UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computacionales

TEMA:

IMPLEMENTACIÓN DEL MÓDULO DE AUDITORÍA INFORMÁTICA PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE (CSOFT) DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO LA CARACTERÍSTICA DE SEGURIDAD DEL ESTÁNDAR ISO/IEC 25010.

Trabajo de grado previo a la obtención del título de Ingeniera en Sistemas Computacionales

Autora:

Silvana Mireya Armas Armas

Directora:

Msc. Daisy Elizabeth Imbaquingo Esparza

Ibarra, 2020

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

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

1. 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:	100413666-7
APELLIDOS Y NOMBRES:	ARMAS ARMAS SILVANA MIREYA
DIRECCIÓN:	ALBERTO GUERRA Y 10 DE AGOSTO, SAN VICENTE DE PUSIR
EMAIL:	smarmasa@utn.edue.ec, silvanamireyaarmas@gmail.com
TELÉFONO MÓVIL:	0981918075

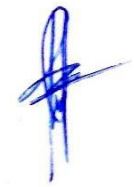
DATOS DE LA OBRA	
TÍTULO:	IMPLEMENTACIÓN DEL MÓDULO DE AUDITORÍA INFORMÁTICA PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE (CSOFT) DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO LA CARACTERÍSTICA DE SEGURIDAD DEL ESTÁNDAR ISO/IEC 25010.
AUTOR (ES):	ARMAS ARMAS SILVANA MIREYA
FECHA:	14/02/2020
PROGRAMA:	[x] **PREGRADO** [ ] **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERA EN SISTEMAS COMPUTACIONALES
ASESOR /DIRECTOR:	MSc. Daisy Imbaquingo

2. CONSTANCIAS

El autor manifiesta 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 el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 14 días del mes de febrero de 2020

EL AUTOR:



……..
Silvana Mireya Armas Armas

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCAS APLICADAS

Ibarra, 12 de febrero de 2020

CERTIFICACIÓN DEL DIRECTOR

Por medio del presente, yo MSc. Daisy Imbaquingo, certifico que la Srta. Silvana Mireya Armas Armas, portadora de la cédula de identidad Nro. 100413666-7. Ha trabajado en el desarrollo del proyecto de grado denominado "**IMPLEMENTACIÓN DEL MÓDULO DE AUDITORÍA INFORMÁTICA PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE (CSOFT) DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO LA CARACTERÍSTICA DE SEGURIDAD DEL ESTÁNDAR ISO/IEC 25010**", previo a la obtención del titulo de Ingeniería en Sistemas Computacionales, lo cual ha realizado en su totalidad con responsabilidad.

Es todo en cuanto puedo certificar en honor a la verdad.

Atentamente,

Msc. Daisy Imbaquingo

DIRECTORA DE TESIS

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

El MSc. Pedro Granda, Coordinador de la Carrera CISIC/CSOFT de la Universidad Técnica del Norte.

CERTIFICA

Que: La Srta. SILVANA MIREYA ARMAS ARMAS, portadora de la cédula de ciudadanía 100413666-7, Estudiante de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad Técnica del Norte, ha desarrollado con el levantamiento de procesos entregados por la Coordinación de la Carrera CISIC/CSOFT, el Proyecto de Tesis "IMPLEMENTACIÓN DEL MÓDULO DE AUDITORÍA INFORMÁTICA PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE (CSOFT) DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO LA CARACTERÍSTICA DE SEGURIDAD DEL ESTÁNDAR ISO/IEC 25010", el software se encuentra funcionanando y el código fuente se ha registrado en el repositorio de proyectos de software de la carrera.

Que: El estudio del proyecto fue entregado a la Coordinación de la Carrera CISIC/CSOFT el 13 de febrero del 2020.

Es todo cuanto puedo certificar, facultando a la interesada hacer uso de este certificado como estime conveniente.

Ibarra, 13 de febrero del 2020

Atentamente,

MSc. Pedro Granda

COORDINADOR DE CARRERA CISIC/CSOFT

Av. 17 de Julio 5-21 y José María Córdova
Ciudadela Universitaria Barrio El Olivo
Teléfono: (06)2997800 Casilla 199
E-mail: info@utn.edu.ec

Ibarra - Ecuador

UNIVERSIDAD TECNICA DEL NORTE
FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

CLUB ETHICAL HACKING UTN
4 de febrero de 2020

Certifica que al trabajo de titulación **Implementación del Módulo de Auditoría Informática para el Sistema Integrado De Actividad Docente (SIAD) de la Carrera de Software (CSOFT) de la Universidad Técnica del Norte, aplicando la característica de Seguridad del Estándar ISO/IEC 25010** perteneciente a la Srta. **Silvana Armas** con cédula de ciudadanía **1004136667**, se realizó una evaluación de seguridad enfocado en hashing de contraseñas, SQL injection blind, conexión segura utilizando HTTPS, entre otros, debido a que este componente fue desarrollado utilizando buenas prácticas de seguridad, no se encontró ninguna vulnerabilidad relacionada y logró superar con éxito las pruebas realizadas.

Es todo cuanto puedo mencionar en honor a la verdad, el propietario puede hacer libre uso de este documento.

Atentamente

Sr. Leonardo Ibujés
Vicepresidente CEH-UTN

Sr. Nelson Cacoango
Responsable de pruebas CEH-UTN

DEDICATORIA

El presente trabajo va dedicado principalmente a Dios por haberme dado la vida y darme la fuerza para obtener uno de los anhelos más deseados.

A mis padres Silvio y Anabela, por su amor, paciencia y sacrificio en todos estos años permitieron que logre culminar mi carrera universitaria, por su apoyo constante y por brindarme valiosos concejos que me ayudan a motivarme y a seguir adelante.

A mi novio Israel por ser mi apoyo fundamental e incondicional, por ser mi pareja idónea, por reanimarme a seguir cuando parecía que iba a desistir, por creer en mi capacidad y estar siempre brindándome su cariño, comprensión y amor.

A mi hijo Joancito que cada día con una sonrisa me daba las fuerzas de seguir, convirtiéndose en mi principal motivación para culminar este sueño.

A mis hermanos porque me han brindado su apoyo incondicional, contribuyendo a lograr los objetivos propuestos.

Finalmente quiero dedicar a mis amigos con quien compartí momentos de alegría dentro y fuera de las aulas, quienes sin esperar nada a cambio compartieron su conocimiento, y a todas aquellas personas que de una u otra manera contribuyeron para que pueda culminar esta meta.

Silvana Armas

AGRADECIMIENTOS

Agradezco a Dios por todas las bendiciones recibidas por ser la fortaleza en los momentos de debilidad y ser el inspirador para seguir adelante.

Gracias a mis padres por ser los pilares fundamentales, quienes en todo momento fueron el sustento tanto moral y económico, por los valores que han inculcado, por ser ejemplo de vida y por dedicar tiempo y esfuerzo para ser una mujer de bien. A mis hermanos por ser parte importante en mi vida y haberme apoyado en todo momento.

De todo corazón a mis dos hombrecitos, a quienes amo mucho, mi novio Israel y a mi hijo Joancito que han sido y son mi soporte para seguir adelante gracias a su amor y compresión me dieron las fuerzas necesarias para seguir y demostrar que si se puede.

A mis amigas Lizeth y Helen por todos los momentos compartidos y haber hecho de mi etapa universitaria un trayecto de vivencias que nunca olvidaré.

A mi tutora de tesis Daisy Imbaquingo y a mis asesores Mauricio Rea y Marco Pusdá por haberme guiado en la elaboración de la tesis y también por sus conocimientos compartidos a lo largo de la carrera universitaria.

Silvana Armas

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

RESUMEN

El presente trabajo de titulación nombrado “IMPLEMENTACIÓN DEL MÓDULO DE AUDITORÍA INFORMÁTICA PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE (CSOFT) DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO LA CARACTERÍSTICA DE SEGURIDAD DEL ESTÁNDAR ISO/IEC 25010.”, se encuentra conformado por tres capítulos.

En la parte de la Introducción se define el problema, objetivo general y objetivos específicos. Además, se incluye el alcance que va a tener el proyecto realizado, así como la justificación del desarrollo del mismo.

En el primer capítulo, se presenta el marco teórico que contiene la evolución de la auditoria respecto a las aplicaciones web, se describe la definición de la característica de Seguridad de la norma ISO/IEC 25010, además se incluye una descripción sobre las pistas de auditoria y la metodología que se usó para el desarrollo de software.

En el segundo capítulo, se detalla el desarrollo del Módulo de Auditoria considerando los indicadores de calidad de la característica de Seguridad de la norma ISO/IEC 25010, implementando la Metodología Ágil Scrum

En el tercer capítulo, se muestran los resultados que se obtuvieron al aplicar la característica de Seguridad de la normativa ISO/IEC 25010.

ABSTRACT

The present degree work named “IMPLEMENTATION OF THE COMPUTER AUDIT MODULE FOR THE INTEGRATED SYSTEM OF TEACHING ACTIVITY (SIAD) OF THE SOFTWARE CAREER (CSOFT) OF THE NORTH TECHNICAL UNIVERSITY, APPLYING THE SECURITY CHARACTERISTICS OF THE ISO / IEC STANDARD 25010. ”, is composed of three chapters.

In the part of the Introduction, the problem, general objective and specific objectives. It also includes the scope that the project will have, as well as the justification for carrying it out.

In the first chapter, is presented the theoretical framework that contains the evolution of the audit with respect to web applications, it is described the definition of the Security characteristic of the ISO / IEC 25010 standard, also is included a description of the audit trails and the methodology that was used for software development.

In the second chapter, it is detailed the development of the Audit Module considering the quality indicators of the Safety characteristic of the ISO / IEC 25010 standard, implementing the Scrum Agile Methodology

In the third chapter, the results obtained by applying the Safety characteristic of the ISO / IEC 25010 standard are shown.

INTRODUCCIÓN

Antecedentes

En la Carrera de Software (CSOFT) de la Universidad Técnica del Norte (UTN) se desarrolló el Sistema Integrado de Actividad Docente (SIAD) con el propósito de mejorar los procesos que realizan los docentes.

Mediante el levantamiento del proceso sobre la entrega de informes de las actividades que realizan los docentes de la CSOFT, se necesitó implementar un sistema de auditoría informática dentro del SIAD que permitiera minimizar inicidentes tales como: pérdida de tiempo, información y dinero, no se dispone de un historico digital, información inconsistente, conflictos personales y se vio reflejado el desaprovechamiento de tecnología, para mitigar estos aspectos se requirió conocer el control previo y de ejecución de las actividades de los docentes que se presentan al realizar las actividades dentro del proceso descrito.

En toda auditoría que se lleve a cabo en una empresa con el fin de establecer la razonabilidad de datos, funciones, operaciones, actividades, informes y reportes, la mayor parte del trabajo consiste en la recopilación de evidencias para obtener un mejor criterio a la hora de determinar y esclarecer ciertos hallazgos, así como para tener mayor certeza a la hora de efectuar una revisión detallada de una determinada función u operación que sirva para sustentar las conclusiones y recomendaciones.(Econ, 2012)

Uno de los elementos de control que puede ayudar mucho en la lucha por mantener a los sistemas, datos e información libre de actos irregulares, es el uso y aplicación de las denominadas “bitácoras”, que constituyen un espacio en disco en donde se almacenan datos relevantes de cualquier evento, que por su naturaleza sea conveniente archivarla para usos posteriores.(Econ, 2012)

Situación Actual

Los docentes de la Carrera de Software entregan informes de sus actividades manualmente, para cumplir las tareas y actividades planificadas y ejecutadas, al no contar con un módulo de auditoría informática en el sistema integrado de la CSOFT que se desarrolló, se presentan ciertos problemas ocacionando irregularidades al momento de realizar una verificación de una actividad que se haya ejecutado.

Los informes son archivados y al presentarse algún inconveniente se tendría pérdida de tiempo al buscar la inconsistencia lo cual se busca fortalecer el proceso mediante un sistema de auditoría informática, realizando una bitácora en base a una normativa,

permitiendo llevar un control sobre las actividades que desempeñan los docentes, de la misma manera se exponen a ciertos riesgos como son: fuego, agua o robo del documento entre otros.

Prospectiva

El módulo de auditoría informática permite contar con pistas de control de la información en el proceso de entrega de informes mediante la característica de seguridad del estándar ISO/IEC 25010 garantizando la confidencialidad e integridad de la información, asegurando la optimización y agilización en la toma de decisiones teniendo un control de seguimiento y análisis mucho más eficiente y rentable y así se pueda evidenciar el cumplimiento de las actividades a cargo.

Evitar el alto consumo de papel y contar con una solución tecnológica que permita contar con histórico digital, y no se encuentren expuestos ciertos riesgos.

Planteamiento del Problema

En la Coordinación de la Carrera de Software de la Universidad Técnica del Norte se necesitó la implementación de un módulo de auditoría informática dentro del sistema SIAD que se desarrolló, permitiendo minimizar ciertos inicidentes que se presentan en el transcurso del proceso, mediante controles detectivos de auditoría, para obtener hallazgos y evaluar objetivamente evidencias sobre las operaciones que se efectúan en el sistema, garantizando la seguridad de la información.

En la Fig. 1 se presenta el árbol de problemas que permite identificar el problema central, de esta manera se procura solventar analizando los vínculos de tipo causa – efecto.

Fig. 1 Árbol de problemas
Fuente: Propia

Objetivo General

Implementar el módulo de auditoría informática para el Sistema Integrado de Actividad Docente (SIAD) de la Carrera de Software (CSOFT) de la Universidad Técnica del Norte (UTN), aplicando la característica de seguridad del estándar ISO/IEC 25010.

Objetivos Específicos

1. Elaborar un marco teórico sobre la característica de seguridad del estándar ISO/IEC 25010 y las pistas de auditoría.
2. Desarrollar el módulo de auditoría informática mediante la característica de seguridad del estándar ISO/IEC 25010 y la metodología Scrum.
3. Validar los resultados

Alcance

Implementación del módulo de auditoría para automatizar el proceso de entrega de informes de las actividades de los docentes, acompañada de la característica de seguridad de la ISO/IEC 25010 que permita verificar el procesamiento de la información asegurando una mayor integridad, confidencialidad y confiabilidad de la información.

La auditoría es el análisis exhaustivo de los sistemas informáticos con la finalidad de detectar, identificar y describir las distintas vulnerabilidades que puedan presentarse.(Auditoría de seguridad informática (MF0487_3), 2014)

El sistema SIAD genera una gran cantidad de información para lo cual se implementó una bitácora que ayuda a verificar incidentes de seguridad ya que hoy en día los sistemas se exponen a diferentes amenazas, por lo tanto las vulnerabilidades aumentarían.

La bitácora registra información acerca de eventos relacionados con el sistema SIAD lo cual toma importancia en los incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas y evidencia legal.(Econ, 2012)

Para la realización se procedió a analizar la característica de seguridad de la ISO/IEC 25010 para poder implementar en el desarrollo del módulo de auditoría informática.

Las tecnologías que se utilizó para el desarrollo del módulo de auditoría y el sistema en general fue la siguiente:

- Arquitectura Java enterprise monolitica
- Lenguaje de programación Java Enterprise
- IDE Eclipse 2018-09, v4.9

- Servidor de aplicaciones Wildlfy v14.0
- GitHub
- Servidor de aplicaciones Java EE

Luego de un estudio se determinó el método que permitió validar los resultados.

Justificación

El presente proyecto tiene un enfoque hacia dos de los objetivos de desarrollo sostenible:

Objetivo 4.- Educación de calidad (edX, 2019)

El objetivo de lograr una educación inclusiva y de calidad para todos se basa en la firme convicción de que la educación es uno de los motores más poderosos y probados para garantizar el desarrollo sostenible. (Programa de las Naciones Unidas para el Desarrollo, 2020)

Objetivo 9.- Industria, innovación e infraestructura (edX, 2019)

Los avances tecnológicos también son esenciales para encontrar soluciones permanentes a los desafíos económicos y ambientales.

9.b Apoyar el desarrollo de tecnologías, la investigación y la innovación nacionales en los países en desarrollo, incluso garantizando un entorno normativo propicio a la diversificación industrial y la adición de valor a los productos básicos, entre otras cosas.

9.c Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020. (Programa de las Naciones Unidas para el Desarrollo, 2020)

Ambiental

Como es notorio, la fabricación del papel es un material contaminante de alto nivel, aunque no todo el papel tiene el mismo impacto ambiental, pues los procesos de elaboración y su ciclo de vida son variables, por norma la producción de papel es sinónimo de contaminación y se ve la necesidad de reducir el consumo de papel automatizando el proceso y que todo lo que se realiza sea digital.

Tecnológico

Con el pasar de los años, nos encontramos en una actualidad muy tecnológica, donde el Internet es fundamental en nuestras vidas. De igual manera es el caso de las instituciones educativas se deben adaptarse a la tecnología y estar lo más actualizadas posible para aumentar su competitividad y desarrollo.

Se empleó la metodología Scrum ya que ha ganado la mayor tracción en el sector tecnológico y ha contribuido a tiempos de mercado más rápidos, mayor flexibilidad, productos de mayor calidad, y satisfacción del cliente. (Gonçalves, 2018)

Scrum es un modelo de desarrollo ágil definido por Ikujiro Nonaka e Hirotaka Takeuchi en los años ochenta del siglo pasado, y adaptado por Ken Schwaber y Jeff Sutherland como procedimiento de desarrollo de software en 1995. (Implantar scrum con éxito, 2016)

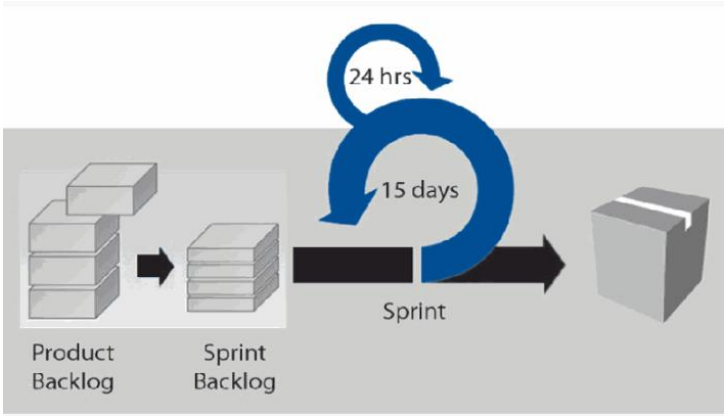


Fig. 2 Proceso Scrum
Fuente: (Implantar scrum con éxito, 2016)

CAPÍTULO I

1. Marco Teórico

En un entorno cambiante, el éxito de una organización se ha relacionado estrechamente con su capacidad para gestionar los riesgos. La importancia de las auditorías informáticas radica en que permiten determinar las fortalezas y debilidades del sistema de información de las organizaciones, a medida que las empresas se vuelven cada vez más dependientes de la información para su ventaja competitiva y la información gana incluso mayor proporción en el valor agregado incorporado en los productos y servicios de las empresas, la capacidad de proteger información valiosa y sensible se ha convertido en una capacidad estratégica para asegurar la sostenibilidad empresarial, y el valor total de una empresa. (Caycedo-casas & Central, 2017)

Para las organizaciones, es muy importante que se evalúen constante y regularmente todos los procesos que en ellas se llevan a cabo, con el fin de verificar su calidad y suficiencia en cuanto a los requerimientos de negocio para la información: control, integridad y confidencialidad.(Venegas, 2018)

Es por eso que la auditoría consiste en el análisis exhaustivo de los sistemas informáticos con la finalidad de detectar, identificar y describir las distintas vulnerabilidades que puedan presentarse.(Chicano, 2014)

1.1 Evolución de la auditoría con respecto a las aplicaciones web

1.1.1 Introducción

En la actualidad los temas relativos a la auditoría informática cobran cada vez más relevancia, tanto a nivel nacional como internacional, debido a que la información se ha convertido en el activo más importante de las empresas, representando su principal ventaja estratégica, por lo que éstas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información con el fin de obtener la mayor productividad y calidad posibles.(Piatiini, 2001)

1.1.2 Seguridad Informática

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra

cualquier tipo de amenazas, minimizando los riegos tanto físicos como lógicos, a los que está expuesta. (Urbina, 2016)

La auditoría de seguridad informática analiza procesos referentes a la seguridad informática, tanto física como lógica. En este caso tomaremos en cuenta la seguridad lógica puesto que compete para la realización del módulo de auditoría.

La seguridad lógica, es la protección del software, procesos, programas del sistema y su auditoría consistiría en analizar la correcta protección y actualización de estos componentes, además de la protección de los datos que forman parte del sistema.(Chicano, 2014).

1.1.3 Seguridad de la Información

En las organizaciones o instituciones, la gestión de la información se puede identificar como el método que se encarga de todo lo relacionado con el proceso de obtener información acorde a las necesidades, libre de errores, para la persona indicada, a un coste conveniente, en el tiempo determinado y articulando todas estas operaciones para el desarrollo de una tarea correcta.

Lla información es lo más valioso para cualquier tipo de empresa, así como también para la sociedad en general (Urbina, 2016), por ello, es de gran importancia la seguridad de la información y la utilización de un modelo adecuado que pueda precautelar todos los datos y la utilización de los mismos.(Lara, 2019)

- ✓ **¿Qué es seguridad de la información?**

La seguridad de la información permite asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización.(Veracruzana, 2019)

En este sentido, debemos entender a la seguridad de la información como un proceso integrado por un conjunto de estrategias, medidas preventivas y medidas reactivas que se ponen en práctica en las instituciones para proteger la información y mantener su confidencialidad, disponibilidad e integridad de la misma.

En la Fig. 3 se da a conocer las características que posee la información:

Fig. 3. Características de la información
Fuente: Propia

En la TABLA 1 se presenta cada característica con su respectiva definición:

TABLA 1 Definiciones de las características de la información

Característica	Definición
Efectividad	Información necesaria y adecuada para realizar los procesos del negocio proporcionándola de manera oportuna, correcta, consistente y accesible.
Eficiencia	Información generada y procesada, use de manera óptima los recursos que tiene la empresa para este fin.
Confidencialidad	En todas las etapas del procesamiento de la información, esta se encuentre protegida contra accesos no autorizados.
Integridad	La información que se recibe sea precisa y este completa para los fines que se persiguen con su procesamiento.
Disponibilidad	La información necesaria para realizar cualquiera de las etapas del proceso administrativo este a la mano cuando sea requerida por los procesos del negocio en cualquier momento
Apego a estándares	El procesamiento de la información se deberán atacar leyes de uso general o reglamentos, acuerdos internos y contractuales a los cuales este sujeto el proceso de negocio.
Confiabilidad	Significa que la información no haya sido alterada inapropiadamente.

Fuente: Propia

En la TABLA 2 se presentan otros elementos importantes que se deben considerar al hablar de seguridad de la información y que están fuertemente vinculados a la implementación de sistemas de seguridad:

TABLA 2Elementos importantes de la seguridad de la información

Elemento	Definición
Riesgo	Grado de exposición de un activo[1] ante una amenaza que al materializarse causando un impacto adverso. Indica lo que podría pasar a los activos si no se protege con seguridad.
Amenaza	Es un evento que puede desencadenar un incidente que produce daños en los activos.
Vulnerabilidad	Se refiere a la debilidad de un activo o de un control para ser afectado por una o más amenazas.

Fuente: Propia

- ✓ **Importancia de la seguridad de la información**

Las organizaciones y sus activos de información sean estos físicos o digitales, se enfrentan de forma creciente a amenazas como: fraude asistido por computadora, espionaje, sabotaje, vandalismo, fenómenos naturales, descuido, desconocimiento o mal uso del tratamiento de la información por parte del recurso humano. Muchas de esas amenazas provienen de ingenieros sociales, *hackers*, empleados negligentes, errores, entre otros, que buscan dañar la integridad de una organización.(Veracruzana, 2019)

Existen dos factores importantes de la seguridad de la información:

a. La importancia o valor de los datos de acuerdo con los intereses y necesidades de cada persona o institución;
b. La difusión o acceso, autorizado o no, de los mismos.

- ✓ **Daños producidos por falta de seguridad**

Los daños producidos por falta de seguridad pueden causar pérdidas de credibilidad y prestigio a una organización. En la Fig. 4 nos permite verificar los daños según su origen.

[1] Se define como los elementos del sistema de información (estrechamente relacionados con este) que soportan la misión de la organización. Un activo es nuestro, que tiene un valor para la organización y por tanto debe protegerse.

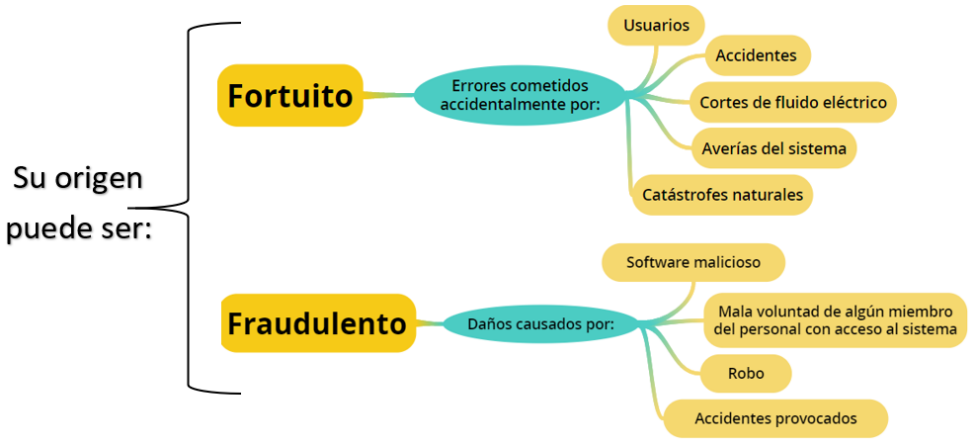


Fig. 4 . Tipos de daños
Fuente: Propia

- ✓ **Propiedades de un sistema seguro**

La Fig. 5 Nos permite conocer que cada una de las propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad.(López, 2010).

Fig. 5 . Propiedades de un sistema seguro
Fuente: Propia

1.1.4 Seguridad en aplicaciones web

La seguridad de la información (SI) también debe considerar los aspectos del software, porque la seguridad no es un parámetro único. En la TABLA 2 se presenta sobre las preocupaciones de la óptica del desarrollo de software:

TABLA 3 Preocupaciones de la óptica del desarrollo

Preocupaciones	Definición
Seguridad en el entorno de desarrollo	Cuando es necesario mantener los códigos fuentes seguros.
Seguridad de la aplicación desarrollada	Teniendo como objetivo desarrollar una aplicación que sea segura y que no contenga fallos que comprometan la seguridad.
Garantizar la seguridad de la aplicación desarrollada	Teniendo como garantizar al cliente la seguridad de la aplicación desarrollada a través de las pruebas adecuadas.

Fuente: (López, 2010).

1.2 Definición de la característica de Seguridad de la norma ISO/IEC 25010

1.2.1 Introducción

La norma ISO/IEC 25010 hace parte de la familia de normas ISO 25000 (calidad del producto software).

La calidad del producto software se puede interpretar como el grado en que dicho producto satisface los requisitos de sus usuarios aportando de esta manera un valor.

Son precisamente estos requisitos (funcionalidad, rendimiento, seguridad, mantenibilidad, etc.) los que se encuentran representados en el modelo de calidad, el cual categoriza la calidad del producto en características y subcaracterísticas.(“ISO 25010,” 2019)

El modelo de calidad del producto definido por la ISO/IEC 25010 se encuentra compuesto por las ocho características de calidad que se muestran en la Fig. 6.

Fig. 6 Características de calidad de la ISO/IEC 25010
Fuente: (“ISO 25010,” 2019)

En el presente proyecto se aplicará la característica de Seguridad lo cual abarca cinco subcaracterísticas que son de vital importancia para el cumplimiento de un software de calidad.

1.2.2 Característica de Seguridad

Capacidad de protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos.

- ✓ **Subcaracterísticas**

En la TABLA 4 se muestra las cinco subcaracterísticas que contiene la característica de Seguridad.

TABLA 4 Subcaracterísticas de la seguridad

Subcaracterísticas	Definición
Confidencialidad	Capacidad de protección contra el acceso de datos e información no autorizados, ya sea accidental o deliberadamente.
Integridad	Capacidad del sistema o componente para prevenir accesos o modificaciones no autorizados a datos o programas de ordenador.
No repudio	Capacidad de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no puedan ser repudiados posteriormente.
Responsabilidad	Capacidad de rastrear de forma inequívoca las acciones de una entidad.
Autenticidad	Capacidad de demostrar la identidad de un sujeto o un recurso.

Fuente: ("ISO 25010," 2019)

La explicación más detallada de cada una de las subcaracterísticas se presentará en el Capítulo 2.

1.2.3 Auditoria

Para llevar a cabo una auditoría, se hace necesario recopilar la evidencia suficiente y apropiada que sirva de base para poder emitir una opinión sobre el trabajo realizado. Debido a que en muchas ocasiones es difícil realizar este proceso, es necesario usar las pistas de auditoría. Lo que se busca con su aplicación, es una orientación hacia la correcta dirección de las pruebas, con el fin de que conduzcan por el camino correcto para hallar la evidencia que sea de utilidad. Este tipo de prueba tiene una función relevante, que permita tener un mejor criterio a la hora de determinar y esclarecer ciertos hallazgos. Lo que se pretende es dar un nuevo enfoque al uso y aplicación de este tipo de instrumento.(Espinoza, 2012).

Dentro del ámbito de la auditoria se presenta el término “hallazgo” a continuación se detalla su significado.

> Chicano Tejada, (2014) afirma: “Un hallazgo se refiere a un conjunto de información, que recopila datos específicos sobre la actividad, tarea, proceso, condición, etc., analizados y evaluados, que sea considerada de interés para la organización”.

En general, los hallazgos obtenidos se emplean a modo de crítica y muestran información sobre deficiencias o debilidades detectadas en el sistema auditado es decir basados en hechos y evidencias concretas que figuren el trabajo y que les permitan ser identificados con facilidad.. No obstante, hay que tener en cuenta que, aunque son menos abundantes, también hay hallazgos positivos.

- ✓ **Tipos de Auditoria**

La auditoría como procedimiento legal ha progresado en las últimas décadas dando lugar a diversas especialidades. En el tiempo actual se conocen diferentes tipos de auditoría que se diferencian básicamente por los objetivos y los representantes que la realizan. En la Fig. 7 se presenta los tipos de auditoría:

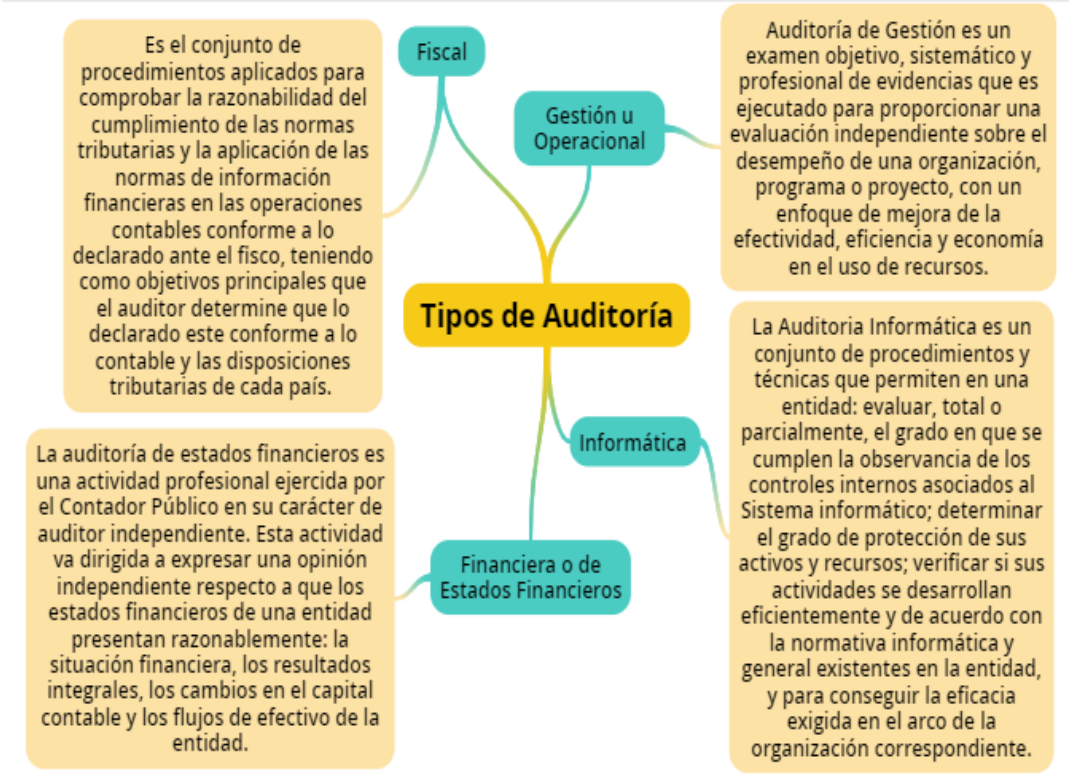


Fig. 7 Tipos de auditoría
Fuente: Propia

- ✓ **Clases de Auditoria**

Según la relación de dependencia del auditor la auditoría se clasifica en Auditoría Interna y Externa, como se detalla en la TABLA 4.

TABLA 5 Clases de auditoría

Clases de Auditoría	Definición
Externa	Es una función de evaluación externa, ejecutada por un ente externo e independiente de la línea jerárquica establecida. Actúa controlando algún aspecto particular de las operaciones o procedimientos establecidos en la organización.
Interna	Es una función de evaluación interna, ejercida por personal perteneciente a los cuadros de la empresa. Actúa como un servicio independiente de la línea jerárquica corriente, por lo que depende directamente de la Dirección de la organización. La auditoría interna mide y evalúa la confiabilidad y eficacia del sistema de control interno de la entidad para lograr su mejoramiento

Fuente: Propia

- ✓ **Auditoria en sistemas informáticos**

José Antonio Echenique (1990) define a la Auditoria Informática como un:

> Examen y evaluación de los procesos del área del procesamiento automático de datos (PAD) y de la utilización de los recursos que en ellas intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados de una INSTITUCIÓN y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.(Venegas, 2018)

Según Piattini en su obra de Auditoria Informática: Un Enfoque Práctico (2003):

> La auditoría en informática se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de la información en la organización, se lleven a cabo de una manera oportuna y eficiente.(Venegas, 2018)

- ✓ **Control en la auditoría**

En general, se reconoce al control como una función administrativa básica; consiste en verificar que las diferentes actividades que se realizan en una organización tiendan a alcanzar sus objetivos. Se considera que el control produce dos tipos de acciones según sea el ámbito donde se aplique:

a) Influencia directiva, intenta que las actividades del sistema se realicen de modo tal que produzcan determinados resultados o alcancen objetivos específicos predefinidos.
b) Influencia restrictiva, la acción se ejerce de tal forma que se evite que las actividades de un sistema produzcan resultados no deseados.(Castello, 2006).

- ✓ **Tipos de Control**

Se mencionó que la auditoría es una actividad de control, por lo tanto, vamos a profundizar un poco, en la TABLA 5 muestra su clasificación:

TABLA 6 Tipos de control

Tipos de control según su:	Clasificación	Definiciones
Objetivo	✓ Correctivos	Son aquellos que cuentan en su estructura con los elementos para medir las desviaciones e informar sobre ellas.
	✓ No correctivos	Son los que prescinden de la medición e información de los desvíos que se pueden producir.
Marco temporal	✓ Retroalimentados	Operan sobre hechos sucedidos. Comparan los resultados ocurridos con los esperados.
	✓ Prealimentados	Operan sobre eventos futuros (en los procesos industriales se denominan “control anticipante”) y previenen la ocurrencia de resultados indeseados.
Pertenencia al sistema operante	✓ De secuencia abierta	El grupo de control no pertenece al sistema operante; es independiente del mismo.
	✓ De secuencia cerrada	Todos los elementos del control pertenecen al propio sistema operante.

Fuente: (Castello, 2006)

1.2.4 Pistas de Auditoria

La serie de documentos, archivos informáticos, y otros elementos de información que se examinan durante una auditoría, y muestran cómo las transacciones son manejadas por una empresa de principio a fin. Puede ser un rastro de papel o un rastro electrónico que proporciona la historia documentada de la actividad en una empresa.

Las pistas de auditoría no son controles por sí mismos, son “pistas”, “huellas” o “rastros” que se requieren para el uso analítico y administrativo; son más que todo un procedimiento que puede estar constituido por uno o varios documentos, informes o simplemente desprenderse de un control o conjunto de controles.(Espinoza, 2012)

En todos los sistemas, sean automatizados o no, las pistas de auditoría deben estar siempre presentes, en la TABLA 6 muestra los tres requisitos básicos que se deben cumplir:

TABLA 7 Requisitos básicos de las pistas de auditoría

Requisitos básicos		
✓ Que cualquier transacción pueda ser seguida, desde el documento fuente que la originó, por medio del proceso a que es sometida, hasta las salidas (archivos, consultas por pantalla o informes) y los totales a los cuales se agrega.	✓ Que cada salida o resumen de datos, se pueda seguir hacia atrás, hasta la transacción cálculos que los produjeron.	✓ Que cualquier transacción generada automáticamente, se pueda rastrear hasta el evento o condición que la generó.

Fuente: Propia

✓ **Propósito de las pistas de auditoria**

Normalmente una pista de auditoría tiene dos propósitos:

a) El propósito de implosión: que permite rastrear una transacción desde su origen, pasando por el proceso de transformación a que es sometida, hasta su almacenamiento y presentación.

b) El propósito de explosión: que permite la reconstrucción de las diferentes operaciones a que ha sido sometida una transacción.

✓ **Necesidad de las pistas de auditoría**

Debido a la gran ayuda que proporciona este tipo de pistas, tanto a la auditoría como a la administración, se ha hecho indispensable su implantación y utilización.

Existen muchas razones que hacen necesario que las pistas de auditoría estén presentes en todo proceso que se lleve a cabo en las empresas; algunas de ellas son:

a) Consultas. Normalmente las consultas se realizan para determinar el estado de una cuenta o un grupo de datos.

b) Para cumplir con necesidades legales. En algunos países, entre ellos Costa Rica, algunas entidades como la Administración Tributaria, Ministerio de Hacienda; Archivos Nacionales, Caja Costarricense del Seguro Social y el Instituto Nacional de Seguros, las municipalidades, entre otras, solicitan para los datos e información que se produce de manera electrónica, deba ser archivada en un medio de almacenamiento masivo.(Espinoza, 2012)

c) Para propósitos de seguimiento. La pista de auditoría ofrece un medio para darle seguimiento a una aplicación. A menudo, de acuerdo con el sistema, las transacciones y la periodicidad con que estas se presenten, los movimientos que afectan los archivos deben ser rastreados a través de la aplicación para determinar si todos los procesos están funcionando correctamente.

d) Para descubrir fraudes. El contar con pistas de auditoría contribuye a reducir la posibilidad de que un fraude no se pueda detectar. Si la persona que perpetra el acto ilícito o irregularidad sabe que las funciones, eventos y registros, tanto de las operaciones normales como del acto que intentan realizar, están siendo grabados y monitoreados, deberán realizar tareas complementarias y/o adicionales para evitar ser descubierto.

e) Como elemento de control: debido al doble propósito que tienen, es indudable que, al ser utilizadas también por la administración, pueden ser de gran utilidad para controlar ciertos procesos, que, al ser revisados, ya sea por medio de un reporte, de una consulta o de un análisis detallado, sean de utilidad para detectar posibles actos irregulares o anomalías.

f) Para determinar las consecuencias de un error. Si por alguna razón se descubre que se ha cometido un error (no perder de vista que la diferencia entre un error y acto irregular es la intención); podría ser necesario obtener información adicional para determinar los efectos de este error.

Un error podría ocasionar serios daños, perjuicios y problemas a una entidad, pero también podría pasar desapercibido y no suceder nada, al menos por un tiempo; pero cuanto más tiempo pase, más difícil será determinar con precisión cuáles son las consecuencias. La pista puede ayudar a determinar, por ejemplo, quién le dio acceso al dato, quién tomó decisiones basado en esos datos, y si el error tiene consecuencias significativas en las decisiones que se han tomado; asimismo la pista de auditoría podría permitir que el efecto de un error pueda ser rastreado.

g) Para fines de respaldo y recuperación. Algunos de los datos almacenados en una pista de auditoría también podrían ser útiles como elemento de respaldo, por un tiempo prudencial y temporal, mientras hacen el soporte definitivo, así como de recuperación, en caso de que no exista el respaldo o que se haya extraviado. Por ejemplo, si por alguna razón no se guardan los diferentes tipos de interés que se han pagado por los certificados de depósitos a plazo, la pista sería un excelente medio para recuperarlas y tenerlas, como información histórica.(Espinoza, 2012).

1.2.5 Utilización de bitácoras

Las bitácoras que tienen incorporados la mayoría de los sistemas operativos, así como administradores de bases de datos, aunque ofrecen facilidades para obtener información valiosa para una auditoría, también están muy limitadas con respecto al proceso de las transacciones en sí, que es lo que realmente se necesita en una revisión.(Espinoza, 2012).

- ✓ **Revisión y análisis de bitácoras**

Actualmente, los sistemas basados en tecnología de información se encuentran expuestos a diferentes clases de riesgos, debido a las vulnerabilidades que ellos mismos presentan por la deficiencia en los controles que tienen incorporados o porque algunos carecen de ellos; a esa situación debe agregarse que cada vez presentan un mayor grado de complejidad; ante tal panorama, el número de ataques ha aumentado de manera considerable.(Espinoza, 2012). Uno de los elementos de control que puede ayudar mucho en la lucha por mantener a los sistemas, datos e información libres de atentados y de actos irregulares, es el uso y aplicación de las denominadas “bitácoras”, que constituyen un espacio en disco en donde se almacenan los datos relevantes de cualquier evento, que por su naturaleza sea conveniente

archivarla para usos posteriores; lo que se acostumbra activar es una bitácora de transacciones, en la TABLA 8 se presenta los campos que se almacenan en la bitácora del módulo de auditoria:

TABLA 8 Campos que contiene la bitácora

Campos	Información
❖ ID	Registra el ID de la pista
❖ Fecha y Hora	Registra la fecha y la hora que se ejecutó el movimiento
❖ IP - PC	Registra la terminal desde donde se originó el evento
❖ Usuario	Registra el nombre del usuario que ejecutó el movimiento
❖ Rol	Registra el rol que tiene asignado el usuario que ejecuto el movimiento
❖ Clasificación del evento	Registra el nombre del módulo en el cual se ejecutó el movimiento.
❖ Nombre del evento	Registra el nombre del evento que se realizó en el sistema
❖ Descripción del evento	Registra la descripción del evento que se realizó en el sistema
❖ Método y Clase	Registra el nombre del método y clase que se ejecutó para la realización del movimiento
❖ Prioridad	Registra el tipo de prioridad sea alta, media o baja. Dependiendo del tipo de prioridad las pistas se pintan de color verde si es baja, amarillo si es media y roja si es alta

Fuente: Propia

✓ **Como hacer un buen uso de las bitácoras**

Las bitácoras contienen una gran cantidad de datos de toda clase y tipo, y dependiendo de su diseño, son entendibles solo por quienes lo hicieron, por lo tanto, es requisito esencial, que sean diseñadas de acuerdo con las necesidades, tanto de la administración como de auditoría, de manera que contengan los datos y la información necesaria para poder realizar cualquier operación o función que se necesite, de acuerdo con la revisión que se vaya a efectuar. La utilidad de su uso consiste en recuperar de ella toda la información posible, que oriente hacia el fin que se persigue, ya sea de manera administrativa, operativa, de control o de examen. La persona que necesite utilizar la información de las bitácoras establecerá el medio adecuado para tener acceso a ella, acorde con sus requerimientos. La información para almacenar deberá ser determinada con antelación, con base en la aplicación, las transacciones que se procesan, los controles establecidos, los cálculos realizados, el proceso de transformación a que

es sometida la información, y la necesidad de reconstruir algún proceso. (Espinoza, 2012)

1.3 Metodología para el desarrollo de software

En la actualidad, las metodologías ágiles como Scrum, Agile RUP, eXtreme Programming, Lean Development, Cristal Methods, entre otras, se convierten en un modelo para los iniciados en el desarrollo de software, estas metodologías presentan algunas ventajas ante las metodologías pesadas, pero son limitadas por el tamaño del proyecto y el número de programadores que pueden intervenir. Sin embargo, resultan muy atractivas para el desarrollo de aplicaciones en empresas de software que estén iniciando o para el desarrollo de software por módulos, sin descuidar la calidad y garantizando la actualización de la documentación.(Pereira., 1995)

1.3.1 Metodologías Ágiles de Desarrollo de Software

En la TABLA 9 se presenta las convergencias y divergencias entre las principales metodologías ágiles.

TABLA 9 Tabla de convergencias y divergencias entre las principales metodologías ágiles.

Metodología	Acrónimo	Creación	Tipo de modelo	Característica
Adaptive Software Development	ASD	Highsmith 2000	Prácticas + ciclo de vida	Inspirado en sistemas adaptativos complejos
Agile Modeling	AM	Ambler 2002	Metodología basada en la práctica	Suministra modelado ágil a otros métodos
Cristal Methods	CM	Cockbum 1998	Familia de metodologías	Metodología ágil con énfasis en modelo de ciclos
Agile RUP	dX	Booch, Martin, Newkirk 1998	Framework/Disciplina	XP dado vuelta con artefactos RUP
Dynamic Solutions Delivery Model	DSDM	Stapleton 1997	Framework/modelo de ciclo de vida	Creado por 16 expertos en RAD
Evolutionary Proyect Management	EVO	Gilb 1976	Framework adaptativo	Primer método ágil existente
eXtreme Programming	XP	Beck 1999	Disciplina en prácticas de ingeniería	Método ágil radical
Feature-Driven Development	FDD	De Luca & Coad 1998 Palmer & Felsing 2002	Metodología	Método ágil de diseño y construcción
Lean Development	LD	Charette 2001, Mary y	Forma de pensar – modelo logístico	Metodología basada en

		Tom Poppendieck		procesos productivos
Rapid Development	RAD	McConnell 1996	Survey de técnicas y modelos	Selección de *best practices*, no método
Microsoft Solutions Framework	MSF	Microsoft 1994	Lineamientos, disciplinas, prácticas	Framework de desarrollo de soluciones
Scrum	Scrum	Sutherland 1994 Schwaber 1995	Proceso – framework de management	Complemento de otros métodos, ágiles o no

Fuente:(Calderón, Valverde, 2007)

1.3.2 El Manifiesto Ágil

Para asegurar el éxito durante el desarrollo de software no es suficiente contar con notaciones de modelado y herramientas, hace falta un elemento importante: la metodología de desarrollo, la cual nos provee de una dirección a seguir para la correcta aplicación de los demás elementos.(Calderón, Valverde, 2007)

En febrero del 2001 en Utah-EEUU, se reunieron 17 empresarios de la industria de software que se basaban en procesos para discutir temas referentes al desarrollo de software, con el objetivo de proponer los valores y principios permitiendo a los equipos desarrollar software rápidamente y respondiendo a los cambios que puedan surgir a lo largo del proyecto(Letelier, Canós, Sánchez, 2003), como resultado del debate respecto a las metodologías, principios y valores que deben regir el desarrollo de software de buena calidad, en tiempos cortos y flexible a los cambios, se aceptó el término ágil para hacer referencia a nuevos enfoques metodológicos en el desarrollo de software.(Pereira., 1995)

Podríamos utilizar como definición de agilidad la ofrecida por Quomer y Henderson Selles:

> "La agilidad es un comportamiento persistente o habilidad, de entidad sensible, que presenta flexibilidad para adaptarse a los cambios esperados o inesperados, rápidamente; persigue la duración más corta en tiempo, usa instrumentos económicos; y utiliza los conocimientos y experiencias previos para aprender tanto del entorno interno como del externo".(Trigas & Domingo, 2012)

Tras esta reunión se creó The Agile Alliance, una organización, sin ánimo de lucro, dedicada a promover los conceptos relacionados con el desarrollo ágil de software y ayudar a las organizaciones para que adopten dichos conceptos. El punto de partida fue el Manifiesto Ágil.(Letelier, Canós, Sánchez, 2003)

- ✓ **Valores principales**

El manifiesto hace énfasis en cuatro valores principales que deben soportar el desarrollo de software (Calderón, Valverde, 2007):

a) **Al individuo y las interacciones del equipo de desarrollo sobre el proceso y las herramientas,** la gente es el principal factor de éxito de un proyecto software. Es más importante construir un buen equipo que construir el entorno.
b) **Desarrollar software que funciona más que conseguir una buena documentación,** la regla a seguir es “no producir documentos a menos que sean necesarios de forma inmediata para tomar una decisión importante”. Estos documentos deben ser cortos y centrarse en lo fundamental.
c) **La colaboración con el cliente más que la negociación de un contrato** se propone que exista una interacción constante entre el cliente y el equipo de desarrollo. Esta colaboración entre ambos será la que marque la marcha del proyecto y asegure su éxito
d) **Responder a los cambios más que seguir estrictamente un plan,** la habilidad de responder a los cambios que puedan surgir a lo largo del proyecto (cambios en los requisitos, en la tecnología, en el equipo, etc.) determina también el éxito o fracaso del mismo. Por lo tanto, la planificación no debe ser estricta sino flexible y abierta.

1.3.3 Principios del Manifiesto Ágil

El manifiesto ágil nos presenta los 12 principios siguientes(López, 2018):

a) **Satisfacer al cliente,** mediante tempranas y continuas entregas de software que le aporte un valor.
b) **Requisitos cambiantes en el proceso de desarrollo de software,** se capturan los cambios para que el cliente tenga una ventaja competitiva.
c) **Entrega de software funcional en periodos cortos de tiempo**, los cuales pueden ser en un par de semanas o hasta meses con el menor intervalo de tiempo posible entre entregas.
d) **Trabajo en colaboración entre desarrolladores y personas del negocio,** durante todas las etapas del proyecto deben de trabajar juntos.
e) **Motivación a los integrantes del equipo,** Darles el entorno, el apoyo que necesitan y la oportunidad de generar confianza en ellos para la realización de sus tareas y así conseguir finalizar el trabajo.

f) **Dialogo cara a cara,** con la finalidad de tener una comunicación es el método más eficiente y efectivo para comunicar información dentro del equipo de desarrollo.
g) **Software funcional** como medida principal de progreso.
h) **Los procesos ágiles promueven un desarrollo sostenible**, como promotores, desarrolladores y usuarios deben ser capaces de promover una paz constante.
i) **La atención continua a la calidad técnica y al buen diseño,** dándole atención continua para mejorar la agilidad.
j) **Simplicidad** es muy esencial como arte encargada de la maximización de trabajo realizado.
k) **Autoorganización dentro del equipo**, dando como resultado mejores requisitos, arquitecturas y diseños.
l) **Revisiones periódicas,** el equipo reflexiona respecto a cómo llegar a ser más efectivo, y según esto ajusta su comportamiento.

1.3.4 Agilismo en el desarrollo de software

Agilismo no es perfeccionismo, es más, el agilista reconoce que el software es propenso a errores por la naturaleza de quienes lo fabrican y lo que hace es tomar medidas para minimizar sus efectos nocivos desde el principio. No busca desarrolladores perfectos, sino que reconoce que los humanos nos equivocamos con frecuencia y propone técnicas que nos aportan confianza a pesar de ello. La automatización de procesos es uno de sus pilares. La finalidad de los distintos métodos que componen el agilismo es reducir los problemas clásicos de los programas de ordenador, a la par que dar más valor a las personas que componen el equipo de desarrollo del proyecto, satisfaciendo al cliente, al desarrollador y al analista de negocio.(Jurado, Gutiérrez, Reyes, 2010)

La esencia del agilismo es la habilidad para adaptarse a los cambios. Ejecutando las diversas técnicas que engloba, con la debida disciplina, se obtienen resultados satisfactorios sin lugar para el caos.

Labrin (2004) afirma:

> Una metodología tradicional potencia la planificación detallada y de largo alcance prácticamente de todo el desarrollo de software (ejemplo Modelo Cascada). En contraste, las metodologías ágiles proponen procesos que se adaptan y progresan con el cambio, llegando incluso hasta el punto de cambiar ellos mismos.

1.3.5 SCRUM como marco de trabajo ágil

Scrum fue diseñado para aumentar la velocidad de desarrollo, definir una cultura centrada en el rendimiento, apoyar la creación de valor, tener una buena comunicación de los resultados a todos los niveles, mejorar el desarrollo individual y la calidad de vida. Scrum ha ganado su popularidad en los últimos años y ha demostrado ser muy útil.(Srivastava, Bhardwaj, Saraswat, 2017)

Scrum al ser una metodología de desarrollo ágil tiene como finalidad la colaboración en equipo para el cumplimiento en el desarrollo de proyectos de software complejos(Levy, Romero, 2016), tiene como base la idea de creación de ciclos breves para el desarrollo, que comúnmente se llaman iteraciones y que en Scrum se denominan "Sprints".

- ✓ **Fases que definen el ciclo de desarrollo ágil**

a) Concepto: Se define de forma general las características del producto y se asigna el equipo que se encargara de su desarrollo.

b) Especulación: en esta fase se realizan disposiciones con la información obtenida y se establecen los límites que marcaran el desarrollo del producto, tales como costes y agendas.

Se construirá el producto a partir de las ideas principales y se comprueban las partes realizadas y su impacto en el entorno.

Esta fase se repite en cada iteración y consiste, en rasgos generales, en:

- ✓ Desarrollar y revisar los requisitos generales.
- ✓ Mantener la lista de las funcionalidades que se esperan.
- ✓ Plan de entrega. se establecen las fechas de las versiones, hitos e iteraciones. Medirá el esfuerzo realizado en el proyecto.

c) Exploración: Se incrementa el producto en el que se añaden las funcionalidades de la fase de especulación.

d) Revisión: El equipo revisa todo lo que se ha construido y se contrasta con el objetivo deseado.

e) Cierre: Se entregará en la fecha acordada una versión del producto deseado. Al tratarse de una versión, el cierre no indica que se ha finalizado el proyecto, sino que seguirá habiendo cambios, denominados "mantenimiento", que hará que el producto final se acerque al producto final deseado.(Trigas & Domingo, 2012)

- ✓ **Roles de Scrum**

En la TABLA 9 se presenta la constitución del equipo de Scrum (Scrum Team).

TABLA 10 Constitución del equipo SCRUM

Nombre	Definición
Dueño del producto (Product Owner):	Se encarga de la gestión expresando con claridad sus elementos y es la única persona que puede encomendar tareas al quipo de desarrollo.
El equipo de desarrollo (Development Team):	Es el equipo de trabajo que tiene los conocimientos necesarios para entregar un incremento de producto terminado en cada uno de los **sprint**[2].
Scrum Master:	Es la persona responsable que dirige al equipo de trabajo asegurándose de que el equipo Scrum trabaje ajustándose a la teoría, prácticas y reglas de Scrum

Fuente: (Levy, Romero, 2016)

- ✓ **Eventos de Scrum**

Sprint: Es el bloque de tiempo en el que el equipo Scrum realiza un incremento en el producto terminado y utilizable de software.(Levy, Romero, 2016) Un sprint a su vez está conformado por otros eventos como son:

a) **Reunión de planificación de Sprint (Sprint Planning Meeting):** se realiza la planificación de forma conjunta con todos los miembros del equipo para el trabajo a realizarse.
b) **Scrum diario (Daily Scrum):** es una reunión que tiene una duración de 15 minutos en la que los miembros del equipo sincronizan sus actividades y debaten sobre el progreso en el día anterior.
c) **Revisión del Sprint (Sprint Review):** al final de cada sprint se realiza una revisión del mismo para verificar el avance que se ha venido realizado y se efectúa una adecuación en la lista del producto en caso de ser necesario.
d) **Retrospectiva de Sprint (Sprint Retrospective):** el quipo Scrum debe de realizarse una autoevaluación con el fin de establecer mejoras para el posterior sprint.

- ✓ **Artefactos de Scrum**

[2] Iteración de tiempo en la que el equipo trabaja para convertir las historias de usuario en una versión del producto totalmente operativo.

Los artefactos de Scrum son los elementos que los miembros del equipo usan como apoyo para el cumplimiento del trabajo. En la TABLA 11 se presenta cada elemento.

TABLA 11 Artefactos de SCRUM

Nombre	Definición
Lista de producto (Product Backlog):	Es una lista ordenada de todo lo necesario que el cliente solicita.
Lista de tareas del Sprint (Sprint Backlog):	Es el conjunto de tareas que se va a realizar durante el sprint.
Incremento:	Es una parte añadida o desarrollada en un Sprint es decir una versión del producto resultante de lo trabajado.

Fuente: Propia

CAPÍTULO II

2. Desarrollo

2.1 Definición del proceso del Módulo de Auditoría

La complejidad y el progreso de los sistemas informáticos hace indispensable contar con una inspección que brinde información acerca de diferentes pistas de auditoria que se generan durante el proceso de uso del sistema, así como la evaluación del correcto funcionamiento y localización de ciertos puntos débiles que requieran el acogimiento de medidas correctivas y preventivas para impedir pérdida de información relevante que podría implicar ciertos percances en la toma de decisiones. (Chicano, 2014).

Para la realización del presente proyecto previamente se desarrolló el levantamiento del proceso de Actividades Docentes por lo que se vio necesario contar con el Módulo de Auditoría.

En la Fig. 8 se da a conocer el proceso del Módulo de Auditoría:

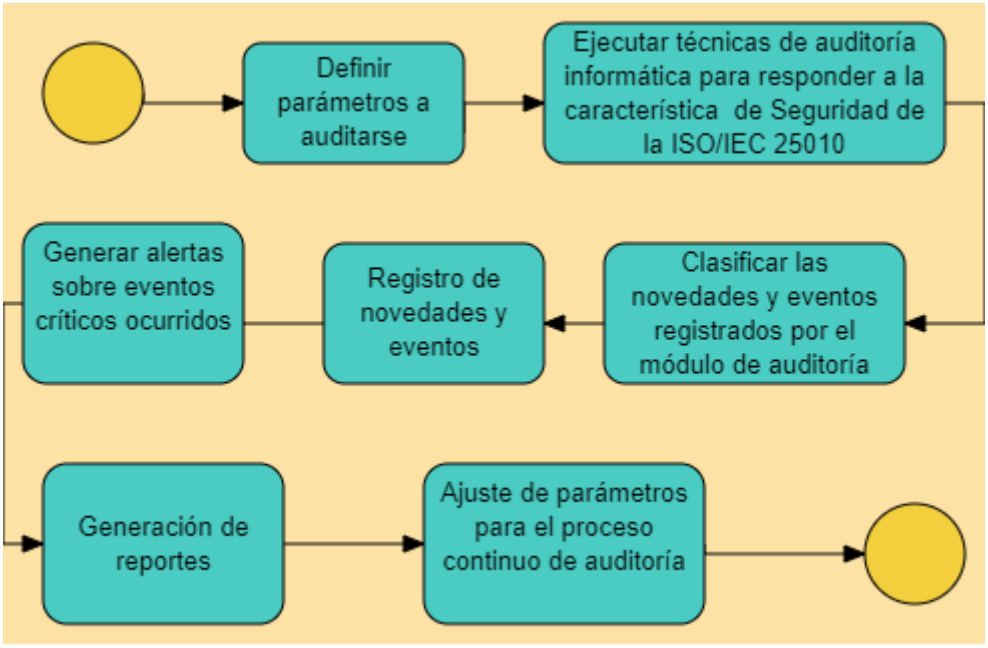


Fig. 8 Proceso del módulo de auditoría
Fuente: Propia

2.2 Definición de indicadores de calidad considerando la característica de Seguridad de la norma ISO/IEC 25010.

En la Fig. 9 se muestra de manera general como está distribuida la norma ISO/IEC 25010, la caracteristica en la cual nos vamos a apoyar es la de Seguridad puesto que contiene subcaracteriticas que son de vital importancia para obtener información consistente.

Fig. 9 Estructura General de la norma ISO/IEC 25010:2011
Fuente: Propia

La característica de Seguridad de la norma ISO/IEC 25010 contiene las siguientes subcaracterísticas: confidencialidad, integridad, no repudio, responsabilidad y autenticidad mismas que se aplicaron en base a ciertos indicadores que se presentan a continuación:

a) Confidencialidad

"La confidencialidad hace referencia a la protección de la información frente a su divulgación a entidades o individuos no autorizados (organizaciones, personas, máquinas, procesos). Nadie debe poder leer los datos a excepción de las entidades específicas previstas"(Soriano, 2014, p.32).

- ✓ **Capacidad de control de acceso**

El sistema cuenta con control de accesos, mediante el módulo de usuarios, roles y asignaciones pueden acceder a las páginas que correspondan dependiendo de los roles que tengan asignados.

Existe una persona encargada de administrar el servidor, para el buen funcionamiento de la aplicación web.

- ✓ **Encriptación de datos**

El sistema cuenta con un método seguro para garantizar una comunicación estable entre el navegador del usuario y el servidor web, mediante la encriptación de datos a través de HTTPS ya que es una versión segura del Protocolo de transferencia de Hipertexto (HTTP), la "S" significa "Seguro".

Las contraseñas de los usuarios se encuentran encriptadas, se utilizó SHA-256 (algoritmo de hash seguro) este algoritmo genera un hash de 256 bits (32 bytes) de tamaño fijo.

b) Integridad

La integridad de datos es la protección de los datos frente a la modificación, supresión, duplicación o reordenación realizada por entidades no autorizadas (organizaciones, personas, máquinas, procesos). Más concretamente, la integridad se refiere a la fiabilidad de los recursos de información. Una violación de la integridad se debe siempre a un ataque activo. La integridad de un sistema de información implica garantizar que no ha habido ninguna corrupción en los datos que han sido transmitidos o almacenados en el sistema, detectando cualquier posible manipulación. Para ello, es necesario el uso de técnicas criptográficas.(Soriano, 2014, p.33).

Indicadores evaluados:

- ✓ **Prevención de corrupción de datos**

La información de una entidad debe ser en lo más mínimo protegida y accesible solo a personal autorizado, cuando la información viaja desde el servidor hasta el cliente o viceversa la información va encriptada se asegura de que en el trayecto del viaje no se modificó dicha información entonces se considera que la información es integra, cuando llega al servidor llega a los EJB el EJB[3] toma la información y con JPA[4] guarda en la base de datos JPA es un framework de java ya probado mundialmente desarrollado por la empresa Oracle y da la garantía de mantener una información integra, una vez guardada la información en las tablas de la base de datos PostgreSQL este motor de base de datos tiene funciones de integridad de datos el siguiente link contiene información acerca de la integridad que tiene PostgreSQL: https://byspel.com/seguridad-de-bases-de-datos-postgresql/.

Una vez que la información se guarda en las tablas estas se almacenan en el disco duro, si por algún caso existe un daño en una parte del disco duro PostgreSQL puede detectar y la cantidad de archivos que posee, copea en otro espacio del disco duro y recupera la información, PostgreSQL es una base de datos bien avanzada.

Por otro lado, en el servidor que se instaló la aplicación web cuenta con cabezas de lectura y escritura en el disco y RAID[5] debido a esto también se cuenta con funciones de integridad en el hardware.

c) No repudio

Para tener comunicaciones seguras se requiere integrar un servicio encargado de generar evidencias digitales que permitan resolver posibles controversias surgidas en caso de errores de red o de mal comportamiento de alguna de las entidades que participan en el intercambio de información.

No repudio es el servicio de seguridad que utiliza estas evidencias para proporcionar protección contra la negación de una de las entidades de haber participado en la totalidad o parte de una comunicación.(Soriano, 2014, p.37).

[3] Los JavaBeans empresariales (Enterprise JavaBeans, EJB) son una tecnología (API) que forma parte del estándar de Java EE. Están diseñados para desarrollo y despliegue de aplicaciones (distribuidas) de negocio basadas en componentes del lado del servidor.
[4] JPA fue creado con Java EE 5 para resolver problemas de persistencia de datos. Proporciona un modelo de persistencia para mapear bases de datos relacionales
[5] RAID es la sigla para “Redundant Array of Independent Disks”. Su definición en español sería «Matriz Redundante de Discos Independientes» es un conjunto de discos rígidos que funcionan como si fueran uno solo.

Indicadores evaluados:

- ✓ **Eventos que requieran la propiedad de no- repudio**

La existencia de la bitácora permitirá contar con evidencias porque registra acciones que han realizado los usuarios que interactúan en el sistema, si por alguna razón un usuario realizó la eliminación de un dato la bitácora contendrá que usuario realizó dicha acción y no podrá negar, si existiera razones como: se realizó el hackeo de la contraseña, el sistema cuenta con contraseñas, base de datos y canal de información encriptados.

d) Responsabilidad

"Evalúa la capacidad de rastrear de forma inequívoca las acciones de una entidad"(Calabrese et al., 2017, p.4).

Indicadores evaluados:

- ✓ **Capacidad de auditoría de acceso**

Mediante el registro de las pistas de auditoría que se almacena en la bitácora se tiene el medio de rastrear las acciones realizadas en el sistema ya que registra desde el ingreso al sistema hasta la última acción ejecutada.

e) Autenticidad

"El servicio de autenticación se encarga de asegurar la identidad de las entidades que participan en la comunicación. Es decir, el servicio de autenticación evita que un usuario o entidad pueda suplantar la identidad de otro" (Soriano, 2014, p.35).

Indicadores evaluados:

- ✓ **Métodos de autenticación**

El proceso de autenticación corresponde a que los usuarios se identifiquen en el sistema mediante la obtención de credenciales que permitan el acceso mediante la autenticación simple que consta de dos elementos el identificador que es la cédula y la contraseña, este método de autenticación es el más común y el más conocido por su simplicidad y robusteza.

2.3 Metodología de desarrollo

La metodología de desarrollo que se está utilizando para el desarrollo del módulo de auditoría es SCRUM ya que es una metodología de desarrollo ágil que tiene como finalidad el cumplimiento en el desarrollo de proyectos de software.

2.4 Roles SCRUM

En la TABLA 9 muestra los roles SCRUM que se destinaron a las personas correspondientes de acuerdo con el proyecto realizado.

TABLA 12 Roles SCRUM

Persona	Descripción	Rol
Ing. Pedro Granda	Coordinador de la Carrera de Software de la Universidad Técnica de Norte	Propietario del Producto (Product Owner)
Ing. Mauricio Rea	Dirigente del Sistema SIAD, docente de la Universidad Técnica del Norte	Jefe Proyecto (Scrum Master)
Silvana Armas	Tesista	Equipo de Desarrollo (Development Team)

Fuente: Propia

2.5 Artefactos SCRUM

2.5.1 Matriz de planificación

PLANIFICACIÓN DE TRABAJOS DE DESARROLLO

Sprint: 1

Total horas: 28

Fecha Inicio SP1: 10/06/2019

Fecha Final SP1: 21/06/2019

TABLA 13 Planificación del sprint 1

Historia de usuario	Desarrollador	Fase Desarrollo	Tarea	Tipo	Tiempo Estimado (Horas)	Tiempo Real (Horas)	Estado
Matriz de planificación	Silvana Armas	Planificación	Formalización de la matriz de planificación	Nueva	2:00	1:00	HECHO
			Organización y análisis de los documentos para los Sprint 1 - 2 - 3		1:00	1:00	HECHO
Acta de constitución	Silvana Armas	Desarrollo	Recolección de información del proyecto (Datos, Patrocinadores)	Nueva	0:30	0:10	HECHO
			Identificación de Propósito y Justificación del proyecto		0:30	0:20	HECHO
			Descripción del Proyecto y Entregable		0:30	0:30	HECHO
			Descripción de Requerimientos de alto nivel (Requisitos de producto y proyecto)		1:00	1:00	HECHO
			Cronograma de hitos principales		0:30	0:20	HECHO
			Definición de Presupuesto estimado		0:30	0:20	HECHO
			Lista de Interesados (stakeholders)		0:20	0:10	HECHO
			Identificación de Requisitos de aprobación del proyecto		0:30	0:30	HECHO

			Asignación del Gerente de Proyecto y nivel de autoridad		0:10	0:10	HECHO
			Asignación de Personal y recursos preasignados		0:30	0:20	HECHO
Especificación de requisitos	Silvana Armas	Desarrollo	Desarrollo de la parte introductoria (Propósito - Alcance - Personal Involucrado - Definiciones, Abreviaturas - Referencias - Resumen)	Nueva	1:00	0:30	HECHO
			Desarrollo de la descripción general (Perspectiva del Producto - Funcionalidad del Producto - Características de los Usuarios - Restricciones - Suposiciones y dependencias - Evolución del Sistema)		1:00	0:40	HECHO
			Análisis de los requisitos específicos y requisitos de Interfaz (De Usuario - De Hardware - De Software - De Comunicación)	Nueva	1:00	1:25	HECHO
			Análisis de los requisitos funcionales		1:00	2:00	HECHO
			Análisis de los requisitos no funcionales (De Seguridad)	Nueva	1:00	0:35	HECHO
Cartillas de historias de usuario	Silvana Armas	Desarrollo	Creación de las historias de usuario: Módulo Auditoría	Nueva	5:00	4:00	HECHO
Backlog de historias de usuario	Silvana Armas	Desarrollo	Llenado de la matriz de H.U: Módulo de Auditoría	Nueva	5:00	4:40	HECHO
Casos de uso	Silvana Armas	Desarrollo	Desarrollo de los diagramas de casos de uso: Módulo de Auditoría	Nueva	5:00	4:35	HECHO
			TOTAL, SPRINT		28:00	24:15	

Fuente: Propia

Sprint: 2

Total, horas: 28

Fecha Inicio SP2: 24/06/2019

Fecha Final SP2: 05/07/2019

TABLA 14 Planificación sprint 2

Historia de usuario	Desarrollador	Fase Desarrollo	Tarea	Tipo	Tiempo Estimado (Horas)	Tiempo Real (Horas)	Estado
Diagrama conceptual	Silvana Armas	Desarrollo	Diagrama conceptuale: Módulo de Auditoría	Nueva	3:00	4:20	HECHO
Arquitectura de software	Silvana Armas	Desarrollo	Desarrollo de la parte introductoria y descripción de la parte arquitectónica	Nueva	1:00	0:30	HECHO
			Análisis de arquitectura y definición de las herramientas y tecnologías a utilizarse		1:00	0:50	HECHO
Wireframe	Silvana Armas	Desarrollo	Realización del prototipado: Módulo de Auditoría	Nueva	5:00	7:00	HECHO
Instalación y configuración de herramientas a usar	Silvana Armas	Desarrollo	Instalación de PostgreSQL, Servidor de Aplicaciones WildFly, IDE de desarrollo Eclipse, entre otros	Nueva	2:00	2:00	HECHO
			Configuración de WildFly y Jboos Tools en eclipse		1:00	0:30	HECHO
			Configuración de WildFly 14 en eclipse IDE		1:00	0:30	HECHO
Creación y configuración del proyecto	Silvana Armas	Desarrollo	Creación del proyecto en el WorkSpace	Nueva	1:00	0:30	HECHO
			Configuración de JPA y JSF		1:00	0:30	HECHO
			Estructuración de carpetas para el proyecto		1:00	0:45	HECHO
			Importación de librerías a utilizar		1:00	0:15	HECHO
			Mapeo de modelo de Base de Datos al proyecto		1:00	1:00	HECHO
Diseño de plantillas	Silvana Armas	Diseño	Investigación de plantillas	Nueva	2:00	5:00	HECHO
			Creación de plantilla		7:00	11:00	HECHO
			TOTAL, SPRINT		28:00	29:40	

Fuente: Propia

Sprint : 3

Total, horas: 28

Fecha Inicio SP3: 08/07/2019

FechaFinal SP3: 19/07/2019

TABLA 15 Planificación sprint 3

Historia de usuario	Desarrollador	Fase Desarrollo	Tarea	Tipo	Tiempo Estimado (Horas)	Tiempo Real (Horas)	Estado
Diseño y codificación general	Silvana Armas	Diseño	Diseño y Codificación de la pantalla principal del Módulo de Auditoría	Nueva	5:00	7:00	HECHO
		Desarrollo	Codificación del Manager y Controller		3:00	3:00	HECHO
			Vinculación de la pantalla principal con el Controller		3:00	2:30	HECHO
		Desarrollo	Creación y codificación de métodos para Manager y Controller del Módulo de Auditoría		13:00	12:15	HECHO
Plan de pruebas	Silvana Armas	Pruebas	Llenado de las matrices de pruebas	Nueva	1:00		HECHO
			Identificación de la herramienta de reportes y control de incidencias		1:00	0:30	HECHO
Informe del plan de pruebas	Silvana Armas	Pruebas	Llenado de la matriz de pruebas del Módulo de Auditoría	Nueva	1:00	1:00	HECHO
			Llenado de la lista de chequeo		1:00	1:00	HECHO
			TOTAL, SPRINT		28:00	27:15	

Fuente:Propia

2.5.2 Cartillas de Historia de Usuario

En la TABLA 16 muestra la Historia de Usuario Nro. 1: Pantalla principal del Módulo de Auditoría.

TABLA 16 Historia de usuario: pantalla principal del módulo de auditoría

Historia de Usuario

Número: 1 **Usuario:** Auditor

Nombre historia: Diseño Módulo Auditoría

Prioridad en negocio:
Alta
Puntos estimados: 3

Riesgo en desarrollo:
Alta
Sprint asignada: 3

Programador responsable: Silvana Armas

Descripción: El módulo de Auditoría, debe mostrar el listado de todas las pistas de auditoria posibles que se procesan en el sistema, los campos de la bitácora deben contener los siguientes atributos: id, fecha, nombre del usuario que genero la acción, el rol del usuario, clasificación de eventos, nombre del evento ocurrido, IP de donde se realizó el evento, nombre de la clase y método que se ejecutó para que se genere el evento.
Observaciones:
Solo el usuario auditor tendrá acceso al Módulo de Auditoría

Fuente: Propia

En la TABLA 17 muestra la Historia de Usuario Nro. 2: Prioridad de evento en la bitácora.

TABLA 17 Historia de usuario: prioridad de evento en la bitácora

Historia de Usuario

Número: 2 **Usuario:** Auditor

Nombre historia: Prioridad de evento

Prioridad en negocio:
Alta
Puntos estimados: 3

Riesgo en desarrollo:
Alta
Sprint asignada: 3

Programador responsable: Silvana Armas

Descripción: El módulo de Auditoría contará con prioridad de evento el mismo que contendrá el id y nombre, el campo nombre hará referencia a ciertos tipos de avisos que represente cada pista de auditoría siendo los siguientes: alto, medio y bajo.

Observaciones:
Dependiendo de la pista de auditoria se genera la prioridad de evento.

Fuente: Propia

En la TABLA 18 muestra la Historia de Usuario Nro. 3: Tipo de evento en la bitácora.

TABLA 18 Historia de usuario tipo de evento en la bitácora

Historia de Usuario	
Número: 3	**Usuario:** Auditor
Nombre historia: Tipo de evento	
Prioridad en negocio: Alta	**Riesgo en desarrollo:** Alta
Puntos estimados: 3	**Sprint asignada:** 3
Programador responsable: Silvana Armas	
Descripción: El módulo de Auditoría dispondrá de tipos de eventos mismo que contendrá el id y nombre, el nombre es el tipo de modulo al que corresponde cada pista de auditoria.	
Observaciones: *Los tipos de eventos serán registrados dependiendo de los módulos con los que cuenta el sistema.*	

Fuente: Propia

En la TABLA 19 muestra la Historia de Usuario Nro. 4: Búsqueda de pistas mediante un número de registro.

TABLA 19 Historia de usuario búsqueda de pistas mediante un número de registro

Historia de Usuario	
Número: 4	**Usuario:** Auditor
Nombre historia: Búsqueda de pistas mediante un número de registro	
Prioridad en negocio: Alta	**Riesgo en desarrollo:** Alta
Puntos estimados: 3	**Sprint asignada:** 3
Programador responsable: Silvana Armas	
Descripción: El módulo de Auditoría dispondrá de un campo que permitirá ingresar un número de registro a consultar.	
Observaciones: *Mediante el ingreso del número a consultar se desplegarán las pistas en la bitácora.*	

Fuente: Propia

En la TABLA 20 muestra la Historia de Usuario Nro. 5: Búsqueda de pistas por fechas

TABLA 20 Historia de usuario búsqueda de pistas por fechas

Historia de Usuario

Número: 5 **Usuario:** Auditor

Nombre historia: Búsqueda de pistas por fechas

Prioridad en negocio:
Alta

Riesgo en desarrollo:
Alta

Puntos estimados: 3

Sprint asignada: 3

Programador responsable: Silvana Armas

Descripción: El módulo de Auditoría dispondrá de dos campos que contendrán la fecha inicial y la fecha final, mediante las fechas ingresadas se podrá visualizar las pistas en la bitácora que están dentro de las fechas que se ingresó para consultar.

Observaciones:
Los tipos de eventos serán registrados dependiendo de los módulos con los que cuenta el sistema.

Fuente: Propia

2.5.3 Casos de Uso

En la Fig. 8 se presenta el caso de uso para el proceso de gestión de eventos por parte del administrador del sistema.

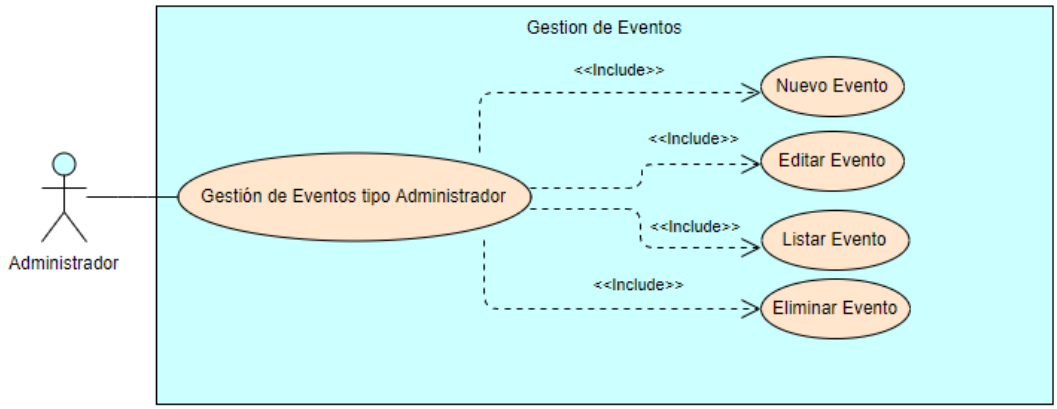


Fig. 10 Caso de uso 1 – gestión de eventos
Fuente: Propia

En la Fig. 9 se presenta el caso de uso para el proceso de gestión de prioridades por parte del administrador del sistema.

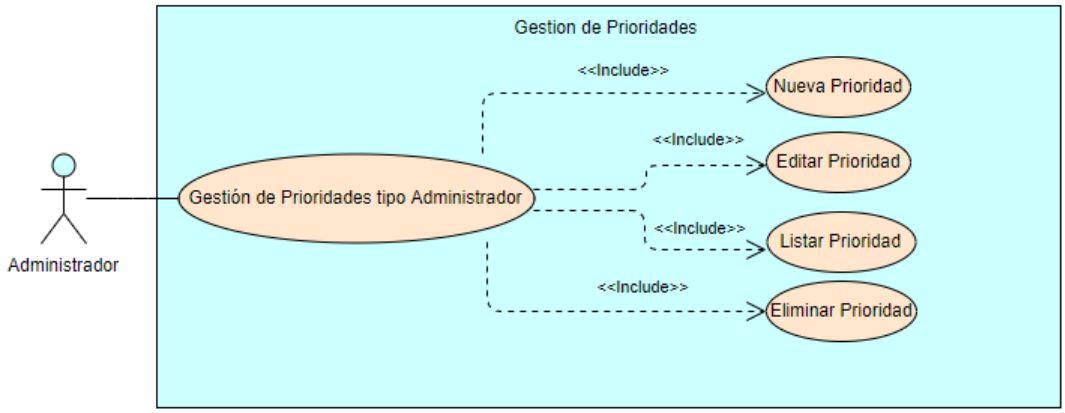


Fig. 11 Caso de uso 2 - gestión de prioridades
Fuente: Propia

En la Fig. 10 se presenta el caso de uso para el proceso de gestión de pistas de auditoria por parte del auditor del sistema.

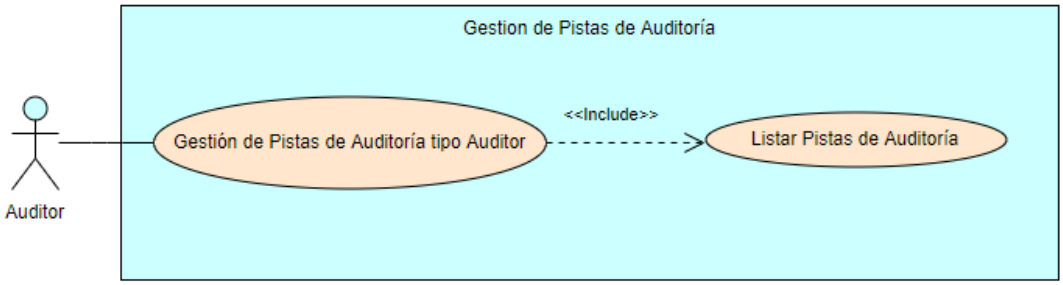


Fig. 12 Caso de uso 3 - gestión de pistas de auditoría
Fuente: Propia

En la Fig. 11 se presenta el caso de uso para el proceso de búsqueda de pistas de auditoria mediante el ingreso de un número de registro, así como también de una fecha inicial y una fecha final que desea consultar el auditor del sistema.

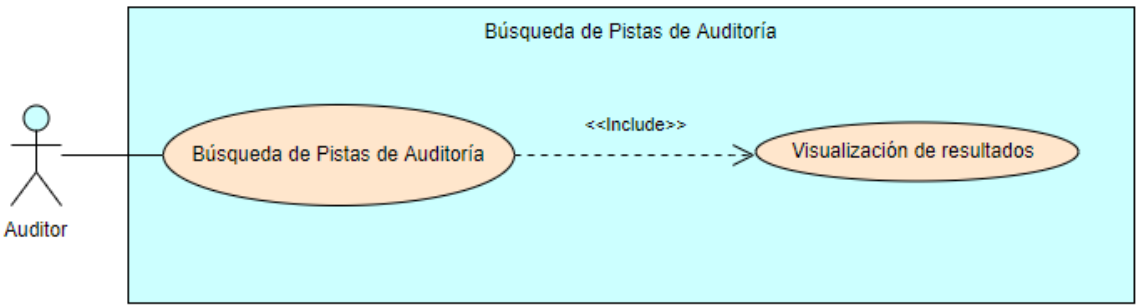


Fig. 13 Caso de uso 4 - búsqueda de pistas de auditoría
Fuente: Propia

2.5.4 Diagrama conceptual

En la Fig. 12 se presenta el Modelo de la Base de Datos del mòdulo de Auditoría.

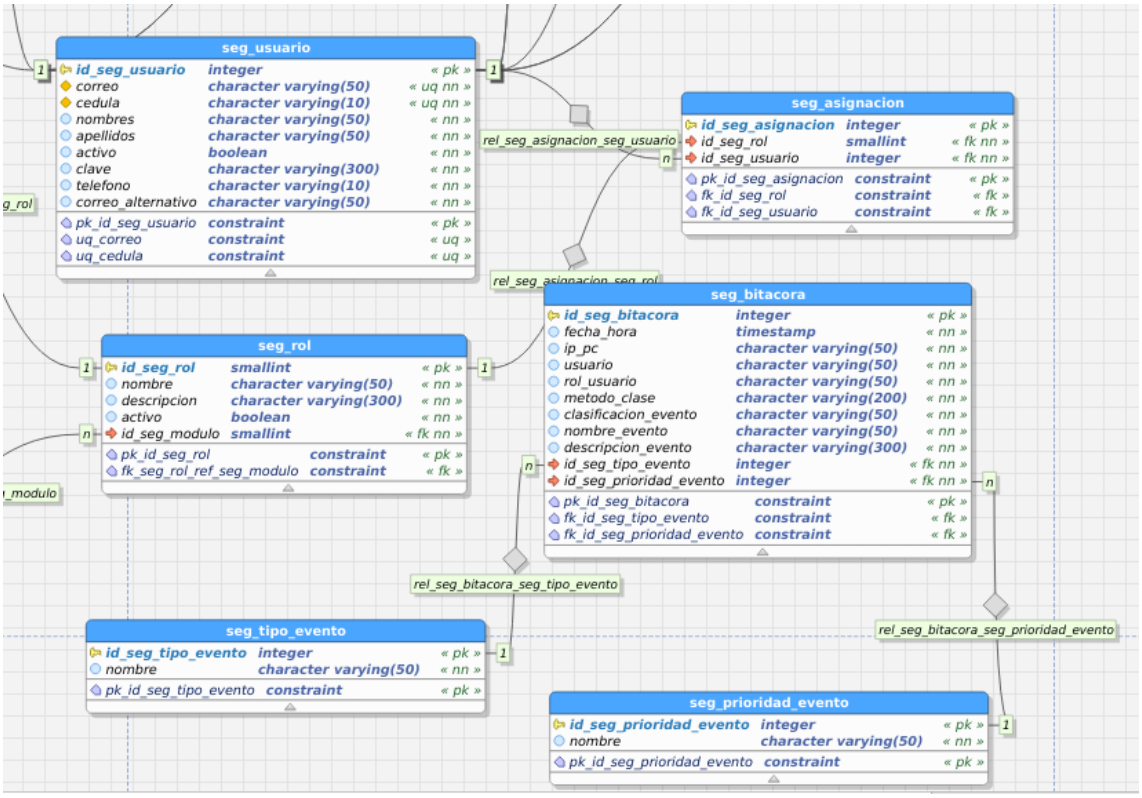


Fig. 14 Modelo de la base de datos del módulo de auditoría
Fuente: Propia

2.5.5 Arquitectura del Software

En el presente proyecto se utilizará como base la Arquitectura Java enterprise monolitica.

El patrón de arquitectura de software del proyecto será la Arquitectura Modelo Vista Controlador (MVC) (Model – View – Controller).

A continuación, la Fig. 13 muestra la Arquitectura del Patrón MVC.

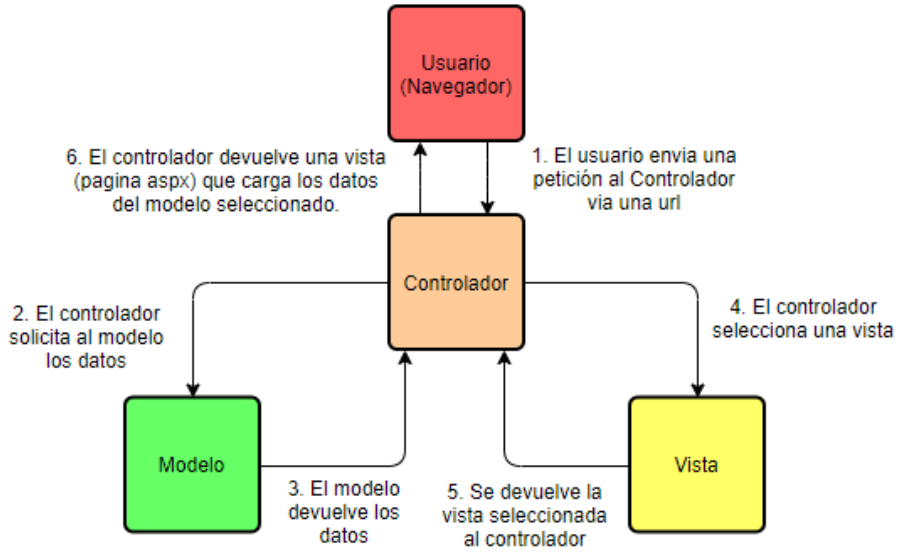


Fig. 15 Arquitectura del patrón MVC
Fuente: Propia

- **Herramientas y Tecnologías**

En la TABLA 21 se muestra las herramientas y tecnologías que se utilizaron para el desarrollo del Módulo de Auditoría.

TABLA 21 Herramientas y Tecnologías

Especificaciones	Herramientas
Entorno de desarrollo	IDE Eclipse JEE 2018-09
Entorno de producción	Servidor Web WildFly 14.0.1 Final
Base de Datos	PostgreSQL 9.6
Sistema Operativo	Windows 7, 8, 8.1, 10
Herramienta Case para manejo de la Base de Datos	pgAdmin 3
Metodología de Desarrollo	Scrum

Fuente: Propia

- **Diagrama de la Arquitectura de Software**

La Fig. 13 muestra el diagrama de la arquitectura de software del presente proyecto.

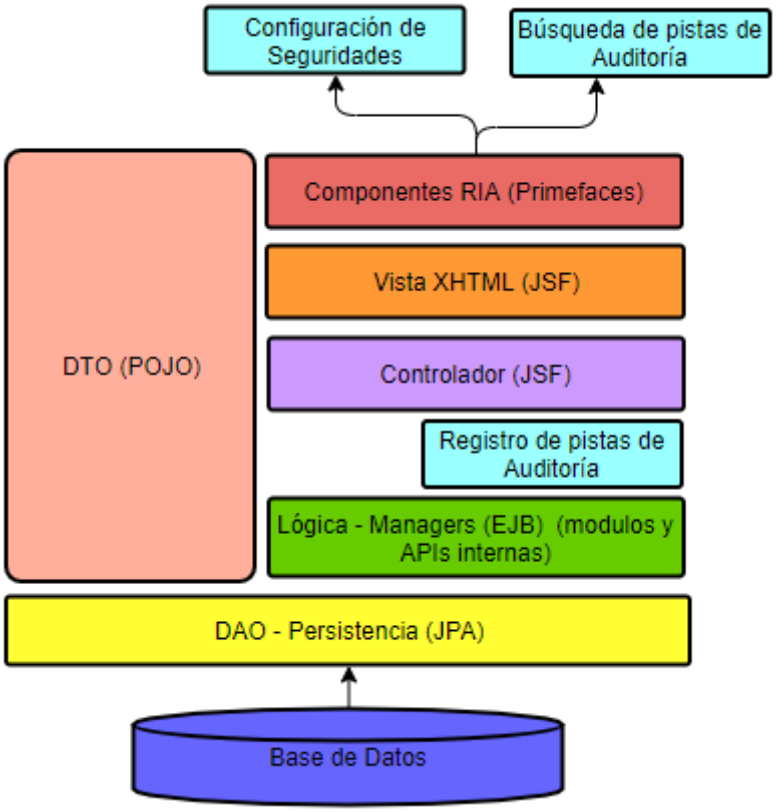


Fig. 16 Diagrama de la arquitectura de software
Fuente: Propia

2.5.6 Wireframe

Se realizó un prototipo para el desarrollo del módulo de Auditoría con la ayuda de la herramienta Adobe XD. En el presente proyecto se aplicó las siguientes interfaces.

- **Página principal Módulo de Auditoría**

En la Fig. 15 se muestra el wireframe de la página principal del módulo de Auditoría donde se puede observar una bitácora donde se almacena todas las pistas de auditoría que se genera en el sistema.

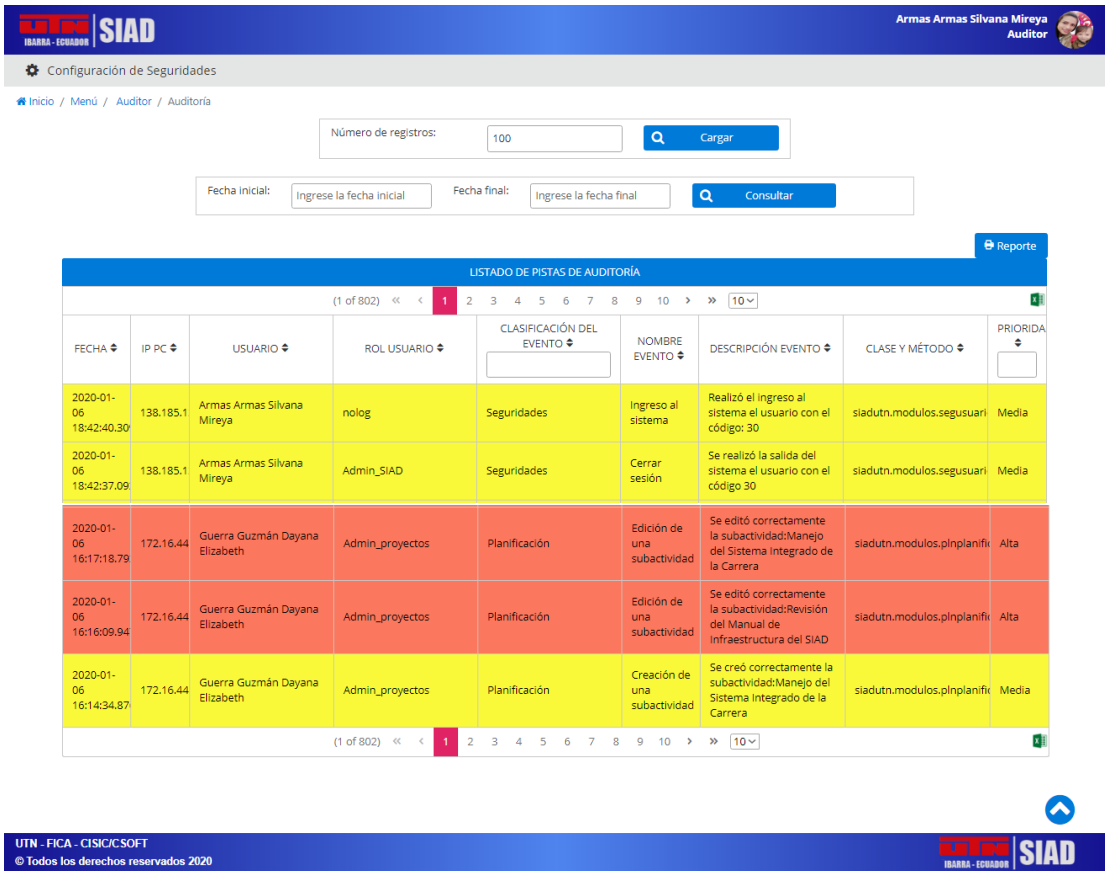


Fig. 17 Wireframe página principal del módulo de auditoría
Fuente: Propia

- **Configuración de Seguridades**

En la Fig. 16 se muestra el wireframe de la página de configuración de seguridades.

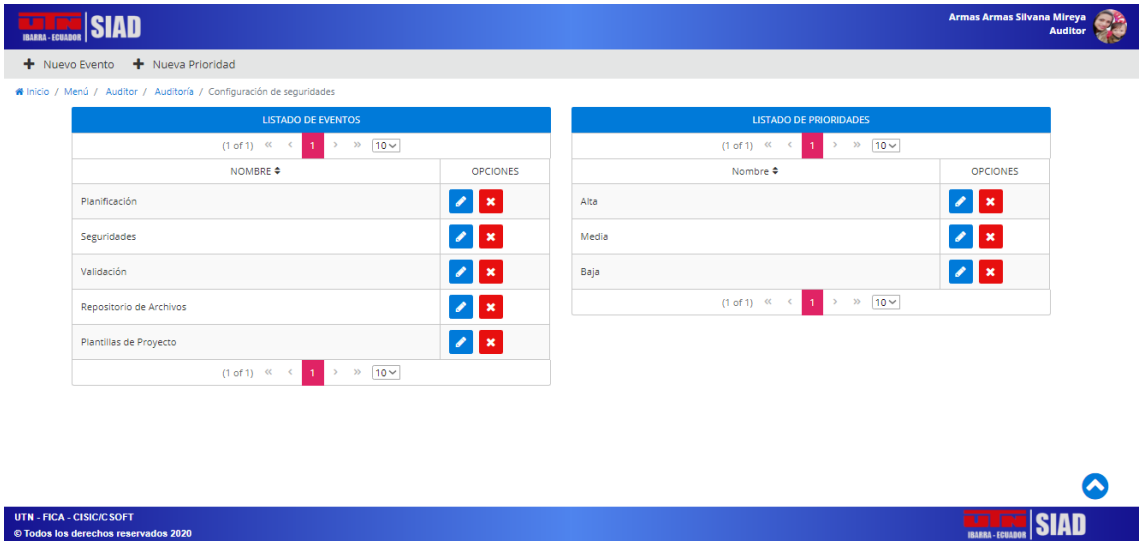


Fig. 18 Wireframe de la página de configuración de seguridades
Fuente: Propia

2.6 Resultado final del Módulo de Auditoria

En la Fig. 17 se muestra el inicio de sesión para ingresar al sistema SIAD, la cual contiene el ingreso del correo y su respectiva contraseña.

Fig. 19 Pantalla de inicio de sesión
Fuente: Propia

En la Fig. 18 muestra las opciones Usuarios, Roles y Asignaciones en las que el Administrador del sistema puede acceder.

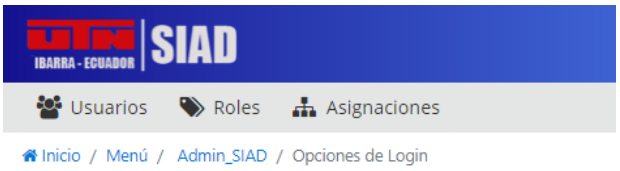


Fig. 20 Pantalla de opciones del administrador
Fuente: Propia

En la Fig. 19 muestra la administración de usuarios donde se puede visualizar la lista de los usuarios registrados en el sistema.

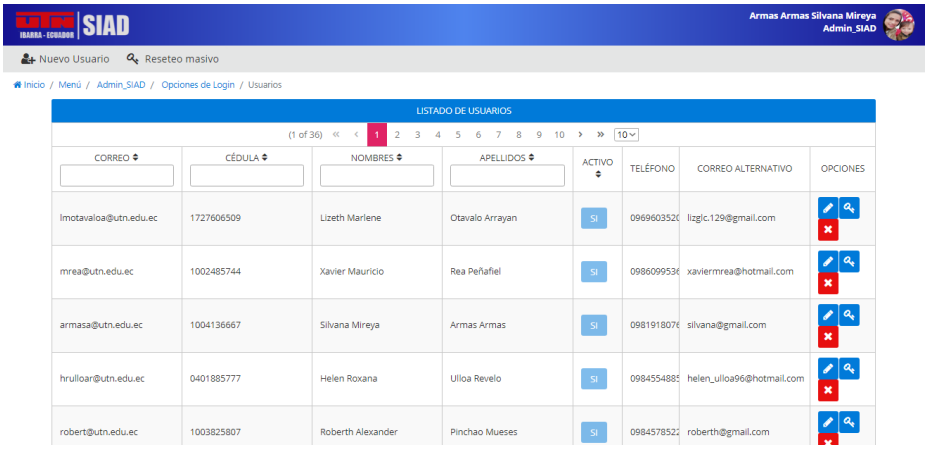


Fig. 21 Administración de usuarios
Fuente: Propia

En la Fig. 20 muestra la ventana de registro de usuarios, que tiene como campos obligatorios a llenar: correo, identificación sea nacional o extranjera, nombres, apellidos, estado, teléfono, correo alternativo y como opcional la fotografía.

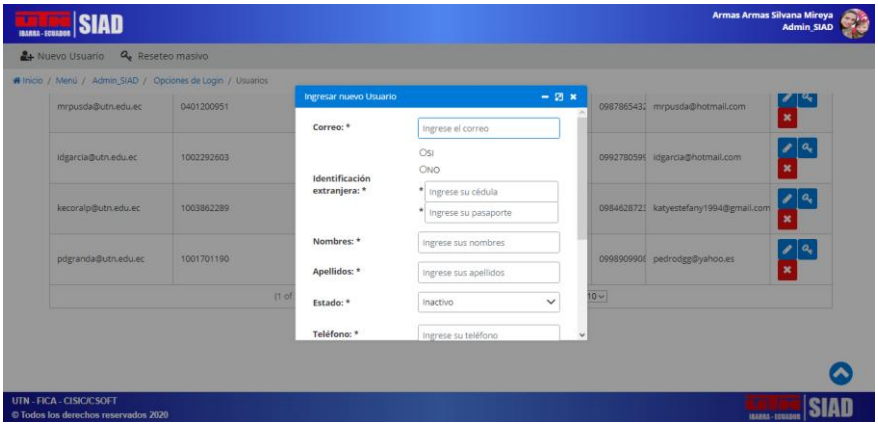


Fig. 22 Ventana de registro de usuarios
Fuente: Propia

En la Fig. 21 muestra la pantalla para poder realizar un reseteo masivo de claves, ingresando el Id inicial y el Id final.

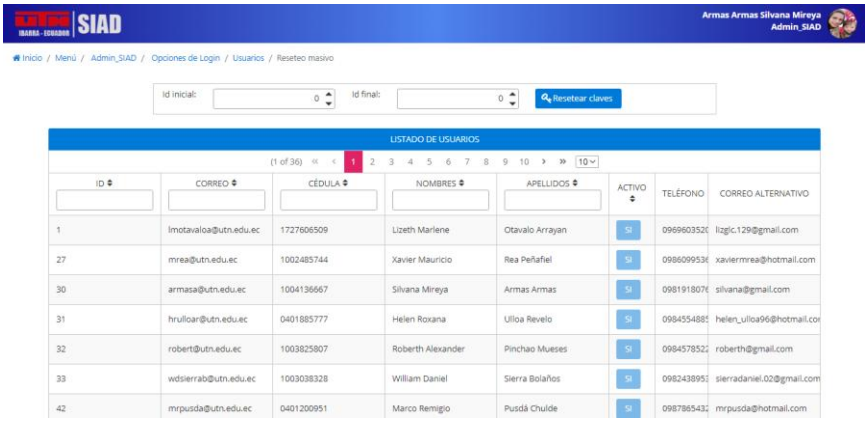


Fig. 23 Administración de reseteo masivo de claves
Fuente: Propia

En la Fig. 22 muestra la ventana para poder actualizar los datos del usuario.

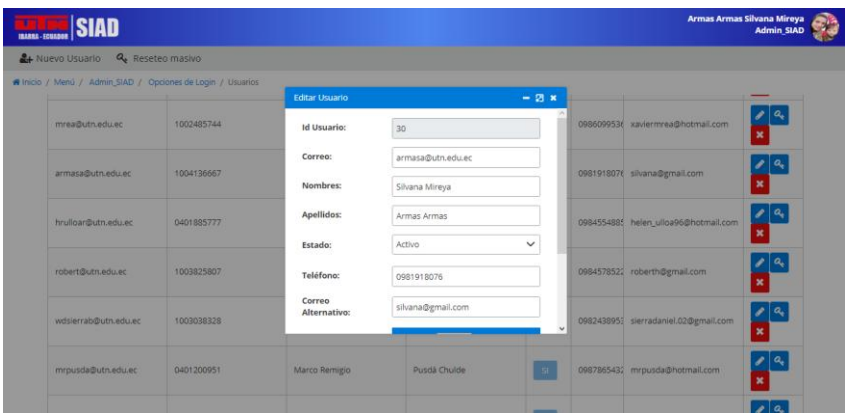


Fig. 24 Ventana de actualización de datos del usuario
Fuente: Propia

En la Fig. 23 muestra la administración de roles donde se puede visualizar la lista de los roles registrados en el sistema.

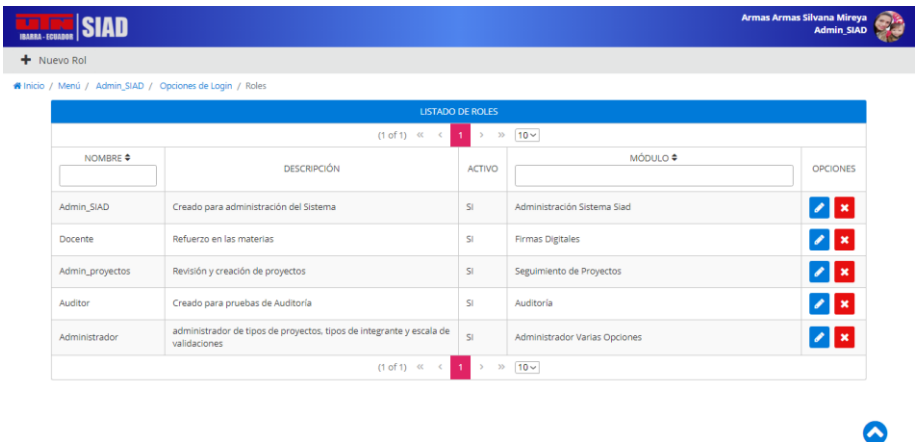


Fig. 25 Administración de roles
Fuente: Propia

En la Fig. 24 muestra la ventana de registro de roles, se tiene como campos obligatorios a llenar: nombre, descripción, estado y el módulo.

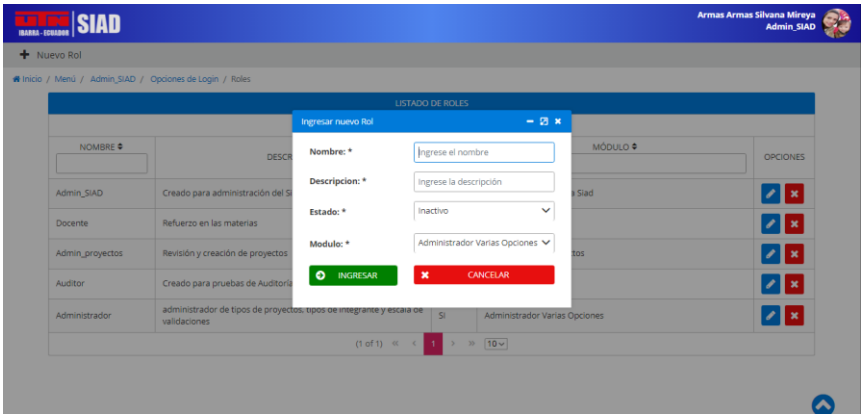


Fig. 26 Ventana de registro de roles
Fuente: Propia

En la Fig. 25 muestra la ventana para poder actualizar los datos de los roles.

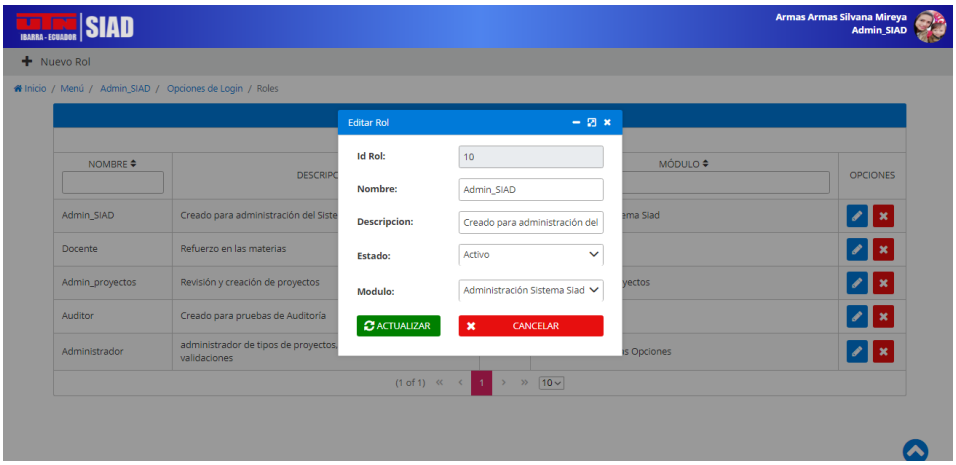


Fig. 27 Ventana de actualización de datos de los roles
Fuente: Propia

En la Fig. 25 muestra la la administración de asignaciones donde se puede visualizar la lista de las asignaciones registradas en el sistema.

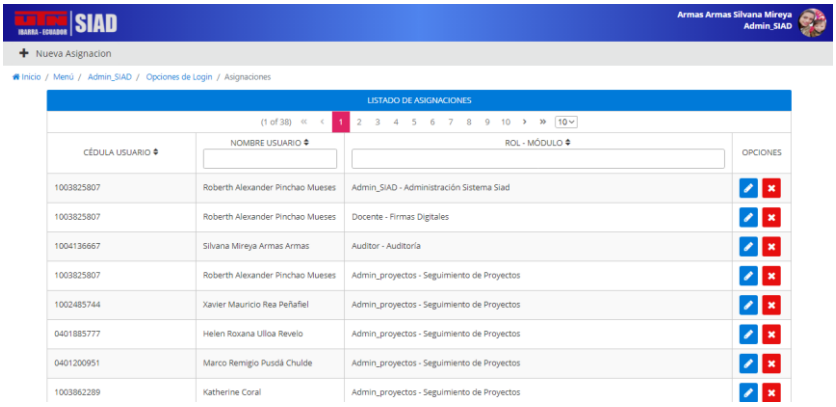


Fig. 28 Administración de asignaciones
Fuente: Propia

En la Figura 26 muestra la ventana de registro de asignaciones teniendo como campos obligatorios a llenar: usuario y rol.

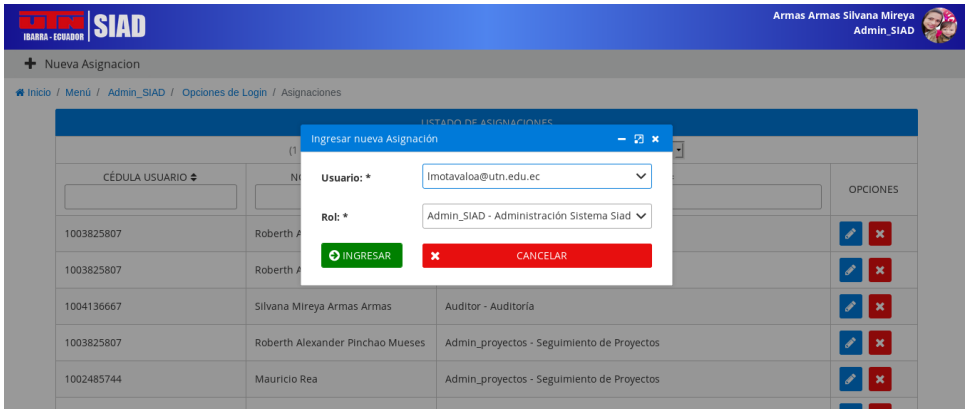


Fig. 29 Ventana de registro de una asignación
Fuente: Propia

En la Fig. 27 muestra la ventana para poder actualizar los datos de la asignación.

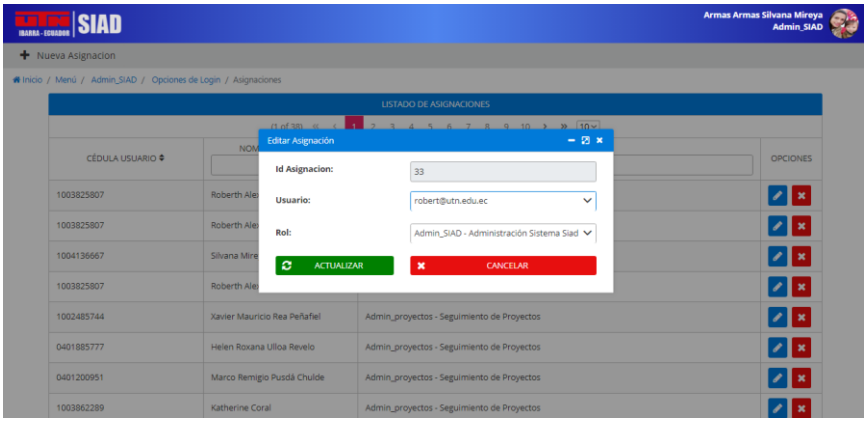


Fig. 30 Ventana de actualización de datos de la asignación
Fuente: Propia

En la Fig. 28 muestra la pantalla de configuración donde tiene las opciones cambiar contraseña y cambiar fotografía.

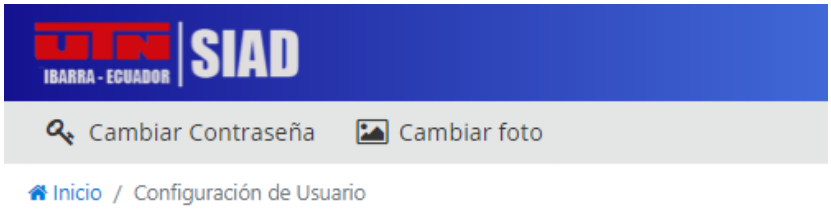


Fig. 31 Configuraciones
Fuente: Propia

En la Fig. 29 muestra la ventana para poder realizar el cambio de fotografía.

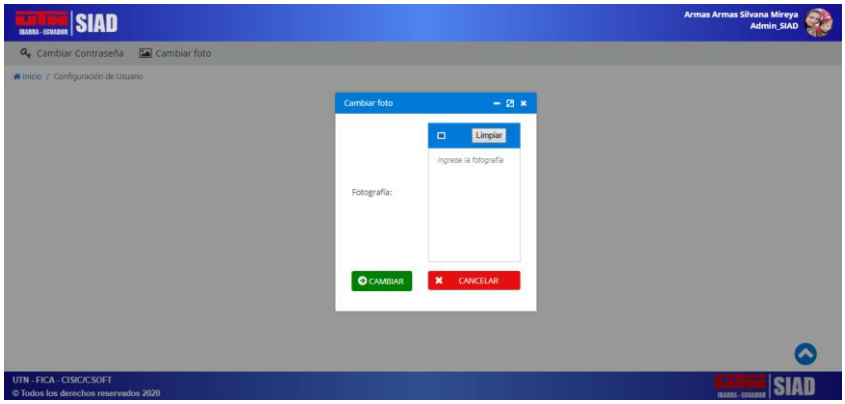


Fig. 32 Ventana cambio de fotografía
Fuente: Propia

En la Fig. 30 muestra la pantalla para realizar el cambio de contraseña, se tiene como campos a llenar: contraseña actual, nueva contraseña y repetición de la nueva contraseña. Teniendo como especificación la necesidad de establecer una contraseña segura. Especificando entre 8 y 256 caracteres, no incluir palabras ni nombres comunes y combinar letras mayúsculas, minúsculas, números y símbolos.

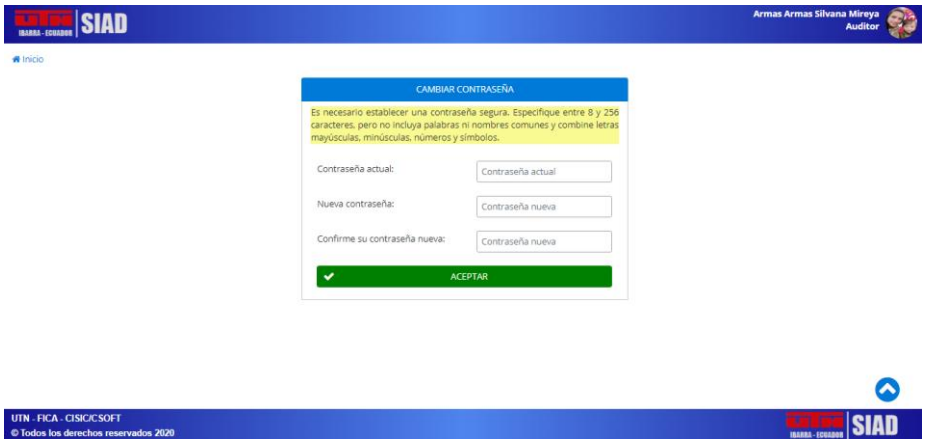


Fig. 33 Cambio de contraseña
Fuente: Propia

En la Fig. 31 se muestra la pantalla principal del módulo de auditoría donde se presenta la bitácora con las pistas registradas, donde se puede visualizar la fecha, IP-PC, usuario, rol del usuario, clasificación de evento, nombre del evento, descripción del evento, clase y método que se ejecutó para la generación de la pista y la prioridad.

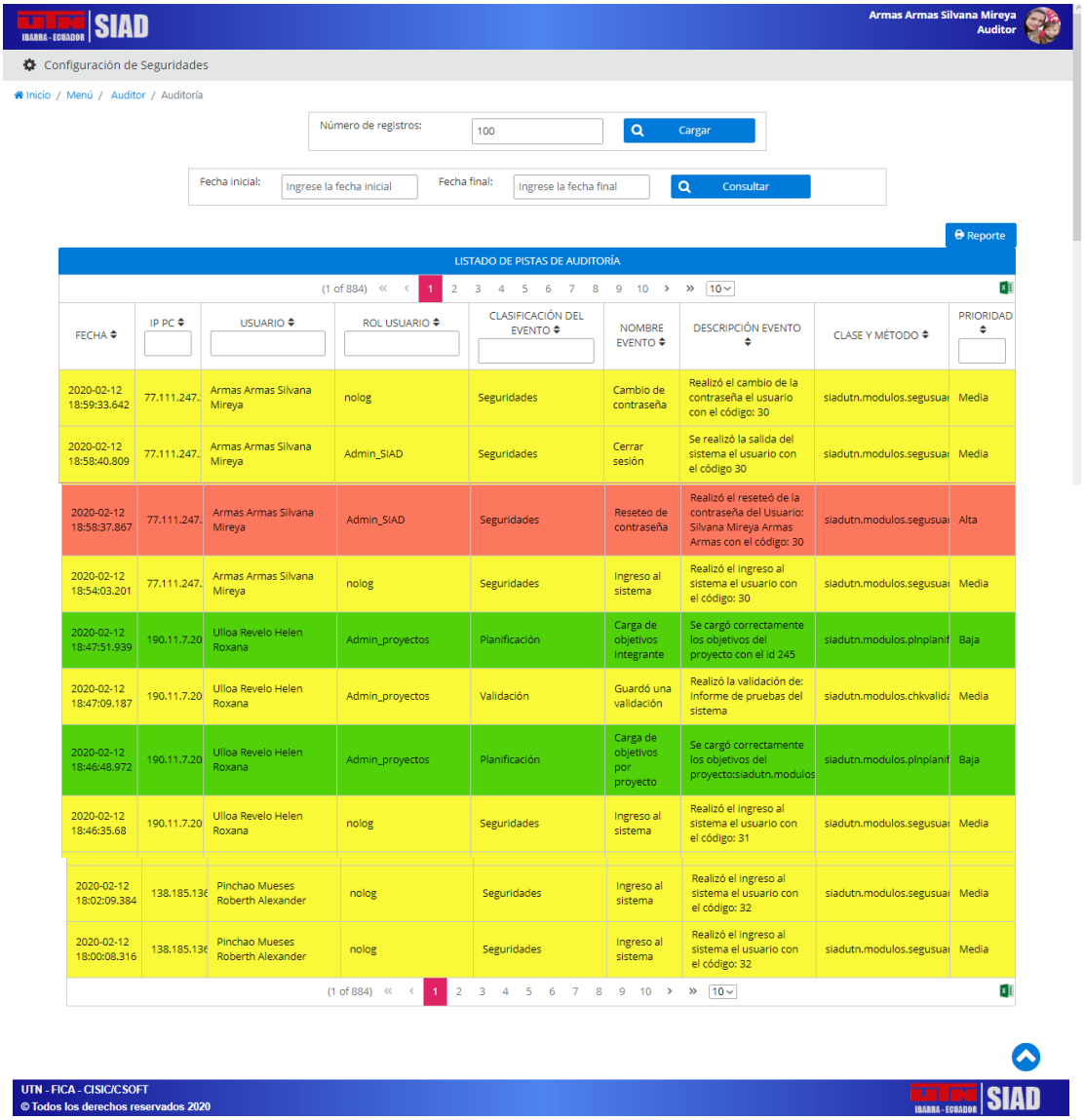


Fig. 34 Página principal del módulo de auditoria
Fuente: Propia

En la Fig. 32 muestra la pantalla de configuración de seguridades.

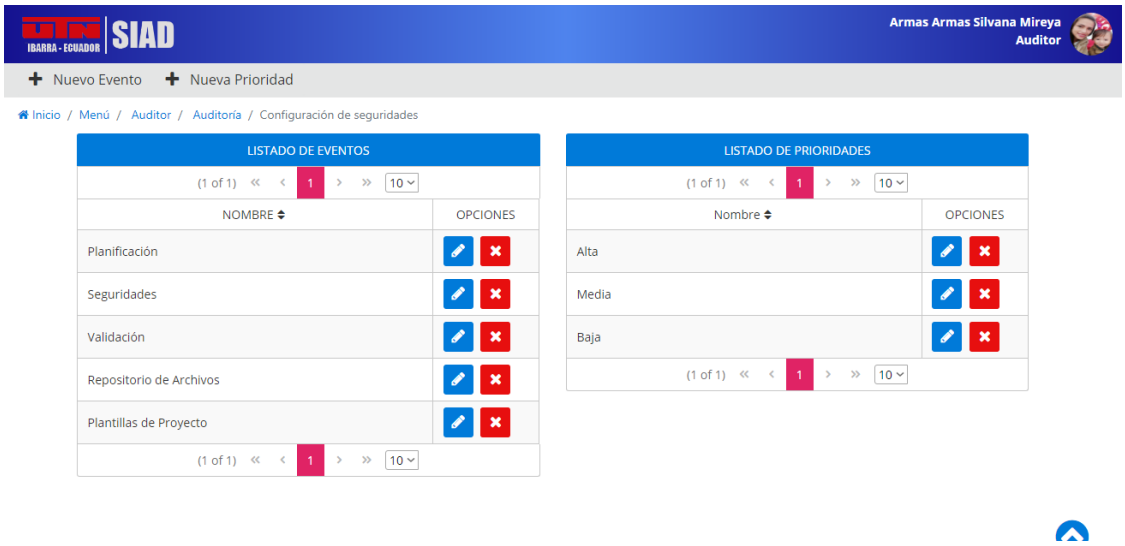


Fig. 35 Página de configuración de seguridades
Fuente: Propia

CAPÍTULO III

3 Validación de Resultados

3.1 Introducción

En esta sección se procede a evaluar el cumplimiento de la característica de Seguridad en el Sistema Integrado de Actividades Docentes de la Carrera CISIC – CISOFT de la Universidad Técnica del Norte.

Para realizar la evaluación se solicitó al Club Ethical Hacking de la Universidad Técnica del Norte que realizaran el checklist de las diferentes preguntas planteadas en el apartado 3.2; la misma que es el asistente para evaluar las características del producto de software, propuestas por la ISO/IEC 25010 mediante el enfoque GQM (Goal, Question, Metric). En el checklist se tomó en cuenta un conjunto de preguntas cuyas respuestas combinadas de forma lógica permiten obtener una métrica aplicable a las características que propone ISO/IEC 25010. Para este proyecto se consideró la característica de Seguridad, se definieron las métricas y luego se obtuvieron los resultados de la aplicación del sistema mencionado.

GQM es un método orientado a lograr una métrica que mida cierto objetivo de una manera determinada. En la TABLA 22 se muestra los niveles del modelo de medición:

TABLA 22 Niveles del modelo de medición GQM

Nivel	Definición
Nivel Conceptual (Goal/Objetivo):	se define un objetivo para un objeto, el cual puede ser un producto, un proceso o un recurso, con respecto a varios modelos de calidad, desde varios puntos de vista y relativo a un entorno particular.
Nivel Operativo (Question/Pregunta):	se refina un conjunto de preguntas a partir del objetivo, con el propósito de verificar su cumplimiento. Las preguntas tratan de caracterizar el objeto de medición (producto, proceso o recurso) con respecto a una cuestión de calidad seleccionada y determinar su calidad desde el punto de vista seleccionado.
Nivel Cuantitativo (Metric/Métrica):	se asocia un conjunto de métricas, que pueden ser objetivas o subjetivas, para cada pregunta, de modo de responder a cada una de un modo cuantitativo.

Fuente: (Calabrese, Muñoz, Pasini, Esponda, Boracchia, 2017)

Un modelo GQM se desarrolla identificando un conjunto de objetivos de calidad y/o productividad, a nivel corporativo, de división o de proyecto. A partir de esos objetivos y en base a modelos del objeto de medición, se elaboran preguntas que definen esos objetivos de la manera más completa posible. El siguiente paso consiste en especificar las medidas que deben ser tomadas para responder a esas preguntas y para realizar un seguimiento de la conformidad de los productos y procesos con los objetivos. Una vez especificadas las medidas, es necesario desarrollar los mecanismos de recopilación de

información, incluidos los mecanismos de validación y análisis.(Calabrese, Muñoz, Pasini, Esponda, Boracchia, 2017)

3.2 Cuestionario

El siguiente instrumento tuvo como fin recabar datos sobre la aplicación de la característica de calidad enfocado en la seguridad referente al cumplimiento de las subcaracterísticas Confidencialidad, Integridad, No-repudio, Responsabilidad y Autenticidad de la ISO/IEC 25010, en el SIAD. En la TABLA 23 se muestra la valoración del cuestionario emitido por el Club Ethical Hacking.

TABLA 23 Cuestionario para la característica de seguridad

NRO.	DETALLE	SI	NO
P1	¿Se requiere que la contraseña posea al menos 8 caracteres?	X	
P2	¿Se requiere que la contraseña posea letras mayúsculas y minúsculas?		X
P3	¿Se requiere que la contraseña posea números y letras?		X
P4	¿Se requiere que la contraseña posea caracteres especiales?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee los datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema permite que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X
P17	¿El sistema posee un historial de acciones realizadas?	X	

P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee un mecanismo criptográfico, como firma digital?		X
P20	¿El sistema solicita confirmación a la hora de realizar una acción?	X	
P21	¿El sistema posee una protección con certificados SSL?	X	
P22	¿El sistema da aviso cuando se accede desde una ubicación desconocida?		X
P23	¿El sistema informa vía mail las operaciones realizadas?	X	
P24	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P25	¿El sistema registra el tipo de navegador y sistema de operación utilizado para ingresar al sitio?		X
P26	¿El sistema registra la dirección IP desde la cual se ingresa al sitio?	X	
P27	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P28	¿El sistema posee un sistema de verificación en dos pasos?		X
P29	¿Es requerida una clave de segundo nivel para el ingreso al sistema?		X
P30	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P31	¿El sistema realiza una comprobación de identidad mediante tarjeta de coordenadas?		X
P32	¿El sistema realiza una comprobación de identidad mediante credenciales?	X	
P33	¿El sistema realiza una comprobación de identidad mediante una firma electrónica?		X

Fuente: Propia

3.3 Descripción de criterios de evaluación

En la TABLA 24 se muestra la descripción de criterios de evaluación (CE) para cada subcaracterística.

TABLA 24 Descripción de criterios de evaluación

ID	NOMBRE	DESCRIPCIÓN	FÓRMULA	PUNTOS
C-1	Conexiones seguras	Una conexión se considera segura si se utiliza HTTPS y si no se tienen redireccionamientos hacia sitios no seguros	P5 & ~P12 = V	1
C-2	Control de acceso	Se debe controlar que no se permita acceder a funcionalidades sin autorización, tampoco a la base de datos, al código de la aplicación ni a los servidores, físico ni remoto	si P7 | P8 | P9 | P10 | P11 = F	1
C-3	Encriptación de datos	Los datos de la base de datos deben estar encriptados	P6 = V	1

	Contraseña de bajo nivel	La contraseña se considera de bajo nivel si posee menos de 8 caracteres, no posee letras mayúsculas y minúsculas, no posee letras y números y no posee caracteres especiales	P1 | P2 | P3 | P4 = F	0
C-4	Contraseña de medio nivel	La contraseña se considera de medio nivel si posee al menos 8 caracteres o letras mayúsculas y minúsculas o letras y números o símbolos	P1 | P2 | P3 | P4 = V	0.5
	Contraseña de alto nivel	La contraseña se considera de alto nivel si posee al menos 8 caracteres, letras mayúsculas y minúsculas, letras y números y caracteres especiales	P1 & P2 & P3 & P4 = V	1
I-5	Prevención de accesos	Se debe prevenir que no se permita acceder a funcionalidades sin autorización, tampoco a la base de datos ni al código de la aplicación, y que no se permitan inyecciones SQL	P7 | P8 | P9 | P16 = F	1
I-6	Prevención de modificaciones	Se debe prevenir que no se permita modificar datos de la base de datos ni modificar el código de la aplicación sin autorización	P14 | P15 = F	1
I-7	Confirmación de datos	Se debe realizar una confirmación de registro por mail	P13 = V	1
NR-8	Operaciones realizadas	Se debe poseer un historial de acciones realizadas o las mismas deben ser enviadas por mail	P17 | P23 = V	1
NR-9	Mecanismos de cifrado	Se debe poseer un algoritmo de cifrado de datos o un mecanismo criptográfico, como firma digital, o una protección con certificados SSL	P18 | P19 | P21 = V	1
NR-10	Confirmación de acciones	Se debe solicitar una confirmación al realizar una determinada acción	P20 = V	1
NR-11	Registro de ubicación	Se debe informar si se accedió al sistema desde una ubicación desconocida	P22 = V	1
R-12	Registro de acciones y datos	Se debe poseer un historial de acciones realizadas, o un registro de fecha y hora de ingreso al sistema o de la dirección IP desde la cual se ingresa o del tipo de navegador y sistema de operación utilizado	P17 | P24 | P25 | P26 = V	1
R-13	Control de ubicación	Se debe dar aviso cuando se accede al sistema desde una ubicación desconocida	P22 = V	1
A-14	Comprobación de identidad	El sistema debe realizar una comprobación de identidad mediante alguno de los siguientes métodos: datos biométricos, tarjeta de coordenadas,	P27 | P30 | P31 | P32 | P33 = V	1

		credenciales, firma electrónica o certificado digital		
A-15	Comprobación es adicionales	Se debe poseer un sistema de verificación en dos pasos, o se debe requerir una clave de segundo nivel para el ingreso al sistema o una confirmación de registro mediante un mail	P28 | P29 | P13 = V	1

Fuente: (Calabrese, Muñoz, Pasini, Esponda, Boracchia, 2017)

3.4 Métricas para cada subcaracterística.

Se combinaron los CE para definir las métricas que satisfacen los objetivos de las subcaracterísticas. Para cada una se definió un nombre, un propósito, un método de aplicación, valores de entradas y formula aplicada.

3.4.1 Confidencialidad

En la TABLA 25 se muestra datos para la evaluación de la subcaracterística Confidencialidad.

TABLA 25 Valoración de la subcaracterística confidencialidad

Métrica: Confidencialidad	
Propósito:	¿Cuán eficiente es el sistema a la hora de proteger el acceso de datos e información no autorizados, ya sea accidental o deliberadamente?
Método de aplicación:	Contestar las preguntas de los CE correspondientes a la subcaracterística "Confidencialidad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. “Puntaje total” hace referencia al máximo puntaje que se puede obtener.
Entradas:	A = Puntaje obtenido. B = Puntaje total.
Fórmula:	X = A/B
Observaciones: Los CE a utilizar son: C-1, C-2, C-3 y C-4.	

Fuente: Propia

En la TABLA 26 se muestra la clasificación de preguntas que corresponden a la subcaracterística Confidencialidad.

TABLA 26 Clasificación de preguntas de la subcaracterística confidencialidad

ID	DETALLE	SI	NO
P5	¿El sistema utiliza conexión segura mediante HTTPS?	x	
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?	x	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		x

P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		x
P9	¿El sistema permite que cualquier persona tenga acceso al código del servidor de la aplicación?		x
P10	¿Cualquier persona tiene acceso al servidor físico?		x
P11	¿Cualquier persona tiene acceso al servidor remoto?		x
P6	¿La base de datos posee los datos encriptados?	x	
P1	¿Se requiere que la contraseña posea al menos 8 caracteres?	x	
P2	¿Se requiere que la contraseña posea letras mayúsculas y minúsculas?		x
P3	¿Se requiere que la contraseña posea números y letras?		x
P4	¿Se requiere que la contraseña posea caracteres especiales?	x	

Fuente: Propia

En la Fig. 36 nos muestra gráficamente los resultados de las preguntas que corresponden a la subcaracterística Confidencialidad.

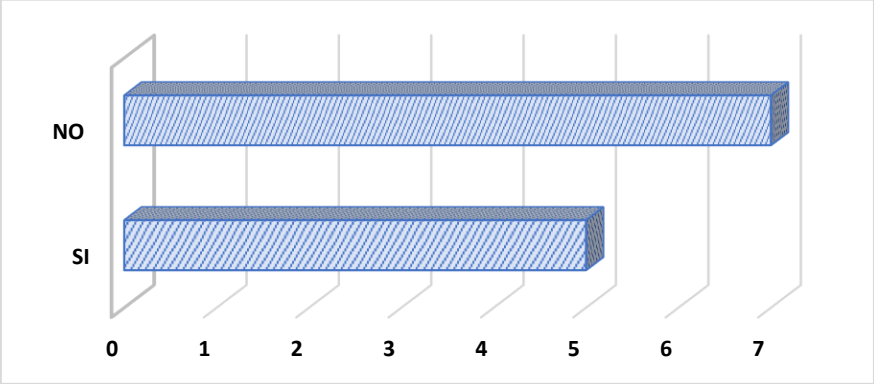


Fig. 36 Respuestas de la subcaracterística confidencialidad

Fuente: Propia

En la TABLA 27 se muestra la aplicación de las fórmulas para obtener la valoración de la subcaracterística Confidencialidad.

TABLA 27 Aplicación de la valoración subcaracterística confidencialidad

ID	NOMBRE	FORMULA	PUNTOS
C-1	Conexiones seguras	P5 &~P12=V	1
C-2	Control de acceso	P7|P8|P9|P10|P11=F	1
C-3	Encriptación de datos	P6=V	1
C-4	Contraseña de bajo nivel	P1|P2|P3|P4=V	0.5
Total, B=	4	Total, A =	3.5
		Formula X = A/B	3.5/4
		TOTAL	0.87
			Total, en porcentaje= 87%

Fuente: Propia

3.4.2 Integridad

En la TABLA 28 se muestra datos para la evaluación de la subcaracterística Integridad.

TABLA 28 Valoración de la subcaracterística integridad

Métrica: Integridad	
Propósito:	¿Cuán capaz es el sistema a la hora de prevenir accesos o modificaciones no autorizados a datos o programas de ordenador?
Método de aplicación:	Contestar las preguntas de los CE correspondientes a la subcaracterística "Integridad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. “Puntaje total” hace referencia al máximo puntaje que se puede obtener.
Entradas:	A = Puntaje obtenido. B = Puntaje total.
Fórmula:	X = A/B
Observaciones: Los CE a utilizar son: I-5, I-6 e I-7.	

Fuente: Propia

En la TABLA 29 se muestra la clasificación de preguntas que corresponden a la subcaracterística Integridad.

TABLA 29 Clasificación de preguntas de la subcaracterística Integridad

ID	DETALLE	SI	NO
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X
P14	¿El sistema permite que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	

Fuente: Propia

En la Fig. 37 nos muestra gráficamente los resultados de las preguntas que corresponden a la subcaracterística Integridad.

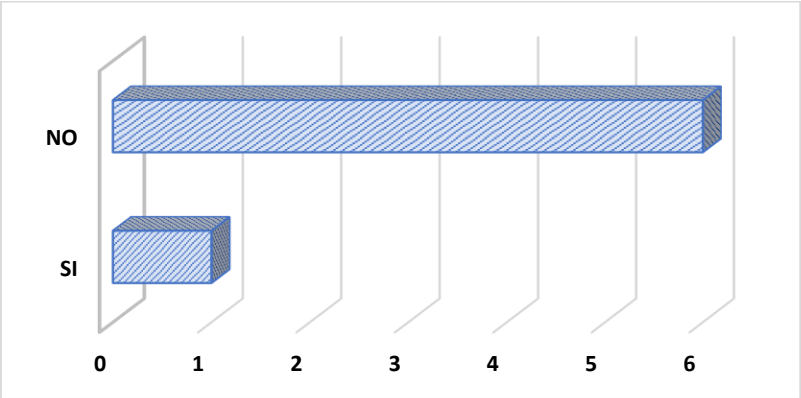


Fig. 37 Respuestas de la subcaracterística integridad
Fuente: Propia

En la TABLA 30 se muestra la aplicación de las fórmulas para obtener la valoración de la subcaracterística Integridad.

TABLA 30 Aplicación de la valoración subcaracterística confidencialidad

ID	NOMBRE	FORMULA	PUNTOS
I-5	Prevención de accesos	P7 | P8 | P9 | P16 = F	1
I-6	Prevención de modificaciones	P14 | P15 = F	1
I-7	Confirmación de datos	P13 = V	1
Total, B=	3	Total, A =	3
		Formula X = A/B	3/3
		TOTAL	1
			Total, en porcentaje= 100%

Fuente: Propia

3.4.3 No-repudio

En la TABLA 31 se muestra datos para la evaluación de la subcaracterística No-repudio.

TABLA 31 Valoración de la subcaracterística No-repudio

Métrica: No-repudio	
Propósito:	¿Cuán capaz es el sistema de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no puedan ser repudiados posteriormente?
Método de aplicación:	Contestar las preguntas de los CE correspondientes a la subcaracterística "No-Repudio" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. “Puntaje total” hace referencia al máximo puntaje que se puede obtener.
Entradas:	A = Puntaje obtenido. B = Puntaje total.
Fórmula:	X = A/B
Observaciones: Los CE a utilizar son: NR-8, NR-9, NR-10 y NR-11.	

Fuente: Propia

En la TABLA 32 se muestra la clasificación de preguntas que corresponden a la subcaracterística No-repudio.

TABLA 32 Clasificación de preguntas de la subcaracterística No-repudio

ID	DETALLE	SI	NO
P17	¿El sistema posee un historial de acciones realizadas?	X	
P23	¿El sistema informa vía mail las operaciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee un mecanismo criptográfico, como firma digital?		X
P21	¿El sistema posee una protección con certificados SSL?	X	
P20	¿El sistema solicita confirmación a la hora de realizar una acción?	X	
P22	¿El sistema da aviso cuando se accede desde una ubicación desconocida?		X

Fuente: Propia

En la Fig. 38 nos muestra gráficamente los resultados de las preguntas que corresponden a la subcaracterística No-Repudio.

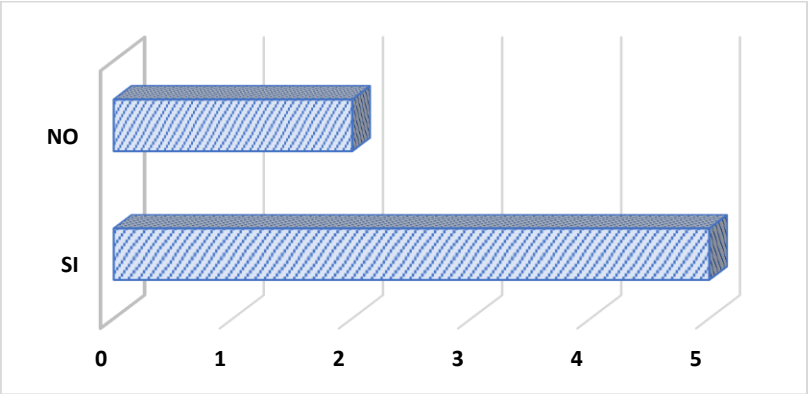


Fig. 38 Respuestas de la subcaracterística no-repudio
Fuente: Propia

En la TABLA 33 se muestra la aplicación de las fórmulas para obtener la valoración de la subcaracterística No-repudio.

TABLA 33 Aplicación de la valoración subcaracterística No-repudio

ID	NOMBRE	FORMULA	PUNTOS
NR-8	Operaciones realizadas	P17 | P23 = V	1
NR-9	Mecanismos de cifrado	P18 | P19 | P21 = V	1
NR-10	Confirmación de acciones	P20 = V	1
NR-11	Registro de ubicación	P22 = V	0
Total, B=	4	Total, A =	3
		Formula X = A/B	3/4
		TOTAL	0.75
			Total, en porcentaje= 75%

Fuente: Propia

3.4.4 Responsabilidad

En la TABLA 34 se muestra datos para la evaluación de la subcaracterística Responsabilidad.

TABLA 34 Valoración de la subcaracterística Responsabilidad

Métrica: Responsabilidad	
Propósito:	¿Cuán capaz es el sistema de rastrear de forma inequívoca las acciones de una entidad?
Método de aplicación:	Contestar las preguntas de los CE correspondientes a la subcaracterística "Responsabilidad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. “Puntaje total” hace referencia al máximo puntaje que se puede obtener.
Entradas:	A = Puntaje obtenido. B = Puntaje total.
Fórmula:	X = A/B
Observaciones: Los CE a utilizar son: R-12 y R-13.	

Fuente: Propia

En la TABLA 35 se muestra la clasificación de preguntas que corresponden a la subcaracterística Responsabilidad.

TABLA 35 Clasificación de preguntas de la subcaracterística Responsabilidad

ID	DETALLE	SI	NO
P17	¿El sistema posee un historial de acciones realizadas?	X	
P24	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P25	¿El sistema registra el tipo de navegador y sistema de operación utilizado para ingresar al sitio?		X
P26	¿El sistema registra la dirección IP desde la cual se ingresa al sitio?	X	
P22	¿El sistema da aviso cuando se accede desde una ubicación desconocida?		X

Fuente: Propia

En la Fig. 39 nos muestra gráficamente los resultados de las preguntas que corresponden a la subcaracterística Responsabilidad.

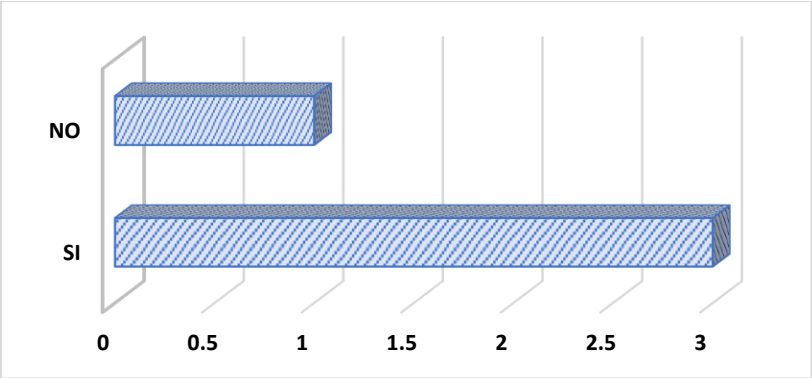


Fig. 39 Respuestas de la subcaracterística Responsabilidad
Fuente: Propia

En la TABLA 36 se muestra la aplicación de las fórmulas para obtener la valoración de la subcaracterística Responsabilidad.

TABLA 36 Aplicación de la valoración subcaracterística Responsabilidad

ID	NOMBRE	FORMULA	PUNTOS
R-12	Registro de acciones y datos	P22 = V	0
R-13	Control de ubicación	P27 | P30 | P31 | P32 | P33 = V	1
Total, B=	2	Total, A =	2
		Formula X = A/B	1/2
		TOTAL	0.5
			Total, en porcentaje= 50%

Fuente: Propia

3.4.5 Autenticidad

En la TABLA 37 se muestra datos para la evaluación de la subcaracterística Autenticidad.

TABLA 37 Valoración de la subcaracterística Autenticidad

Métrica: Autenticidad	
Propósito:	¿Cuán capaz es el sistema de demostrar la identidad de un sujeto o un recurso?
Método de aplicación:	Contestar las preguntas de los CE correspondientes a la subcaracterística "Autenticidad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. “Puntaje total” hace referencia al máximo puntaje que se puede obtener.
Entradas:	A = Puntaje obtenido. B = Puntaje total.
Fórmula:	X = A/B
Observaciones: Los CE a utilizar son: A14 y A15.	

Fuente: Propia

En la TABLA 38 se muestra la clasificación de preguntas que corresponden a la subcaracterística Autenticidad.

TABLA 38 Clasificación de preguntas de la subcaracterística Autenticidad

ID	DETALLE	SI	NO
P28	¿El sistema posee un sistema de verificación en dos pasos?		X
P29	¿Es requerida una clave de segundo nivel para el ingreso al sistema?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P27	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P31	¿El sistema realiza una comprobación de identidad mediante tarjeta de coordenadas?		X
P32	¿El sistema realiza una comprobación de identidad mediante credenciales?	X	
P33	¿El sistema realiza una comprobación de identidad mediante una firma electrónica?		X

Fuente: Propia

En la Fig. 40 nos muestra gráficamente los resultados de las preguntas que corresponden a la subcaracterística Autenticidad.

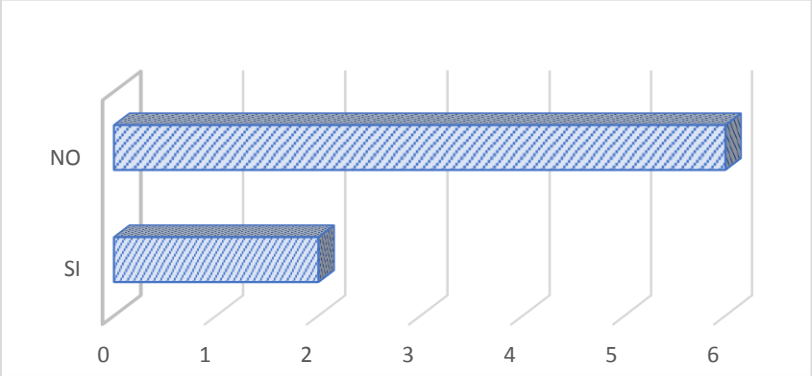


Fig. 40 Respuestas de la subcaracterística autenticidad
Fuente: Propia

En la TABLA 39 se muestra la aplicación de las fórmulas para obtener la valoración de la subcaracterística Autenticidad.

TABLA 39 Aplicación de la valoración subcaracterística Autenticidad

ID	NOMBRE	FORMULA	PUNTOS
A-14	Comprobación de identidad	P27 | P30 | P31 | P32 | P33 = V	1
A-15	Comprobación es adicionales	P28 | P29 | P13 = V	1
Total, B=	2	Total, A =	2
		Formula X = A/B	2/2
		TOTAL	1
			Total, en porcentaje= 100%

Fuente: Propia

3.5 Especificación de la evaluación

En la TABLA 40 se muestra los criterios de aceptación para las subcaracterísticas:

TABLA 40 Criterios de aceptación

CRITERIOS DE ACEPTACIÓN	
Inaceptable:	0 <= X < 40
Mínimamente aceptable:	40 <= X < 60
Rango objetivo:	60 <= X < 90
Excede los requerimientos:	90 <= X <=100

Fuente: (Calabrese, Muñoz, Pasini, Esponda, Boracchia, 2017)

El propósito se considerará aceptado si todas las subcaracterísticas se encuentran entre los rangos mínimamente aceptables y excede los requerimientos.

3.6 Ejecución de la evaluación

Se ejecutó la evaluación según lo planificado, en la TABLA 41 se muestra los resultados obtenidos:

TABLA 41 Resultados de la evaluación

Subcaracterísticas	Porcentaje Obtenido	Criterios de Aceptación
Confidencialidad	87%	Rango Objetivo
Integridad	100%	Excede los requerimientos
No-Repudio	75%	Rango Objetivo
Responsabilidad	50%	Mínimamente aceptable
Autenticidad	100%	Excede los requerimientos

Fuente: Propia

3.7 Análisis de la característica de Seguridad

Se considera que el SIAD cumple con el propósito de la evaluación ya que la subcaracterística: Confidencialidad se encuentra en el criterio "*Rango objetivo*" (87%), No-Repudio en el criterio "*Rango Objetivo*" (75%), Integridad y Autenticidad en el criterio "*Excede los requerimientos*" (100%) y Responsabilidad en el criterio "*Mínimamente aceptable*" (50%).

Para que las subcaracterísticas Confidencialidad, No-Repudio, y Responsabilidad se encuentren en el criterio *"Excede los requerimientos"* se necesita implementar:

- ✓ En la subcaracterística Confidencialidad: se debe implementar una contraseña de alto nivel, esto quiere decir que la contraseña posee al menos 8 caracteres, letras mayúsculas y minúsculas, letras y números y caracteres especiales.
- ✓ En las subcaracterísticas No-Repudio y Responsabilidad se debe implementar el registro de ubicación es decir se debe informar si se accedió al sistema desde una ubicación desconocida.

En la Fig. 41 se muestra gráficamente los resultados de la evaluación de las subcaracterísticas de la Seguridad.

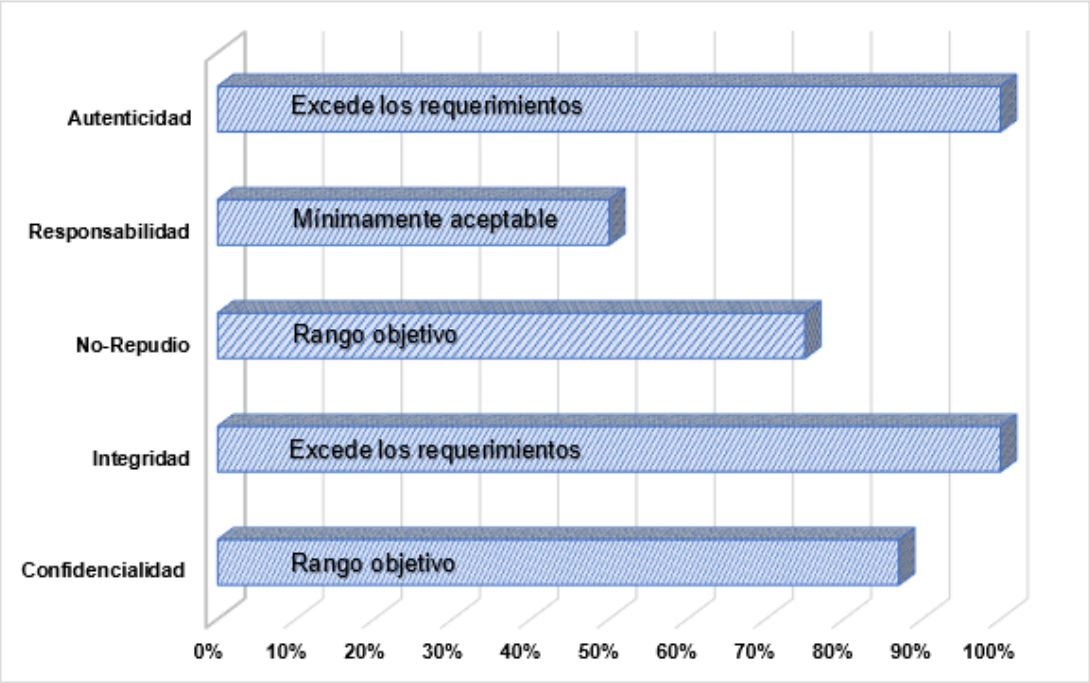


Fig. 41 Evaluación de la característica seguridad
Fuente: Propia

CONCLUSIONES

- Al finalizar la investigación de la característica de Seguridad de la ISO/IEC 25010 y las pistas de auditoria se adquirió una base conceptual para el desarrollo del Módulo de Auditoría.
- La adaptación de la característica de Seguridad del estándar ISO/IEC 25010 en el SIAD permite proteger la información de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos.
- En todos los sistemas se debe contar con una bitácora de pistas de auditoría ya que, permite tener un mejor criterio a la hora de determinar y esclarecer ciertos hallazgos que influyan en la toma de decisiones de la organización.
- La aplicación de la característica de Seguridad de la ISO / IEC 25010 cumple con el propósito de evaluación en el SIAD, debido a que la subcaracterística Confidencialidad se encuentra en el criterio "*Rango objetivo*" (87%), No-Repudio en el criterio "*Rango Objetivo*" (75%), Integridad y Autenticidad en el criterio "*Excede los requerimientos*" (100%) y Responsabilidad en el criterio "*Mínimamente aceptable*" (50%).
- El desarrollo de software ayuda en gran parte a la formación profesional porque se tiene un conocimiento más claro y amplio.
- En el desarrollo del proyecto se notó el trabajo colaborativo, puesto que se utilizó una plataforma basada en sistema de control de versiones.

RECOMENDACIONES

- Para garantizar la protección de datos se recomienda aplicar la característica de Seguridad de la ISO/IEC 25010 que cumplan de mejor manera con los requisitos de los usuarios.
- Continuar con la mejora del módulo de Auditoría en el cumplimiento del 100%, en la evaluación de los criterios de la característica de Seguridad.
- Se recomienda que el administrador de base de datos sea una persona con los perfiles profesionales y éticos que garantice la seguridad, integridad y estabilidad de las bases de datos.
- Emplear la metodología Scrum para tener un mejor entendimiento con los miembros del equipo y de esta manera obtener un proyecto de software de calidad.
- La seguridad de la información es muy importante para una entidad, es por eso que se debe seguir aplicando métodos de seguridad para reducir vulnerabilidades en la información que tiendan a perjudicar a la organización.
- Utilizar el repositorio GitHub para trabajar colaborativamente, puesto que es una herramienta que nos permite organizar cualquier cambio en el código del proyecto de software.

REFERENCIAS

Calabrese, Muñoz, Pasini, Esponda, Boracchia, P. (2017). *Asistente para la evaluación de características de calidad de producto de software propuestas por ISO/IEC 25010 basado en métricas definidas usando el enfoque GQM*. 660–671. Retrieved from http://sedici.unlp.edu.ar/bitstream/handle/10915/63778/Documento_completo.pdf-PDFA.pdf?sequence=1

Calderón, Valverde, R. (2007). Metodologías Ágiles. *Escuela de Informatica.*, 1–37. Retrieved from https://uvirtual.unet.edu.ve/pluginfile.php/268695/mod_resource/content/1/Metodologias Agiles.pdf

Castello, R. J. (2006). *Auditoría en entornos informáticos*.

Caycedo-casas, X., & Central, C. (2017). *Auditoría informática: un enfoque efectivo Computer audit: an effective approach Auditoria informática: uma abordagem efetiva*. *3*, 157–173.

Chicano. (2014). *Auditoría de seguridad informática (MF0487_3).* Retrieved from ooooooooobooks.google.com.ec/books?hl=es&lr=&id=8a3KCQAAQBAJ&oi=fnd&pg=PT4&dq=+auditoría+informática&ots=ja2oGHU5Lx&sig=aTOqrPTZGJQP4OBSJFD_Um9VczU#v=onepage&q&f=false

Econ, C. (2012). *Las pistas de auditoría*. (1), 467–482.

edX. (2019). Curso | ODS101x | edX. Retrieved February 16, 2019, from https://courses.edx.org/courses/course-v1:UPValenciaX+ODS101x+1T2018/course/

Espinoza, G. S. (2012). Las pistas de auditoría. *Revista Ciencias Económicas*, *30*(1), 467–482. https://doi.org/10.1136/bmj.e349

Implantar scrum con éxito. (2016). Barcelona, UNKNOWN: Editorial UOC.

ISO 25010. (2019). Retrieved January 13, 2020, from https://iso25000.com/index.php/normas-iso-25000/iso-25010

Jurado, Gutiérrez, Reyes, M. (2010). *Diseño Ágil con TDD*. [Lulu].

Labrin, B. C. (2004). Gestión del conocimiento en enfoques de desarrollo de software tradicional y agilista. *VI Workshop de Investigadores En Ciencias de La Computación*.

Lara, C. (2019). Comparación de modelos tradicionales de seguridad de la información para centros de educación. *Tierra Infinita*, *4*(1), 20. https://doi.org/10.32645/26028131.742

Letelier, Canós, Sánchez, E. (2003). Métodologías Ágiles en el Desarrollo de Software.

VIII Jornadas de Ingeniería Del Software y Bases de Datos - JISBD 2003, 1–8.

Levy, Romero, P. (2016). Implementación práctica del agilismo en proyecto de Ingeniería de Software. *19º Concurso de Trabajos Estudiantiles*, 351–359.

López. (2018). *Estudio comparativo de metodologías tradicionales y ágiles para proyectos de Desarrollo de Software*. 139. Retrieved from http://uvadoc.uva.es/handle/10324/32875

López, P. A. (2010). *Seguridad informática*. Retrieved from https://books.google.com.ec/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=seguridad+informatica&ots=PqoqRDzJWZ&sig=1LSCHWZDRKciG2QITHAY9IztzQg#v=onepage&q=seguridad informatica&f=false

Pereira., U. T. de. (1995). Scientia et technica. In *Scientia Et Technica*. Retrieved from https://www.redalyc.org/html/849/84934064/

Piatiini. (2001). Auditoria informática. *Un Enfoque Práctico*, *6*.

Programa de las Naciones Unidas para el Desarrollo. (2020a). Objetivo 4: Educación de calidad | PNUD. Retrieved February 16, 2019, from http://www.undp.org/content/undp/es/home/sustainable-development-goals/goal-4-quality-education.html

Programa de las Naciones Unidas para el Desarrollo. (2020b). Objetivo 9: Industria, innovación e infraestructura | PNUD. Retrieved February 16, 2019, from http://www.undp.org/content/undp/es/home/sustainable-development-goals/goal-9-industry-innovation-and-infrastructure.html

Soriano, M. (2014). Seguridad en redes y seguridad de la información. In *Improvet*. Retrieved from http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

Srivastava, Bhardwaj, Saraswat, S. (2017). SCRUM model for agile methodology. *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, *2017-Janua*, 864–869. https://doi.org/10.1109/CCAA.2017.8229928

Trigas, M., & Domingo, A. C. (2012). Gestión de Proyectos Informáticos. Metodología Scrum. *Openaccess.Uoc.Edu*, 56. Retrieved from http://www.quimbiotec.gob.ve/sistem/auditoria/pdf/ciudadano/mtrigasTFC0612memoria.pdf%5Cnhttp://openaccess.uoc.edu/webapps/o2/bitstream/10609/17885/1/mtrigasTFC0612memoria.pdf

Urbina, B. (2016). *Introducción a la seguridad informática*. Retrieved from https://books.google.com.ec/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=Introducción+a+la+seguridad+informática+Escrito+por+Gabriel+Baca+Ur

bina&ots=0WPB5zugIt&sig=M9l7U-OdG3dw2hOxafBRTBI3KxA#v=onepage&q=Introducción a la seguridad informática Escrito

Venegas, E. (2018). GUÍA METODOLÓGICA PARA LA EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ... - Leopoldo Venegas Loor, Fredy Esparza Bernal - Google Libros. Retrieved May 13, 2019, from https://books.google.com.ec/books?id=jKRjDwAAQBAJ&pg=PA17&dq=las+organizaciones,+es+muy+importante+que+se+evalúen+constante+y+regularmente+todos+los+procesos&hl=es-419&sa=X&ved=0ahUKEwj0q6WkipniAhWnl-AKHS8ZC5sQ6AEIKDAA#v=onepage&q=las organizacione

Veracruzana, U. (2019). Seguridad de la información. Retrieved January 22, 2020, from https://www.uv.mx/celulaode/seguridad-info/tema1.html

ANEXOS

Anexo 1: Checklist

NRO.	DETALLE	SI	NO	OBSERVACIONES
P1	¿Se requiere que la contraseña posea al menos 8 caracteres?			
P2	¿Se requiere que la contraseña posea letras mayúsculas y minúsculas?			
P3	¿Se requiere que la contraseña posea números y letras?			
P4	¿Se requiere que la contraseña posea caracteres especiales?			
P5	¿El sistema utiliza conexión segura mediante HTTPS?			
P6	¿La base de datos posee los datos encriptados?			
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?			
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?			
P9	¿El sistema permite que cualquier persona tenga acceso al código del servidor de la aplicación?			

P10	¿Cualquier persona tiene acceso al servidor físico?			
P11	¿Cualquier persona tiene acceso al servidor remoto?			
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?			
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?			
P14	¿El sistema permite que cualquier persona pueda modificar la base de datos?			
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?			
P16	¿El sistema permite inyecciones SQL?			
P17	¿El sistema posee un historial de acciones realizadas?			
P18	¿El sistema posee algoritmos de cifrado de datos?			
P19	¿El sistema posee un mecanismo criptográfico, como firma digital?			
P20	¿El sistema solicita confirmación a la hora de realizar una acción?			

P21	¿El sistema posee una protección con certificados SSL?			
P22	¿El sistema da aviso cuando se accede desde una ubicación desconocida?			
P23	¿El sistema informa vía mail las operaciones realizadas?			
P24	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?			
P25	¿El sistema registra el tipo de navegador y sistema de operación utilizado para ingresar al sitio?			
P26	¿El sistema registra la dirección IP desde la cual se ingresa al sitio?			
P27	¿El sistema realiza una comprobación de identidad mediante un certificado digital?			
P28	¿El sistema posee un sistema de verificación en dos pasos?			
P29	¿Es requerida una clave de segundo nivel para el ingreso al sistema?			
P30	¿El sistema realiza una comprobación de identidad mediante datos biométricos?			

P31	¿El sistema realiza una comprobación de identidad mediante tarjeta de coordenadas?			
P32	¿El sistema realiza una comprobación de identidad mediante credenciales?			
P33	¿El sistema realiza una comprobación de identidad mediante una firma electrónica?			

Anexo 2: Manual de Usuario

Revisar Documento de “Manual de Usuario” (Disponible en CD)