REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

PROTOTIPO WEB FUNCIONAL UTILIZANDO MECANISMOS DE AUTENTIFICACIÓN 2FA EN LA PROTECCIÓN DE DATOS DEL PROCESO DE DONACIÓN Y TRASPLANTE DE ÓRGANOS BASADO EN OWASP Y LA NORMA ISO/IEC 27002:2022.

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

AUTOR: Johanna Marianela Murillo Esparza

DIRECTOR: MSc. José Guillermo Jácome León

ASESOR: Dra. Daysi Elizabeth Imbaquingo Esparza

IBARRA - ECUADOR

2025

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1716185218		
APELLIDOS Y NOMBRES:	Murillo Esparza Johanna Marianela		
DIRECCIÓN:	QUITO, El Recreo Calle Nono S10-120		
EMAIL:	jmmurilloe@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0992519075

DATOS DE LA OBRA	
TÍTULO:	Prototipo web funcional utilizando mecanismos de autentificación 2FA en la protección de datos del proceso de donación y trasplante de órganos basado en OWASP y la norma ISO/IEC 27002:2022
AUTOR (ES):	Murillo Esparza Johanna Marianela
FECHA: DD/MM/AAAA	19/05/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en Seguridad Informática
ASESOR /DIRECTOR:	**Director:** MSc. José Guillermo Jácome León **Asesor:** Dra. Daysi Elizabeth Imbaquingo Esparza PHD

1. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 19 días del mes de mayo de 2025

EL AUTOR:

(Firma)..

.....

Nombre Johanna Marianela Murillo Esparza

Ibarra, 27 de marzo de 2025

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado Prototipo web funcional utilizando mecanismos de autentificación 2FA en la protección de datos del proceso de donación y trasplante de órganos basado en OWASP y la norma ISO/IEC 27002:2022 de la maestrante Johanna Marianela Murillo Esparza, de la Maestría en Computación Mención Seguridad Informática certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	Firma
Director/a	MsC. José Jácome	JOSE GUILLERMO JACOME LEON
Asesor/a	MsC. Daysi Imbaquingo	1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA Firmado digitalmente por 1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA Fecha: 2025.03.27 11:04:16 -05'00'

DEDICATORIA

Este trabajo de investigación lo dedico a mi madre, quien, aunque físicamente ya no me acompaña, sigue iluminando mi camino con su amor infinito. Cada logro en mi vida, incluida esta meta alcanzada, lleva su huella, su esfuerzo y sus enseñanzas. Este trabajo es un homenaje a su fortaleza, su dedicación y todo lo que me inculcó.

A mi familia, mi refugio incondicional, gracias por su apoyo constante, por creer en mí en cada desafío y por ser mi mayor motivación. Sin su amor, paciencia y aliento, este sueño no sería posible.

AGRADECIMIENTOS

En primer lugar, a Dios, por darme la fortaleza, la perseverancia y la sabiduría para superar cada obstáculo y alcanzar esta meta.

A mi madre, quien, aunque ya no está físicamente, sigue presente en mi corazón y en cada uno de mis logros. Su amor, sus enseñanzas y su ejemplo de esfuerzo y valentía han sido mi mayor inspiración. Este trabajo es también un homenaje a su memoria.

A mi familia, por ser mi refugio incondicional, por su apoyo constante y por brindarme el aliento necesario en los momentos de duda. Gracias por su paciencia, su comprensión y su amor inquebrantable.

A la Universidad Técnica del Norte de Ibarra, y a todos mis maestros y en especial a mi tutor MSc. José Jácome y mi asesora PhD Daysi Imbaquingo, quienes, con su conocimiento, guía y exigencia, me han impulsado a dar lo mejor de mí. Su enseñanza ha sido clave en mi formación académica y profesional.

ÍNDICE DE CONTENIDO

IDENTIFICACIÓN DE LA OBRA ii

CONSTANCIA iv

DEDICATORIA v

AGRADECIMIENTOS vi

ÍNDICE DE CONTENIDO vii

ÍNDICE DE TABLAS x

ÍNDICE DE FIGURAS xii

RESUMEN xiv

ABSTRACT xv

CAPÍTULO I 1

1. EL PROBLEMA 1

1.1. Problema de investigación 1

1.2. Interrogantes de la investigación 3

1.3. Objetivos de la investigación 3

1.3.1. Objetivo general 4

1.3.2 Objetivos específicos 4

1.3. Justificación 4

CAPÍTULO II 7

2.1. Revisión de literatura 7

2.1.1. Preguntas de investigación 7

2.1.2. Búsqueda de documentación 8

2.1.3. Selección de artículos 9

2.1.4. Selección de datos importantes 13

2.2. Marco referencial 14

2.2.1. Antecedentes 14

2.3. Marco conceptual 15
2.3.1. Seguridad de la información 15
2.3.2. Seguridad informática 16
2.3.3. Ciberseguridad 17
2.3.4. Aplicación Web 17
2.3.4.1. Características. 18
2.3.4.2. Arquitectura. 18
2.3.4.3. Componentes de la arquitectura de una aplicación web. 19
2.3.4.4. Seguridad en los sistemas Web. 20
2.3.5. Autentificación 21
2.3.5.1. Técnicas de autentificación. 21
2.3.5.2. Tipos de Mecanismos de autenticación. 22
2.3.6. OWASP 26
2.3.6.1. OWASP TOP 10 26
2.3.6.2. Controles según OWASP Relacionados a la autentificación de un sistema web 28
2.3.7. Normas ISO/IEC 27000:2022 31
2.3.7.1. Norma ISO/IEC 27001 32
2.3.7.2. Norma ISO/IEC 27002 32
2.3.7.3. Controles Relacionados a la autentificación de un sistema web 34
2.4. Arquitectura del sistema y Herramientas Tecnológicas 37
2.4.1. Herramientas Tecnológicas 38
2.4.2. Desarrollo de la solución 38
2.4.2.1. Autentificación de Dos Factores (2FA) 38
2.4.2.2. Fortalecimiento de la Gestión de Contraseñas 42
2.4.2.3. Fortalecimiento de los Procesos de Recuperación de Credenciales 44

2.4.2.4. Actualización del Hashing de Contraseñas: De MD5 a SHA-256 47
2.5. Marco legal 49
CAPITULO III 51
3. MARCO METODOLÓGICO 51
3.1. Descripción del área de estudio / Descripción del grupo de estudio 51
3.2. Enfoque y tipo de investigación 51
3.3. Procedimiento de investigación 52
CAPITULO IV 65
4. RESULTADOS Y DISCUSIÓN 65
4.1. Resultados 65
4.1.1. Encuesta dirigida a usuarios del Sistema a nivel nacional 65
4.1.2. Aplicación de la encuesta 65
4.2. Discusión 84
4.3. CONCLUSIONES 85
4.4. Recomendaciones 87
REFERENCIAS 89
ANEXO 1 Encuesta 93
ANEXO 2 Informe Parsifal 94

ÍNDICE DE TABLAS

Tabla 1 Preguntas de investigación planteadas 7

Tabla 2 Base de datos bibliográficas buscadores académicos..... 9

Tabla 3 Bases de datos bibliográficas de instituciones de Educación Superior 9

Tabla 4 Fases de búsqueda 10

Tabla 5 Documentos seleccionados..... 11

Tabla 6 Relación preguntas de investigación y documentos..... 13

Tabla 7 Lista de controles relacionados con la autentificación 28

Tabla 8 Controles tecnológicos ISO/IEC 27002:2022 34

Tabla 9 Herramientas utilizadas 38

Tabla 10 Vulnerabilidades halladas..... 53

Tabla 11 Evaluación del Sistema informático con ISO 27002:2022..... 55

Tabla 12 Evaluación del Sistema Informático con OWASP Top 10 55

Tabla 13 Vulnerabilidades halladas en el prototipo 57

Tabla 14 Vulnerabilidades halladas vs filtros aplicados para mitigar 58

Tabla 15 Evaluación al prototipo con ISO 27002:2022 63

Tabla 16 Evaluación al prototipo con OWASP Top 10 63

Tabla 17 Medidas de tendencia y dispersión Pregunta 1..... 66

Tabla 18 Pregunta 1. ¿Cuánto tiempo ha estado utilizando el sistema de donación y trasplante de órganos? 66

Tabla 19 Medidas de tendencia y dispersión Pregunta 2..... 68

Tabla 20 Pregunta 2. ¿Qué tan fácil le resulta encontrar la información que necesita en el Sistema Nacional Informático de Donación y Trasplante? 68

Tabla 21 Medidas de tendencia y dispersión Pregunta 3..... 69

Tabla 22 Pregunta 3. ¿Qué aspectos del sistema considera más difíciles de usar? 70

Tabla 23 Medidas de tendencia y dispersión Pregunta 4..... 72

Tabla 24 Pregunta 4. ¿Considera usted que la información en el sistema está suficientemente protegida? 72
Tabla 25 Medidas de tendencia y dispersión Pregunta 5 74
Tabla 26 Pregunta 5. ¿Qué tan segura considera su contraseña actual en el sistema? ... 74
Tabla 27 Medidas de tendencia y dispersión Pregunta 6 76
Tabla 28 Pregunta 6. ¿Conoce las políticas de seguridad utilizadas en el sistema para autentificación de los usuarios? 76
Tabla 29 Medidas de tendencia y dispersión Pregunta 7 78
Tabla 30 Pregunta 7. ¿Estaría dispuesto a cambiar su contraseña con regularidad en el sistema, siguiendo las pautas de seguridad recomendadas? 78
Tabla 31 Medidas de tendencia y dispersión Pregunta 8 80
Tabla 32 Pregunta 8. ¿Estaría dispuesto a agregar una capa adicional de seguridad a su cuenta, como un código o una medida de protección adicional, si estuviera disponible? 80
Tabla 33 Medidas de tendencia y dispersión Pregunta 9 81
Tabla 34 Pregunta 9. ¿Ha experimentado o conocido algún incidente de seguridad relacionado con el sistema? 82

ÍNDICE DE FIGURAS

Figura 1 Diagrama causa-efecto del problema 3

Figura 2 Seguridad de la Información y Seguridad Informática 16

Figura 3 Arquitectura de una aplicación web 19

Figura 4 Componentes de una aplicación web 19

Figura 5 Concepto de autentificación 21

Figura 6 Categorías de autentificación 22

Figura 7 Autentificación en dos pasos 25

Figura 8 Vulnerabilidades OWASP Top 10 2021 27

Figura 9 Controles de la ISO/IEC 27002:2022 33

Figura 10 Arquitectura tecnológica de un proyecto Maven con GWT, Spring, Hibernate y Oracle 37

Figura 11 Interfaz anterior inicio de sesión 39

Figura 12 Interfaz nueva inicio de sesión 40

Figura 13 Correo con código de validación 41

Figura 14 Administración de usuarios sin opción de activar 2FA 41

Figura 15 Administración de usuarios con opción de activar o desactivar 2FA 42

Figura 16 Método para generar el código único 42

Figura 17 Interfaz actualizar cuenta de usuario anterior 43

Figura 18 Interfaz actualizar cuenta de usuario nueva 44

Figura 19 Tabla de base de datos para almacenar historial de contraseñas 44

Figura 20 Interfaz proceso de recuperación de contraseñas antes 46

Figura 21 Interfaz recuperación de contraseñas actual 46

Figura 22 Método para crear una cadena con MD5 47

Figura 23 Método para crear un texto con SHA256 47

Figura 24 Ubicación del Instituto de Donación y Trasplante de Órganos Tejidos y Células 51
Figura 25 Test de Autentificación 54
Figura 26 Análisis de puertos 59
Figura 27 Búsqueda de rutas del login 60
Figura 28 Intercepción de sesión 61
Figura 29 Captura de sesión 61
Figura 30 Prueba ataque sin 2FA 62
Figura 31 Prueba ataque con 2FA 62
Figura 32 Campos de base de datos después del ataque 63
Figura 33 Tiempo de uso del sistema por parte de los encuestados 67
Figura 34 Facilidad de uso del sistema 69
Figura 35 Aspectos difíciles de usar del sistema 71
Figura 36 Protección de la información en el sistema 73
Figura 37 Seguridad de la contraseña 75
Figura 38 Política de seguridad 77
Figura 39 Cambio de contraseña 79
Figura 40 Capa de protección adicional 81
Figura 41 Incidentes de seguridad 83

RESUMEN

En el desarrollo de este proyecto se identificó la presencia de vulnerabilidades en el sistema informático que maneja la actividad trasplantológica del país, principalmente en el proceso de autenticación, almacenamiento de contraseñas, esto representaba un gran riesgo de accesos no autorizados, suplantación de identidad y exposición de información médica en el proceso de donación y trasplante de órganos; con el fin de dar solución a este problema se planteó como objetivo desarrollar un prototipo web funcional que incorpore mecanismos de autenticación de doble factor (2FA) siguiendo las buenas prácticas de OWASP y la norma ISO/IEC 27002:2022, con el fin de fortalecer la seguridad de los datos; para cumplir con lo planteado, se llevó a cabo un análisis de vulnerabilidades seguido de encuestas a usuarios del sistema para identificar percepciones y debilidades en el uso actual del sistema, luego se diseñó e implementó un sistema de 2FA basado en contraseñas de un solo uso (OTP), utilizando una gestión de usuarios que permite habilitar o deshabilitar la autentificación 2FA dependiendo del usuario, para garantizar la accesibilidad sin comprometer la funcionalidad del sistema, se realizó fortalecimiento de políticas de contraseñas(caducidad periódica, historial de contraseñas, política de complejidad), migración del algoritmo de hashing de MD5 a SHA-256 y corrección de vulnerabilidades detectadas mediante filtros, como resultados se obtiene la integración del 2FA y buenas prácticas internacionales en el sistema informático al cual se le realizaron análisis de vulnerabilidades, pruebas de penetración para concluir que es una solución viable para proteger la información sensible del sistema.

Palabras clave: seguridad de la información, autenticación de doble factor, OWASP, SHA-256.

ABSTRACT

During the development of this project, vulnerabilities were identified in the computer system that manages the country's transplant activity, mainly in the authentication process and password storage, which represented a great risk of unauthorized access, identity theft and exposure of medical information in the process of organ donation and transplantation; In order to solve this problem, the objective was to develop a functional web prototype that incorporates two-factor authentication (2FA) mechanisms following OWASP best practices and ISO/IEC 27002: 2022, in order to strengthen data security; to comply with this, a vulnerability analysis was carried out followed by surveys of system users to identify perceptions and weaknesses in the current use of the system, then a 2FA system based on one-time passwords (OTP) was designed and implemented, using a user management system that allows enabling or disabling 2FA authentication depending on the user, to ensure accessibility without compromising the functionality of the system, Password policies were strengthened (periodic expiration, password history, complexity policy), migration of the hashing algorithm from MD5 to SHA-256 and correction of vulnerabilities detected through filters. As a result, the integration of 2FA and international good practices in the computer system was obtained, and vulnerability analysis and penetration tests were performed to conclude that it is a viable solution to protect the sensitive information of the system.

Keywords: information security, to-factor authentication, OWASP, SHA-256.

CAPÍTULO I

1. EL PROBLEMA

1.1. Problema de investigación

Instituto Nacional de Donación y Trasplante de Órganos, Tejidos y Células (INDOT), es una "entidad adscrita a la Autoridad Sanitaria Nacional, esté normará, regulará y controlará la actividad trasplantológica" (Ley Orgánica de Donación y Trasplante de Órganos, Tejidos y Células, 2011) sus actividades se sustentan en un Sistema Informático. Este sistema gestiona y administra de forma centralizada la información del proceso de donación y trasplante de órganos y tejidos a nivel nacional". (INDOT)

Los sistemas web se ejecutan en servidores accesibles a través de Internet o de redes locales mediante diferentes navegadores, esto ha transformado la manera en que las personas acceden a la información Lamentablemente, esta accesibilidad también plantea varios problemas de seguridad, dejando los datos e información vulnerable a fugas, accesos no autorizados, ataques de fuerza bruta, problemas de autenticación, inyecciones de código, phishing, entre otros riesgos.

" El sector sanitario es particularmente susceptible a ataques cibernéticos debido a varias razones intrínsecas. La información de salud y los datos sanitarios son extremadamente valiosos para los ciberdelincuentes, ya que pueden ser utilizados para el robo de identidad, fraudes médicos o incluso extorsión, tanto a las empresas proveedoras como a los pacientes." (Cervera García & Goussens, 2024)

Según OWASP a partir del año 2022, las fallas de autentificación en los sistemas web se han convertido en un problema importante. Los ataques de fuerza bruta, el uso de credenciales débiles o predeterminadas y la falta de autenticación multifactor (MFA) son los errores más comunes. En industrias como la medicina, donde la protección de datos es esencial para mantener la privacidad de los pacientes, este tipo de vulnerabilidades sigue siendo explotado.

Actualmente, el sistema Informático de donación y trasplante maneja datos sensibles, y no cuenta con mecanismos adecuados de autenticación, buenas prácticas de seguridad, faltan actualizaciones y parches en las herramientas de desarrollo, no se toma en cuenta el factor humano, ya que este puede llevar a prácticas inseguras, como compartir contraseñas o utilizar contraseñas débiles.

Por estos fallos de seguridad y otros más, las vulnerabilidades podrían ser aprovechadas por ciberdelincuentes y apoderarse de información sensible lo que implicaría que la información se vea comprometida, lo cual podría llevar problemas legales y sanciones.

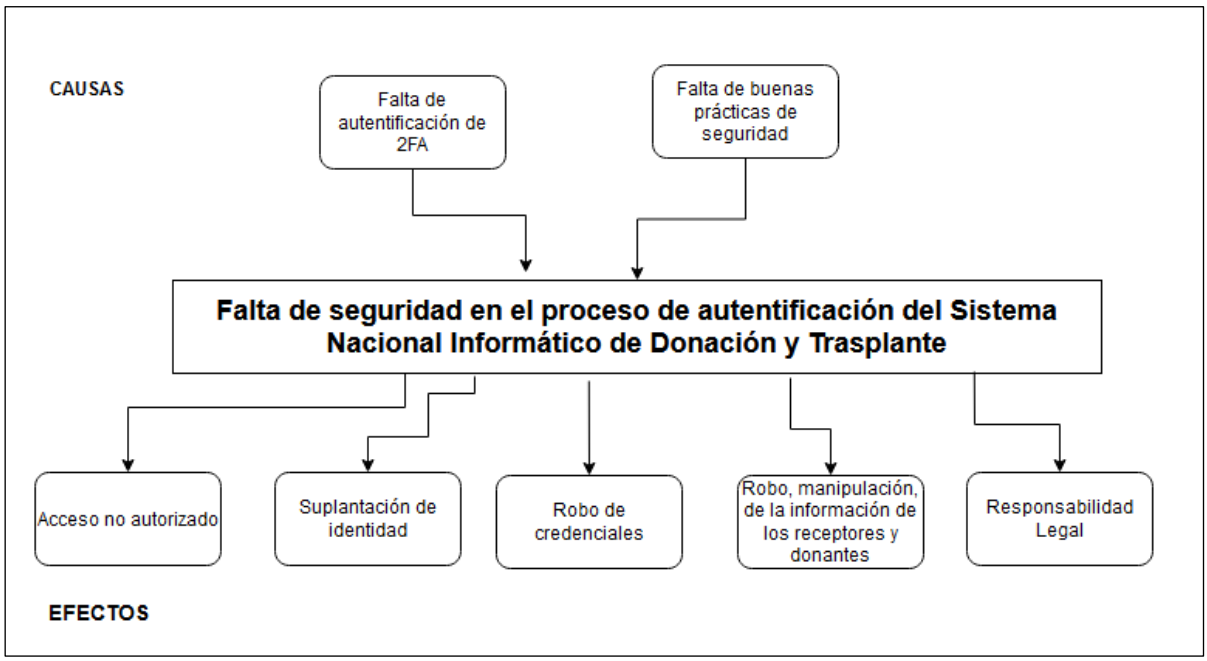
Para mejorar la seguridad en el proceso de donación y trasplante de órganos, el prototipo web funcional utilizará autenticación de doble factor (2FA). Esto garantizará que, además de la contraseña, el usuario deba verificar su identidad mediante un código temporal, lo que añade una capa de protección adicional contra accesos no autorizados.

Con este proyecto se pretende minimizar los riesgos de violaciones de seguridad, protegiendo los datos sensibles del sistema y garantizando el cumplimiento normativo en la gestión de la información.

En la Figura 1 podemos observar el diagrama causa-efecto del problema planteado.

Figura 1

Diagrama causa-efecto del problema



Nota. Árbol de problemas

1.2. Interrogantes de la investigación

¿Cuál será el nivel de mejora al implementar un mecanismo de autentificación de dos factores (2FA) y las mejores prácticas de seguridad en el Sistema Nacional Informático de Donación y Trasplante?

1.3. Objetivos de la investigación

Desarrollar un prototipo web funcional que utilice mecanismos de autentificación de dos factores (2FA) para proteger los datos del proceso de donación y trasplante de órganos.

1.3.1. Objetivo general

Desarrollar un prototipo web funcional que utilice mecanismos de autenticación de doble factor (2FA) para fortalecer la protección de datos en el proceso de donación y trasplante de órganos, siguiendo las directrices y mejores prácticas establecidas por OWASP y la norma ISO/IEC 27002:2022.

1.3.2 Objetivos específicos

1. Investigar y analizar las vulnerabilidades y riesgos relacionados con la protección de datos en el proceso de donación y trasplante de órganos.
2. Desarrollar el prototipo web funcional utilizando tecnologías y herramientas apropiadas, asegurando la integración adecuada de los mecanismos de autenticación 2FA.
3. Evaluar la eficiencia y seguridad del prototipo mediante análisis de vulnerabilidades, pruebas de penetración y comparaciones con estándares establecidos.

1.3. Justificación

La investigación propuesta contribuirá en el Objetivo de Desarrollo Sostenible planteado por las Naciones Unidas No. 9 Industria, innovación e infraestructura.

Según (Naciones Unidas, 2018), “Las inversiones en infraestructura (transporte, riego, energía y tecnología de la información y las comunicaciones) son fundamentales para lograr el desarrollo sostenible y empoderar a las comunidades en numerosos países” (p. 43).

También contribuirá con algunos puntos importantes del Plan de Creación de Oportunidades 2021-2025 de la Secretaría Nacional de Planificación que se encuentran en el Eje de Seguridad Integral en el objetivo No. 10 Garantizar la soberanía nacional, integral, territorial y seguridad del Estado.

Según (Secretaría Nacional de Planificación, 2021) la política es "Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del ciberespacio y proteger su infraestructura crítica" y como meta "Incrementar el índice de ciberseguridad global de 26.3 a 51.3" (p. 80).

Según la (Ley Orgánica de Donación y Trasplante de Órganos, Tejidos y Células, 2011) en el Artículo 10. Protección de datos y confidencialidad, es deber de la Autoridad Sanitaria Nacional: a) Adoptar medidas que garanticen la seguridad de los datos y la imposibilidad de su revelación no autorizada, así como establecer salvaguardias para evitar adiciones, supresiones o modificaciones de los datos en las fichas registros de las y los donantes; b) Establecer procedimientos para solventar posibles discrepancias en los datos.

El sistema informático que maneja los datos de donación y trasplante al momento no cuenta con un mecanismo de autentificación que garantice la protección de los datos sensibles de donantes y receptores, esto representa una vulnerabilidad importante, ya que la falta de mecanismos de autentificación deja al sistema expuesto a accesos no autorizados, robo de información y violaciones de privacidad.

La implementación de mecanismos de autentificación de doble factor (2FA) es importante para reforzar la seguridad del sistema, agregando una capa adicional de protección al exigir dos formas verificación (como una contraseña y un código temporal),

dificultando el acceso indebido, incluso si las credenciales de los usuarios han sido comprometidas. Al aumentar la seguridad del acceso, se minimiza el riesgo de ciberataques y se protege la integridad de los datos sensibles.

Con este proyecto se busca proporcionar un sistema más seguro y confiable. Optimizando el proceso de donación y trasplante al reducir interrupciones o brechas de seguridad que pudieran ralentizar o comprometerlo, usando normas o estándares internacionales como OWASP y la norma ISO/IEC 27002:2022, que proporcionan un marco sólido para la implementación de controles de seguridad en sistemas de información.

Al cumplir con normas internacionales, se garantiza que la institución cumpla con las leyes y regulaciones vigentes en materia de protección de datos, como lo establece la Ley Orgánica de Donación y Trasplante de Órganos, tejidos y células en su Artículo 10. Beneficiando a todas las partes involucradas, desde los pacientes hasta el personal médico encargado.

La línea de investigación en la Universidad Técnica del Norte de la presente investigación está relacionada con la No. 10 “Desarrollo, aplicación de software y cyber security (seguridad cibernética)” (UTN, 2023) vigente y aprobada por el Honorable Consejo Universitario.

CAPÍTULO II

2.1. Revisión de literatura

La revisión de la literatura es un enfoque previo para empezar una investigación y tiene la finalidad clínica o académica. Constituye una síntesis crítica y exhaustiva de la literatura existente sobre un tema específico, ofreciendo una visión integral y actualizada que respalda la investigación y la práctica en un campo determinado. (Goris & Adolf, 2015)

El uso de técnicas de la revisión de literatura aplicadas a la investigación como la lectura crítica, base de datos confiables, garantizará la estructura del marco teórico y la metodología. (Calle, 2016)

2.1.1. Preguntas de investigación

Para esta investigación se han desarrollado 4 preguntas que permitirán el definir aspectos clave para abordar y desarrollar el tema de investigación planteado, y también el manejo de la información recopilada.

Tabla 1

Preguntas de investigación planteadas

Nro.	Pregunta	Motivación
P1	¿Cuáles son las principales vulnerabilidades y riesgos asociados en sistemas informáticos de salud?	Conocer cuáles son las vulnerabilidades y riesgos a los que se enfrentan los sistemas informáticos de salud
P2	¿Cuáles son los diferentes tipos de métodos de autenticación de doble	Conocer los métodos de autenticación de 2FA disponibles

	factor (2FA) disponibles para sistemas web	
P3	¿Cuáles son las directrices de OWASP y la norma ISO/IEC 27002:2022?	Conocer las directrices de seguridad establecidas por OWASP y la norma ISO/IEC 27002:2022, para fortalecer la seguridad y cumplir con las regulaciones, para mantener la confianza de los usuarios en un entorno digital cada vez más amenazante.
P4	¿Cómo se puede evaluar de manera efectiva la eficiencia y seguridad de un prototipo a través del análisis de vulnerabilidades y pruebas de penetración?	Conocer cómo se puede evaluar el prototipo utilizando varios análisis de vulnerabilidades y pruebas de penetración.

Nota. Esta tabla muestra las preguntas planteadas para la investigación.

2.1.2. Búsqueda de documentación

Con base en las preguntas de investigación planteadas, se ha llevado a cabo una exhaustiva búsqueda de datos relevantes a partir del año 2022 en los buscadores académicos designados: académicos designados: IEEE Digital Library, Science@Direct y Scopus con uso de la herramienta PARSIFAL.

El propósito fundamental de esta búsqueda ha sido recopilar información actualizada y pertinente que pueda contribuir significativamente al abordaje de las cuestiones planteadas en el estudio.

Y se ha utilizado la siguiente cadena de búsqueda *("Two-Factor Authentication") AND ("Web System") AND ("ISO 27002:2022" OR "OWASP").*

Tabla 2

Base de datos bibliográficas buscadores académicos

BDD Bibliográficas	Artículos Encontrados
IEEE Digital Library	22
Science@Direct	34
Scopus	39
Total	95

Nota. En esta tabla se muestra los artículos encontrados con la cadena de búsqueda en las bases Bibliográficas seleccionadas

También se realizó una búsqueda en 3 repositorios de Instituciones de Educación Superior para que sirva como referencia para el tema planteado, utilizando la siguiente cadena de búsqueda "vulnerabilidades de sistemas web owasp"," vulnerabilidades de sistemas web ISO 27002:2022".

Tabla 3

Bases de datos bibliográficas de instituciones de Educación Superior

Repositorios	Tesis encontradas
Repositorio PUCE	36
Repositorio EPN	44
Repositorio UTN	35
Total	121

Nota. En esta tabla se muestra los artículos encontrados con la cadena de búsqueda en los repositorios seleccionados

2.1.3. Selección de artículos

Se utilizan tres etapas para escoger artículos. En la primera etapa, se aplican criterios de inclusión y exclusión, estos abarcan: Artículos científicos, revisiones de

literatura y otros trabajos y tesis. Toda esta documentación está relacionada con el tema de investigación y abarca los últimos 5 años.

En la segunda etapa, se evaluaron los artículos identificados a través de la cadena de búsqueda para determinar cuáles eran más relevantes y fundamentales para la revisión.

En la última fase, se examinó y analizó la información contenida en cada artículo, enfocándose en el resumen, la introducción y las recomendaciones. Solo se consideraron aquellos documentos de investigación que estaban directamente relacionados con el tema de estudio.

Tabla 4

Fases de búsqueda

	Fase I	**Fase II**	**Fase II**
Nro. Artículos	95	38	6
Nro. Tesis	121	11	6

Nota. En esta tabla se muestran las tres fases de búsqueda para la selección de artículos y tesis.

Tabla 5

Documentos seleccionados

Código	Título	BBD Bibliográfica	Año	País
A1	Enforcing security policies on interacting authentication systems	Science@Direct	2024	Italia
A2	A User-Friendly Two-Factor Authentication Method against Real-Time Phishing Attacks	IEEE Digital Library	2022	Estados Unidos
A3	Implementation and analysis of Web application security measures using OWASP Guidelines	IEEE Digital Library	2022	India
A4	Online Banking User Authentication Methods: A Systematic Literature Review	IEEE Digital Library	2023	Jordania
A5	Two Factor Authentication: Voice Biometric and Token-Based Authentication	Scopus	2024	Malaysia
A6	Ciberseguridad y uso de las TIC en el Sector Salud	Science@Direct	2023	España
T1	Vulnerabilidades en aplicaciones web utilizando la metodología de “proyecto abierto de seguridad de aplicaciones web”	PUCE	2021	Ecuador
T2	Evaluación de la seguridad de software mediante el uso de las herramientas SonarQube y OWASP ZAP: Estudio de caso en la plataforma tecnológica GastroEc	UTN	2024	Ecuador

T3	Desarrollo de un simulador web aplicando la norma ISO/IEC 27002 enfocado a ingeniería social	UTN		Ecuador
T4	Creación de un prototipo de Sistema de One-Time Password para un Sistema de autenticación de dos factores: implementación de un prototipo de sistema generador de OTP basado en TOTP y su envío mediante.	EPN	2023	Ecuador
T5	Creación de un prototipo de sistema de one-time password (otp) para un sistema de autenticación de dos factores: implementación de un prototipo de sistema generador otp basado en hotp y envió por correo	EPN	2023	Ecuador
T6	Creación de un prototipo de un sistema de one-time password (OTP) para un sistema de autenticación de dos factores: diseño e implementación de un prototipo de un sistema de one-time password (OTP)	EPN	2023	Ecuador

Nota. En esta tabla se muestra los artículos y tesis seleccionados

2.1.4. Selección de datos importantes

Después de revisar los documentos seleccionados se realizó una matriz de temas importantes en relación con las preguntas de investigación y posteriormente realizar un análisis más minucioso.

Tabla 6

Relación preguntas de investigación y documentos

Artículo - Concepto	Vulnerabilidades de sistemas web	Métodos de autenticación de 2FA	Norma ISO/IEC 27002	Owasp
A1	x	x		
A2	x	x		x
A3	x	x		x
A4	x	x		x
A5	x	x		
A6	x	x		
T1	x	x		x
T2				
T3				
T4		x		x
T5		x		
T6		x		

Nota. En la tabla se muestra las variables encontradas en los documentos

2.2. Marco referencial

2.2.1. Antecedentes

> El sector sanitario es particularmente susceptible a ataques cibernéticos debido a varias razones intrínsecas. La información de salud y los datos sanitarios son extremadamente valiosos para los ciberdelincuentes ya que pueden ser utilizados para el robo de identidad, fraudes médicos o incluso extorsión, tanto a las empresas proveedoras como a los pacientes. (Cervera García & Goussens, 2024)

El Instituto Nacional de Donación y Trasplante de Órganos, Tejidos y Células (INDOT) lanzó a producción el Sistema Informático de Donación y Trasplante en el año 2016.

Según la consulta realizada al Sistema informático se encuentran registrados 389 usuarios activos los cuales ingresan a la aplicación en función de los roles asignados.

Este sistema web presenta varios problemas de seguridad, entre ellos la ausencia de un mecanismo de autenticación de doble factor (2FA), la falta de implementación de estándares de seguridad como OWASP o ISO 27002, y la existencia de amenazas que comprometen la protección de los datos.

El OWASP Top 10 presenta los 10 riesgos de seguridad más críticos en aplicaciones web y detalla las medidas de prevención necesarias para mantener la seguridad de la aplicación. Según OWASP la confirmación de la identidad, la autenticación y la gestión de sesiones del usuario son fundamentales para protegerse contra ataques relacionados con la autenticación (OWASP Top 10 team, 2021)

La Norma ISO 27002:2022 detalla los controles recomendados para proteger la información, Según dicha norma la autenticación segura es el método principal con el que

interactúan los usuarios humanos y no humanos cuando intentan utilizar los activos de TIC de una organización. (ISO/IEC, 2022)

> En todo momento es necesario mantener una adecuada y correcta seguridad aplicada a sistemas web que, dentro de una organización, se mantiene así un correcto funcionamiento de las mismas y asegurar que la información dentro de ellas sea de total confianza para el usuario final, que evita, que personas malintencionadas sustraigan información, que luego, se vea afectada la integridad y la disponibilidad por parte una determinada organización a sus clientes de la misma. (Gamboa, 2021)

Situación Actual

Actualmente el SINIDOT cuenta con un método de autentificación de factor único basado en contraseñas que es el más usado y más conocido por los usuarios.

Además, no se cumple con algunos controles de seguridad que se pueden implementar para mejorar la seguridad de la información como el uso de contraseñas fuertes, rotación de contraseñas, para tratar de mitigar las vulnerabilidades.

Tales falencias hacen que el sistema pueda presentar fallas de identificación y autenticación. Y los datos sensibles que se encuentran registrados en el sistema puedan ser robados, modificados o eliminados, incumpliendo la normativa legal “Ley Orgánica de Protección de Datos Personales”.

2.3. Marco conceptual

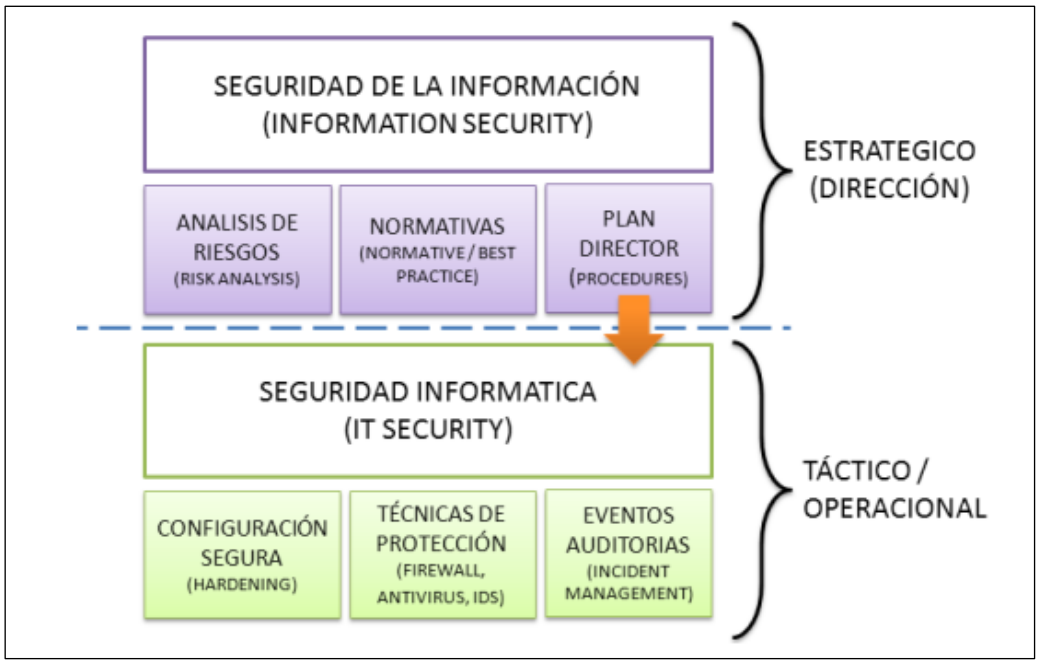
2.3.1. Seguridad de la información

La seguridad de la información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Se centra en toda la empresa abarca todos los activos que deben protegerse.

La seguridad de la información es una cuestión que afecta a toda la compañía, ya que toda la organización trabaja con información y que, por tanto, requiere de una gestión coordinada y transversal, lo cual comporta planificación y gestión, y no puede ser improvisado, sino que debe ser considerado como un proceso más de la compañía que interactúa con el resto de los procesos del negocio. (Garre Gui, s.f.)

Figura 2

Seguridad de la Información y Seguridad Informática



Fuente. (Seguridad y Etica, 2013)

2.3.2. Seguridad informática

"La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información." (Romero Castro, y otros, 2018)

Según (Mila, 2012) la seguridad informática es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

2.3.3. Ciberseguridad

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software y datos contra amenazas cibernéticas.

El conjunto de acciones, políticas, medidas y procedimientos de carácter técnico, organizativo y legal, que se aplican para proteger la infraestructura crítica, los sistemas informáticos, las redes de comunicación y la información contenida en ellos, de amenazas o ataques provenientes del mundo digital. (Castillo Medina, 2021)

2.3.4. Aplicación Web

Una aplicación web es un software que se ejecuta en el navegador web. Las empresas tienen que intercambiar información y proporcionar servicios de forma remota. Utilizan aplicaciones web para comunicarse con los clientes cuando lo necesiten y de una forma segura. Le permiten acceder a funcionalidades complejas sin la necesidad de instalar o configurar un software. (Amazon Web Services, 2023)

La aplicación web es una forma de software que generalmente se usa a través de los navegadores web, y comúnmente usa una combinación de un script del lado

del servidor y un script del lado del cliente. Puede estar escrito en todo tipo de lenguajes y ejecutarse en todo tipo de sistema operativo. (Murat, Çig˘dem, Evren, & Alperen, 2021)

2.3.4.1. Características.

Las aplicaciones web tienen ciertas características en común:

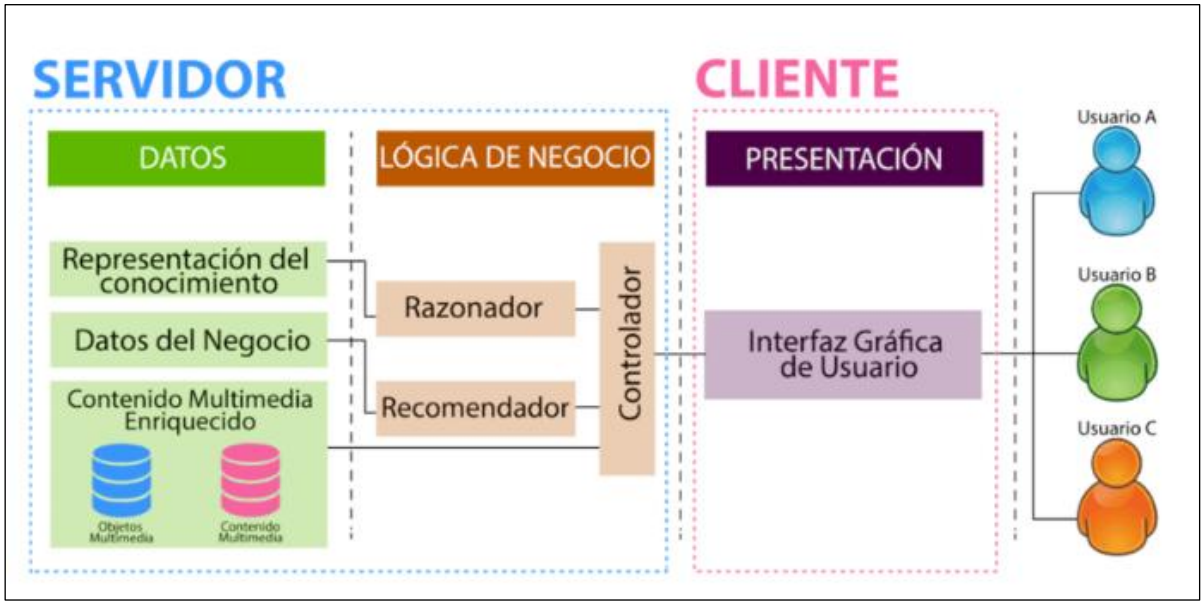
- Funcionan independiente de la versión del sistema operativo instalado en el lado del usuario.
- Los requerimientos del hardware son menores.
- El usuario emplea un navegador web, la aplicación no necesita ser descargada.
- El usuario puede acceder desde cualquier lugar del mundo.

2.3.4.2. Arquitectura.

Las aplicaciones web usan una arquitectura cliente-servidor, es un modelo de comunicación en el cual el cliente realiza pedidos de servicios y el servidor procesa las solicitudes del cliente y envía una respuesta.

Figura 3

Arquitectura de una aplicación web



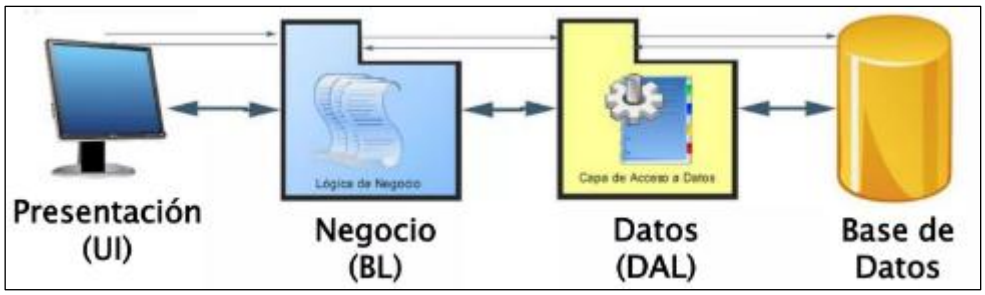
Ref. (Sastoque Hernández, Mancilla, Narvaez, & Iregui, 2015)

2.3.4.3.Componentes de la arquitectura de una aplicación web.

Los componentes de una aplicación web suele seguir un patrón de tres niveles o componentes:

Figura 4

Componentes de una aplicación web



Ref. (Ropero, 2015)

Lógica de negocio: Es la que permite el correcto funcionamiento del sistema, aquí se encuentran todos los procesos, métodos, algoritmos que el usuario va a ejecutar.

Administración de los datos: Es la que permite el manejo de la base de datos es decir realizar las siguientes transacciones crear, recuperar, actualizar los datos.

Interfaz: Esa la parte que puede ver el usuario, y accede a esta por medio de un navegador.

2.3.4.4. Seguridad en los sistemas Web.

La seguridad en los sistemas Web es de vital importancia porque está nos permite proteger la información. Estas con el avance de la tecnología vienen acompañada de gran variedad de vulnerabilidades.

"La seguridad de las aplicaciones web es un componente principal de cualquier negocio basado en la web. Debido a la naturaleza de Internet, las aplicaciones web están sujetas a ataques desde diferentes ubicaciones en varios niveles de escala y complejidad." (Murat, Çig˘dem, Evren, & Alperen, 2021)

La seguridad en las aplicaciones web es de mucha importancia para las organizaciones, y una tarea primordial para probarlas son las pruebas de seguridad.

Algunas guías de prueba de aplicaciones que se puede usar como referencia son OWASP (Open Web Application Security Project) tiene documentación que se puede usar para el desarrollo de aplicaciones seguras.

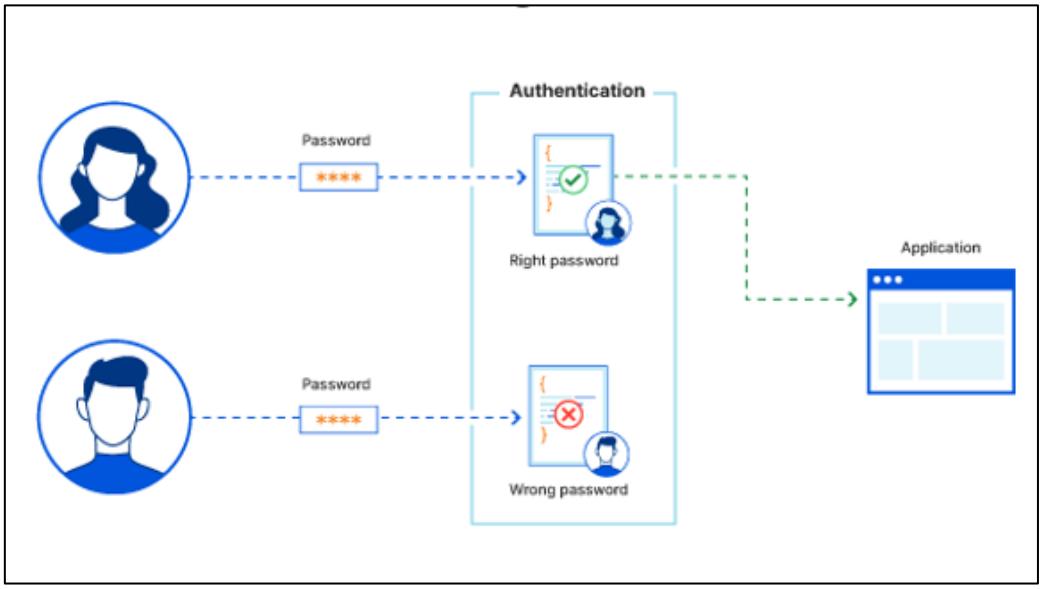
Las tres herramientas de pruebas de seguridad de aplicaciones web populares según el uso son: Burp Suite, OWASP ZAP, Acunetix. Según (Murat, Çig˘dem, Evren, & Alperen, 2021)

2.3.5. Autentificación

"La autenticación es el proceso de probar que usted es quien dice ser. Esto se logra mediante la verificación de la identidad de una persona o dispositivo". (Werner, y otros, 2023)

Figura 5

Concepto de autentificación



Ref. Imagen recuperada de What is authentication?, Cloudflare (s. f.). En https://www.cloudflare.com/es-es/learning/access-management/what-is-authentication/.

2.3.5.1. Técnicas de autentificación.

Según (Papathanasaki, Maglaras, & Ayres, 2022) tenemos las siguientes técnicas de autentificación:

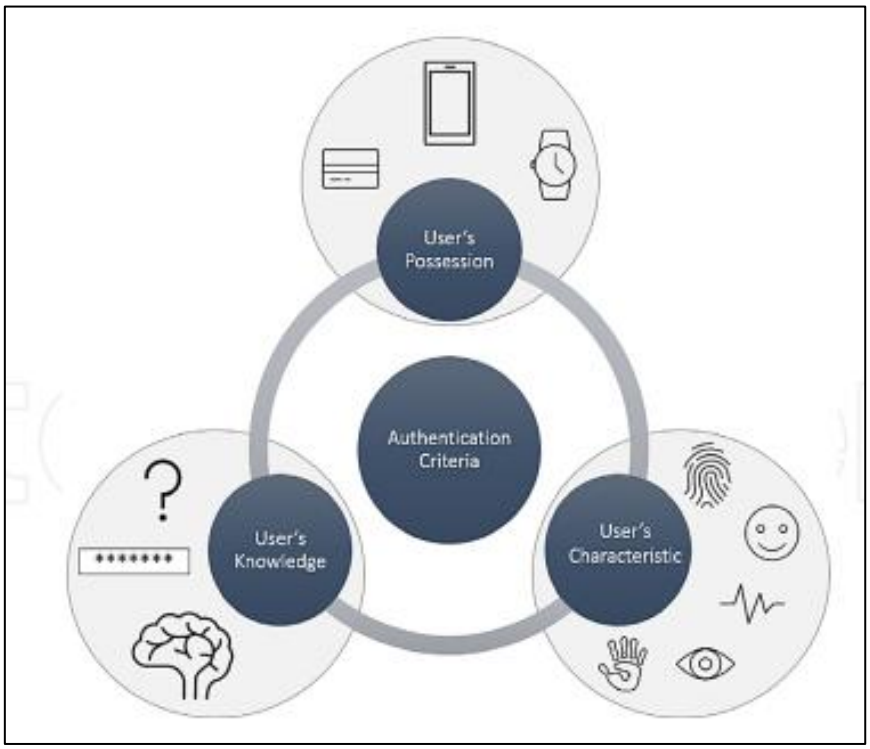
Autentificación por conocimiento: el conocimiento de información que solo conoce el usuario como contraseñas.

Autentificación por pertenencia o posesión: el usuario debe poseer un objeto físico o dispositivo para autentificarse como token de seguridad.

Autentificación por características físicas: utiliza alguna característica física del usuario como una huella dactilar.

Figura 6

Categorías de autentificación



Ref. (Papathanasaki, Maglaras, & Ayres, 2022)

2.3.5.2. Tipos de Mecanismos de autenticación.

Algunos tipos de mecanismos se describen a continuación:

Autenticación de un solo factor

Es un método de autenticación basado solo en un factor de verificación de la identidad del usuario, puede ser un PIN, una contraseña, un patrón gráfico, etc. Sin embargo, el uso de contraseñas fáciles o débiles representa una vulnerabilidad significativa porque las contraseñas pueden ser fáciles de adivinar para los atacantes y pueden comprometer las cuentas y la información de estas.

Ventajas

- Las contraseñas se componen de una de letras, números y caracteres únicos mientras más compleja sea la combinación, más complicado será para el atacante apoderarse de la misma.

Desventajas

- Las personas usan contraseñas débiles o fáciles y estás son vulnerables a ataques de phishing.
- Las personas comparten las contraseñas con personas no autorizadas.
- Un usuario no autorizado puede utilizar ataques de fuerza bruta en forma de ataques de diccionario o técnicas de ingeniería social para obtener acceso.

Autenticación de doble factor

En vista que la autentificación de un solo factor tiene este problema surge la Autenticación de dos factores 2FA. La Autenticación de dos factores 2FA combina dos factores de autentificación es decir cumple con una capa de seguridad adicional al proceso de autentificación.

Este mecanismo permite solicitar al usuario con dos factores distintos para la autentificación. Por ejemplo (Autentificación por conocimiento+ Autentificación por pertenencia o posesión), es decir se basa en los tipos de autentificación y se necesitan de 2 tipos una por conocimiento y la otra puede ser por pertenencia o característica física.

Hay una variedad de soluciones diferentes utilizar el segundo factor:

Según (Markert, Farke, & Dürmuth, 2019)

(i) Transmitir una contraseña de un solo uso (OTP) a través de SMS o por llamadas telefónicas automatizadas (llamadas automáticas) a un número preregistrado; Algunos servicios también ofrecen agregar una dirección de correo electrónico para recibir el código.

(ii) Tokens de autenticación que contienen una clave criptográfica y participan en un protocolo de autenticación con el servidor.

(iii) Aplicaciones de autenticación que se emparejan una vez con la cuenta y generan continuamente un código de inicio de sesión. Esta autenticación basada en aplicaciones también se conoce como token de software y, al igual que para SMS, llamadas o correo electrónico, requiere que el usuario proporcione el código en un formulario web adicional.

Ventajas

- Ofrece mayor seguridad, ya que añade un segundo mecanismo de autentificación, al que el atacante no tiene acceso.

Desventajas

- La autentificación 2FA incurre en hardware adicional, lo que aumenta el costo y a menudo reduce la usabilidad.
- Si no se tiene acceso a ambos mecanismos de autentificación el usuario no podrá acceder a la aplicación.
- La conectividad con estos dispositivos inteligentes representa un desafío dentro del procedimiento de 2FA.

Figura 7

Autentificación en dos pasos

Nota. Imagen generada por inteligencia artificial en DALL·E, 2025. Derechos reservados por OpenAI.

Autenticación de múltiple factor (AMF)

Es un método de autentificación que utiliza múltiples factores para verificar la identidad del usuario. Proporciona un nivel más alto de nivel de seguridad se reduce la probabilidad de acceso no autorizado y se fortalece la seguridad de la autenticación. Se combinan factores de conocimiento y posesión con factores biométricos para aumentar la prueba de identidad, dificultando que un actor malintencionado engañe al sistema a través de la suplantación

Ventajas

- Dificultad para los atacantes para la suplantación de identidad

Desventajas

- La facilidad de uso afecta la experiencia del usuario.

- El costo en la implementación de hardware adicional.
- Las tasas de aceptación falsa (FAR) y las tasas de rechazo falso (FRR) son cuestiones relacionadas con la autenticación biométrica.

2.3.6. OWASP

El Open Worldwide Application Security Project ® (OWASP) es una fundación sin fines de lucro que trabaja para mejorar la seguridad del software. Es la fuente para que los desarrolladores y tecnólogos protejan la web.

- Herramientas y recursos
- Comunidad y Redes
- Educación y Formación

El Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP) ha desempeñado un papel fundamental en la gestión del complejo horizonte de la seguridad de aplicaciones web. OWASP, una comunidad global que trabaja a la vanguardia para mejorar la seguridad de las aplicaciones web, se dedica a identificar, categorizar y mitigar vulnerabilidades en aplicaciones web. La compilación periódica de los riesgos de seguridad más críticos en aplicaciones web es una de sus iniciativas emblemáticas, publicada como el OWASP Top 10. (Fredj, Cheikhrouhou, Krichen, Hamam, & Derhab, 2021)

2.3.6.1. OWASP TOP 10

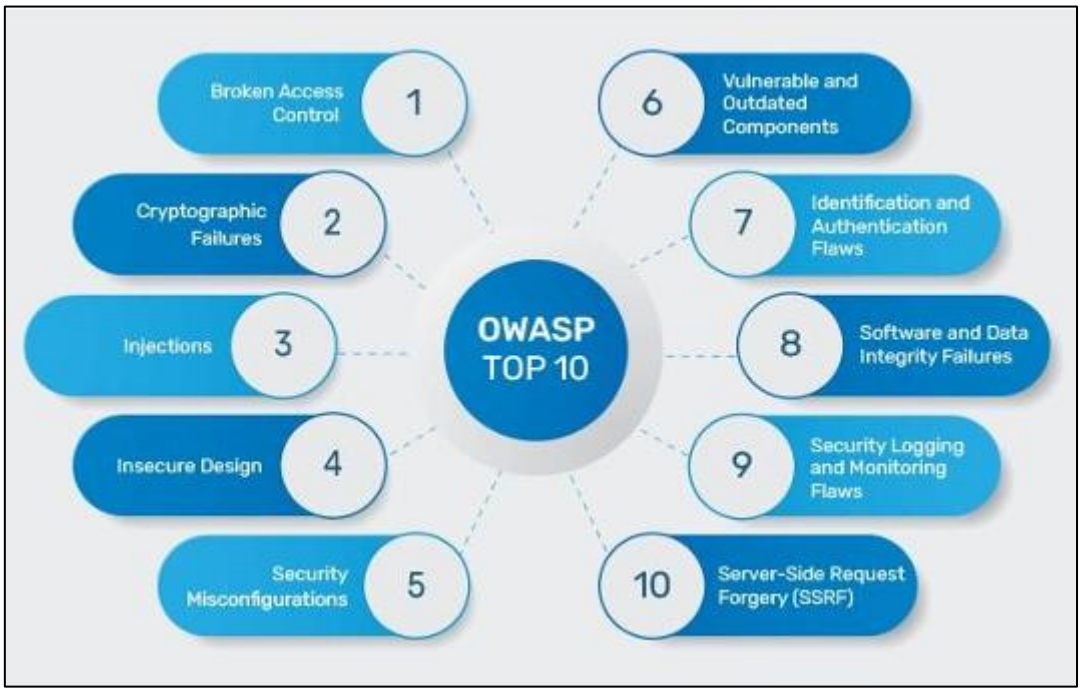
La última versión de OWASP fue lanzada el año 2021. OWASP Top 10 es una lista con los diez riesgos de seguridad más comunes y peligrosos de las aplicaciones web.

Ayudan a identificar y mitigar los riesgos de seguridad críticos de las aplicaciones web.

Está lista se actualiza periódicamente.

Figura 8

Vulnerabilidades OWASP Top 10 2021



Fuente: (Devendra & Nilesh, 2023)

2.3.6.2.Controles según OWASP Relacionados a la autentificación de un sistema web

A continuación, se presenta el detalle de los controles según OWASP más relevantes identificados relacionados con la autentificación de un sistema web.

Tabla 7

Lista de controles relacionados con la autentificación

Lista	DESCRIPCIÓN
A01:2021 – Pérdida de Control de Acceso	Eludir las comprobaciones de control de acceso modificando la URL (alteración de parámetros o navegación forzada), el estado interno de la aplicación o la página HTML, o mediante el uso de una herramienta que modifique los pedidos a APIs. Elevación de privilegios. Actuar como usuario sin haber iniciado sesión o actuar como administrador cuando se inició sesión como usuario regular.
A02:2021 - Fallas Criptográficas	¿Se utilizan algoritmos o protocolos criptográficos antiguos o débiles de forma predeterminada o en código antiguo? ¿Se utilizan claves criptográficas predeterminadas, se generan o reutilizan claves criptográficas débiles, o es inexistente la gestión o rotación de claves adecuadas? ¿Se incluyen las claves criptográficas en los repositorios de código fuente? ¿Se utilizan funciones hash en obsoletas, como MD5 o SHA1, o se utilizan funciones hash no criptográficas cuando se necesitan funciones hash criptográficas?

A04:2021 – Diseño Inseguro	Riesgos relacionados con el diseño y las fallas arquitectónicas
A06:2021 – Componentes Vulnerables y Desactualizados	Si el software es vulnerable, carece de soporte o no está actualizado. Esto incluye el sistema operativo, el servidor web/de aplicaciones, el sistema de administración de bases de datos (DBMS), las aplicaciones, las API y todos los componentes, los entornos de ejecución y las bibliotecas. Si no analiza en búsqueda de vulnerabilidades de forma regular y no se suscribe a los boletines de seguridad relacionados con los componentes que utiliza. Si no repara o actualiza la plataforma subyacente, frameworks y dependencias de manera oportuna y basada en el riesgo. Esto suele ocurrir en entornos en los que la aplicación de parches de seguridad es una tarea mensual o trimestral bajo control de cambios, lo que deja a las organizaciones abiertas a días o meses de exposición innecesaria a vulnerabilidades con soluciones disponibles. Si los desarrolladores de software no testean la compatibilidad de las bibliotecas actualizadas, actualizadas o parcheadas.
A07:2021 – Fallas de Identificación y Autenticación	Permite contraseñas por defecto, débiles o bien conocidas, como "Password1" o "admin/admin". Posee procesos débiles o no efectivos para las funcionalidades de olvido de contraseña o recuperación de credenciales, como "respuestas basadas en el conocimiento", las cuales no se pueden implementar de forma segura.

	No posee una autenticación multi-factor o la implementada es ineficaz. Reutiliza el identificador de sesión después de iniciar sesión.
A09:2021 – Fallas en el Registro y Monitoreo	Las pruebas de penetración y los escaneos utilizando herramientas de pruebas dinámicas de seguridad en aplicaciones (como ser OWASP ZAP) no generan alertas.

Fuente: (OWASP Top 10 team, 2021)

2.3.7. Normas ISO/IEC 27000:2022

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional(IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnología. (Vasquez, 2023)

La familia de normas ISO/IEC 27000 se publicó en el año 1995 como Estándar Británico BS779, luego de varios años y revisiones en 2000 se convirtió en ISO 17799 hasta convertirse posteriormente en ISO/IEC 27000.

Las normas ISO/IEC 27000 establecen un marco para implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) dentro de una organización. Tienen como objetivo orientar a la mejora continua y mitigar los riesgos de la organización.

ISO 27000 plantean un enfoque sistemático, este mejora la gestión de la seguridad de nuestra información, lo cual permite a las diferentes organizaciones identificar y tratar de manera adecuada los riesgos de la SI de manera correcta, dicha implementación brinda beneficios a largo plazo, como es la mejora de la eficiencia, la reducción de los costos, lo cual trae como consecuencia beneficiosa la mejora de la reputación de las organizaciones, aumenta con ello la confianza de los clientes y las partes involucradas en la seguridad. (Cárdenas , 2020)

2.3.7.1.Norma ISO/IEC 27001

La norma ISO/IEC 27001 es un estándar a nivel mundial que da directrices para la gestión Seguridad de la información, y estas permiten salvaguardar la información de la organización. Tiene por objetivo mantener la Confidencialidad, Integridad y Disponibilidad de la información.

ISO 27001 es el único estándar de toda la familia de normas ISO 27000 que se utiliza para brindar certificaciones a las organizaciones. Las demás normas de esta familia se usan para brindar un apoyo robusto y profundo para que la organización pueda construir e implementar un Sistema de Gestión de la Seguridad de la Información de manera correcta y duradera. (De La Cruz Rodríguez, Méndez Fernández, & Méndez Fernández, 2023)

2.3.7.2.Norma ISO/IEC 27002

La norma ISO/IEC 27002, es una guía de buenas prácticas que contiene los controles de seguridad de la información en un Sistema de Gestión de la Seguridad de la información. La nueva versión fue publicada el 16 de febrero del 2022. Y su nombre actual es “Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información”. Las organizaciones no están obligadas a adoptar todos los controles, puede seleccionar el o los que más le convengan

La norma ISO/IEC 27002:2022 contiene 93 controles divididos en 4 cláusulas tal como muestra la Figura

Figura 9

Controles de la ISO/IEC 27002:2022

Nota: Imagen Tomada de ISO 27002, (2022)

Los controles organizacionales buscan garantizar que la seguridad de la información sea gestionada de manera integral y de acuerdo a la cultura y operaciones de la organización.

Los controles a personas es el control a las personas y busca garantizar el recurso humano dentro de la organización sea un componente activo en la preservación de la seguridad de la información, complementando los controles técnicos y organizacionales.

Controles físicos son todas las medidas de protección a entradas, áreas u activos de la organización. Y proporcionar una defensa integral contra amenazas físicas y riesgos potenciales.

Controles tecnológicos son esenciales para mantener la seguridad de la información en una organización, son todos los dispositivos, herramientas, sistemas que nos ayudan a proteger la información y mitigar los riesgos.

2.3.7.3.Controles Relacionados a la autentificación de un sistema web

A continuación, se presenta el detalle de los controles según la ISO/IEC 27002:2022 más relevantes identificados relacionados con la autentificación de un sistema web.

Tabla 8

Controles tecnológicos ISO/IEC 27002:2022

Id	Nombre	Control	Propósito	Tipo De Control	Propiedades De La Seguridad De La Información
8.2	Derechos de acceso privilegiado	La asignación y el uso de derechos de acceso privilegiado deben restringirse y gestionarse	Para garantizar que solo los usuarios autorizados, los componentes y servicios de software reciban derechos de acceso privilegiado.	Preventivo	Confidencialidad, Integridad, Disponibilidad
8.3	Restricción de acceso a la información	El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política específica del tema establecida sobre el control de acceso	Para garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.	Preventivo	Confidencialidad, Integridad, Disponibilidad

8.5	Autenticación segura	Las tecnologías y los procedimientos de autentificación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso	Para garantizar que un usuario o entidad se autentica de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios.	Preventivo	Confidencialidad, Integridad, Disponibilidad
8.15	Registro	Se deben producir, almacenar, proteger y analizar registros que registren actividades, excepciones, fallas y otros eventos relevantes	Para registrar eventos, genera evidencia, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y respaldar investigaciones.	Detective	Confidencialidad, Integridad, Disponibilidad
8.24	Uso de criptografía	Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas	Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo a los requisitos comerciales y de seguridad de la información, y teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.	Preventivo	Confidencialidad, Integridad, Disponibilidad

8.26	Requisitos de seguridad de la aplicación	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones	Para garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones	Preventivo	Confidencialidad, Integridad, Disponibilidad

Nota: Tomado de ISO 27002, (2022)

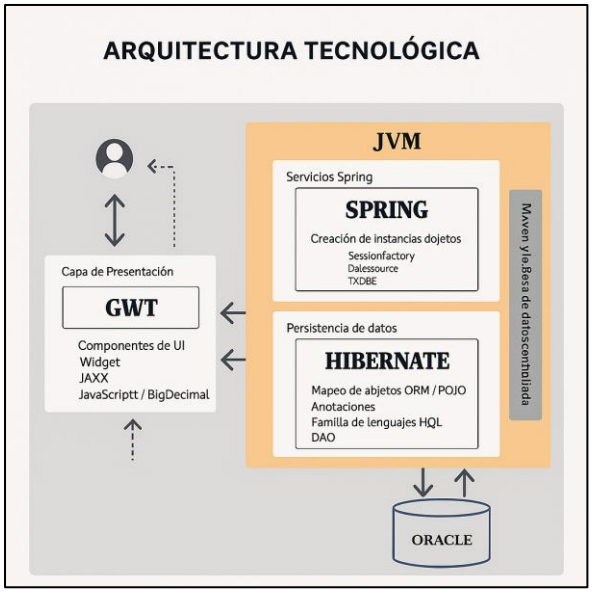
2.4. Arquitectura del sistema y Herramientas Tecnológicas

El sistema esta implementado con dos proyectos: Lógica de negocio y Configuración web. El patrón de diseño de la aplicación es MVP propio de GWT, y para el acceso a las implementaciones de lógica de negocio se utiliza el patrón de diseño MVC

La arquitectura del sistema lo podemos ver en la siguiente figura:

Figura 10

Arquitectura tecnológica de un proyecto Maven con GWT, Spring, Hibernate y Oracle



Nota: Imagen original editada con ayuda de inteligencia artificial

Al momento cuenta con los siguientes módulos:

- Administración de usuarios
- Establecimientos de salud acreditados y servicios de apoyo
- Lista de Espera Única Nacional (corneal, renal, hepática, pulmonar, cardiaca)
- Donante Cadavérico
- Registro Ecuatoriano de Diálisis y Trasplantes

2.4.1. Herramientas Tecnológicas

Para el desarrollo de esta aplicación web se utilizaron las siguientes herramientas

Tabla 9

Herramientas utilizadas

Nombre	Versión	Descripción
Java	Java 1.7	Lenguaje de Programación jdk1.8.0_281
SPRING	4.1.2	Configuración de Beans, Transacciones
HIBERNATE	4.2.3	DataSources, SessionFactory, Persistencia y acceso de datos
GWT	2.5.1	Framework de desarrollo para UI
MAVEN	3.8.5	Configuración de dependencias(jar's)
NEXUS	2.11.4	Repositorio de librerías SNAPSHOT Y RELEASE
Oracle	11g	Base de Datos
SVN		Herramienta de control de versiones
Tomcat	8.0	Despliegue de la aplicación
Eclipse	2021-03	Entorno de desarrollo

Nota: Información tomada del sistema informático

2.4.2. Desarrollo de la solución

2.4.2.1.Autentificación de Dos Factores (2FA)

En el marco de este proyecto, se desarrolló e implementó un sistema de contraseña de un solo uso (OTP) como una medida adicional para fortalecer la seguridad en el proceso de autenticación. Este mecanismo complementa la autenticación tradicional basada en el nombre de usuario y contraseña, proporcionando una capa adicional de protección contra accesos no autorizados.

El proceso funciona de la siguiente manera: después de que el usuario ingresa su nombre de usuario y contraseña en el sistema, este genera automáticamente un código OTP

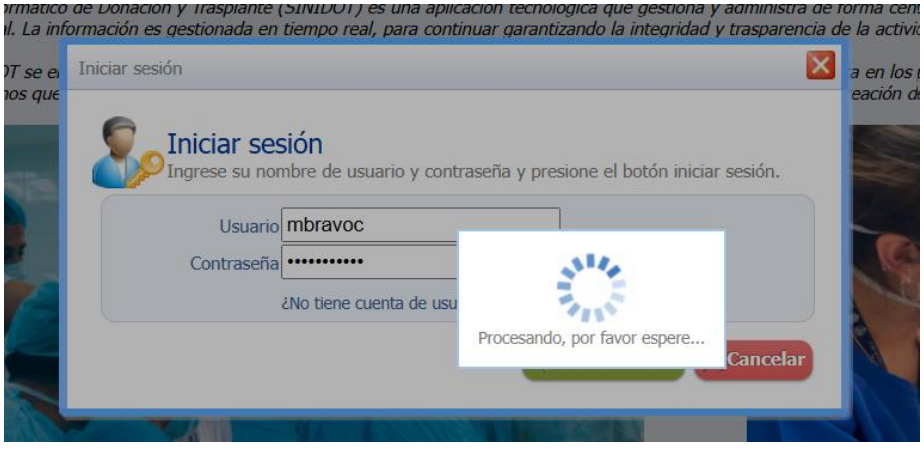
único y aleatorio. Este código es enviado de manera inmediata al correo electrónico registrado por el usuario, garantizando que solo el propietario legítimo de la cuenta, con acceso a su dirección de correo electrónico, pueda completar el proceso.

El OTP tiene una validez temporal limitada, lo que minimiza el riesgo de que sea interceptado o utilizado de forma indebida por actores malintencionados. Además, el sistema está diseñado para invalidar automáticamente el código una vez que se ha utilizado o cuando expira el tiempo asignado, asegurando que el código no pueda ser reutilizado.

Esta medida responde a la necesidad de prevenir ataques como el robo de credenciales, phishing y fuerza bruta, que representan riesgos significativos en sistemas que dependen únicamente de contraseñas estáticas. Al combinar la autenticación basada en contraseña con un segundo factor dinámico como el OTP, el sistema refuerza significativamente la seguridad y dificulta el acceso no autorizado, incluso si las credenciales primarias han sido comprometidas.

Figura 11

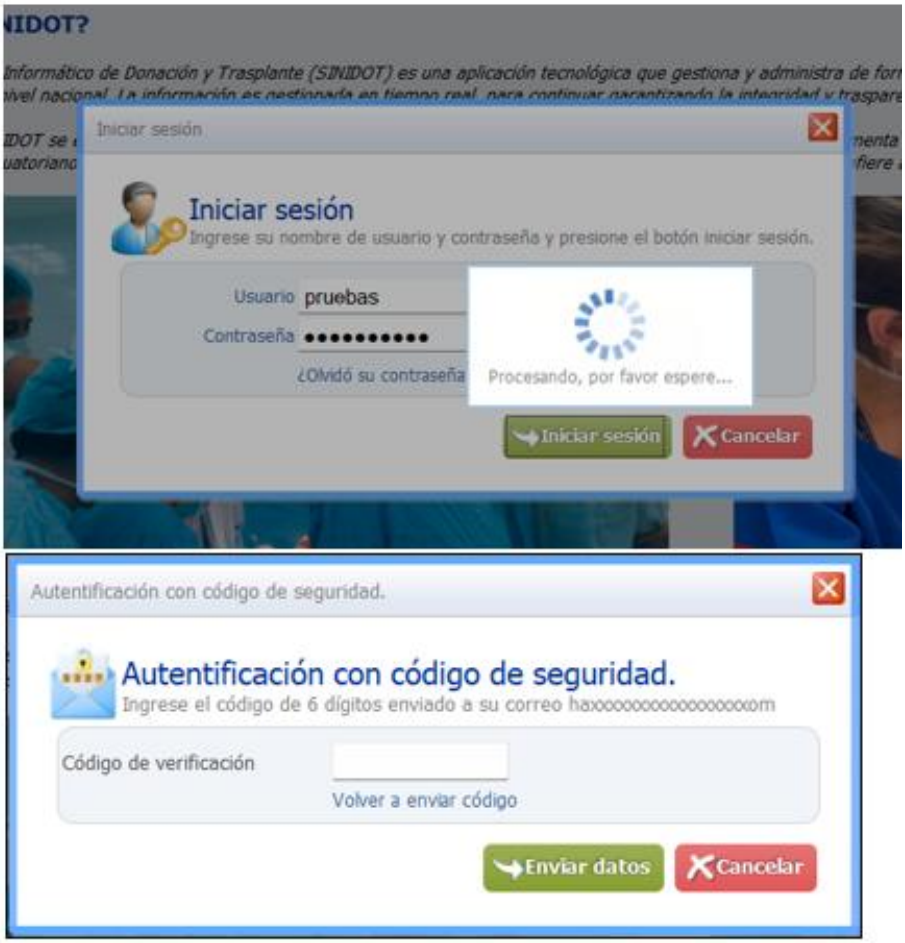
Interfaz anterior inicio de sesión



Nota: Imagen tomada del sistema informático

Figura 12

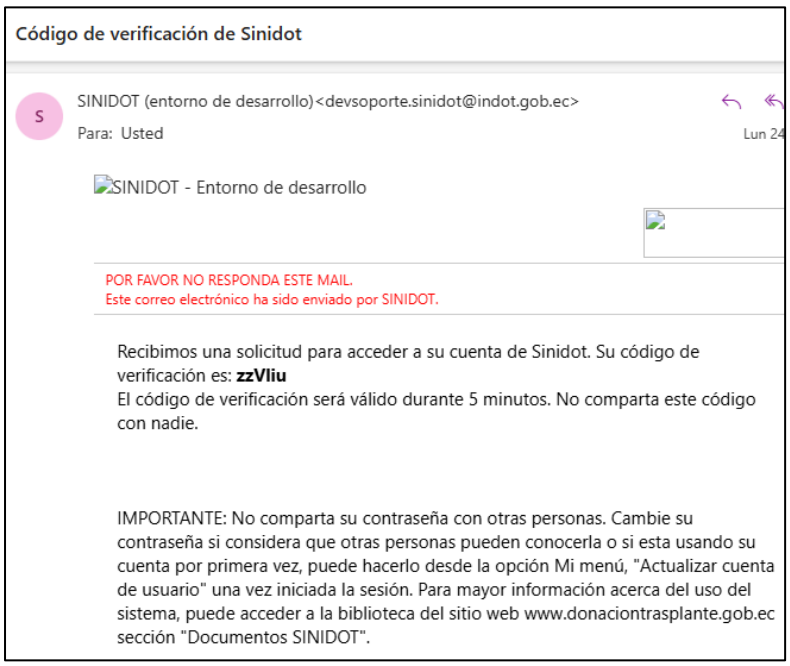
Interfaz nueva inicio de sesión



Nota: Imagen tomada del sistema informático

Figura 13

Correo con código de validación



Nota: Imagen tomada de correo registrado

Además, se cuenta con la administración de usuarios del Sistema, en la última columna el administrador puede activar o desactivar el 2FA. Tal como se muestra en la figura 11.

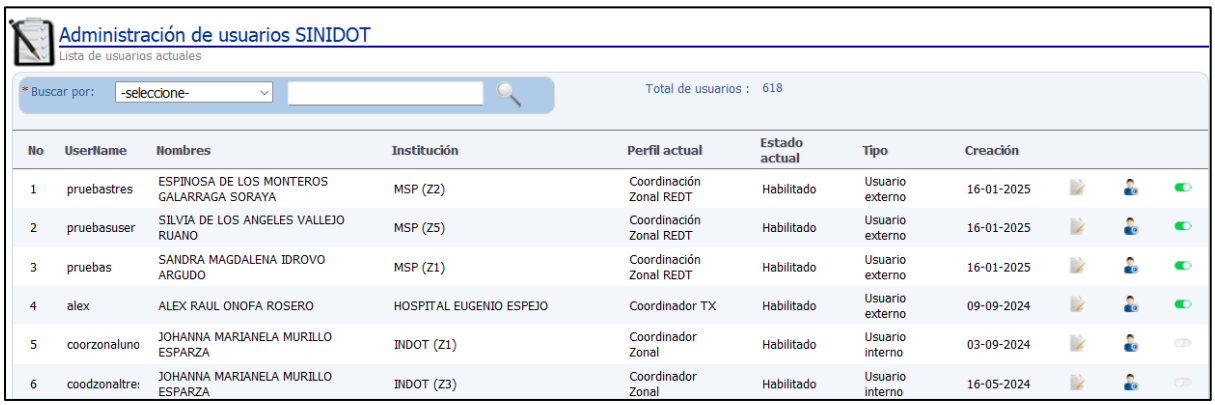
Figura 14

Administración de usuarios sin opción de activar 2FA

Nota: Imagen tomada del sistema informático

Figura 15

Administración de usuarios con opción de activar o desactivar 2FA



No	UserName	Nombres	Institución	Perfil actual	Estado actual	Tipo	Creación
1	pruebastres	ESPINOSA DE LOS MONTEROS GALARRAGA SORAYA	MSP (Z2)	Coordinación Zonal REDT	Habilitado	Usuario externo	16-01-2025
2	pruebasuser	SILVIA DE LOS ANGELES VALLEJO RUANO	MSP (Z5)	Coordinación Zonal REDT	Habilitado	Usuario externo	16-01-2025
3	pruebas	SANDRA MAGDALENA IDROVO ARGUDO	MSP (Z1)	Coordinación Zonal REDT	Habilitado	Usuario externo	16-01-2025
4	alex	ALEX RAUL ONOFA ROSERO	HOSPITAL EUGENIO ESPEJO	Coordinador TX	Habilitado	Usuario externo	09-09-2024
5	coorzonaluno	JOHANNA MARIANELA MURILLO ESPARZA	INDOT (Z1)	Coordinador Zonal	Habilitado	Usuario interno	03-09-2024
6	coodzonaltre:	JOHANNA MARIANELA MURILLO ESPARZA	INDOT (Z3)	Coordinador Zonal	Habilitado	Usuario interno	16-05-2024

Nota: Imagen tomada del sistema informático

Para la generación del código único se utilizó el algoritmo de la siguiente figura

Figura 16

Método para generar el código único

```
public static String generarCodigoUnico(Integer numCaracteres) {
     String codigoSeguridad="";
    if (numCaracteres != null) {
        String caracteresPermitidos = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";
        SecureRandom random = new SecureRandom();

        StringBuilder codigo = new StringBuilder(numCaracteres);
        for (Integer i = 0; i < numCaracteres; i++) {
            int index = random.nextInt(caracteresPermitidos.length());
            codigo.append(caracteresPermitidos.charAt(index));
        }

        codigoSeguridad = codigo.toString();
    }
    return codigoSeguridad;
}
```

Nota: Imagen tomada del sistema informático

2.4.2.2.Fortalecimiento de la Gestión de Contraseñas

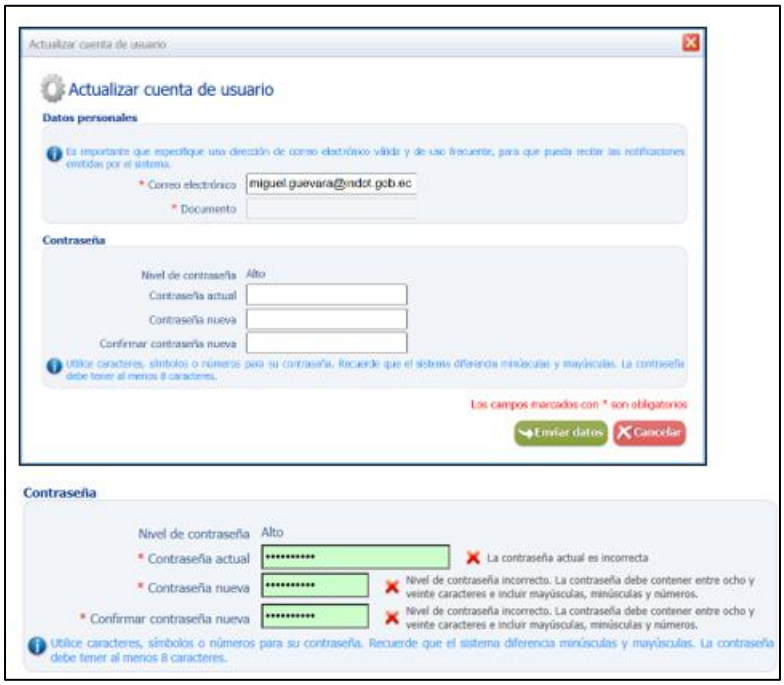
Se desarrolló e implementó un proceso automatizado que establece la caducidad periódica de las contraseñas, con el objetivo de garantizar un nivel adicional de seguridad en el acceso a las cuentas de usuario. Este mecanismo obliga a los usuarios a cambiar su contraseña después de un período de tiempo predefinido, lo que ayuda a mitigar los riesgos asociados con contraseñas obsoletas o comprometidas.

Una vez que la contraseña caduca, el sistema requiere que el usuario elija una nueva contraseña antes de permitirle acceder a su cuenta. Esta nueva contraseña debe cumplir con los requisitos de seguridad establecidos, como una longitud mínima, la inclusión de caracteres especiales, mayúsculas y números, lo que refuerza aún más la seguridad.

Esta política de caducidad periódica contribuye significativamente a reducir los riesgos derivados de contraseñas estáticas y fáciles de adivinar, como las que se utilizan durante un largo período sin actualización. Al obligar a los usuarios a cambiar sus contraseñas con regularidad, se dificulta el acceso no autorizado a las cuentas, incluso si las credenciales anteriores se ven comprometidas.

Figura 17

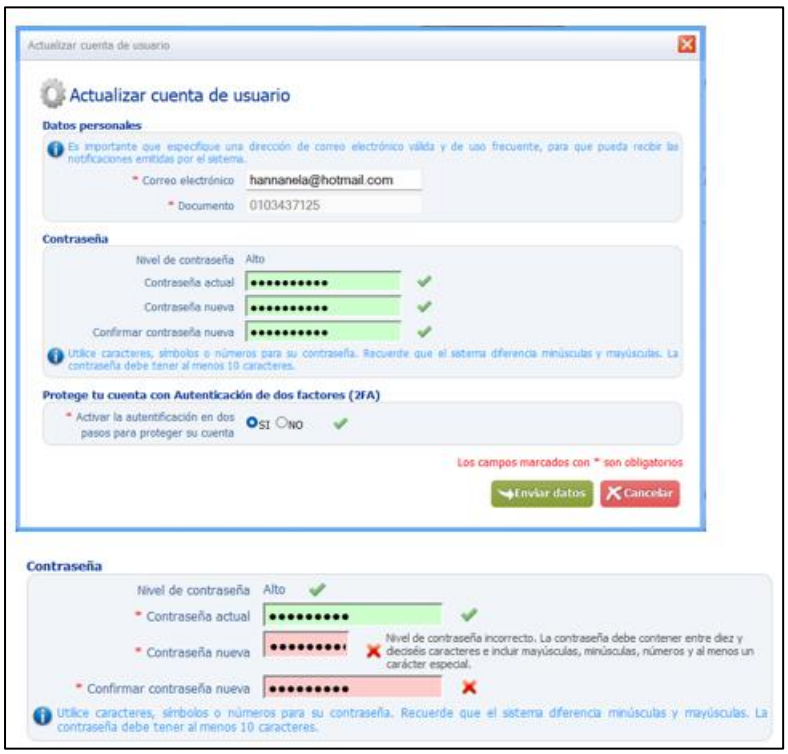
Interfaz actualizar cuenta de usuario anterior



Nota: Imagen tomada del sistema informático

Figura 18

Interfaz actualizar cuenta de usuario nueva



Nota: Imagen tomada del sistema informático

El almacenamiento de un historial de contraseñas evita la reutilización de credenciales y mejora la seguridad del usuario para esto se creó una tabla con el historial. Tal como se muestra en la imagen.

Figura 19

Tabla de base de datos para almacenar historial de contraseñas

123 ID_DET_USR_PASSWORD	123 ID_USR_USUARIO	ABC PASSWORD	FECHA_REGISTRO_PASSW
3	77.354	0f12f3f27296665dd2c0d6b7c2273780	2025-01-17 09:10:30.000
5	77.354	8b72f7cf6d69b53e60848c3076e92b30520edb51e230319ef8cc16ccf1ccacf2	2025-01-17 12:46:57.000
6	77.354	e107d6e4c2f219a150e213b024c84cb25f26f0849e741eb169108d727dbc48b8	2025-01-17 12:51:39.000
7	77.354	8b72f7cf6d69b53e60848c3076e92b30520edb51e230319ef8cc16ccf1ccacf2	2025-01-17 15:08:58.000

Nota: Imagen tomada de la base de datos del sistema informático

2.4.2.3.Fortalecimiento de los Procesos de Recuperación de Credenciales

Se desarrolló e implementó un proceso seguro para la recuperación de contraseñas en el sistema. Este mecanismo está diseñado para activarse automáticamente cuando una cuenta

de usuario se bloquea debido a múltiples intentos fallidos de inicio de sesión, lo que previene accesos no autorizados.

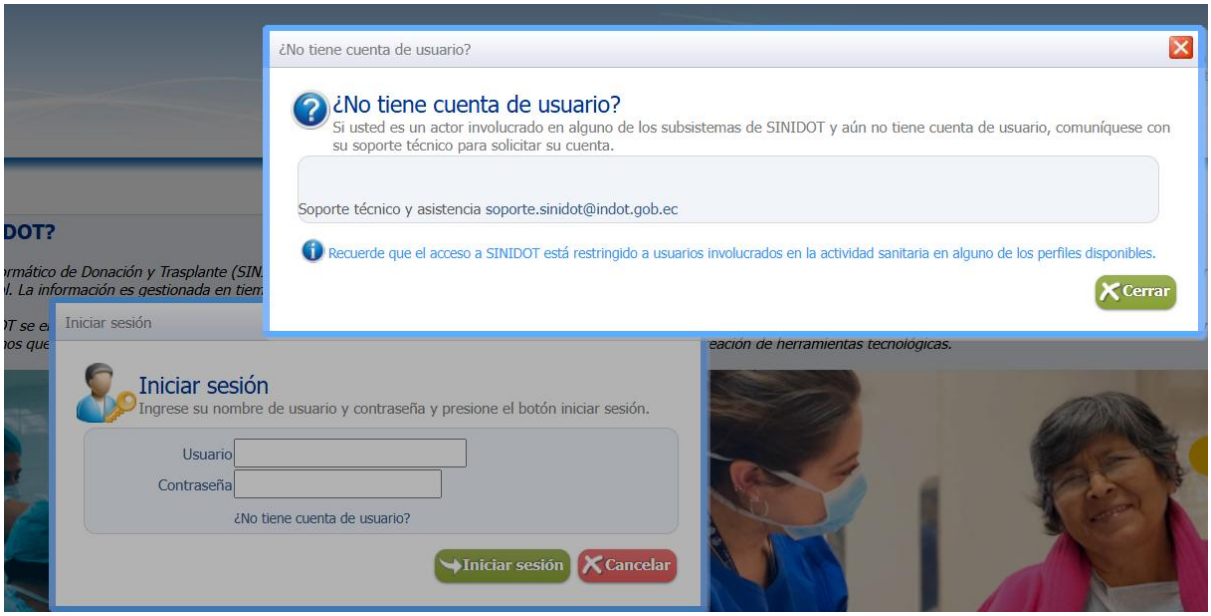
El proceso consiste en el envío de un código único de recuperación al correo electrónico registrado por el usuario al momento de la creación de su cuenta. Este código tiene una validez temporal limitada, lo que garantiza su inutilidad después de un periodo de tiempo predefinido o tras ser utilizado exitosamente.

Esta solución asegura que solo el propietario legítimo de la cuenta, con acceso a su correo registrado, pueda iniciar el proceso de restablecimiento de la contraseña. Además, se refuerza la seguridad al limitar los intentos de uso del código y al notificar al usuario cualquier actividad relacionada con la recuperación de credenciales, brindando mayor control y transparencia sobre el estado de su cuenta.

Este enfoque sustituye métodos menos seguros, como las preguntas de seguridad o respuestas basadas en el conocimiento, los cuales son susceptibles a ataques de ingeniería social y acceso a información pública. Asimismo, se alinea con las mejores prácticas de seguridad recomendadas por estándares como OWASP, asegurando la confidencialidad y privacidad del usuario en todo momento.

Figura 20

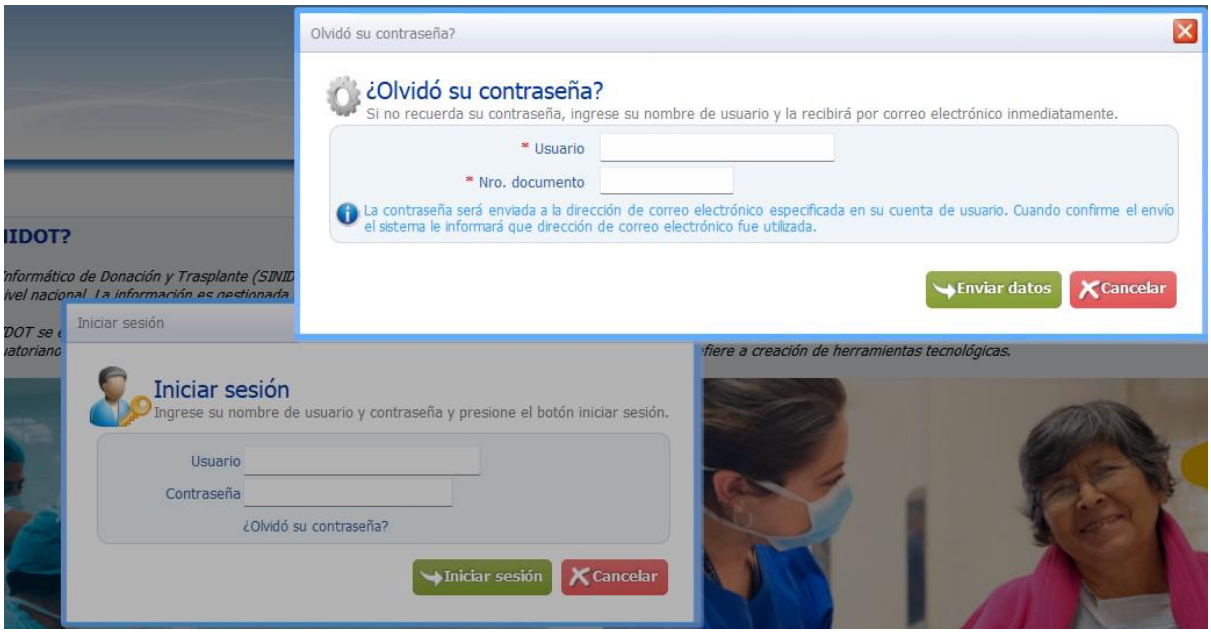
Interfaz proceso de recuperación de contraseñas antes



Nota: Imagen tomada del sistema informático

Figura 21

Interfaz recuperación de contraseñas actual



Nota: Imagen tomada del sistema informático

2.4.2.4.Actualización del Hashing de Contraseñas: De MD5 a SHA-256

La actualización del almacenamiento de contraseñas de MD5 a SHA-256 es una mejora fundamental para la seguridad del sistema. El MD5 (Message Digest Algorithm 5) fue muy utilizado para la protección de contraseñas, pero presenta múltiples vulnerabilidades que lo hacen inseguro en la actualidad. El algoritmo SHA-256 (Secure Hash Algorithm 256-bit) forma parte de la familia SHA-2, desarrollada por la NSA y recomendada por organismos internacionales para la protección de datos.

Figura 22

Método para crear una cadena con MD5

```
private String md5EncryptString(String cadena) throws SinidotException{
    StringBuilder sqlQuery = new StringBuilder();
    SQLQuery query = null;
    String newCadena = null;
    try{
        Session session = hibernate.getSessionFactory().getCurrentSession();
        session.clear();

        if(cadena == null) throw new SinidotException("Error la cadena de texto es nula");

        sqlQuery.append("select SNDTOWN.md5Encrypt('"+cadena+"') from dual");
        query = session.createSQLQuery(sqlQuery.toString());
        newCadena =  (String) query.uniqueResult();
        return newCadena;
    }catch(Exception e){
        log.error("Error en md5EncryptString", e);
        throw new SinidotException("Error al intentar encriptar la cadena de texto: "+cadena,e);
    }
}
```

Nota: Imagen tomada del entorno de desarrollo sistema informático.

Figura 23

Método para crear un texto con SHA256

```
public String encriptarSHA256(String texto) {
    try {
        MessageDigest digest = MessageDigest.getInstance("SHA-256");
        byte[] hash = digest.digest(texto.getBytes("UTF-8"));
        StringBuilder hexString = new StringBuilder();
        for (byte b : hash) {
            String hex = Integer.toHexString(0xff & b);
            if (hex.length() == 1) hexString.append('0');
            hexString.append(hex);
        }
        return hexString.toString();
    } catch (Exception e) {
        throw new RuntimeException("Error al encriptar con SHA-256", e);
    }
}
```

Nota: Imagen tomada del entorno de desarrollo sistema informático.

2.5. Marco legal

La Constitución de la República del Ecuador que es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico, establece en el artículo 66 numeral 19

> El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley. (Constitución de la República del Ecuador , 2008)

La Ley Orgánica de Protección de Datos Personales tiene por objeto "garantizar el ejercicio del derecho de protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección" y entre sus principios tenemos la seguridad de datos personales que incluye "implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas de la técnica, sean estas organizativas, técnicas o de cualquier otra índole para proteger los datos personales" (Ley Orgánica de Protección de Datos Personales, 2021)

En la Ley Orgánica de Donación y Trasplante de Órganos, Tejidos y Células en su Art. 10 "

> Protección de datos y confidencialidad. - La Autoridad Sanitaria Nacional, a través del organismo regulador designado, adoptará las medidas necesarias para garantizar que la información generada del proceso de donación y trasplante, se convierta en anónima, a fin de que la o el donante y la o el receptor no sean identificables. (Ley Orgánica de Donación y Trasplante de Órganos, Tejidos y Células, 2011)

Con esta investigación se trata de proteger el acceso a la información de los receptores y donantes que se encuentran registrados en el sistema de donación y trasplante de órganos fortaleciendo el proceso de autentificación con las mejores prácticas de seguridad y así garantizar el cumplimiento legal del manejo de datos.

CAPITULO III

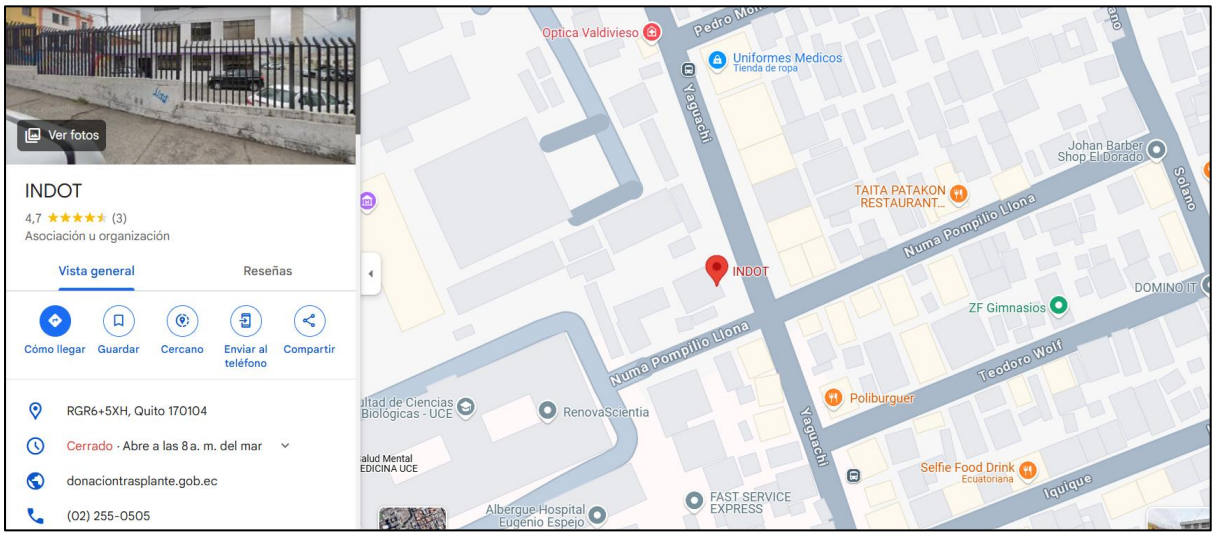
3. MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

Este proyecto fue llevado a cabo en el Instituto de Donación y Trasplante de Órganos, Tejidos y Células, que se encuentra situada en la ciudad de Quito, Ecuador.

Figura 24

Ubicación del Instituto de Donación y Trasplante de Órganos Tejidos y Células



Nota. La figura muestra la ubicación aproximada del INDOT *(Google, 2023)*

3.2. Enfoque y tipo de investigación

El presente trabajo de investigación adoptó un enfoque cualitativo con el objetivo de recopilar información detallada y comprender las necesidades específicas de todos los usuarios involucrados en el proceso de donación y trasplante de órganos. Este enfoque permitió identificar no solo las barreras que podrían dificultar la implementación de mejoras en el sistema, sino también otros factores relevantes que podrían influir en la aceptación y eficacia de integrar un proceso de autenticación de doble factor, así como la aplicación de mejores prácticas de seguridad de la información.

Como parte del estudio, se utilizó la encuesta como instrumento principal de investigación. Este método fue fundamental para explorar la percepción y las opiniones de los usuarios sobre la viabilidad y aplicabilidad del uso de la autenticación de doble factor. Además, permitió recolectar datos relevantes para evaluar cómo las medidas de seguridad propuestas podrían mejorar la protección de los datos sensibles dentro del sistema. Los resultados obtenidos brindaron una visión integral sobre las necesidades, expectativas y posibles desafíos asociados con la implementación de estas mejoras, aportando así un marco valioso para el desarrollo de un sistema más robusto y seguro.

3.3. Procedimiento de investigación

Fase 1. Investigar y analizar las vulnerabilidades y riesgos relacionados con la protección de datos en el proceso de donación y trasplante de órganos

Se realizó un análisis de las vulnerabilidades del sistema web utilizando la herramienta OWASP ZAP.

Se obtuvo el informe con las vulnerabilidades medias, bajas e informativas. El análisis realizado es el automático.

Después de realizado el análisis de vulnerabilidades se identificador 14 vulnerabilidades, con la siguiente clasificación:

Tabla 10

Vulnerabilidades halladas

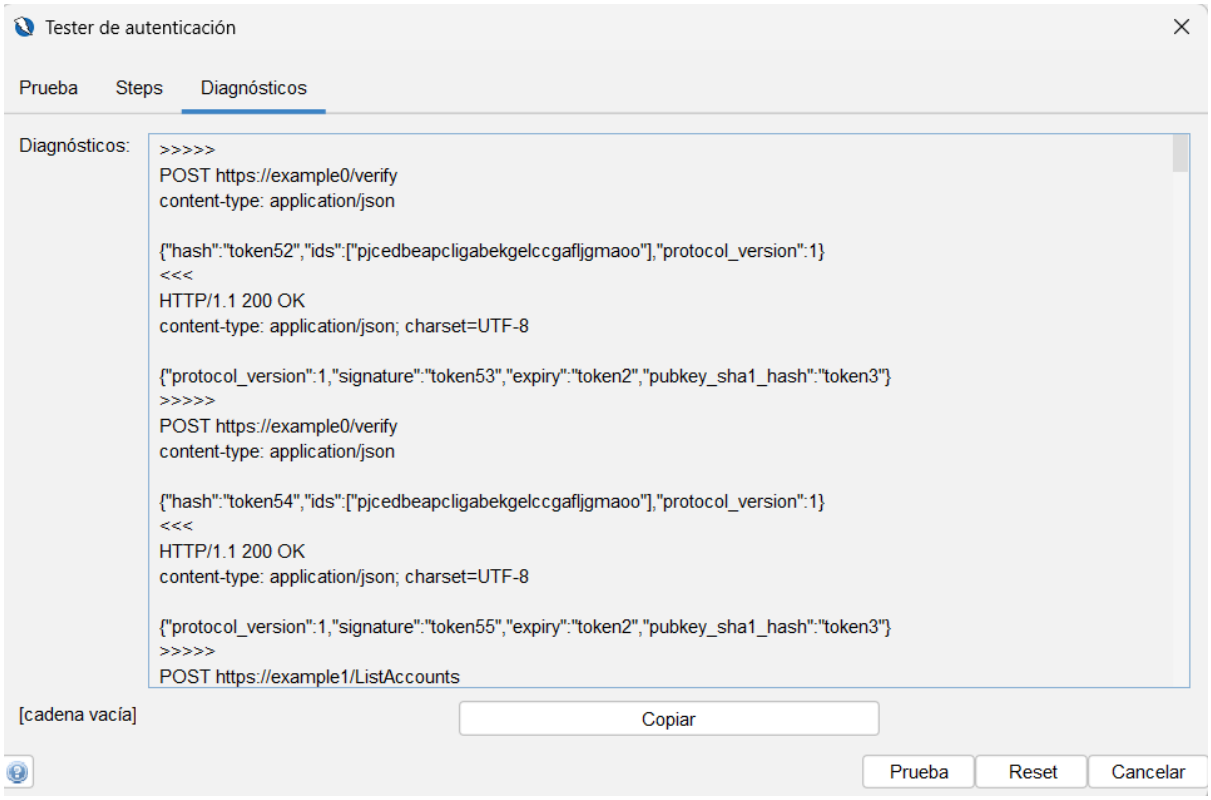
Riesgo	Cantidad	Vulnerabilidad
Crítico (Alto)	1	Librería JavaScript Vulnerable.
Medio	3	Falta de Content Security Policy (CSP). Falta de Cabecera Anti-Clickjacking. Uso de jQuery Vulnerable.
Bajo	6	Cookie Sin Flag de Seguridad. Cookie sin el atributo SameSite. Divulgación de Marcas de Tiempo – Unix. El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP. Falta encabezado X-Content-Type-Options. Strict-Transport-Security Header No Establecido.
Informativo	4	Aplicación Web Moderna. Divulgación de comentarios sospechosos en código fuente. Reexaminar las Directivas de Control de Caché. Respuesta de Gestión de Sesión Identificada.
Total	14	

Nota. Tomado del resumen generado de OWASP ZAP

Además, se realizó el Tester de autentificación y OWASP devolvió lo que se muestra en la Figura 22.

Figura 25

Test de Autentificación



Nota. Diagnóstico realizado con OWASP ZAP

Según el análisis realizado las cookies de sesión no están protegidas correctamente. No se aplican configuraciones clave de seguridad en encabezados HTTP, aumentando el riesgo de ataques como Clickjacking y Cross-Site Scripting (XSS). Y se utilizan librerías JavaScript vulnerables, lo que podría facilitar ataques de inyección de código en los clientes.

Se realizo la revisión de las solicitudes POST enviadas al servidor tras el ingreso del usuario y contraseña, y no encontró ningún parámetro adicional que indique que existe 2FA, esto significa que el sistema permite el acceso solo con un usuario y contraseña.

Si hubiera 2FA, deberíamos ver un segundo paso de verificación después de la autenticación inicial, como un código OTP, una verificación biométrica, etc. Nada de esto está presente en el tráfico.

El análisis de la protección de datos se realizó mediante una verificación de la implementación de los mecanismos de autenticación del sistema, basándose en las directrices de ISO 27002:2022 y las mejores prácticas de OWASP, antes de la implementación de la autenticación en dos factores (2FA).

Tabla 11

Evaluación del Sistema informático con ISO 27002:2022

Id	Nombre	Cumple	No cumple
8.2	Derechos de acceso privilegiado	X	
8.3	Restricción de acceso a la información	X	
8.5	Autenticación segura		X
8.15	Registro	X	
8.24	Uso de criptografía		X
8.26	Requisitos de seguridad de la aplicación		X

Nota. Análisis realizado con los datos obtenidos de OWASP ZAP

Tabla 12

Evaluación del Sistema Informático con OWASP Top 10

Nombre	VULNERABLE
A01:2021 – Pérdida de Control de Acceso	Seguro
A02:2021 - Fallas Criptográficas	En Riesgo
A04:2021 – Diseño Inseguro	En Riesgo
A06:2021 – Componentes Vulnerables y Desactualizados	En Riesgo
A07:2021 – Fallas de Identificación y Autenticación	En Riesgo
A09:2021 – Fallas en el Registro y Monitoreo	Seguro

Nota. Análisis realizado con los datos obtenidos de OWASP ZAP

De acuerdo a la Normativa que se investigó la Ley Orgánica de Donación y Trasplante de Órganos, Tejidos y Células en la Segunda Sección de la Confidencialidad establece medidas

para proteger la confidencialidad y seguridad de la información generada en el proceso de donación y trasplante.

Fase 2. Revisión bibliográfica de OWASP y la ISO/IEC 27002:2022

Se realizó la investigación de la literatura en las siguientes bases bibliográficas IEEE Digital Library, Science@Direct y Scopus y en los repositorios de la Pontificia Universidad Católica del Ecuador, Escuela Politécnica Nacional y la Universidad Técnica del Norte.

Fase 3. **Diseño, desarrollo e implementación del prototipo**

Se realizó el diseño, desarrollo e implementación del prototipo adaptando al sistema existente según los controles y buenas prácticas establecidas en la ISO/IEC 27002:2022 y Owasp, todo esto enfocado en el proceso de autentificación, todo quedó implementado en el ambiente de desarrollo.

Fase 4. Pruebas y validación

Se realizaron pruebas del funcionamiento del prototipo en el entorno de desarrollo para verificar el correcto desempeño del proceso de autenticación. Estas pruebas permitieron evaluar la estabilidad, el rendimiento y la respuesta del sistema ante diferentes escenarios de uso.

Fase 5. Evaluación y análisis de resultados

Se realizaron varias pruebas al prototipo con las siguientes herramientas:

OWASP ZAP.

Se realizó un análisis automático de vulnerabilidades en el prototipo, cuyos resultados se presentan en la Tabla 14. En este análisis, se identificaron 13 vulnerabilidades, lo que representa una reducción de una respecto al análisis anterior

Tabla 13

Vulnerabilidades halladas en el prototipo

Riesgo	Cantidad	Vulnerabilidad
Crítico (Alto)	1	Librería JavaScript Vulnerable.
Medio	3	Falta de Content Security Policy (CSP). Falta de Cabecera Anti-Clickjacking. Uso de jQuery Vulnerable
Bajo	5	Cookie sin el atributo SameSite. Divulgación de Marcas de Tiempo – Unix. El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP. Falta encabezado X-Content-Type-Options. Strict-Transport-Security Header No Establecido.
Informativo	4	Aplicación Web Moderna. Divulgación de comentarios sospechosos en código fuente. Reexaminar las directivas de Control de Caché Respuesta de Gestión de Sesión Identificada.
Total	13	

Nota. Tomado del resumen generado de OWASP ZAP

Se crearon filtros en Java para tratar de solucionar las vulnerabilidades halladas, los siguientes filtros además fueron agregados en web.xml. Y creados en una carpeta de Seguridad del Proyecto.

Tabla 14

Vulnerabilidades halladas vs filtros aplicados para mitigar

Vulnerabilidad	Riesgo	Filtro Asociado
Librería JS Vulnerable	Alto	N/A
Cabecera Content Security Policy (CSP) no configurada	Medio	CSPFilter
Falta de cabecera Anti-Clickjacking	Medio	ClickjackingFilter
Librería JS Vulnerable	Medio	N/A
Cookie Sin Flag de Seguridad	Bajo	SecureSessionCookieFilter
Cookie sin el atributo SameSite	Bajo	SecureSessionCookieFilter
Divulgación de Marcas de Tiempo - Unix	Bajo	TimestampHeaderFilter
El servidor filtra información de versión a través del campo 'Server' del encabezado de respuesta HTTP	Bajo	RemoveServerHeaderFilter
Falta encabezado X-Content-Type-Options	Bajo	N/A
Strict-Transport-Security Header No Establecido	Bajo	HSTSFilter
Aplicación Web Moderna	Informativo	N/A
Divulgación de información - Comentarios sospechosos	Informativo	RemoveCommentsFilter
Reexaminar las Directivas de Control de Caché	Informativo	N/A
Respuesta de Gestión de Sesión Identificada	Informativo	SecureSessionCookieFilter

Nota. Elaborado por el autor

A pesar de la implementación de los siguientes filtros en el web.xml del proyecto, el análisis de vulnerabilidades realizado con OWASP ZAP muestran que la mayoría de problemas continúan. Se logró mitigar la vulnerabilidad Cookie Sin Flag de Seguridad con el uso del filtro SecureSessionCookieFilter. Sería recomendable mejorar la configuración a nivel del servidor, proxy, etc.

METASPLOIT

El análisis realizado con Metasploit proporcionó los siguientes resultados, el análisis realizado a los puertos el sistema tiene accesibles los puertos 80, 443 y 8443.

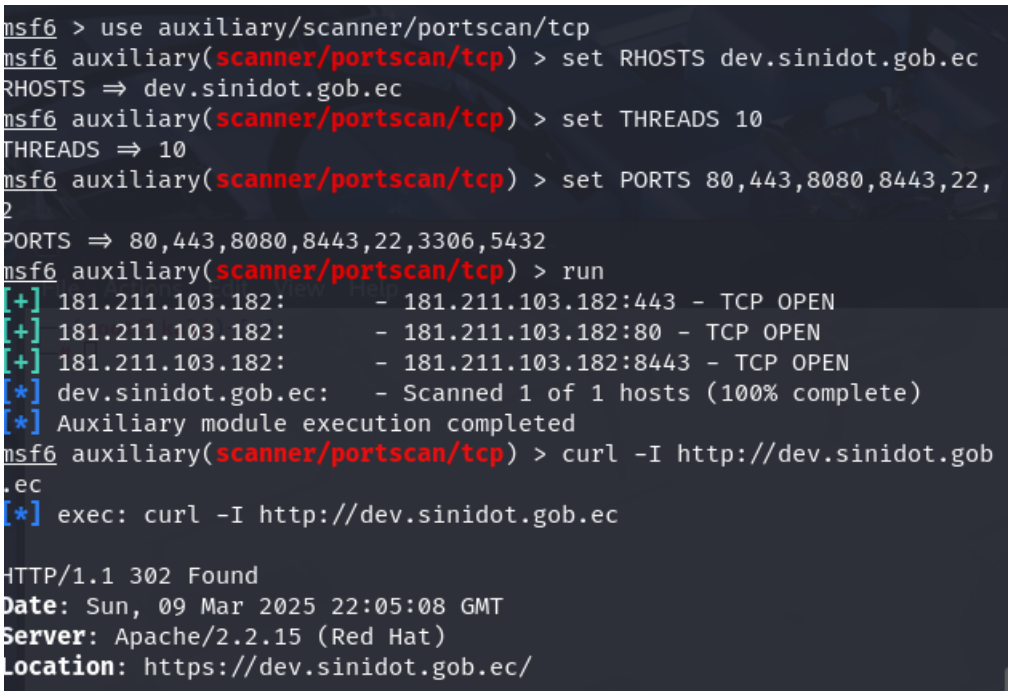
El puerto 443 indica que el servidor está usando HTTPS y en producción se utiliza certificado SSL/TLS.

El puerto 80 se está utilizando para forzar el uso HTTPS fue confirmado con el comando curl -I http://dev.sinidot.gob.ec.

El puerto 8443 está abierto porque debe estar corriendo un servicio, pero después de varias pruebas no se puedo concluir cual es el servicio por el firewall.

Figura 26

Análisis de puertos



Nota. Tomado de la consola de Metasploit

Se intento realizar un ataque de fuerza bruta al sistema y a la prueba de autentificación débil, pero no hay una ruta directa como /login, sino que el login se maneja dentro del endpoint /dispatch a través de una llamada GWT-RPC que ejecuta LoginAction. Se realizo la búsqueda de la ruta tal como muestra la Figura 23.

Figura 27

Búsqueda de rutas del login

Nota. Tomado de la consola de Metasploit

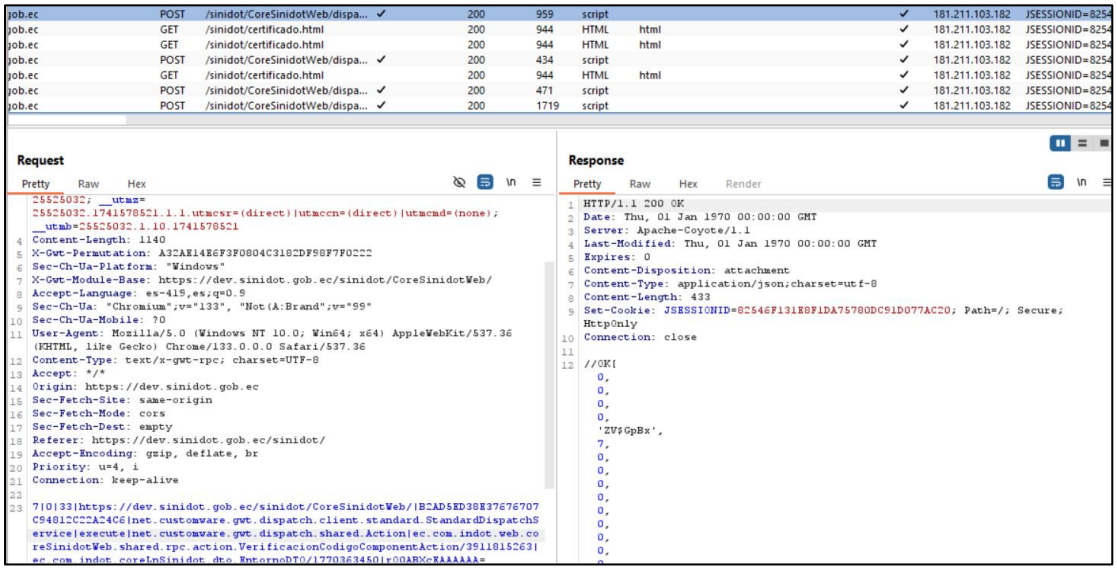
En GWT-RPC, el payload está en un formato serializado, lo que hace que sea más difícil manipularlo sin conocer su estructura exacta.

El sistema al momento cuenta con doble factor de seguridad 2FA, un ataque de fuerza bruta tradicional no servirá porque, se necesita el código 2FA, los códigos cambian cada cierto tiempo, y es complicado adivinarlos por fuerza bruta.

Al no poder realizar las pruebas con Metasploit se cambió a Burp Suite. Primero se realizó la intercepción de la sesión del sistema para realizar las pruebas tal como se muestra en la Figura 24.

Figura 28

Intercepción de sesión



Nota. Tomado de Burp Suite

A continuación, se capturó la sesión como lo muestra Figura 25. Aquí se puede observar que hay una verificación del código para realizar el ingreso al sistema.

Figura 29

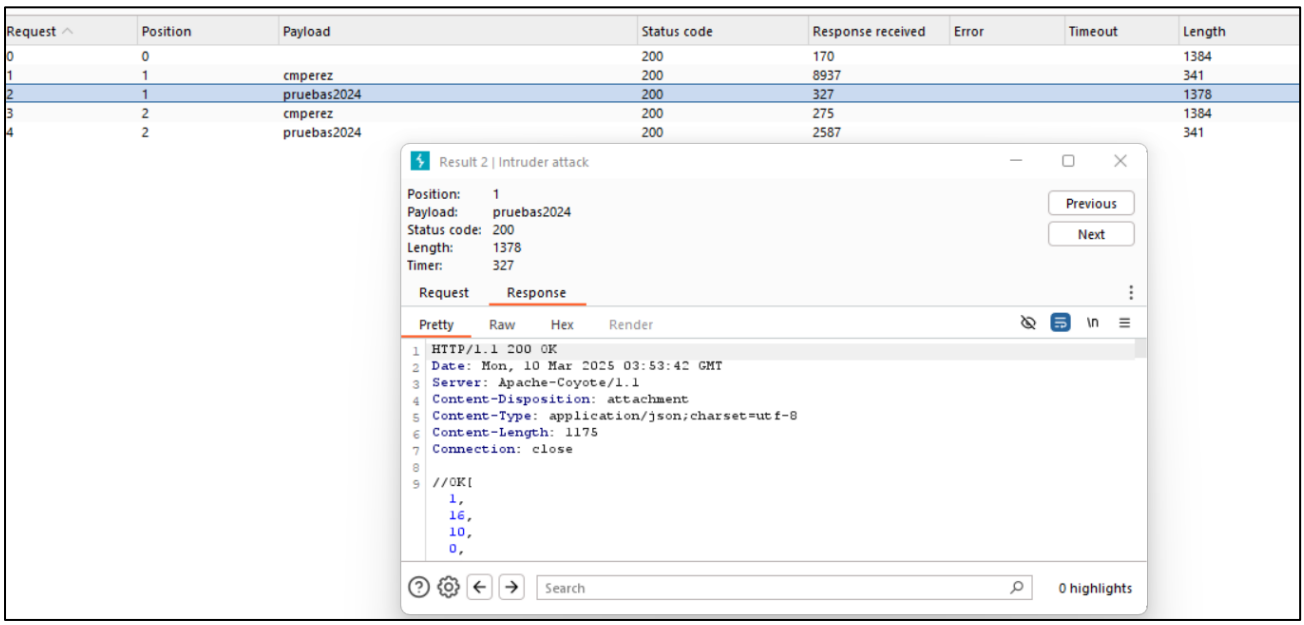
Captura de sesión

Nota. Tomado de Burp Suite

Después de realizar el ataque, se evidencia que no fue posible acceder al sistema. Se observa que, en la prueba realizada sin 2FA (*Figura X*), el tiempo de respuesta recibido es bajo. En contraste, con el sistema que tiene 2FA implementado (*Figura X*), el tiempo de respuesta es significativamente mayor, lo que indica la presencia de una validación adicional que dificulta los intentos de acceso no autorizados.

Figura 30

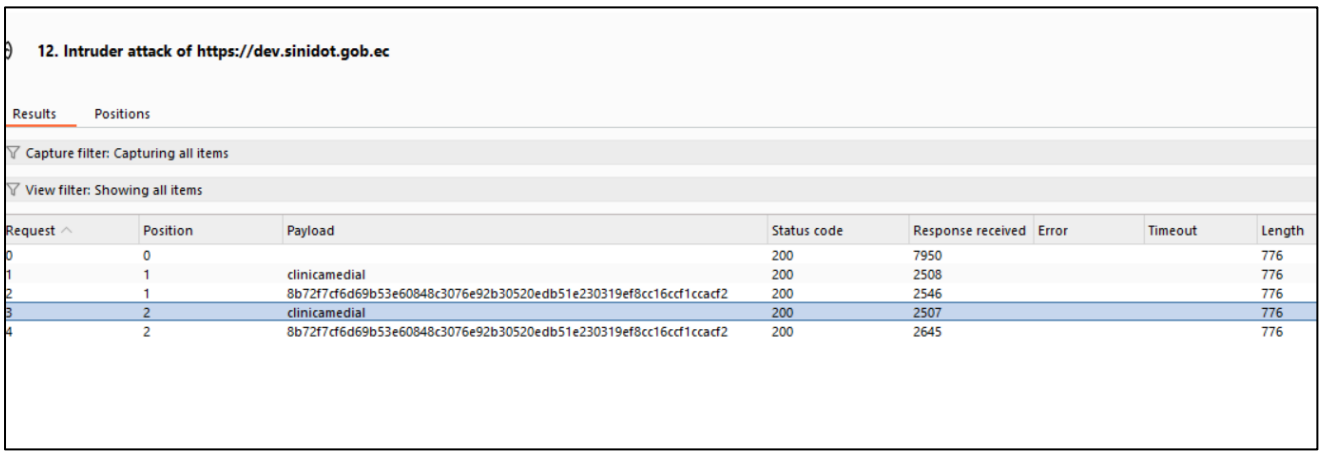
Prueba ataque sin 2FA



Nota. Tomado de Burp Suite

Figura 31

Prueba ataque con 2FA

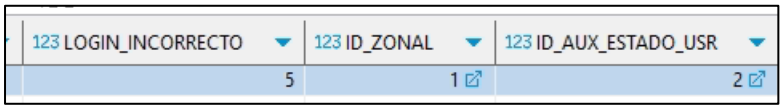


Nota. Tomado de Burp Suite

Además, se observa en la Figura 28 en el campo de la base de datos ID_AUX_ESTADO_USR = 2 que significa que el usuario este "bloqueado" tras múltiples intentos fallidos (LOGIN_INCORRECTO = 5) de ingreso de contraseña, lo que evidencia la implementación de un mecanismo de seguridad para prevenir accesos no autorizados.

Figura 32

Campos de base de datos después del ataque



Nota. Tomado de la base de datos del sistema

El análisis se realizó nuevamente con base en una verificación de la implementación de los mecanismos de autenticación del sistema, siguiendo las directrices de ISO 27002:2022 y las mejores prácticas de seguridad definidas por OWASP.

Tabla 15

Evaluación al prototipo con ISO 27002:2022

Id	Nombre	Cumple	No cumple
8.2	Derechos de acceso privilegiado	X	
8.3	Restricción de acceso a la información	X	
8.5	Autenticación segura	X	
8.15	Registro	X	
8.24	Uso de criptografía	X	
8.26	Requisitos de seguridad de la aplicación	X	

Nota. Análisis realizado con los datos obtenidos de OWASP ZAP Y BURP SUITE

Tabla 16

Evaluación al prototipo con OWASP Top 10

Nombre	ESTADO
A01:2021 – Pérdida de Control de Acceso	Seguro
A02:2021 - Fallas Criptográficas	Seguro

A04:2021 – Diseño Inseguro	Seguro
A06:2021 – Componentes Vulnerables y Desactualizados	En Riesgo
A07:2021 – Fallas de Identificación y Autenticación	Seguro
A09:2021 – Fallas en el Registro y Monitoreo	Seguro

Nota. Análisis realizado con los datos obtenidos de OWASP ZAP Y BURP SUITE

Consideraciones bioéticas

Está investigación se la realizó con los permisos por parte del Instituto de Donación y Trasplante de Órganos Tejidos y Células. La máxima autoridad emitió una autorización por escrito para llevarla a cabo el proceso de desarrollo del prototipo.

Los usuarios del sistema fueron informados sobre varios aspectos de la investigación para que puedan participar en el proceso.

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

En este capítulo se presentarán los resultados y discusión de manera detallada, ordenada durante la investigación, todo esto se desarrolló de acuerdo a la etapa de investigación y siguiendo los objetivos planeados.

4.1. Resultados

4.1.1. Encuesta dirigida a usuarios del Sistema a nivel nacional

La encuesta fue dirigida a 75 usuarios del sistema, en el cual se presentaron 9 preguntas enfocados a recolectar información sobre el uso del sistema, y la percepción de seguridad, usabilidad, conocimiento sobre el proceso de autentificación, y la estarían de acuerdo en implementar mecanismos de seguridad en el Sistema.

Para determinar cuántas personas deben ser encuestadas, se utilizó un nivel de confianza del 95% y un margen de error del 10%, aplicado a una población de 300 usuarios del sistema. Se optó por un margen de error del 10% debido a que, en encuestas anteriores, la participación ha sido baja, lo que ha limitado la capacidad de obtener respuestas representativas.

4.1.2. Aplicación de la encuesta

Pregunta 1. ¿Cuánto tiempo ha estado utilizando el sistema de donación y trasplante de órganos?

Tabla 17

Medidas de tendencia y dispersión Pregunta 1

N.	Válido	75
	Media	2,54
	Mediana	1,50
	Moda	0,50
	Desv. estándar	1,90
	Varianza	3,61

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

La media de 2.54 indica que la experiencia de los usuarios en el uso del sistema se encuentra principalmente entre 1-2 años y 3-4 años, lo que sugiere un nivel intermedio de experiencia. La mediana de 1.5 refleja que al menos la mitad de los usuarios tiene entre 1-2 años de experiencia con el sistema. La moda de 0.5 señala que el grupo más representativo es el de usuarios con menos de un año de experiencia. La desviación estándar de 1.9 sugiere una amplia diversidad en los niveles de experiencia, desde usuarios novatos con menos de un año hasta aquellos con más tiempo en el sistema. Finalmente, la varianza de 3.61 confirma que la experiencia de los usuarios está considerablemente distribuida entre diferentes niveles

Tabla 18

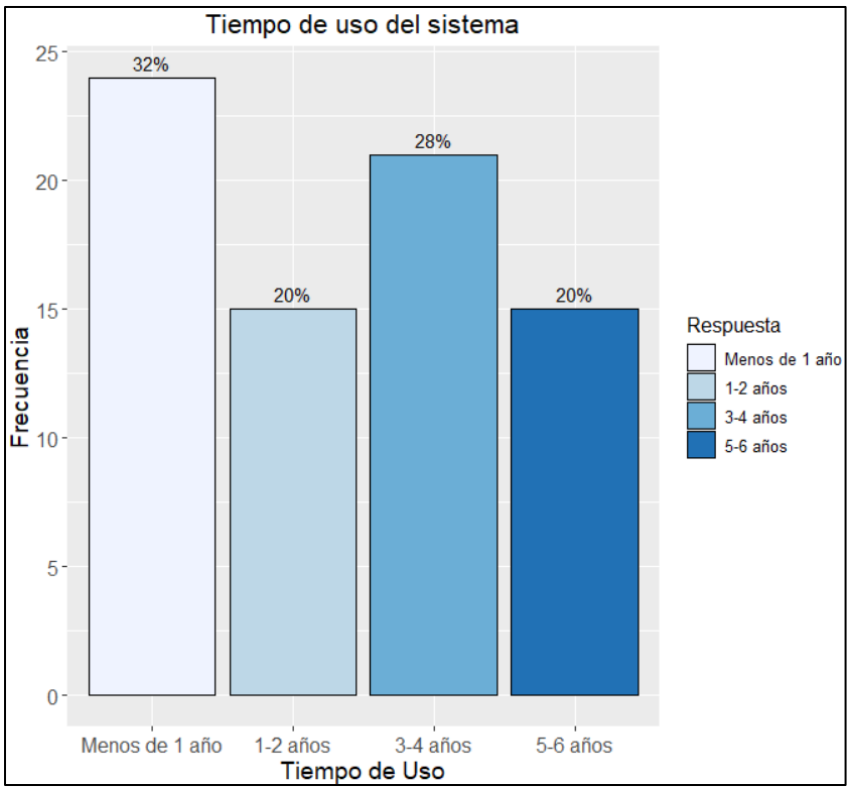
Pregunta 1. ¿Cuánto tiempo ha estado utilizando el sistema de donación y trasplante de órganos?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Menos de 1 año	24	32	32	32
	1 - 2 años	15	20	20	52
	3 - 4 años	21	28	28	80
	5 - 6 años	15	20	20	100
	Total	75	100	100	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 33

Tiempo de uso del sistema por parte de los encuestados



*Nota***:** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

Según los resultados obtenidos, los usuarios del sistema de donación y trasplante de órganos con menos de 1 año de experiencia representan un 32% del total. Por otro lado, los usuarios con 1 a 2 años de experiencia sumaron el 20%. Este grupo cuenta con un conocimiento básico del sistema. Finalmente, el 48% restante corresponde a usuarios con más de 3 años de experiencia en el sistema. Estos son los usuarios más experimentados.

En base a las respuestas obtenidas es importante implementar interfaces intuitivas y procesos simples para que faciliten la adaptación al sistema de 2FA.

Pregunta 2. ¿Qué tan fácil le resulta encontrar la información que necesita en el Sistema Nacional Informático de Donación y Trasplante?

Tabla 19

Medidas de tendencia y dispersión Pregunta 2

N.	Válido	75
	Media	2,00
	Mediana	2,00
	Moda	1,15
	Desv. estándar	1,31
	Varianza	3,61

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

Media de 2 indica o sugiere que los usuarios perciben el uso del sistema es más fácil que difícil, es decir las respuestas se acercan a la categoría de Fácil. Mediana que es el valor central de los datos, también es 2, lo que indica que la mayoría de usuarios eligieron esta categoría o una cercana. Moda de 1.15 confirma que la percepción predominante de los usuarios es que encuentran el uso del sistema encuentra es Muy fácil. Desviación estándar de 1.31 indica que, aunque la mayoría de las respuestas están cerca de Fácil existe una variabilidad moderada. Algunos usuarios perciben la tarea como más difícil. La varianza de 3.61 confirma que las respuestas están dispersas alrededor de la media, pero no de manera extrema.

Tabla 20

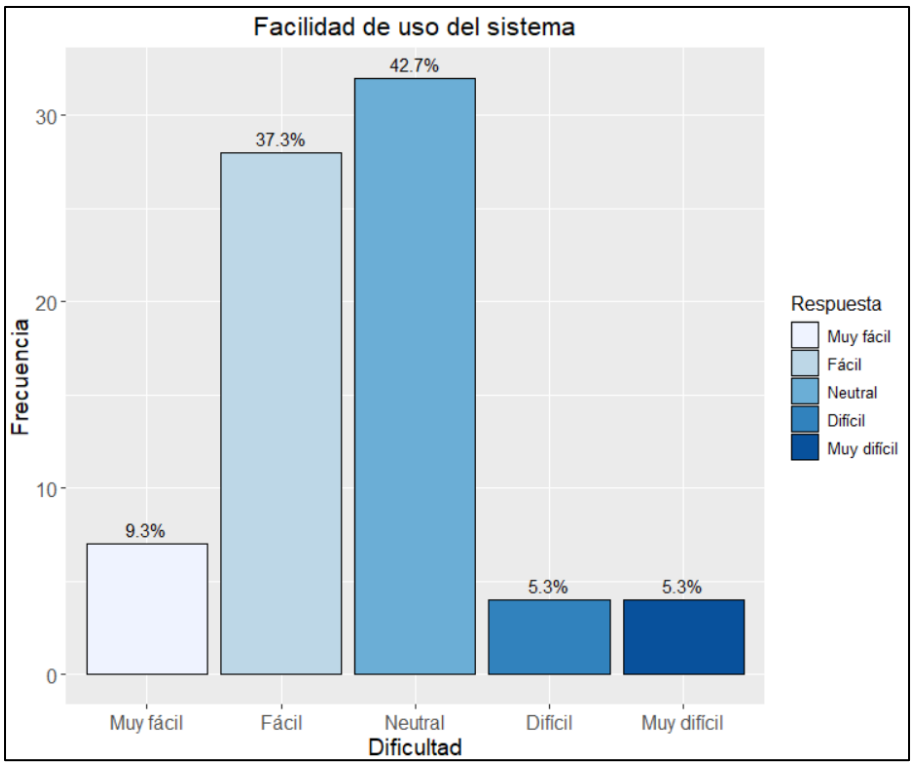
Pregunta 2. ¿Qué tan fácil le resulta encontrar la información que necesita en el Sistema Nacional Informático de Donación y Trasplante?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Muy fácil	7	9,33	9,33	9,33
	Fácil	28	37,33	37,33	46,67
	Neutral	32	42,67	42,67	89,33
	Difícil	4	5,33	5,33	94,67
	Muy difícil	4	5,33	5,33	100
	Total	75	1 00	100	

Nota. Datos obtenidos a partir de la aplicación de la encuesta

Figura 34

Facilidad de uso del sistema



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

El 42.67% de los usuarios se muestra indiferente con respecto a esta pregunta, lo que nos podría mostrar esta neutralidad que no se experimenta problemas graves o significativos, es decir el sistema cumple con las funciones básicas, pero no hay una satisfacción ni confianza destacada. Puede que este grupo se sienta insatisfecho al introducir la nueva funcionalidad de 2FA. Para lo cual sería importante mejorar la personalización y soporte al usuario y garantizar una experiencia positiva.

Pregunta 3. ¿Qué aspectos del sistema considera más difíciles de usar?

Tabla 21

Medidas de tendencia y dispersión Pregunta 3

N.	Válido	75
	Media	3,21
	Mediana	3,00

	Moda	1,00
	Desv. estándar	1,75
	Varianza	3,06

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

Media de 3.21 los usuarios encuentran dificultadas en el acceso de datos personales, el tiempo de respuesta del sistema. Mediana de 3 indica la mayoría de los usuarios consideran que los aspectos más difíciles están relacionados con el "Acceso a datos personales o resultados". Moda de 1 muestra que la dificultad más frecuentemente reportada es la "Búsqueda de información específica". Desviación estándar de 1.75 indica que hay una tendencia hacia ciertos aspectos, las experiencias de los usuarios varían y no todos enfrentan los mismos problemas. Varianza de 3.06 reafirma la diversidad en las percepciones de dificultad.

Tabla 22

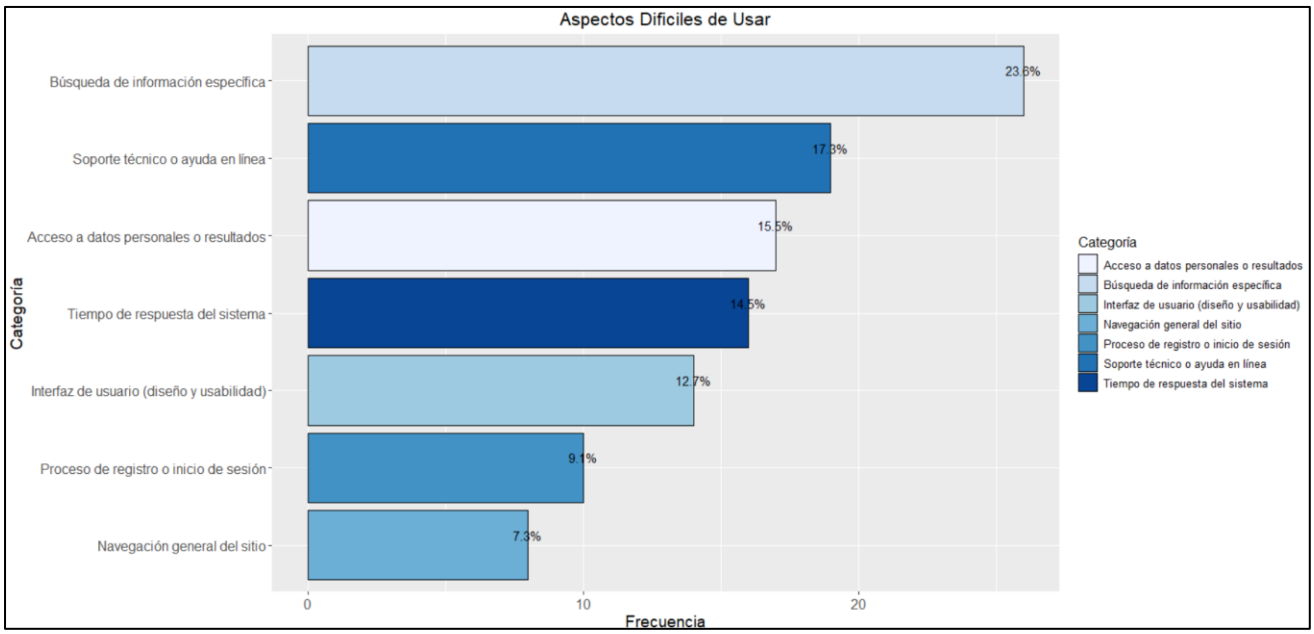
Pregunta 3. ¿Qué aspectos del sistema considera más difíciles de usar?

		Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje acumulado
Válido	Búsqueda de información específica	26	23,64	23,64	23,64
	Soporte técnico o ayuda en línea	19	17,27	17,27	40,91
	Acceso a datos personales o resultados	17	15,45	15,45	56,36
	Tiempo de respuesta del sistema	16	14,55	14,55	70,91
	Interfaz de usuario (diseño y usabilidad)	14	12,73	12,73	83,64
	Proceso de registro o inicio de sesión	10	9,09	9,09	92,73
	Navegación general del sitio	8	7,27	7,27	100,00
	Total	110	100,00	100,00	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 35

Aspectos difíciles de usar del sistema



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

El 23.64% de usuarios considera que la búsqueda de información específica es difícil, es un hallazgo importante, porque es esencial para la experiencia del usuario, especialmente en un sistema que maneja datos sensibles relacionados con la donación y trasplante de órganos.

El 17,27% de los usuarios identifica problemas en los canales de asistencia, específicamente en el soporte técnico o la ayuda en línea. Esto refleja que los usuarios encuentran dificultades para obtener ayuda de manera oportuna.

El acceso a datos personales o resultados muestra un porcentaje del 15.45% esto refleja que resulta complicado consultar información. El Tiempo de respuesta del sistema con un porcentaje de 14,55% quiere decir que la lentitud afecta la experiencia de los usuarios, lo que genera frustración con el sistema.

La navegación general del sitio tiene un 7.27% indica problemas para orientarse dentro del sistema o para moverse entre los diferentes módulos.

Las áreas deben a las cuales se debe dar prioridad es la búsqueda de información específica, el soporte técnico y el acceso a datos personales al diseñar el prototipo con 2FA.

Pregunta 4. ¿Considera usted que la información en el sistema está suficientemente protegida?

Tabla 23

Medidas de tendencia y dispersión Pregunta 4

N.	Válido	75
	Media	3,39
	Mediana	3,00
	Moda	4,00
	Desv. estándar	0,84
	Varianza	0,7

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

La media de 3.39 sugiera que la mayoría de respuestas se inclinan hacia "De acuerdo", pero también es cercano a Neutral. La mediana de 3 confirma que el valor central es Neutral, los usuarios se mantienen sin opinión marcada. La moda de 4 indica que la tendencia general es favorable o positiva siendo "De acuerdo" (4). La desviación estándar de 0.84 indica que las respuestas están cercanas al promedio, hay homogeneidad en las percepciones. Y la varianza de 0.7 la mayoría de usuarios comparten opiniones similares, no hay mayores diferencias entre sí.

Tabla 24

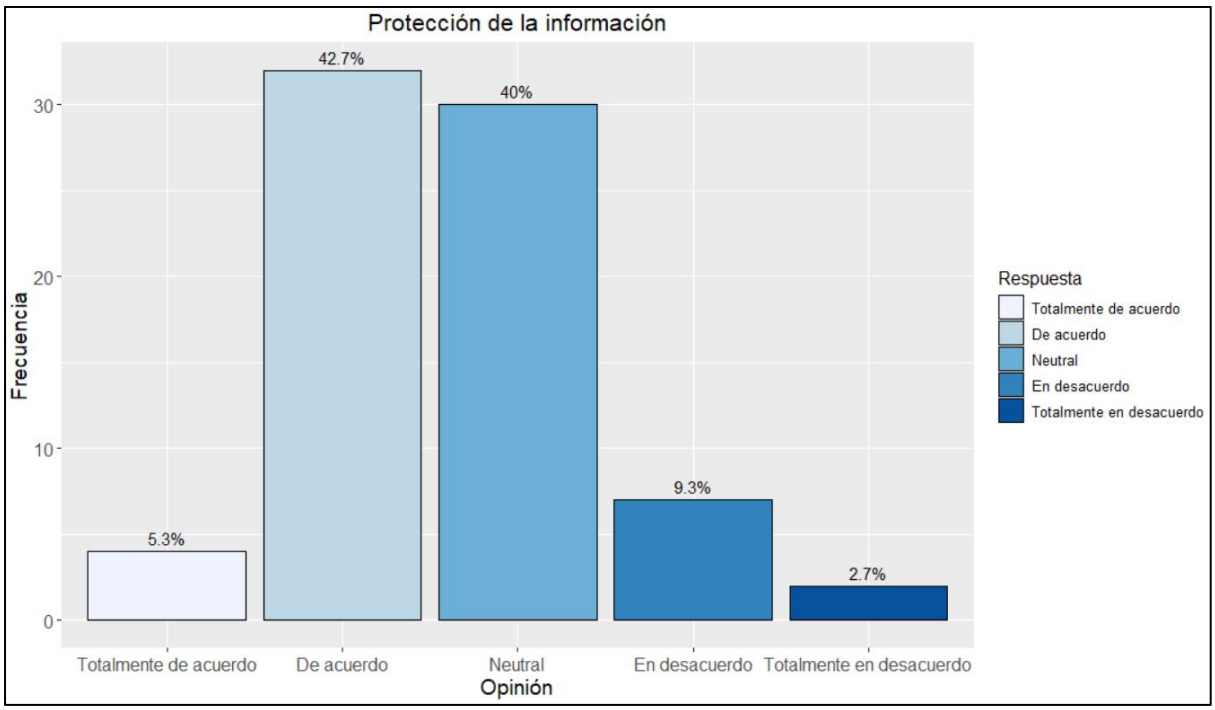
Pregunta 4. ¿Considera usted que la información en el sistema está suficientemente protegida?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Totalmente de acuerdo	4	5,33	5,33	5,33
	De acuerdo	32	42,66	42,66	48,00
	Neutral	30	40,00	40,00	88,00
	En desacuerdo	7	9,33	9,33	97,33
	Totalmente en desacuerdo	2	2,66	2,66	100,00
	Total	75	100,00	100,00	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 36

Protección de la información en el sistema



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

La mayoría de usuarios considera que la información está suficientemente protegida (Totalmente de acuerdo 5,33 % y De acuerdo 42,66 %) esto refleja que cerca de la mitad de los usuarios tienen confianza en las medidas actuales de seguridad.

Un 40% de neutralidad muestran que los usuarios no están convencidos que la seguridad sea suficiente. Un 9.33% de usuarios están en desacuerdo y 2,66% totalmente en desacuerdo es decir los usuarios no consideran que la información cuente con la suficiente protección, pueden haber experimentado problemas relacionados o percibir vulnerabilidades en el sistema.

La implementación de un método con 2FA representa una oportunidad para mejorar estas percepciones, fortaleciendo las medidas de seguridad y aumentando la transparencia y la confianza de los usuarios en el sistema.

Pregunta 5. ¿Qué tan segura considera su contraseña actual en el sistema?

Tabla 25

Medidas de tendencia y dispersión Pregunta 5

N.	Válido	75
	Media	3,63
	Mediana	4,00
	Moda	4,00
	Desv. estándar	0,90
	Varianza	0,80

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

La media de 3.63 indica que el promedio es ligeramente superior a neutral y muy cercano a segura, esto sugiere que los usuarios consideran que sus contraseñas son relativamente seguras. La mediana de 4 es segura, es decir la mitad de los usuarios perciben a sus contraseñas con seguras o muy seguras. La moda de 4 confirma lo anterior y nos muestra una tendencia clara hacia a confianza en la seguridad. La desviación estándar de 0.9 indica cierta variabilidad en las respuestas, pero no muy alta, es decir existen algunas opiniones más críticas. Y la varianza de 0.8 hay opiniones diferentes, pero no hay extremos muy pronunciados.

Tabla 26

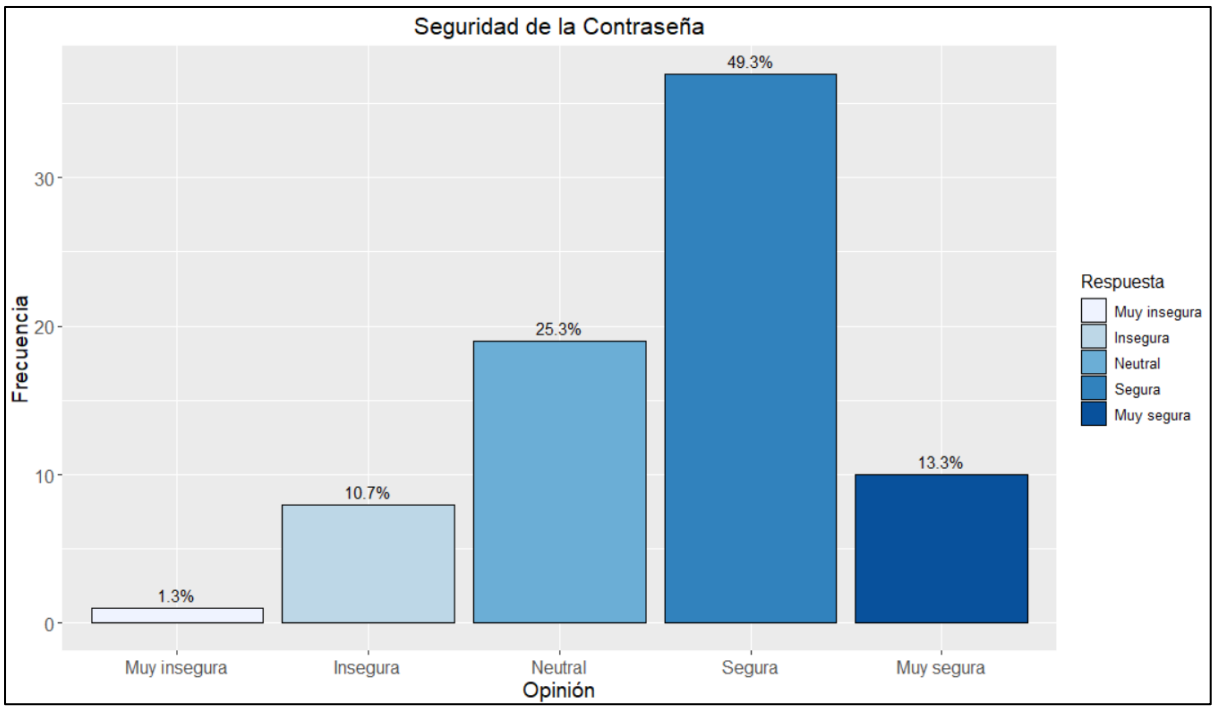
Pregunta 5. ¿Qué tan segura considera su contraseña actual en el sistema?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Muy insegura	1	1,33	5,33	1,33
	Insegura	8	10,66	42,66	12,00
	Neutral	19	25,33	40,00	37,33
	Segura	37	49,33	9,33	86,66
	Muy segura	10	13,33	2,66	100,00
	Total	75	100,00	100,00	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 37

Seguridad de la contraseña



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

La mayoría de usuarios consideran que sus contraseñas son seguras o muy seguras llegando a un porcentaje de 62.66%, pero también puede dar lugar a una falsa sensación de seguridad si las contraseñas no cumplen con ciertas normas recomendadas.

Un porcentaje significativo del 25.33% tiene una percepción neutral sobre la seguridad de las contraseñas, lo que puede reflejar incertidumbre, desconocimiento o falta de confianza en las medidas de seguridad del sistema. Y el 12% tiene una percepción negativa (Muy insegura o insegura), esto resalta la necesidad de implementar mecanismos como el 2FA para fortalecer la seguridad general.

Pregunta 6. ¿Conoce las políticas de seguridad utilizadas en el sistema para autentificación de los usuarios?

Tabla 27

Medidas de tendencia y dispersión Pregunta 6

N.	Válido	75
	Media	3,4
	Mediana	4,00
	Moda	4,00
	Desv. estándar	0,89
	Varianza	0,78

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

La media de 3.4 indican que las respuestas están ligeramente inclinadas hacia "De acuerdo". Los usuarios tienen un conocimiento sobre las políticas de seguridad. La mediana de 4 nos indica que al menos la mitad de los usuarios afirma conocer sobre políticas de usuario para la autentificación. La moda también de 4 confirma lo anterior. La desviación estándar de 0.89 indica cierta dispersión en las respuestas. Y la varianza de 0.89 las respuestas están agrupadas en torno a la media y no hay extremos pronunciados.

Tabla 28

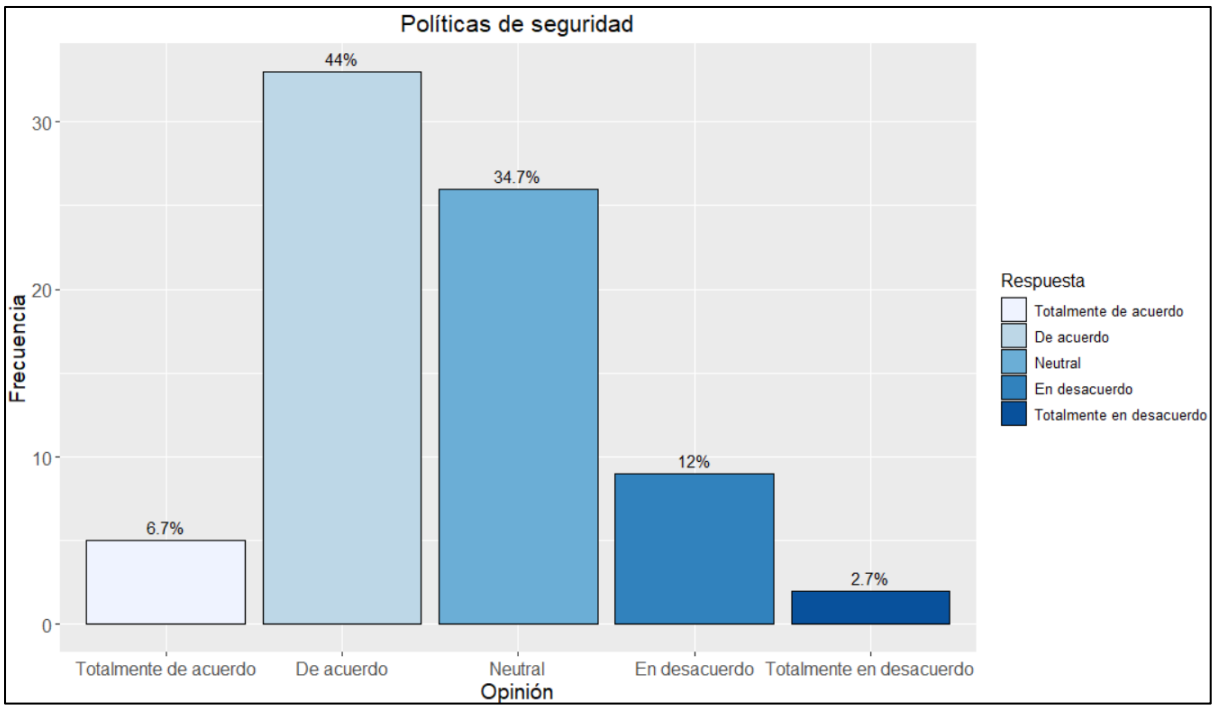
Pregunta 6. ¿Conoce las políticas de seguridad utilizadas en el sistema para autentificación de los usuarios?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Totalmente de acuerdo	5	6,66	6,66	6,66
	De acuerdo	33	44,00	44,00	50,66
	Neutral	26	34,66	34,66	85,33
	En desacuerdo	9	12,00	12,00	97,33
	Totalmente en desacuerdo	2	2,66	2,66	100,00
	Total	75	100,00	100,00	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 38

Política de seguridad



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

El 44% de usuarios afirma conocer las políticas de seguridad, el 34.66 % de los usuarios refleja de falta de claridad o desconocimiento parcial sobre las políticas de seguridad, en la percepción negativa tenemos el 14.66% de usuarios que no tienen conocimiento o no ningún conocimiento de las políticas de seguridad.

Esto evidencia la necesidad de mejorar la comunicación y la educación sobre las medidas de seguridad, especialmente al implementar el método de 2FA, fortalecerá la confianza y satisfacción de los usuarios, y garantizará que todos comprendan y valoren las medidas de seguridad del sistema.

Pregunta 7. ¿Estaría dispuesto a cambiar su contraseña con regularidad en el sistema, siguiendo las pautas de seguridad recomendadas?

Tabla 29

Medidas de tendencia y dispersión Pregunta 7

N.	Válido	75
	Media	3,25
	Mediana	3,00
	Moda	4,00
	Desv. estándar	1,25
	Varianza	1,57

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

La mediana de 3.25 cercana a Neutral y ligeramente inclinada a De acuerdo indica que los usuarios tienen una disposición moderada a cambiar las contraseñas regularmente, pero no todos están convencidos. La mediana de 3 indica que las respuestas mantienen la posición neutral. La moda de 4 De acuerdo indica que hay aceptación de cambiar las contraseñas. La desviación estándar de 1.25 sugiere que las opiniones están divididas, con una notable presencia de valores altos y bajos. La varianza de 1.57 hay dispersión en las percepciones.

Tabla 30

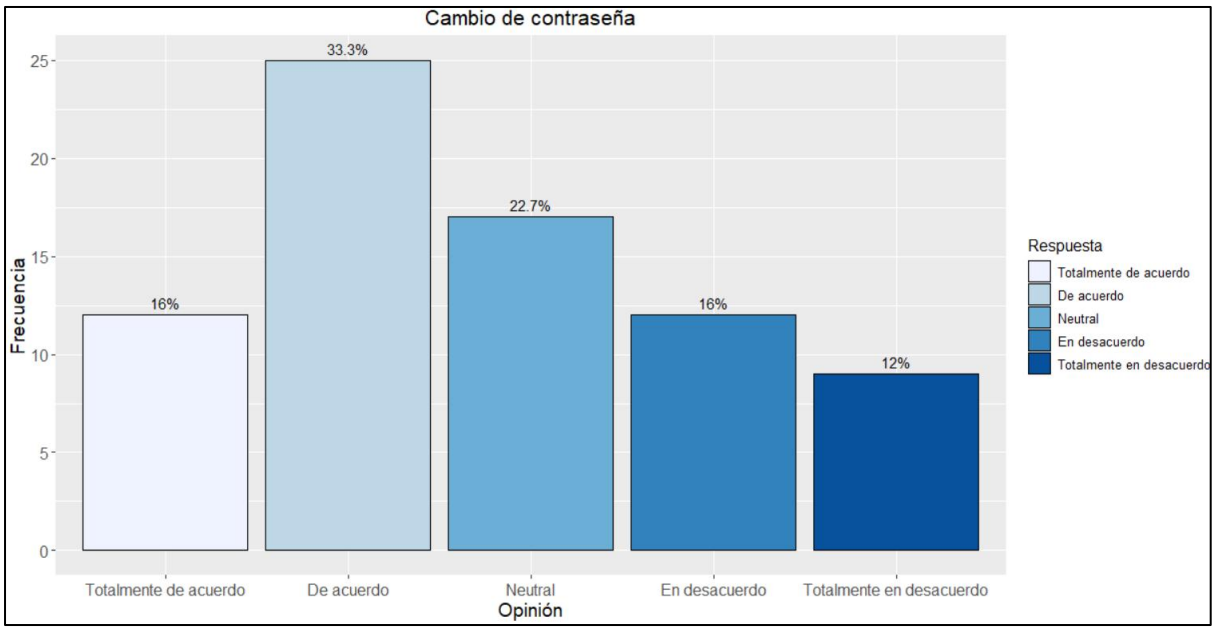
Pregunta 7. ¿Estaría dispuesto a cambiar su contraseña con regularidad en el sistema, siguiendo las pautas de seguridad recomendadas?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Totalmente de acuerdo	12	16,00	16,00	16,00
	De acuerdo	25	33,33	33,33	49,33
	Neutral	17	22,66	22,66	72,00
	En desacuerdo	12	16,00	16,00	88,00
	Totalmente en desacuerdo	9	12,00	12,00	100,00
	Total	75	100,00	100,00	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 39

Cambio de contraseña



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

Según los datos obtenidos el 49.33% de usuarios están dispuestos a cambiar sus contraseñas regularmente, este resultado nos indica que los usuarios están dispuestos a seguir pautas de seguridad, lo que facilita la implementación de políticas de cambio regular de las contraseñas. El 22.66% muestra una tendencia neutral puede representar una oportunidad para educar a los usuarios sobre los beneficios de está práctica y su relación con la protección de datos.

El resto muestra una resistencia al cambio el 28% de usuarios (En desacuerdo y Totalmente en desacuerdo), no están dispuestos a cambiar regularmente la contraseña, lo que nos indica que el proceso debe ser simple y se debe demostrar el impacto positivo en la seguridad.

Pregunta 8. ¿Estaría dispuesto a agregar una capa adicional de seguridad a su cuenta, como un código o una medida de protección adicional, si estuviera disponible?

Tabla 31

Medidas de tendencia y dispersión Pregunta 8

N.	Válido	75
	Media	3,6
	Mediana	4
	Moda	4
	Desv. estándar	1,17
	Varianza	1,38

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

La media de 3.6 es cercana a De acuerdo hay una disposición para aumentar una capa adicional de seguridad. La mediana de 4 los usuarios están de acuerdo o totalmente de acuerdo con la capa de seguridad adicional. La moda de 4 refuerza lo anterior. La desviación estándar de 1.17 las opiniones están algo dispersas entre totalmente de acuerdo y totalmente en desacuerdo. La varianza 1.38 indica que hay diversas opiniones, las respuestas no están distribuidas de manera uniforme.

Tabla 32

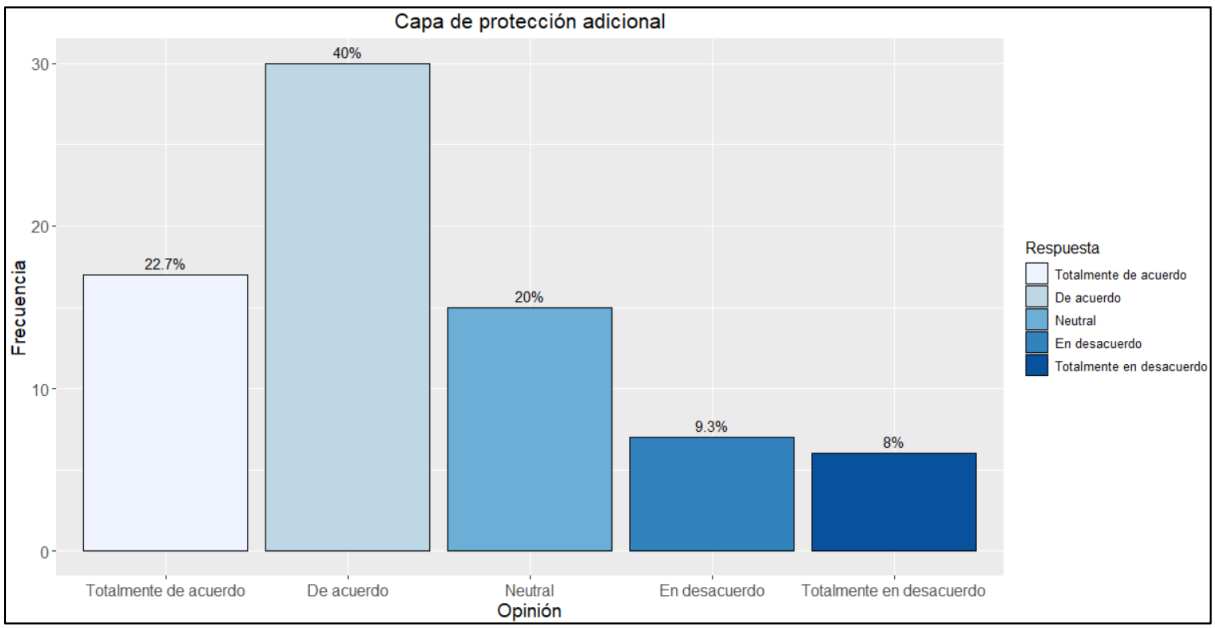
Pregunta 8. ¿Estaría dispuesto a agregar una capa adicional de seguridad a su cuenta, como un código o una medida de protección adicional, si estuviera disponible?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Totalmente de acuerdo	17	22,66	22,66	22,66
	De acuerdo	30	40,00	40,00	62,66
	Neutral	15	20,00	20,00	82,66
	En desacuerdo	7	9,33	9,33	92,00
	Totalmente en desacuerdo	6	8,00	8,00	100,00
	Total	75	100,00	100,00	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 40

Capa de protección adicional



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

El 62.66% de usuarios tienen una disposición positiva (Totalmente de acuerdo + De acuerdo) están dispuesto a agregar una capa adicional de seguridad, esto refleja una aceptación hacia la implementación de un método de 2FA especialmente si se comunica de forma clara.

El 20% de usuarios tiene una percepción neutral y el 17.33% muestran una resistencia al cambio lo que podría indicar un rechazo a la implementación de medidas adicional, pero también podría ser una oportunidad para educar sobre los beneficios de darle seguridad extra al sistema con una comunicación efectiva.

Pregunta 9. ¿Ha experimentado o conocido algún incidente de seguridad relacionado con el sistema?

Tabla 33

Medidas de tendencia y dispersión Pregunta 9

N.	Válido	75
	Media	1,51
	Mediana	1,00

	Moda	1,00
	Desv. estándar	0,88
	Varianza	0,77

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Análisis e interpretación de resultados de las medidas de tendencia y dispersión

La media de 1.51 cercana al valor nunca indica que la mayoría de encuestados ha experimentado o conocido incidentes de seguridad con el sistema. La mediana confirma lo anterior. La moda refuerza la percepción sobre los incidentes de seguridad. La desviación estándar de 0.88 las respuestas están algo dispersas, las opiniones tienen un conceso notable, aunque hay experiencias aisladas. La varianza de 0.77 hay homogeneidad en las respuestas.

Tabla 34

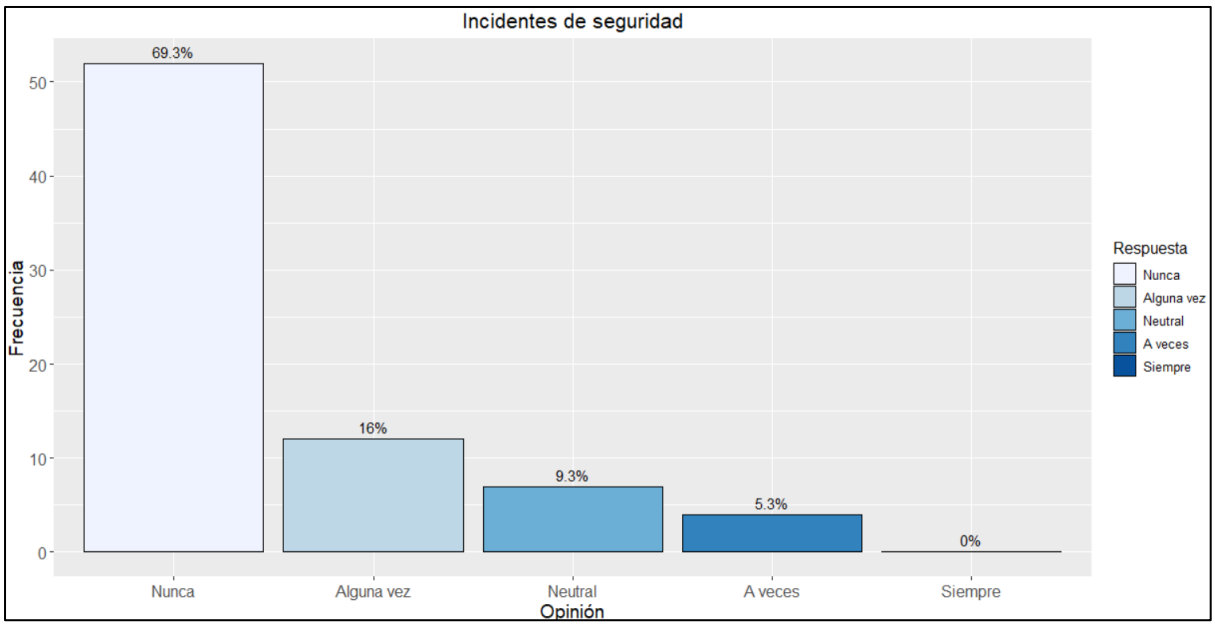
Pregunta 9. ¿Ha experimentado o conocido algún incidente de seguridad relacionado con el sistema?

		Frecuencia	**Porcentaje**	**Porcentaje Válido**	**Porcentaje acumulado**
Válido	Nunca	52	69,33	69,33	69,33
	Alguna vez	12	16,00	16,00	85,33
	Neutral	7	9,33	9,33	94,66
	A veces	4	5,33	5,33	100,00
	Siempre	0	0,00	0,00	100,00
	Total	75	100,00	100,00	

Nota: Datos obtenidos a partir de la aplicación de la encuesta

Figura 41

Incidentes de seguridad



*Nota***.** Elaborado por el autor utilizando la herramienta R con datos de la encuesta

Análisis e interpretación de resultados

Sobre la base de los resultados presentados, la mayoría de los usuarios 69.33% no ha tenido incidentes de seguridad que reportar, indicando una impresión general de fiabilidad de todo el sistema. A pesar de que el 21.33% (Alguna vez y A veces) han experimentado incidentes relacionados con seguridad, lo que sugiere la necesidad de fortalecer las medidas preventivas y educar a los usuarios educar a los usuarios sobre cómo proteger sus cuentas y el 9.33% tiene una tendencia neutral, esto refleja falta de conocimiento respecto a los incidentes de seguridad.

La implementación de un método 2FA da la oportunidad de responder a estas preocupaciones de manera eficaz, proporcionando protección adicional y asi mejorar la percepción de seguridad entre los usuarios del sistema.

4.2. Discusión

El desarrollo del prototipo web con mecanismos de autentificación de doble factor (2FA) para fortalecer la protección de datos en el proceso de donación y trasplante de órganos, representa un avance importante en la seguridad de la información médica. Este se encuentra en el ambiente de desarrollo, el cual permite analizar las fortalezas, limitaciones antes del paso al ambiente de calidad y por último al ambiente de producción.

Al realizar las encuestas se evidencio que los usuarios del Sistema creen que la seguridad es insuficiente o poco confiable, porque más del 40% cree que la información no está suficientemente protegida o tiene una posición neutral. El sistema al no tener un mecanismo de doble factor de seguridad 2FA tiene mayor riesgo de sufrir ataques, accesos no autorizados, etc.

Con el uso de solo contraseñas para el ingreso al sistema, se identificó la falta de políticas para la gestión de contraseñas como por ejemplo falta de caducidad periódica de contraseña, aunque un porcentaje de usuarios encuestados creía que sus contraseñas son seguras esto representaba un riesgo. Razón por la cual fue importante implementar una capa de seguridad adicional para mitigar los riesgos que derivan de esta.

Durante el análisis del sistema, se identificaron varias vulnerabilidades, entre las más importantes tenemos: falta de autentificación segura, uso de criptografía MD5, componentes vulnerables y desactualizados, diseño inseguro, fallas en el registro y monitoreo, no se realizaban pruebas de penetración y escaneos con las herramientas de seguridad.

Para el desarrollo el prototipo se utilizaron las mejores prácticas recomendadas por OWASP y la norma ISO/IEC 27002:2022, para mejora la autentificación y manejo de credenciales.

Se implemento el 2FA con un sistema de contraseña de un solo uso (OTP), se genero la administración de usuarios para activar o desactivar la opción 2FA, para usuarios con nivel

bajo de conocimientos técnicos. Se realizó el fortalecimiento para la gestión de contraseñas, generando una política de caducidad periódica de contraseñas con el almacenamiento del historial de contraseñas para evitar la reutilización de credenciales. Actualización del Hashing de contraseñas de MD5 a SHA256, se implementaron filtros para mitigar las vulnerabilidades encontradas al realizar el escaneo del sistema.

Al realizar las pruebas iniciales del prototipo se ha generado por parte de algunos usuarios con nivel bajo de conocimientos técnicos o falta de experiencia en herramientas digitales, confusión, a pesar que se tomó en consideración para el desarrollo la seguridad y la usabilidad. Por lo que es recomendable para el paso a producción realizar capacitaciones para los usuarios.

En las encuestar realizadas más del 80% de los usuarios estaba dispuesto a utilizar una capa adicional de seguridad para proteger su cuenta y la información del proceso de donación y trasplante de órganos, es decir la implementación del 2FA será bien recibida siempre que la experiencia del usuario se buena.

Finalmente, el prototipo ha sido desarrollo y se han realizado pruebas de seguridad, para el paso a producción será importante una fase de evaluación y monitoreo continuo. Y si es posible pruebas adicionales para asegurarse que no haya problemas técnicos que limiten el acceso al sistema.

4.3. CONCLUSIONES

De acuerdo a los resultados obtenidos se presentan las siguientes conclusiones:

Durante el análisis del sistema se encontraron varias vulnerabilidades que comprometían la seguridad de la información del proceso de donación y trasplante de órganos. Los problemas encontrados tomando en cuenta OWASP Top 2021 y la norma ISO/IEC

27002:2022 fueron falta de autentificación segura no existe un mecanismo de 2FA o multifactor, no existe funcionalidad parar recuperar la contraseñas, uso de criptografía MD5 es decir fallas criptográficas, componentes vulnerables y desactualizados, diseño inseguro, fallas en el registro y monitoreo, no se realizaban pruebas de penetración y escaneos con las herramientas de seguridad, se tomaron en cuenta los relacionados con los problemas de autentificación.

Por lo antes expuesto fue necesario el desarrollo e implementación de un mecanismo de autentificación de 2FA con OTP, conjuntamente con el fortalecimiento de credenciales, mecanismos de recuperación de contraseñas, se realizó la actualización del almacenamiento de contraseñas de MD5 a SHA256, por la limitante de la base de datos no fue posible migrar a una superior ya que no es soportado por Oracle 11g. Con el uso de componentes vulnerables y desactualizados lamentablemente no se logró realizar actualizaciones de herramientas que usa el sistema. Al igual que se integraron filtros para mitigar las vulnerabilidades halladas en el análisis realizado con OWAS ZAP, pero estos no funcionaron o hicieron que el sistema deje de funcionar correctamente. El único filtro que funciono y elimino la vulnerabilidad fue el SecureSessionCookieFilter que sirve para la vulnerabilidad Cookie Sin Flag de seguridad la cual deja expuesto al sistema a queda robo de sesión, ataques XSS y CSRF. Todas estas prácticas fueron tomadas de acuerdo a las mejores prácticas de OWASP Top 2021 y la norma ISO/IEC 27002:2022.

Con la implementación de lo antes mencionado se presenta una solución efectiva para mitigar los riesgos encontrados, no todos, pero si en su mayoría, estos nos ayudan a proteger la información sensible del proceso de donación y trasplante de órganos, de ataques de fuerza bruta, phishing, reutilización de contraseñas, etc. Y garantizar que el sistema cumpla con los estándares internacionales en autentificación y gestión de accesos.

El prototipo fue desarrollado de modo que su uso sea fácil e intuitivo, pero siempre se existe resistencia por parte de los usuarios con poca experiencia en el uso de herramientas digitales.

Las pruebas realizadas al prototipo han demostrado que se reduce significativamente los riesgos de accesos no autorizados, esto confirma que el desarrollo y la implementación de los mecanismos de seguridad fortalecen la seguridad del sistema. Y las otras prácticas implementadas dificultando la reversión de hashes y la recuperación de contraseñas por parte de atacantes. No se pudo realizar pruebas con Metasploit para ataque de fuerza bruta pero el sistema no usa una ruta directa al login ya que usa Dispatch a través de una llamada a GWT-RPC que se ejecuta en LoginAction, pero si se logró realizar las pruebas con Burp suite, evidenciando que el ataque de fuerza bruta no fue posible, claro que no significa que sea imposible realizar este tipo de ataque.

El prototipo debe pasar por pruebas con usuarios reales del sistema, para verificar la facilidad de uso y la experiencia del usuario. Pero, el éxito del prototipo no solo dependerá de los mecanismos implementados en el prototipo, sino también de la capacitación que se brinde a los usuarios.

4.4. Recomendaciones

Realizar capacitaciones para los usuarios sobre la importancia de la autenticación de doble factor, explicando su función y beneficios. Además, enseñarles cómo configurar y utilizar códigos OTP de manera efectiva, junto con otros mecanismos de seguridad implementados, para fortalecer la protección de sus cuentas.

Dado que los filtros de seguridad implementados dentro de la aplicación no funcionaron correctamente, sería recomendable configurarlos a nivel del servidor proxy. Esto permitiría aplicar medidas de seguridad más robustas, como filtrado de tráfico malicioso, control de

accesos y mitigación de ataques, antes de que las solicitudes lleguen a la aplicación, mejorando así la protección del sistema.

Realizar pruebas y monitoreo de los mecanismos implementados, para asegurar que los usuarios puedan autentificarse si problemas, asegurando un acceso seguro y sin fallos en el proceso.

Realizar un análisis de las herramientas utilizadas para identificar posibles actualizaciones, considerando vulnerabilidades de seguridad y falta de soporte. Evaluar si existen versiones más recientes o alternativas que mejoren el rendimiento, la compatibilidad y la protección del sistema.

REFERENCIAS

Amazon Web Services, I. (2023). *AWS*. Obtenido de https://aws.amazon.com/es/what-is/web-application/?nc1=h_ls

Brian, D. (2014). *Kaspersky dialy*. Obtenido de https://latam.kaspersky.com/blog/que-es-la-autenticacion-de-dos-factores-y-donde-debo-utilizarla/3270/

Calderón Arateco, L. L. (10 de Septiembre de 2015). Seguridad informática y seguridad de la información. *Universidad Piloto de Colombia*, 7. Obtenido de http://polux.unipiloto.edu.co:8080/00002658.pdf

Calle, L. A. (Abril de 2016). *Metodologías para hacer la revisión de literatura de una investigación.* Obtenido de https://www.researchgate.net/publication/301748735_Metodologias_para_hacer_la_revision_de_literatura_de_una_investigacion

Cárdenas , R. D. (21 de 12 de 2020). *Gestión Tecnológica Y Buenas Prácticas En Cooporecal : Buenas Prácticas Ti En Cobit5, Itil E Iso 27000.* Obtenido de http://dspace.utb.edu.ec/bitstream/handle/49000/14027/E-UTB-FAFI-SIST-000434.pdf?sequence=1&isAllowed=y

Castillo Medina, C. A. (2021). Ciberseguridad: Por dónde Empezar…. *Revista de Tecnología*, 12.

Cervera García, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud. *Atención Primaria*. doi:10.1016/j.aprim.2023.102854

Claudia, S. (06 de 2006). *Info CITEL.* Obtenido de https://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp

Computerworld. (27 de diciembre de 2022). Obtenido de https://computerworldmexico.com.mx/autenticacion-en-dos-pasos-clave-para-evitar-el-robo-de-cuentas/

Constitución de la República del Ecuador . (2008). Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Coronel Suárez, I. A., & Quirumbay Yagual, D. I. (Diciembre de 2022). *Revista Científica y Tecnológica UPSE (RCTU).* Obtenido de http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-76972022000100097&lng=en&nrm=iso

De La Cruz Rodríguez, G., Méndez Fernández, R., & Méndez Fernández, A. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática. *Revista Innovación y Software*.

Deitel, P., Deitel , H., & Deitel, A. (2014). *Internet y World Wide Web Cómo Programar.* 5ª Edición Pearson Universidad.

Devendra, U., & Nilesh, W. (2023). Evolving Trends in Web Application Vulnerabilities: A Comparative Study of OWASP Top 10 2017 and OWASP Top 10 2021. *International*

Journal of Engineering Technology and Management Sciences. doi:10.46647/ijetms.2023.v07i06.038

Firma Electrónica Ecuador. (s.f.). Obtenido de https://www.firmadigital.gob.ec/que-es-firmaec/#1507128122386-4d037c85-18d8

Frano, C. (21 de marzo de 2022). *Globar Trust Association*. Obtenido de https://globaltrustassociation.org/es/sabes-cuales-son-las-mejoras-de-la-nueva-iso-270022022/

Fredj, O. B., Cheikhrouhou, O., Krichen, M., Hamam, H., & Derhab, A. (2021). An OWASP top ten driven survey on web application protection methods. En *Lecture Notes in Computer Science* (págs. 235-252). Springer International Publishing. doi:https://doi.org/10.1007/978-3-030-68887-5_14

Gamboa, S. D. (2021). Vulnerabilidades en Aplicaciones Web Utilizando La Metodología De "Proyecto Abierto De Seguridad De Aplicaciones Web". *Vulnerabilidades en Aplicaciones Web Utilizando La Metodología De "Proyecto Abierto De Seguridad De Aplicaciones Web".* Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato. Obtenido de https://repositorio.puce.edu.ec/items/24d14d61-c7c5-4956-8fa1-e938b79df38c

Garre Gui, S. (s.f.). *Introducción a la seguridad de la información*. Obtenido de https://openaccess.uoc.edu/bitstream/10609/142807/1/M%C3%B3dulo%201_Introducci%C3%B3n%20a%20la%20seguridad%20de%20la%20informaci%C3%B3n.pdf

Gómez López, J., Guillén Núñez, P., & De Castro Simón, M. (2014). *Hackers: Aprende a atacar y defenderte.* RA-MA S.A. Editorial y Publicaciones.

Google. (2025). *Google Maps*. Obtenido de Google Maps: https://www.google.com/maps/?hl=es

Google Sites. (s.f.). *Confidencialidad de los datos*. Obtenido de https://sites.google.com/site/seguridadinformaticaeeso213/conceptos-utiles/confidencialidad-de-los-datos

Goris, G., & Adolf, S. (Enero de 2015). *Utilidad y tipos de revisión de literatura.* Obtenido de https://doi.org/10.4321/S1988-348X2015000200002

Gupta, S., Buriro, A., & Bruno, C. (2018). Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access. *Sistemas de información móvil*, 16. Obtenido de https://www.hindawi.com/journals/misy/2018/2649598/

INDOT. (s.f.). *Instituto Nacional de Donación y Trasplante de Órganos.* Obtenido de Instituto Nacional de Donación y Trasplante de Órganos: http://www.donaciontrasplante.gob.ec/indot/wp-content/uploads/2016/03/Manual-Usuarios-Internos-V1.pdf

ISO/IEC. (02 de 2022). *ISO/IEC 27002:2022.*

Jason, A. (2011). *The basics of Information Security Understanding the Fundamentals of InfoSec in Theory and Practice.* Elsevier Inc.

Javier, A. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* España: Cengage Learning Paraninfo, S.A.

Leudis, S. (s.f.). *Seguridad en desarrollo del Software.* Obtenido de https://drive.google.com/file/d/1ZTnDhKyVf818n94ZmmkKFbO1ZT3nDKOu/view

Ley Orgánica de Donación y Trasplante de Órganos, Tejidos y Células. (04 de Marzo de 2011). Obtenido de http://www.donaciontrasplante.gob.ec/indot/wp-content/uploads/downloads/2013/11/ley_y_reglamento_a_la_ley_organica_de_donacion_y_trasplantes.pdf

Ley Orgánica de Protección de Datos Personales. (26 de Mayo de 2021). Obtenido de Ley Orgánica de Protección de Datos Personales: http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoicm8iLCJ1dWlkIjoiOTE1ZTIyMDQtY2Q1Zi00ZGMzLWFkYTAtNDE1OTRkNjgyNTEwLnBkZiJ9

López, P. A. (2010). *Seguridad informática.* Editex.

MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2012). Madrid: Ministerio de Hacienda y Administraciones Públicas.

Markert, P., Farke, F., & Dürmuth, M. (2019). View The Email to Get Hacked: Attacking SMS-Based Two-Factor Authentication. Obtenido de https://wayworkshop.org/2019/papers/way2019-markert.pdf

Mila, L. (noviembre de 2012). *Principios de la Seguridad Informática.* Obtenido de https://drive.google.com/file/d/1a0vrkc0GMh6MfhWA83jWm3foRX-0v8dg/view

Murat, A., Çig˘dem, A., Evren, C., & Alperen, S. (2021). Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University - Computer and Information Sciences*, 18.

Naciones Unidas. (2018). *La Agenda 2030 y los Objetivos de Desarrollo Sostenible Una oportunidad para América Latina y el Caribe.*

Navarro, M. (Diciembre de 2017). *Guía del PMBOK para la gestión de pruebas de intrusión a aplicaciones web. PMBOK guide for web application penetration testing management.* Obtenido de https://www.researchgate.net/publication/342545006_Guia_del_PMBOK_para_la_gestion_de_pruebas_de_intrusion_a_aplicaciones_web_PMBOK_guide_for_web_application_penetration_testing_management

OWASP Top 10 team. (2021). *OWASP Top 10* . Obtenido de OWASP Top 10: https://owasp.org/Top10/en/

Pant, P., Singh Rajawat, A., Goyal, S., Pradeep , B., Chaman , V., Raboaca, M., & Enescu, F. (2022). Authentication and Authorization in Modern Web Apps for Data Security Using Nodejs and Role of Dark Web. *4th International Conference on Innovative Data Communication Technology and Application*, 10.

Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods:A Comprehensive Survey. *Computer Science and Robotics*. doi:https://www.intechopen.com/journals/1/articles/100

Positive Technologies. (2019). *Vulnerabilidades y Amenazas en Aplicaciones Web*. Obtenido de https://www.itdigitalsecurity.es/vulnerabilidades/2020/02/el-82-de-las-vulnerabilidades-de-las-aplicaciones-web-estan-en-el-codigo-fuente

Romaniz, S. (2008). Seguridad de aplicaciones web:vulnerabilidades en los controles de acceso. *Seguridad de aplicaciones web:vulnerabilidades en los controles de acceso.* Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/21581/1927+-+Seguridad+de+aplicaciones+web+vulnerabilidades+en+los+controles+de+acceso.pdf?sequence=1

Romero Castro, M. I., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., . . . Castillo Merino, M. (2018). *Introducción a la Seguridad Informática y el Análisis de vulnerabilidades.* Editorial Área de Innovación y Desarrollo,S.L.

Ropero, E. (27 de abril de 2015). *Arquitectura de Capas.* Obtenido de https://es.slideshare.net/eropero1/programacin-i-2-arquitectura-de-capas

Sastoque Hernández, S., Mancilla, D., Narvaez, C., & Iregui, M. (14 de Enero de 2015). Caso de estudio para validar la representación del conocimiento en aplicaciones web centradas en el usuario por medio de contenido multimedia enriquecido. *VIII Encuentro de Investigaciones UMNG.*

Secretaría Nacional de Planificación. (2021). *Plan de Creación de Oportunidades 2021-2025.* Quito.

Seguridad y Etica. (16 de septiembre de 2013). Obtenido de https://seguridadetica.wordpress.com/2013/09/16/seguridad-informatica-o-seguridad-de-la-informacion/

UTN. (2023). *UTN*. Obtenido de UTN: https://www.utn.edu.ec/

Vasquez, J. D. (2023). ISO/IEC 27000. *High Tech- Engineering Journal*, 81.

Werner, C., Wike, R., Owen, R., Marsh, M., Eunice, W., Coulter, D., & Adman, N. (06 de enero de 2023). *Authentication vs. authorization.* Obtenido de https://learn.microsoft.com/en-us/azure/active-directory/develop/authentication-vs-authorization

ANEXOS

ANEXO 1 Encuesta

CUESTIONARIO DIRIGIDO A USUARIOS DEL SISTEMA DE DONACIÓN Y TRASPLANTE DE ÓRGANOS

Descripción del formulario

Este formulario recopila automáticamente los correos electrónicos de todas las personas que lo responden. Cambiar la configuración

Consentimiento informado: ¿Está usted de acuerdo en proporcionar información con fines investigativos para obtener datos reales sobre el tema a investigar? *

- Si
- No

Fecha *

Día, mes, año

Tipo de usuario *

- Interno (Pertenece al Instituto de Donación y Trasplante)
- Externo (Pertenece a un establecimiento de salud)

Institución *

Texto de respuesta breve

¿Cuánto tiempo ha estado utilizando el sistema de donación y trasplante de órganos? *

- Menos de 1 año
- 1-2 años
- 3-4 años
- 5-6 años

¿Qué tan fácil le resulta encontrar la información que necesita en el Sistema Nacional Informático de Donación y Trasplante? *

- Muy difícil
- Difícil
- Neutral
- Fácil
- Muy fácil

¿Qué aspectos del sistema considera más difíciles de usar? *

- Navegación general del sitio
- Búsqueda de información específica
- Acceso a datos personales o resultados
- Proceso de registro o inicio de sesión
- Interfaz de usuario (diseño y usabilidad)
- Tiempo de respuesta del sistema
- Soporte técnico o ayuda en línea

¿Considera usted que la información en el sistema está suficientemente protegida? *

- Totalmente en desacuerdo
- En desacuerdo
- Neutral
- De acuerdo
- Totalmente de acuerdo

¿Qué tan segura considera su contraseña actual en el sistema? *

- Muy insegura
- Insegura
- Neutral
- Segura
- Muy segura

¿Conoce las políticas de seguridad utilizadas en el sistema para autentificación de los usuarios? *

- Totalmente en desacuerdo
- En desacuerdo
- Neutral
- De acuerdo
- Totalmente de acuerdo

¿Estaría dispuesto a cambiar su contraseña con regularidad en el sistema, siguiendo las pautas de seguridad recomendadas? *

- Totalmente en desacuerdo
- En desacuerdo
- Neutral
- De acuerdo
- Totalmente de acuerdo

¿Estaría dispuesto a agregar una capa adicional de seguridad a su cuenta, como un código o una medida de protección adicional, si estuviera disponible? *

- Totalmente en desacuerdo
- En desacuerdo
- Neutral
- De acuerdo
- Totalmente de acuerdo

¿Ha experimentado o conocido algún incidente de seguridad relacionado con el sistema? *

- Nunca
- Alguna vez
- Neutral
- A veces
- Siempre

ANEXO 2 Informe Parsifal

Double security factor authentication mechanisms - Final

Johanna Murillo

Web prototypes with double security factor with Security regulations for authentication.

Planning

web system vulnerabilities

Implement a two-factor authentication (2FA) in system web

OWASP authentication mechanisms

authentication mechanisms ISO/IEC 27002:2022

PICOC

- **Population:** Two-factor authentication methods
- **Intervention:** Web System
- **Comparison:** Authentication rules
- **Outcome:** prototype
- **Context:** health sector

Research Questions

1. What are the main vulnerabilities and risks associated with health information systems?
2. What are the different types of two-factor authentication (2FA) methods available for web systems
3. What are the guidelines from OWASP and the ISO/IEC 27002:2022 standard to apply to a web system
4. How can the efficiency and security of a prototype be effectively evaluated through vulnerability analysis and penetration testing

Keywords and Synonyms

Keyword	Synonyms
Authentication rules	
ISO-27002	
OWASP	
Two-factor authentication methods	

Web System

prototype

Search String

("Two-factor authentication methods") AND ("Web System") AND ("Authentication rules" OR "ISO-27002" OR "OWASP") AND ("prototype")

Sources

- IEEE Digital Library (http://ieeexplore.ieee.org)
- Science@Direct (http://www.sciencedirect.com)
- Scopus (http://www.scopus.com)

Selection Criteria

Inclusion Criteria:

Exclusion Criteria:

- before 2021

Quality Assessment Checklist

Questions:

- What are the main vulnerabilities and risks associated with health information systems?
- What are the different types of two-factor authentication (2FA) methods available for web systems
- What are the guidelines from OWASP and the ISO/IEC 27002:2022 standard to apply to a web system
- How can the efficiency and security of a prototype be effectively evaluated through vulnerability analysis and penetration testing

Answers:

- YES
- PARCIAL
- NO

Data Extraction Form

- What are the main vulnerabilities and risks associated with health information systems?
- What are the different types of two-factor authentication (2FA) methods available for web systems
- What are the guidelines from OWASP and the ISO/IEC 27002:2022 standard to apply to a web system
- How can the efficiency and security of a prototype be effectively evaluated through vulnerability analysis and penetration testing

Imported Studies

- **IEEE Digital Library:** 22
- **Science@Direct:** 34
- **Scopus: 39**