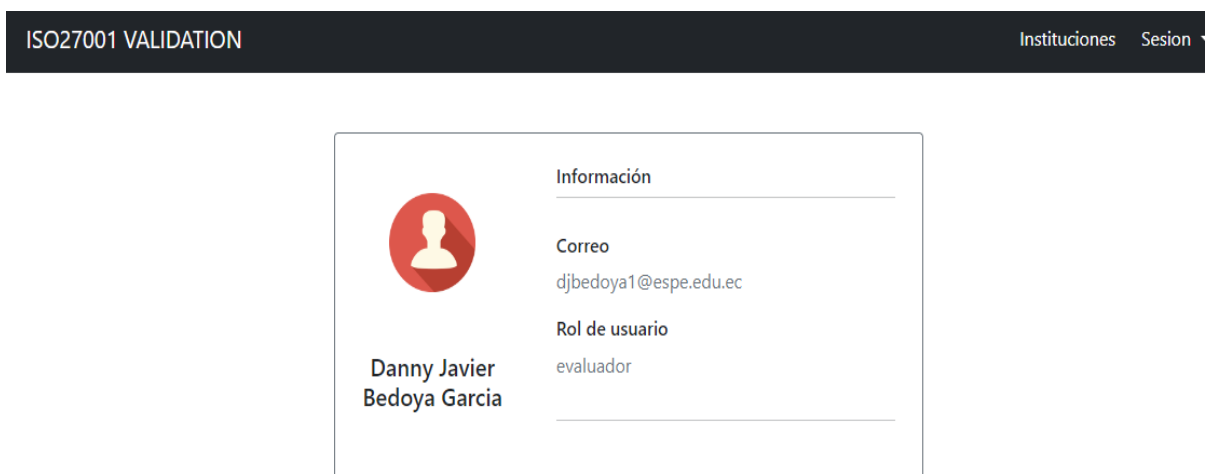


Fig. 7. Interfaz de apartado "Perfil".

Nota: vista de perfil de usuario donde se muestran los datos del usuario que inicia al sistema.

Institución

Unidad Educativa Fe y Alegria

Santo Domingo


Diego Garcia Flores

https://www.feyalegria.org.ec/zona-santc

[Guardar](#) [Cancelar](#)

Fig. 8. Interfaz de registro de institución.

Nota: vista para registrar la institución al sistema.

 Institución creada correctamente

Instituciones registradas

[Registrar una nueva Institución](#)



Unidad Educativa Fe y Alegria
Santo Domingo

[Eliminar](#) [Editar](#) [Evaluar](#)

Fig. 9. Interfaz de lista de instituciones.

Nota: interfaz que muestra las instituciones registradas, en este caso se encuentra la unidad educativa Fe y alegría.

Cada institución cuenta con las opciones de “eliminar”, “editar” y “evaluar” en la Figura 8 se muestran estas opciones. Cuando se quiere eliminar un registro se muestra una ventana de confirmación como se muestra en la Figura 10. Al seleccionar la opción editar se podrá editar los datos de la institución, este es un formulario donde se obtienen los datos de la institución seleccionada, en la Figura 11 se puede observar la vista de edición. El apartado evaluar nos muestra una nueva vista donde nos muestra los datos de la institución, en la Figura 12 se muestra esa vista, esta vista también nos muestra dos botones adicionales los cuales son “Evaluar institución” el cual nos da paso a realizar el proceso de evaluación de la norma ISO 27001, el otro botón “Evaluaciones anteriores” donde se podrán ver procesos de evaluación anteriores en caso de existir registros.

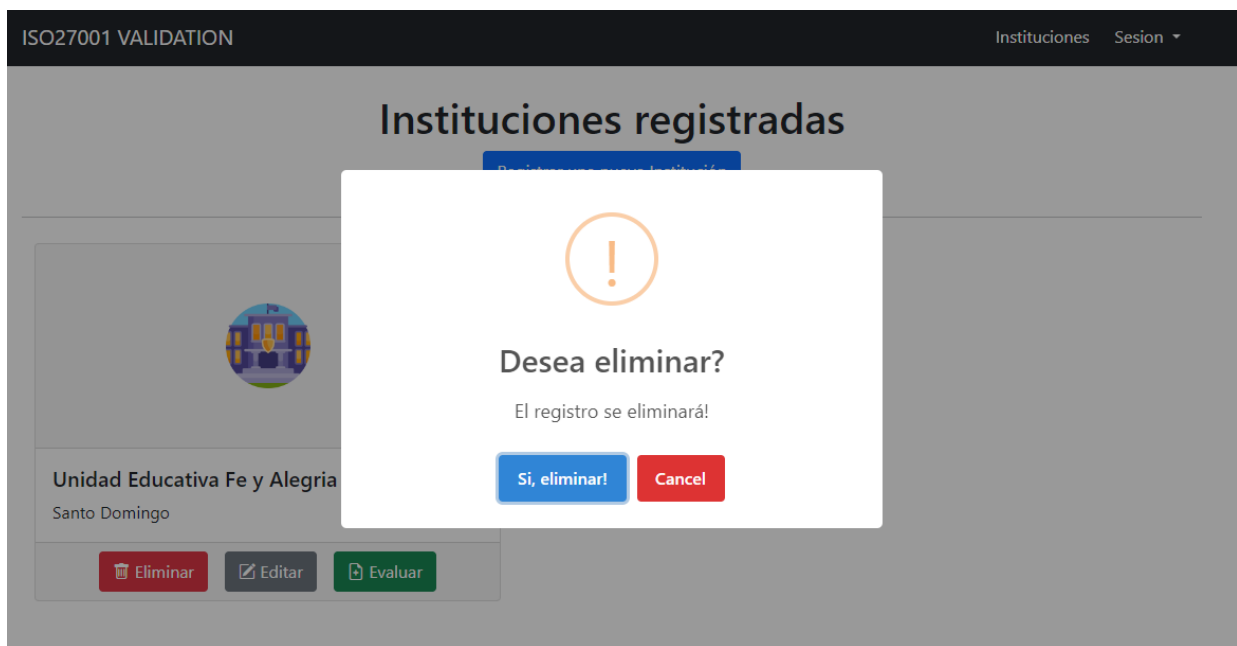



Fig. 10. Confirmación de eliminación de institución.

Nota: alerta de validación para eliminar registros.

Editar Institución

Fig. 11. Vista de editar institución.

Nota: vista para editar el registro de institución.



Unidad Educativa Fe y Alegria

Información

Dirección	Director/a
Santo Domingo	Diego Garcia Flores

[Sitio Web](#)

Fig. 12. Vista de institución.

Nota: vista principal de la institución donde se observan los botones para realizar la evaluación.

La opción evaluar institución nos lleva directamente al formulario de evaluación el cual es el proceso de evaluación, en la Figura 13 podemos observar el formulario, este consta de checkboxes para poder validar cada uno de los controles, estos controles se encuentran clasificados en sus respectivos grupos. Para que la aplicación sea más interactiva se implementó una ventana emergente que nos da información de cada uno de los controles, para acceder a esta se debe dar click al icono de información en la Figura 14 se puede observar la ventana.

Proceso de Evaluación

El proceso de evaluación tiene un rango de ponderación el cual es 0 (Inexistente), 10 (Informal), 50 (Intuitivo), 90 (Proceso definido), 95 (Gestionable y medible) y 100 (Optimizado)

Controles Tecnológicos y Personas	Controles Tecnológicos y Organizacionales
<p>Sistema de gestión de contraseñas. ⓘ</p> <p><input type="radio"/> 0 <input type="radio"/> 10 <input type="radio"/> 50 <input type="radio"/> 90 <input type="radio"/> 95 <input type="radio"/> 100</p> <p>Observaciones</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p style="text-align: center;">Agregar tarea ⓘ</p> <p>Fecha máxima de cumplimiento</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p>Evidencia</p> <div style="border: 1px solid #ccc; padding: 2px;"> Seleccionar archivo Ninguno archivo selec. </div>	<p>Protección de la información de registro. ⓘ</p> <p><input type="radio"/> 0 <input type="radio"/> 10 <input type="radio"/> 50 <input type="radio"/> 90 <input type="radio"/> 95 <input type="radio"/> 100</p> <p>Observaciones</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p style="text-align: center;">Agregar tarea ⓘ</p> <p>Fecha máxima de cumplimiento</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p>Evidencia</p> <div style="border: 1px solid #ccc; padding: 2px;"> Seleccionar archivo Ninguno archivo selec. </div>
<p>Equipo de usuario desatendido. ⓘ</p> <p><input type="radio"/> 0 <input type="radio"/> 10 <input type="radio"/> 50 <input type="radio"/> 90 <input type="radio"/> 95 <input type="radio"/> 100</p> <p>Observaciones</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p style="text-align: center;">Agregar tarea ⓘ</p> <p>Fecha máxima de cumplimiento</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p>Evidencia</p> <div style="border: 1px solid #ccc; padding: 2px;"> Seleccionar archivo Ninguno archivo selec. </div>	<p>Restricciones en la instalación de software. ⓘ</p> <p><input type="radio"/> 0 <input type="radio"/> 10 <input type="radio"/> 50 <input type="radio"/> 90 <input type="radio"/> 95 <input type="radio"/> 100</p> <p>Observaciones</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p style="text-align: center;">Agregar tarea ⓘ</p> <p>Fecha máxima de cumplimiento</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p>Evidencia</p> <div style="border: 1px solid #ccc; padding: 2px;"> Seleccionar archivo Ninguno archivo selec. </div>
<p>Mensajería electrónica. ⓘ</p> <p><input type="radio"/> 0 <input type="radio"/> 10 <input type="radio"/> 50 <input type="radio"/> 90 <input type="radio"/> 95 <input type="radio"/> 100</p> <p>Observaciones</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p style="text-align: center;">Agregar tarea ⓘ</p> <p>Fecha máxima de cumplimiento</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p>Evidencia</p>	<p>Protección de servicios de aplicaciones en redes públicas. ⓘ</p> <p><input type="radio"/> 0 <input type="radio"/> 10 <input type="radio"/> 50 <input type="radio"/> 90 <input type="radio"/> 95 <input type="radio"/> 100</p> <p>Observaciones</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p style="text-align: center;">Agregar tarea ⓘ</p> <p>Fecha máxima de cumplimiento</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <p>Evidencia</p>

Fig. 13. Vista de proceso de evaluación.

Nota: vista de proceso de evaluación donde se mostrarán diferentes Checklist de los controles a evaluar y las respectivas asignaciones de tareas, fecha y evidencia.

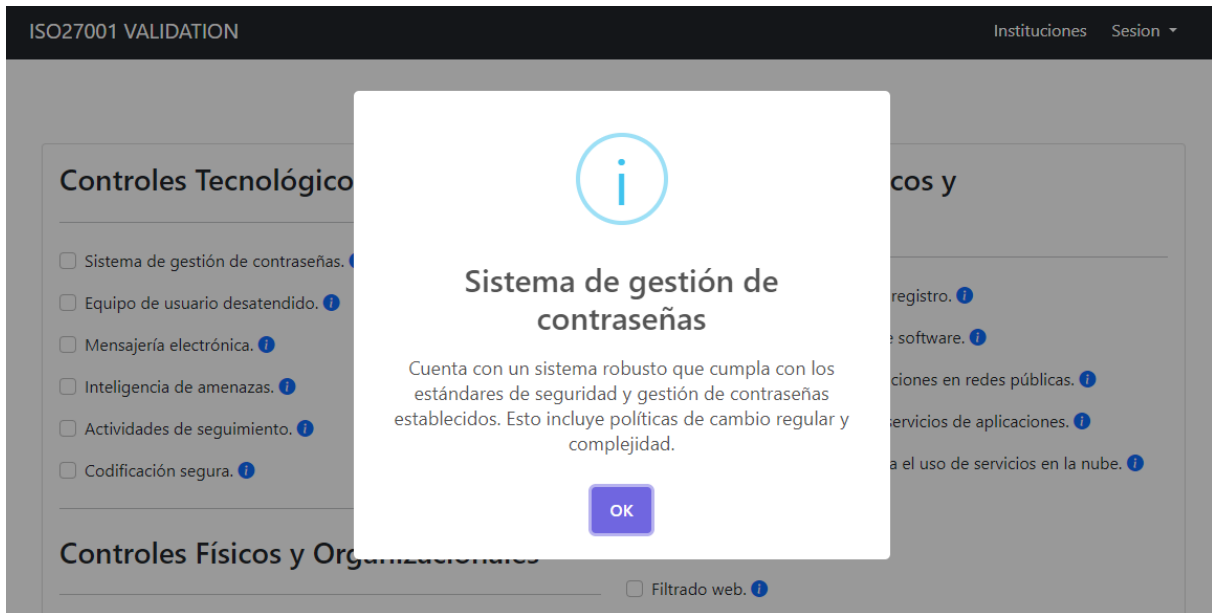


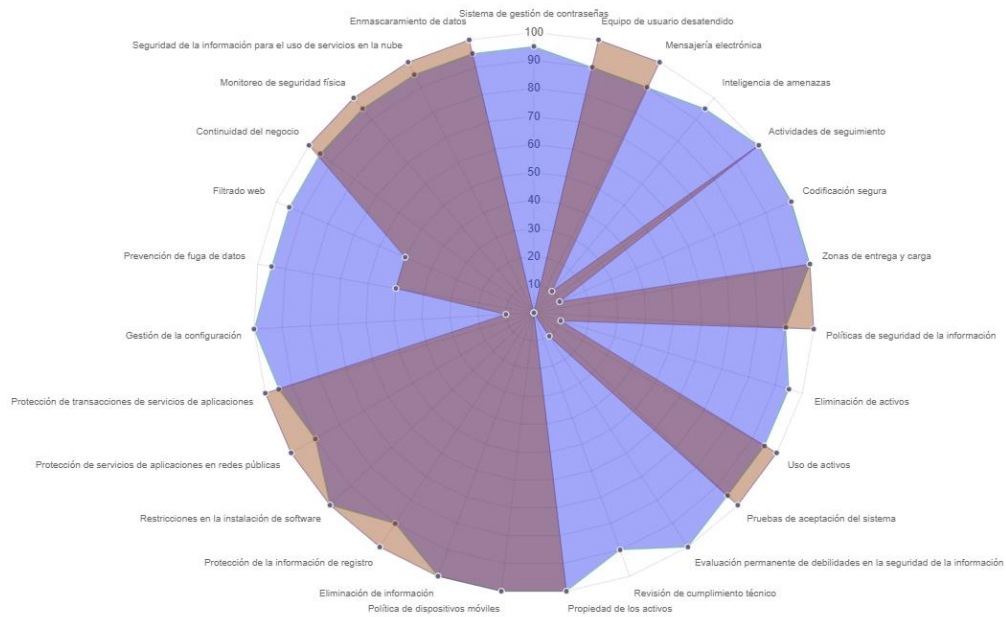
Fig. 14. Ventana emergente de información acerca de los controles.

Nota: alerta emergente donde se muestra información adicional acerca de cada control.

Al terminar con el proceso de evaluación, esto nos redirige a la vista donde se listan todas las evaluaciones realizadas como se puede observar en la Figura 15. La opción imprimir nos genera un reporte PDF el cual fue creado mediante funcionalidades propias de JavaScript, aquí nos genera el reporte físico el cual será impreso y firmado por el evaluador y el director de la institución para su aprobación, en la Figura 16, Figura 17 y Figura 28 se puede observar este reporte.

Evaluaciones registradas

■ Evaluación 1 ■ Evaluación 2




	
Evaluación 1	Evaluación 2
Evaluado: 12 de marzo de 2024, 13:05:17	Evaluado: 12 de marzo de 2024, 13:16:51
Editar	Editar

Fig. 15. Vista de evaluaciones registradas.

Nota: vista donde se muestran las diferentes evaluaciones realizadas con su respectiva gráfica.

Reporte de la evaluación

Unidad educativa Fe y Alegría

La calificación de la evaluación es: 2580

Cumple con los controles evaluados.

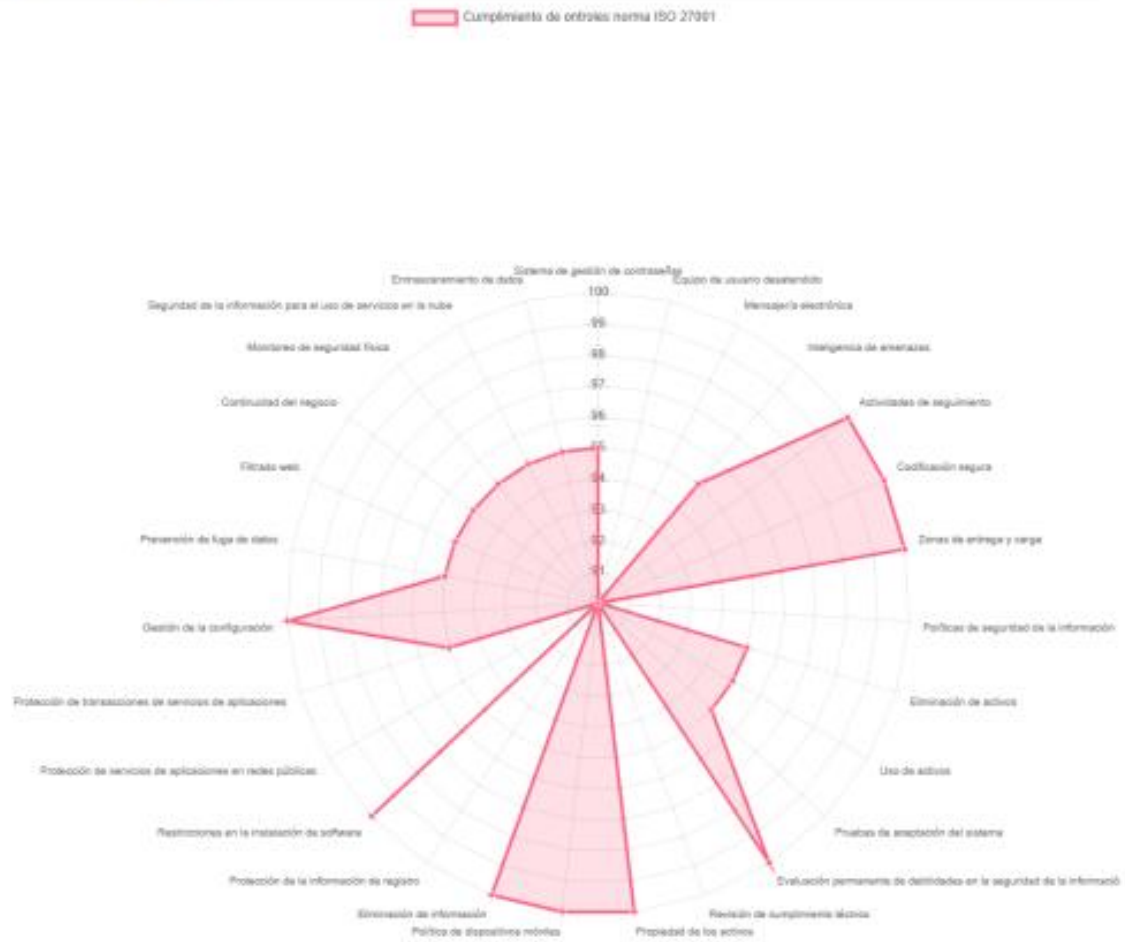


Fig. 16. Reporte PDF de evaluación.

Nota: reporte PDF generado desde el sistema.

Tabla de Evaluación

Calificación	Significado
2565 - 2700	Cumple con los controles evaluados.
2430 - 2565	Cumple, pero se requiere mejora mínima en los controles evaluados.
1350 - 2430	Próximo a cumplir los controles evaluados.
270 - 1350	No cumple con los requisitos de los controles evaluados.
0 - 270	No cumple con ningún control evaluado.

Controles Tecnológicos y Personas

Sistema de gestión de contraseñas

Calificación	95
Tarea 1	Tarea no asignada
Tarea 2	Tarea no asignada
Tarea 3	Tarea no asignada
Tarea 4	Tarea no asignada

Matriz RASCI

Tarea 1	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 2	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Fig. 17. Reporte PDF de evaluación.

Nota: reporte PDF generado desde el sistema.

Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Codificación segura

Calificación	100
Tarea 1	Tarea no asignada
Tarea 2	Tarea no asignada
Tarea 3	Tarea no asignada
Tarea 4	Tarea no asignada

Matriz RASCI

Tarea 1	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 2	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 3	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado

Fig. 18. Reporte PDF de evaluación.

Nota: reporte PDF generado desde el sistema.

IV. Resultados

Con la aplicación web ya funcional se puede proceder a realizar la respectiva evaluación a la unidad educativa Fe y Alegría, para ello se realizó una visita técnica mediante la cual se evaluaron cada uno de los controles, esto con la finalidad de comprobar si la institución cumple con la norma ISO 27001. En este apartado se detallará cada uno de los resultados obtenidos.

Con la finalización de la evaluación realizada a la unidad educativa para comprobar el cumplimiento de la norma ISO 27001, se obtuvieron resultados detallados sobre el cumplimiento de los estándares establecidos por la norma ISO 27001 en la unidad educativa Fe y Alegría. Estos resultados proporcionan una visión integral de la situación actual de la institución en términos de seguridad de la información, identificando áreas de cumplimiento sólidas y posibles áreas de mejora. Además, se destacan un aserie de observaciones específicas para presentar un plan de mejora a la seguridad de los datos.

Cumplimiento de controles

Controles Tecnológicos y Personas

La unidad educativa cumple en gran medida con los controles tecnológicos y personas, no obstante al ser una organización que aun utiliza métodos convencionales para el manejo de datos no cuenta con un manejo apropiado para la seguridad de la información, se recomienda un plan de mejora para fortalecer la manera en la que la organización debe manejar estos controles, es por ello que en el proceso de planificación se realizaron diversas recomendaciones como plan de mejora, mediante la Figura 19 podemos observar una gráfica que representa el porcentaje de cumplimiento, de igual forma en la Tabla 10 los detalles de la evaluación de estos controles.

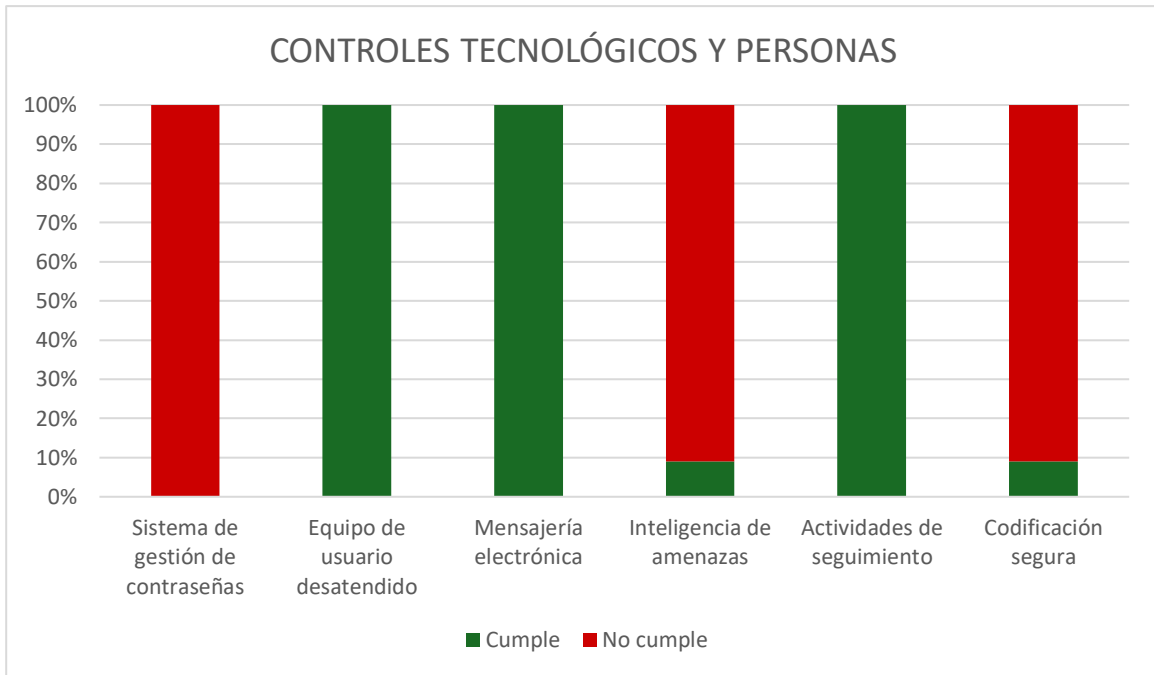


Fig. 19. Gráfica de cumplimiento de controles tecnológicos y personas.

Nota: grafica tipo pastel donde se muestran los resultados obtenidos de la evaluación en base a los controles tecnológicos y personas.

TABLA X
RESULTADOS DE CONTROLES TECNOLÓGICOS Y PERSONAS

Controles tecnológicos y personas		
Control	Estado	Planificación
Sistema de gestión de contraseñas	0%	Implementar un sistema de gestión de contraseñas robusto que cumpla con los estándares de seguridad y gestión de contraseñas, así como políticas de cambio regular y complejidad.
Equipo de usuario desatendido.	100%	Sin observación
Mensajería electrónica.	100%	Sin observación
Inteligencia de amenazas.	10%	Implementar sistemas y procesos para recopilar, analizar y utilizar inteligencia de amenazas. Para anticipar posibles riesgos y fortalecer las medidas de seguridad.
Actividades de seguimiento.	100%	Sin observación
Codificación segura.	10%	Proporcionar capacitación adecuada al personal de desarrollo sobre prácticas seguras de codificación.

Nota: resultados obtenidos de los controles tecnológicos y personas.

Controles Físicos y Organizacionales

La unidad educativa cumple con los controles físicos y organizacionales, entre los cuales se contempla que actualmente cuenta con una sólida estructura física para resguardar tanto la información como los activos de la organización, mediante la Figura 20 podemos observar una gráfica que representa el porcentaje de cumplimiento, de igual forma en la Tabla 11 los detalles de la evaluación de estos controles.



Fig. 20. Gráfica de cumplimiento de controles físicos y organizacionales.

Nota: grafica tipo pastel donde se muestran los resultados obtenidos de la evaluación en base a los controles físicos y organizacionales.

TABLA XI
RESULTADOS DE CONTROLES FÍSICOS Y ORGANIZACIONALES

Controles físicos y organizacionales		
Control	Estado	Planificación
Zonas de entrega y carga	100%	Sin observación

Nota: resultados obtenidos de los controles físicos y organizacionales.

Controles Físicos

La unidad educativa cumple con los controles físicos, mediante la Figura 21 podemos observar una gráfica que representa el porcentaje de cumplimiento, de igual forma en la Tabla 12 los detalles de la evaluación de estos controles.

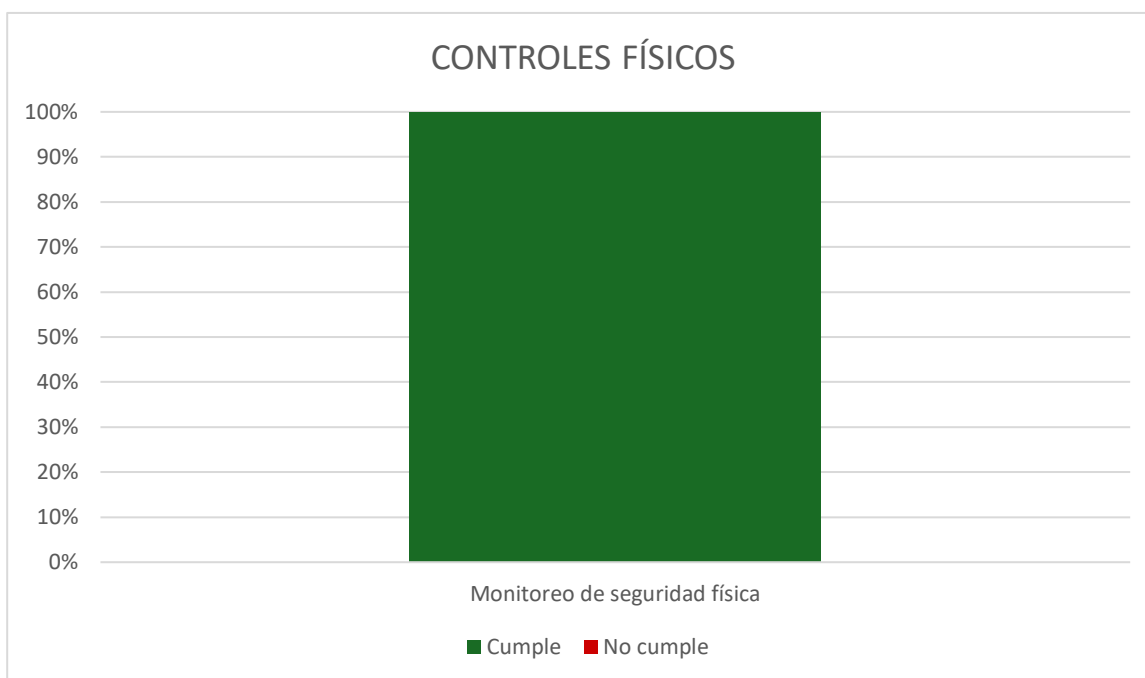


Fig. 21. Gráfica de cumplimiento de controles físicos.

Nota: grafica tipo pastel donde se muestran los resultados obtenidos de la evaluación en base a los controles físicos.

TABLA XII
RESULTADOS DE CONTROLES FÍSICOS

Controles físicos		
Control	Estado	Planificación
Monitoreo de seguridad física.	100%	Sin observación

Nota: resultados obtenidos de los controles físicos.

Controles Tecnológicos y Organizacionales

La unidad educativa cumple en gran medida con los controles tecnológicos y organizacionales, no obstante, se recomienda un plan de mejora en controles en los cuales se pudo detectar que no se están cumpliendo con los procesos, es por ello que en el proceso de planificación se realizaron diversas recomendaciones como plan de mejora, mediante la Figura 22 podemos observar una gráfica que representa el porcentaje de cumplimiento, de igual forma en la Tabla 13 los detalles de la evaluación de estos controles.

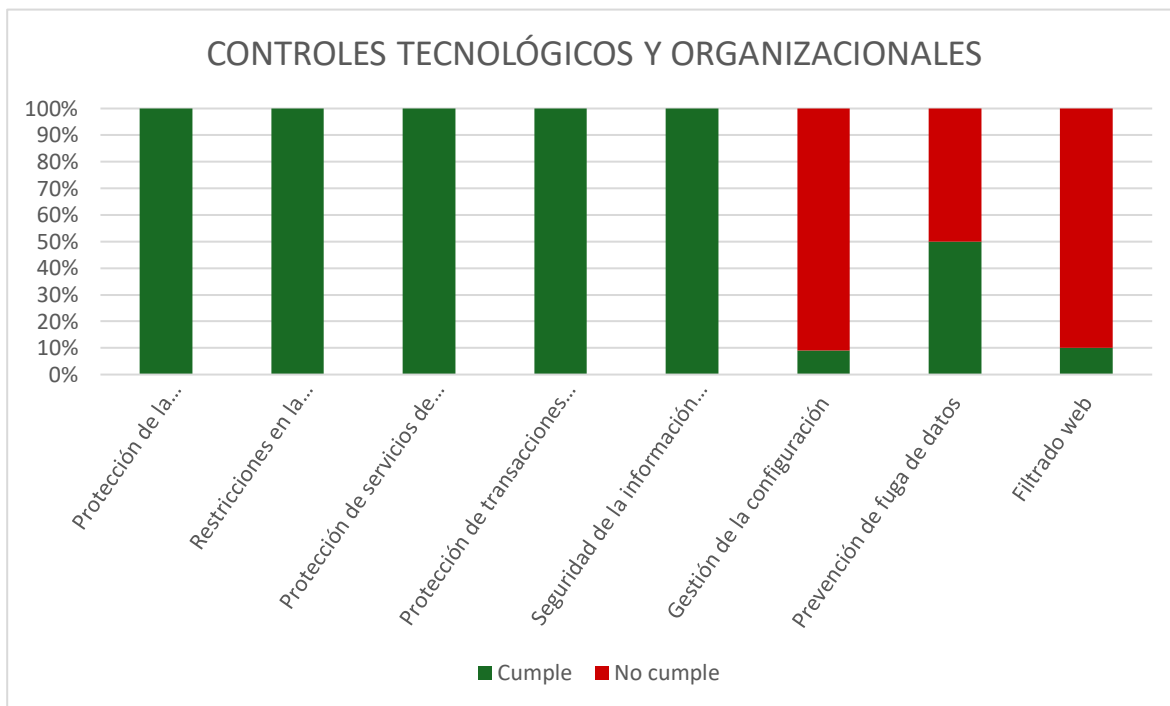


Fig. 22. Gráfica de cumplimiento de controles tecnológicos y organizacionales.

Nota: grafica tipo pastel donde se muestran los resultados obtenidos de la evaluación en base a los controles tecnológicos y organizacionales.

TABLA XIII
RESULTADOS DE CONTROLES TECNOLÓGICOS Y ORGANIZACIONALES

Controles tecnológicos y organizacionales		
Control	Estado	Planificación
Protección de la información de registro.	100%	Sin observación
Restricciones en la instalación de software.	100%	Sin observación
Protección de servicios de aplicaciones en redes públicas.	100%	Sin observación
Protección de transacciones de servicios de aplicaciones	100%	Sin observación
Seguridad de la información para el uso de servicios en la nube.	100%	Sin observación
Gestión de la configuración	10%	Gestionar y controlar las configuraciones de los sistemas y activos de información
Prevención de fuga de datos.	50%	Sin observación
Filtrado web.	10%	Controlar el filtrado web de la red de manera más estricta, esto con la finalidad de evitar posibles vulnerabilidades de filtración de datos. Capacitar al personal acerca de los sitios seguros y del manejo de datos.

Nota: resultados obtenidos de los controles tecnológicos y organizacionales.

Controles Organizacionales

La unidad educativa cumple con los controles organizacionales, mediante la Figura 23 podemos observar una gráfica que representa el porcentaje de cumplimiento, de igual forma en la Tabla 14 los detalles de la evaluación de estos controles.



Fig. 23. Gráfica de cumplimiento de controles organizacionales.

Nota: grafica tipo pastel donde se muestran los resultados obtenidos de la evaluación en base a los controles organizacionales.

TABLA XIV
RESULTADOS DE CONTROLES ORGANIZACIONALES

Controles organizacionales		
Control	Estado	Planificación
Continuidad del negocio.	100%	Sin observación

Nota: resultados obtenidos de los controles organizacionales.

Controles Tecnológicos

La unidad educativa cumple con los controles tecnológicos, mediante la Figura 24 podemos observar una gráfica que representa el porcentaje de cumplimiento, de igual forma en la Tabla 15 los detalles de la evaluación de estos controles.

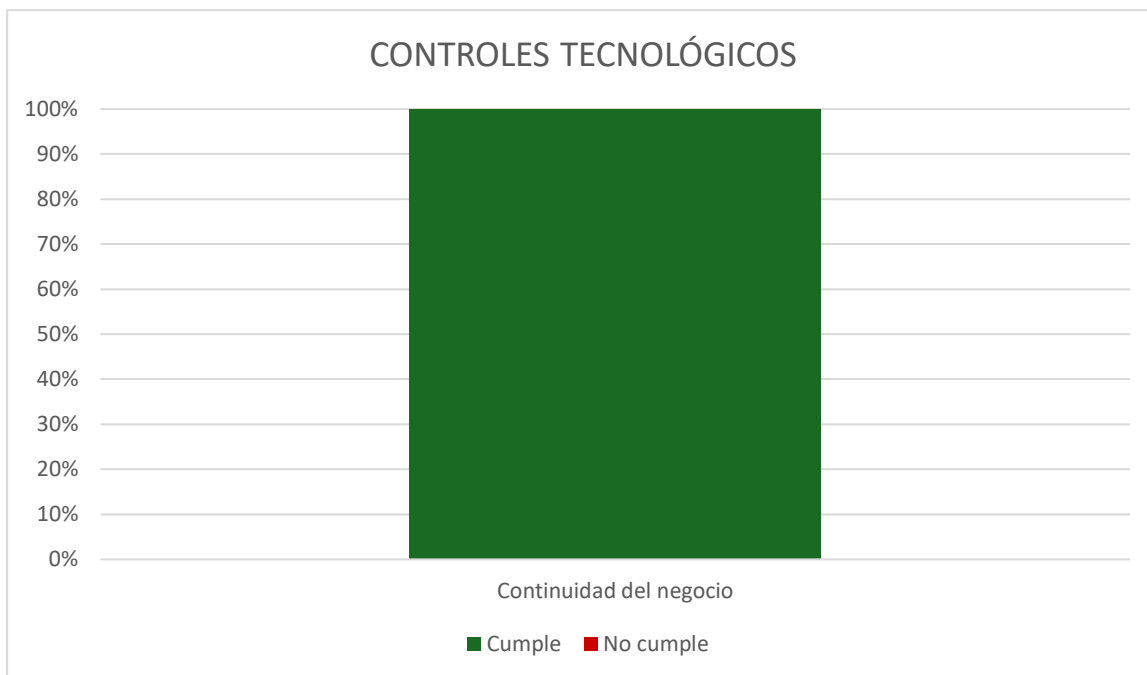


Fig. 24. Gráfica de cumplimiento de controles tecnológicos.

Nota: grafica tipo pastel donde se muestran los resultados obtenidos de la evaluación en base a los controles tecnológicos.

TABLA XV
RESULTADOS DE CONTROLES TECNOLÓGICOS

Controles tecnológicos		
Control	Estado	Planificación
Enmascaramiento de datos.	100%	Sin observación

Nota: resultados obtenidos de los controles tecnológicos.

Controles Organizacionales y Personas

La unidad educativa cumple en gran medida con los controles organizacionales y personas, no obstante, se recomienda un plan de mejora de los mismos, es por ello que en el proceso de planificación se realizaron diversas recomendaciones como plan de mejora, mediante la Figura 25 podemos observar una gráfica que representa el porcentaje de cumplimiento, de igual forma en la Tabla 16 los detalles de la evaluación de estos controles.



Fig. 25. Gráfica de cumplimiento de controles organizacionales y personas.

Nota: grafica tipo pastel donde se muestran los resultados obtenidos de la evaluación en base a los controles organizacionales y personas.

TABLA XVI
RESULTADOS DE CONTROLES ORGANIZACIONALES Y PERSONAS

Controles organizacionales y personas		
Control	Estado	Planificación
Políticas de seguridad de la información	100%	Sin observación
Eliminación de activos	10%	Crear procedimientos para la eliminación de activos, mediante seguimientos y auditorias periódicas (Requiere un encargado auditor).
Uso de activos.	100%	Sin observación
Pruebas de aceptación del sistema.	100%	Sin observación
Evaluación permanente de debilidades en la seguridad de la información.	10%	Asignar personal encargado capacitado para realizar evaluaciones regulares para identificar y abordar debilidades en la seguridad de la información.
Revisión de cumplimiento técnico	0%	Asignar personal encargado capacitado para realizar revisiones periódicas para garantizar el cumplimiento técnico de las normativas y estándares.
Propiedad de los activos.	100%	Sin observación
Política de dispositivos móviles.	100%	Sin observación
Eliminación de información.	100%	Sin observación

Nota: resultados obtenidos de los controles organizacionales y personas.

Reporte de evaluación

A continuación, se puede observar la primera versión del reporte generad. El reporte muestra datos generales de la institución y a su vez se debe evidenciar mediante la respectiva firma del evaluador y del representante de la institución. En la figura 28, Figura 29 y Figura 30 se puede observar el reporte final obtenido.

Página 1 de 3



Unidad Educativa Fe y Alegría

Evaluación norma ISO 27001
Santo Domingo

Nombre de la institución: Unidad Educativa Fe y Alegría

Fecha de Registro: 22/2/2024

Rector/a: Diego García Flores

Evaluado por: Danny Javier Bedoya García

Controles Tecnológicos y Personas

Control	Estado	Planificación
Sistema de gestión de contraseñas.	No cumple	Implementar un sistema de gestión de contraseñas robusto que cumpla con los estándares de seguridad y gestión de contraseñas, así como políticas de cambio regular y complejidad.
Equipo de usuario desatendido.	Cumple	Sin observación.
Mensajería electrónica.	Cumple	Sin observación.
Inteligencia de amenazas.	No cumple	Implementar sistemas y procesos para recopilar, analizar y utilizar inteligencia de amenazas. Para anticipar posibles riesgos y fortalecer las medidas de seguridad.
Actividades de seguimiento.	Cumple	Sin observación.
Codificación segura.	No cumple	Proporcionar capacitación adecuada al personal de desarrollo sobre prácticas seguras de codificación.

Controles Físicos y Organizacionales

Control	Estado	Planificación
Zonas de entrega y carga.	Cumple	Sin observación.

Fig. 26. Primer reporte de evaluación a la institución.

Nota: reporte PDF final generado por el sistema después de haber realizado la evaluación a la unidad educativa.

Control	Estado	Planificación
Monitoreo de seguridad física.	Cumple	Sin observación.

Controles Tecnológicos y Organizacionales

Control	Estado	Planificación
Protección de la información de registro.	Cumple	Sin observación.
Restricciones en la instalación de software.	Cumple	Sin observación.
Protección de servicios de aplicaciones en redes públicas.	Cumple	Sin observación.
Protección de transacciones de servicios de aplicaciones.	Cumple	Sin observación.
Seguridad de la información para el uso de servicios en la nube.	Cumple	Sin observación.
Gestión de la configuración.	No cumple	Gestionar y controlar las configuraciones de los sistemas y activos de información
Prevención de fuga de datos.	Cumple	Sin observación.
Filtrado web.	No cumple	Controlar el filtrado web de la red de manera mas estricta, esto con la finalidad de evitar posibles vulnerabilidades de filtración de datos. Capacitar al personal acerca de los sitios seguros y del manejo de datos.

Controles Organizacionales

Control	Estado	Planificación
Continuidad del negocio.	Cumple	Sin observación.

Fig. 27. Primer reporte de evaluación a la institución.

Nota: reporte PDF final generado por el sistema después de haber realizado la evaluación a la unidad educativa.

Control	Estado	Planificación
Enmascaramiento de datos.	Cumple	Sin observación.

Controles Organizacionales y Personas

Control	Estado	Planificación
Políticas de seguridad de la información.	Cumple	Sin observación.
Eliminación de activos.	No cumple	Crear procedimientos para la eliminación de activos, mediante seguimientos y auditorías periódicas (Requiere un encargado auditor).
Uso de activos.	Cumple	Sin observación.
Pruebas de aceptación del sistema.	Cumple	Sin observación.
Evaluación permanente de debilidades en la seguridad de la información.	No cumple	Asignar personal encargado capacitado para realizar evaluaciones regulares para identificar y abordar debilidades en la seguridad de la información.
Revisión de cumplimiento técnico.	No cumple	Asignar personal encargado capacitado para realizar revisiones periódicas para garantizar el cumplimiento técnico de las normativas y estándares.
Propiedad de los activos.	Cumple	Sin observación.
Política de dispositivos móviles.	Cumple	Sin observación.
Eliminación de información.	Cumple	Sin observación.



Evaluado por:
Danny Javier Bedoya Garcia



Aprobado por:
Diego Garcia Flores

Fig. 28. Primer reporte de evaluación a la institución.

Nota: reporte PDF final generado por el sistema después de haber realizado la evaluación a la unidad educativa.

De manera general los resultados obtenidos en la evaluación realizada a la unidad Educativa Fe y Alegría nos indica que se deben realizar mejoras en varias políticas, procesos y procedimientos de seguridad para obtener la certificación de la norma ISO 27001. Como bien se sabe en la reciente versión de la norma ISO 27001 la cual fue lanzada en 2022 se mostró un total de 93 controles, las organizaciones no están obligadas a cumplir todos estos, no obstante, si deben cumplir con algunos para implementar un Sistema de Gestión de la Seguridad de la Información. En la figura 29 observamos de manera general el porcentaje de cumplimiento de la unidad educativa.

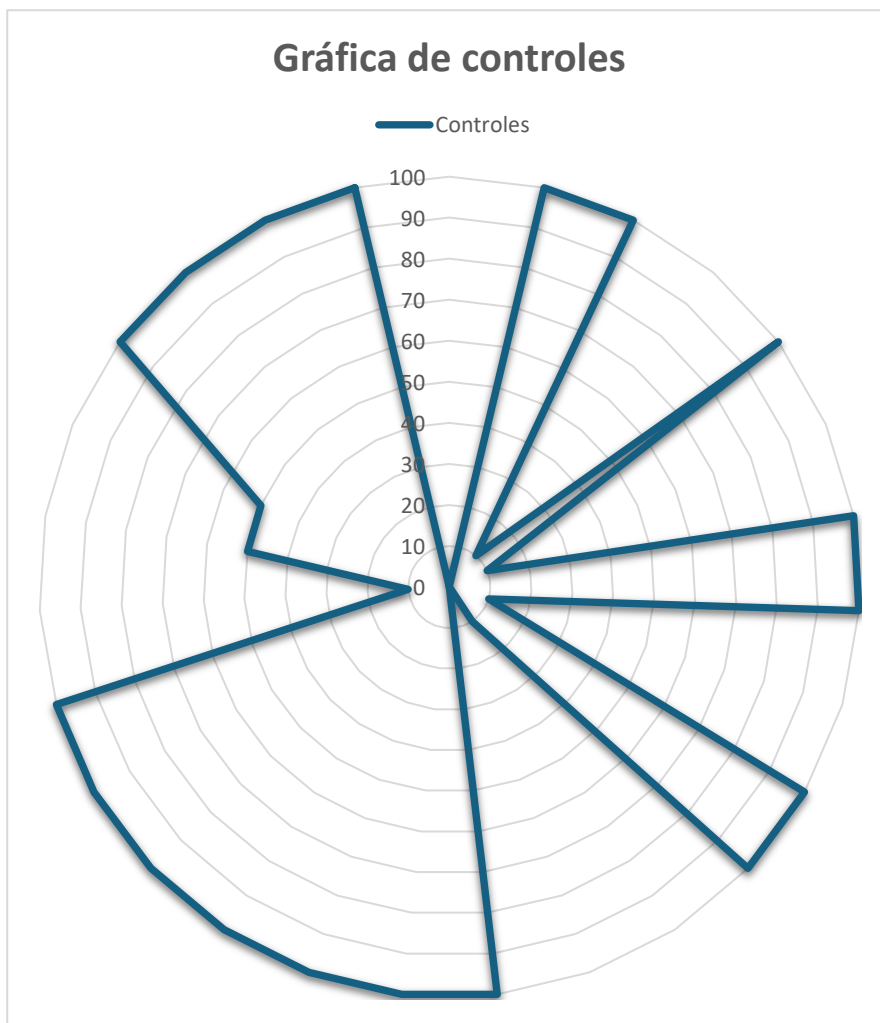


Fig. 29. Gráfica de cumplimiento de controles ISO 27001.

Nota: resultado de la evaluación de cumplimiento de la norma ISO 27001.

El reporte que se muestra de manera final con varios cambios realizados tomando en cuenta diferentes aspectos como la asignación de tareas y responsables bajo la matriz RASCI se puede observar en la Figura 30. Debido a que el reporte cuenta con un número total de 23 páginas únicamente se muestra una parte del reporte generado.

12/3/24, 9:15

Reporte

Reporte de la evaluación

Unidad educativa Fe y Alegría

La calificación de la evaluación es: 1950

Próximo a cumplir los controles evaluados.



about:blank

1/23

Fig. 30. Reporte final.

Nota: Reporte final del resultado de la evaluación de cumplimiento de la norma ISO 27001.

Tabla de Evaluación

Calificación	Significado
2565 - 2700	Cumple con los controles evaluados.
2430 - 2565	Cumple, pero se requiere mejora mínima en los controles evaluados.
1350 - 2430	Próximo a cumplir los controles evaluados.
270 - 1350	No cumple con los requisitos de los controles evaluados.
0 - 270	No cumple con ningún control evaluado.

Controles Tecnológicos y Personas**Sistema de gestión de contraseñas**

Calificación	0
Tarea 1	Implementar un sistema de gestión de contraseñas robusto
Tarea 2	Tarea no asignada
Tarea 3	Tarea no asignada
Tarea 4	Tarea no asignada

Matriz RASCI

Tarea 1	
Responsable de la ejecución	Jorge Zavala
Responsable del proceso en conjunto	Jorge Zavala
Apoyo	Jorge Zavala
Consultado	Jorge Zavala
Informado	Jorge Zavala

Tarea 2	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 3	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 4	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Equipo de usuario desatendido

Fig. 31.Reporte final.

Nota: Reporte final del resultado de la evaluación de cumplimiento de la norma ISO 27001.

Calificación	100
Tarea 1	Tarea no asignada
Tarea 2	Tarea no asignada
Tarea 3	Tarea no asignada
Tarea 4	Tarea no asignada

Matriz RASCI

Tarea 1	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 2	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 3	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 4	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Mensajería electrónica

Calificación	100
Tarea 1	Tarea no asignada
Tarea 2	Tarea no asignada
Tarea 3	Tarea no asignada
Tarea 4	Tarea no asignada

Matriz RASCI

Tarea 1	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado

Fig. 32. Reporte final.

Nota: Reporte final del resultado de la evaluación de cumplimiento de la norma ISO 27001.

Tarea 3	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 4	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Actividades de seguimiento

Calificación	100
Tarea 1	Tarea no asignada
Tarea 2	Tarea no asignada
Tarea 3	Tarea no asignada
Tarea 4	Tarea no asignada

Matriz RASCI

Tarea 1	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 2	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 3	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado
Apoyo	No asignado
Consultado	No asignado
Informado	No asignado

Tarea 4	
Responsable de la ejecución	No asignado
Responsable del proceso en conjunto	No asignado

Fig. 33. Reporte final.

Nota: Reporte final del resultado de la evaluación de cumplimiento de la norma ISO 27001.

Pruebas de funcionalidad del sistema

Para verificar la eficacia del sistema al momento de realizar el proceso de evaluación en la unidad educativa, se realizaron pruebas unitarias en cada uno de los procesos que realiza el sistema. Obteniendo como resultado que el sistema cumple con los requerimientos que se plantearon inicialmente, así podemos obtener errores y tener evidencia para mejoras futuras. Las pruebas se pueden observar a continuación:

ID Prueba:	P01	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Registro de usuario			
Objetivo:	Registrar usuarios al sistema			
Acción:	Debe registrarse el usuario			
Resultado esperado:	Éxito al registrar usuario			
Resultado obtenido:	El usuario se registra de manera exitosa			
Observación:	No debe permitir registrar usuarios ya existentes			
Se encontró algún error:	SI:		NO:	x

Fig. 34. Prueba de funcionalidad P01.

Nota: Esta prueba unitaria corresponde al registro de usuarios al sistema.

ID Prueba:	P02	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Ingreso de usuario			
Objetivo:	Inicio de sesión usuarios al sistema			
Acción:	Debe reiniciar la sesión del usuario			
Resultado esperado:	Éxito al iniciar sesión			
Resultado obtenido:	El usuario se inicia sesión de manera exitosa			
Observación:	Ninguna			
Se encontró algún error:	SI:		NO:	x

Fig. 35. Prueba de funcionalidad P02.

Nota: Esta prueba unitaria corresponde al inicio de sesión de usuarios al sistema.

ID Prueba:	P03	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Registro de institución			
Objetivo:	Registrar institución al sistema			
Acción:	Debe registrarse una nueva institución			
Resultado esperado:	Éxito al registrar institución			
Resultado obtenido:	La institución se registra de manera exitosa			
Observación:	Ninguna			
Se encontró algún error:	SI:		NO:	x

Fig. 36. Prueba de funcionalidad P03.

Nota: Esta prueba unitaria corresponde al registro de instituciones al sistema.

ID Prueba:	P04	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Edición de registro de institución			
Objetivo:	Editar institución ingresada al sistema			
Acción:	Debe editarse la institución institución			
Resultado esperado:	Éxito al editar institución			
Resultado obtenido:	La institución se edita de manera exitosa			
Observación:	Ninguna			
Se encontró algún error:	SI:		NO:	x

Fig. 37. Prueba de funcionalidad P04.

Nota: Esta prueba unitaria corresponde a la edición de registros de instituciones del sistema.

ID Prueba:	P05	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Proceso de evaluación			
Objetivo:	Evaluar el cumplimiento de los controles del sistema			
Acción:	Debe evaluarse a la institución en base a los controles			
Resultado esperado:	Éxito al evaluar institución			
Resultado obtenido:	Se evaluó de manera exitosa			
Observación:	Ninguna			
Se encontró algún error:	SI:		NO:	x

Fig. 38. Prueba de funcionalidad P05.

Nota: Esta prueba unitaria corresponde al proceso de evaluación del sistema.

ID Prueba:	P06	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Proceso de edición de registro de evaluación			
Objetivo:	Editar el registro de evaluación			
Acción:	Debe editarse el registro de la evaluación ingresado			
Resultado esperado:	Éxito al editar evaluación			
Resultado obtenido:	Se editó el registro de evaluación de manera exitosa			
Observación:	Ninguna			
Se encontró algún error:	SI:		NO:	x

Fig. 39. Prueba de funcionalidad P06.

Nota: Esta prueba unitaria corresponde al proceso de edición del registro de evaluación del sistema.

ID Prueba:	P07	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Obtención de resultados de evaluación			
Objetivo:	Visualizar el resultado de la evaluación			
Acción:	Debe mostrar el resultado con la gráfica respectiva			
Resultado esperado:	Visualización de resultado de evaluación y gráfica			
Resultado obtenido:	Se observa el resultado y la gráfica			
Observación:	Mejora en interfaz			
Se encontró algún error:	SI:		NO:	x

Fig. 40. Prueba de funcionalidad P07.

Nota: Esta prueba unitaria corresponde al proceso de obtención de los resultados de evaluación del sistema.

ID Prueba:	P08	Fecha:	12/03/2024	
Nombre del tester:		Danny Bedoya		
Módulo:	Generación de reporte final			
Objetivo:	Generar reporte final de la evaluación realizada			
Acción:	Debe generar un reporte con los resultados de la evaluación			
Resultado esperado:	Generar reporte con todos los resultados de la evaluación			
Resultado obtenido:	Reporte generado satisfactoriamente			
Observación:	Mejora en diseño de reporte			
Se encontró algún error:	SI:		NO:	x

Fig. 41. Prueba de funcionalidad P08.

Nota: Esta prueba unitaria corresponde a la generación del reporte final de la evaluación realizada.

V. Conclusiones y recomendaciones

Conclusiones

El sistema web se limita a la Unidad Educativa Fe y Alegría, no obstante, para trabajos futuros puede ampliar el alcance de este mismo y adaptarlo a las necesidades de otras instituciones.

Mediante la identificación y selección de los controles de la norma ISO 27001 se pudo determinar los controles que pueden ser aplicados a organizaciones enfocadas en la educación, esto se determinó mediante diferentes técnicas para la obtención de requerimientos.

El uso de las metodologías ágiles como SCRUM para el desarrollo de sistemas web es de gran ayuda para enfocar de manera iterativa e incremental el desarrollo de proyectos.

Las pruebas de funcionalidad realizadas determinaron que el sistema es eficaz para evaluar los controles de la norma seleccionados, esto debido a que el sistema ya es funcional y cumple con los requerimientos planteados.

La implementación del sistema web para la verificación del cumplimiento de la norma ISO 27001 es una iniciativa que puede dar un gran aporte para los organismos evaluadores y para la unidad educativa Fe y Alegría.

Recomendaciones

Se recomienda a futuros proyectos usar más técnicas para la obtención de requerimientos, para así poder determinar los controles en base a las necesidades de las organizaciones, para ello se debe clasificar y comprender de qué manera aportan los controles en la gestión de la seguridad información.

Se recomienda la aplicación de la metodología SCRUM para el desarrollo de este tipo de proyectos, para poder enfocar el trabajo en diferentes etapas.

Se recomienda la realización de varias pruebas de funcionalidad en este tipo de proyectos de desarrollo, esto con la finalidad de verificar que el sistema cumpla con los requerimientos necesarios. Esto permitirá poder tener una mayor eficiencia en el sistema y garantizar la calidad y confiabilidad del sistema web.

VI. Referencias bibliográficas

- [1] GlobalSuite Solutions, «¿Qué es la norma ISO 27001 y para qué sirve? | GSS». Accedido: 25 de enero de 2024. [En línea]. Disponible en: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>
- [2] J. L. Tigse Moposita, «Plan de gestión de seguridad informática basado en la Norma ISO 27001 para el Departamento de Tecnología de la Información en la Empresa Plasticaucho Industrial S.A.», 2020, Accedido: 28 de enero de 2024. [En línea]. Disponible en: <https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30696>
- [3] I. I. Solís Granda y Espol, «Desarrollo e implementación de controles de seguridad informática para el sistema ERP Academium de la Unidad Educativa Javier, siguiendo la norma ISO 27001», 2016, Accedido: 28 de enero de 2024. [En línea]. Disponible en: <http://www.dspace.espol.edu.ec/handle/123456789/43614>
- [4] ISOTools, «ISO 27001 - Sistemas de Gestión de Seguridad de la Información». Accedido: 28 de enero de 2024. [En línea]. Disponible en: <https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/>
- [5] ESGinnova, «Estructura de la Norma ISO 27001:2013». Accedido: 28 de enero de 2024. [En línea]. Disponible en: <https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/>
- [6] NormasISO, «ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online». Accedido: 25 de enero de 2024. [En línea]. Disponible en: <https://normaiso27001.es/>
- [7] Pirani, «ISO 27001: de qué se trata y cómo implementarla». Accedido: 25 de enero de 2024. [En línea]. Disponible en: <https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla>
- [8] ISO27000, «SGSI». Accedido: 28 de enero de 2024. [En línea]. Disponible en: <https://www.iso27000.es/sgsi.html>

- [9] «Qué es NodeJS y para qué sirve | OpenWebinars». Accedido: 25 de febrero de 2024. [En línea]. Disponible en: <https://openwebinars.net/blog/que-es-nodejs/>
- [10] «¿Qué es Node.js, y para qué sirve?» Accedido: 25 de febrero de 2024. [En línea]. Disponible en: <https://www.itdo.com/blog/que-es-node-js-y-para-que-sirve/>
- [11] «Qué es MySQL: Características y ventajas | OpenWebinars». Accedido: 25 de febrero de 2024. [En línea]. Disponible en: <https://openwebinars.net/blog/que-es-mysql/>
- [12] «Express - Node.js web application framework». Accedido: 25 de febrero de 2024. [En línea]. Disponible en: <https://expressjs.com/>
- [13] «Crear Editar PDF vía Gratis JavaScript API, Texto embebido Imágenes a PDF». Accedido: 6 de marzo de 2024. [En línea]. Disponible en: <https://products.fileformat.com/es/pdf/javascript/pdftkit/>
- [14] «ISO 27001 Última Versión 2022: Novedades y Cambios Más Importantes». Accedido: 13 de febrero de 2024. [En línea]. Disponible en: <https://blog.innevo.com/iso27001-2022>
- [15] «Controles ISO 27001: cuáles son y qué debes saber para implementarlos». Accedido: 27 de febrero de 2024. [En línea]. Disponible en: <https://blog.innevo.com/controles-iso27001#cualesson>
- [16] «El control interno para la gestión de tecnologías de la información». Accedido: 13 de febrero de 2024. [En línea]. Disponible en: <https://www.eumed.net/rev/caribe/2016/10/informacion.html>