UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE
CIENCIAS Y TECNOLOGÍAS DE LA INFORMACIÓN

DESARROLLO DE UNA APLICACIÓN MÓVIL CON FLUTTER PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27002:2013

Trabajo recepcional bajo la modalidad de Tesis
que para obtener el grado de:

Maestro en Administración
de Tecnologías de la Información

Presenta:

Rigoberto Lázaro Córdova

Director de Trabajo Recepcional:

Dr. Julián Javier Francisco León

Cuerpo Académico o Grupo de Investigación de Director:

Ingeniería de software

Línea de Generación y Aplicación del Conocimiento de la Maestría
que alimenta la investigación:

Administración, diseño e implementación de integración de soluciones de TI.

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE CIENCIAS Y TECNOLOGÍAS DE LA INFORMACIÓN

Cunduacán, Tabasco., a 10 de enero de 2022.

Asunto: Cesión de Derechos

MTE. Óscar Alberto González González
Director de la División Académica de Ciencias y Tecnologías de la Información
Presente

El que suscribe la presente, declara que el trabajo de tesis titulado, "**Desarrollo de una aplicación móvil con Flutter para la implementación de la norma ISO/IEC 27002:2013**" es de mi autoría intelectual y por lo tanto cedo todos los **derechos** sobre este proyecto a la Universidad Juárez Autónoma de Tabasco, a la cual relevamos de cualquier sanción y asumimos responder a cualquier reclamo de derechos de autor ante las autoridades competentes.

Atentamente

Rigoberto Lázaro Córdova

Dr. Julián Javier Francisco León

C.c.p. Dr. Eddy Arquímedes García Alcocer. Encargado del despacho de la Coordinación de Posgrado.
Estudiante.

Recibí 10/01/2022
11:30 hrs

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO
RECIBIDO
10 ENE. 2022
D.A.C.Y.T.I.
DIRECCIÓN

CARTA DE AUTORIZACIÓN

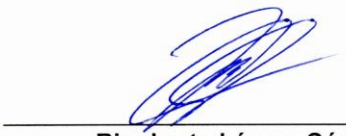
El que suscribe, autoriza por medio del presente escrito a la Universidad Juárez Autónoma de Tabasco para que utilice tanto física como digitalmente la Tesis de grado denominada "**DESARROLLO DE UNA APLICACIÓN MÓVIL CON FLUTTER PARA LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27002:2013**" de la cual soy autor y titular de los derechos de autor.

La finalidad del uso por parte la de Universidad Juárez Autónoma de Tabasco de la tesis antes mencionada, será única y exclusivamente para la difusión, educación y sin fines de lucro, autorización que se hace de manera enunciativa y no limitativa para subir a la Red Abierta de Biblioteca Digital (RABID) y a cualquier otra red académica con la que la Universidad tenga relación institucional.

Por lo antes manifestado, libero a la Universidad Juárez Autónoma de Tabasco de cualquier reclamación legal que se pudiera ejercer respecto al uso y manipulación de la tesis antes mencionada y para los fines estipulados en este documento.

Se firma la presente autorización en la ciudad de Cunduacán, Tabasco a los 12 días de mes de enero del año 2022.

AUTORIZÓ



Rigoberto Lázaro Córdova

Cunduacán, Tabasco a 30 de julio de 2020
Oficio No. 588/2020/DACYTI-D

Asunto: Designación como Director de Tesis.

Dr. Julián Javier Francisco León
Profesor Investigador
Presente

De conformidad con lo establecido en el Reglamento de Estudios de Posgrado Vigente en la Universidad Juárez Autónoma de Tabasco, me permito informarle que ha sido designado como Director de la tesis titulada **"Desarrollo de una aplicación móvil con flutter para la implementación de la norma ISO/IEC 27002:2013"**, a realizar por **Rigoberto Lázaro Córdova** para obtener el grado de Maestro en Administración de Tecnologias de la Información.

Sin otro particular, aprovecho la ocasión para enviarle un afectuoso saludo.

Atentamente

M.T.E. Oscar González González
Director

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO
DIVISIÓN ACADÉMICA DE CIENCIAS Y TECNOLOGÍAS DE LA INFORMACIÓN

c. c. p. MA. María Elena García Ulín. - Encargada de Despacho de la Coordinaión de Posgrado de DACYTI.
Archivo
Consecutivo

Carretera Cunduacán-Jalpa Km. 1, Colonia Esmeralda, C.P. 86690.
Cunduacán, Tabasco, México.
Tel: (993) 358 1500 ext. 6727; (914) 336 0616; Fax: (914) 336 0870
E-mail: direccion.dacyti@ujat.mx
http://ujat.mx/dacyti

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE CIENCIAS Y TECNOLOGÍAS DE LA INFORMACIÓN

F7: Respuesta de jurado

Cunduacán, Tabasco, a 13 de octubre de 2021.

MTE. Óscar Alberto González González
Director de la División Académica de Ciencias y Tecnologías de la Información
Presente

En atención a los oficios girados por usted, en los que se nos designa como parte del jurado para efectuar la revisión de la tesis titulada ***"Desarrollo de una aplicación móvil con Flutter para la implementación de la norma ISO/IEC 27002:2013"***, realizada por el ***C. Rigoberto Lázaro Córdova***, estudiante de la Maestría en Administración de Tecnologías de la Información, nos permitimos informarle que, en virtud de que ha atendido las observaciones realizadas, otorgamos nuestra aprobación para que continúe los trámites para la obtención del grado.

Sin otro particular, aprovechamos la ocasión para enviarle un cordial saludo.

Atentamente integrantes del jurado

MATI. Karla Alejandra Zurita Cruz

Dra. Martha Patricia Silva Payró

Dr. Gerardo Arceo Moheno

c.c.p. Dr. Eddy Arquímedes Garcia Alcocer. Encargada del despacho de la Coordinación de Posgrado.
Estudiante.

"2021, Año de la Independencia de México"

Cunduacán, Tabasco a 12 de noviembre de 2021
Oficio No. 1419/DACYTI/CP/2021

Asunto: Autorización de impresión de Tesis

C. Rigoberto Lázaro Córdova
Matricula 192H19004

En virtud de que cumple satisfactoriamente los requisitos establecidos en el Reglamento General de Estudios de Posgrado vigente en la Universidad, informo a Usted que se autoriza la impresión del trabajo recepcional **"Desarrollo de una aplicación móvil con FLUTTER para la implementación de la norma ISO/IEC 27002:2013"**, para presentar examen y obtener el Grado de Maestro en Administración de Tecnologías de la Información.

Sin otro particular, aprovecho la ocasión para enviarle un afectuoso saludo.

Atentamente

MTE. Óscar Alberto González González
Director

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO
DIVISION ACADEMICA DE CIENCIAS Y TECNOLOGIAS DE LA INFORMACIÓN

C.c.p. Dr. Eddy Arquímedes Garcia Alcocer. - Encargado del Despacho de la Coordinación de Posgrado DACYTI
Archivo.
Consecutivo.

MTE´OAGG/EAGA

Agradecimientos

Agradezco al Consejo Nacional de Ciencia y Tecnología (CONACYT) por brindarme apoyo económico a través de la Beca de Posgrado del Programa Nacional de Posgrados de Calidad (PNPC), lo que permitió que me mantuviera constante hasta culminar esta etapa de mis estudios.

A la Universidad Juárez Autónoma de Tabasco y a la División Académica de Información y Sistemas, por permitirme estudiar y prepararme en la máxima casa de estudios del estado de Tabasco, y una vez más formar parte de su comunidad universitaria.

A mi director de tesis el Dr. Julián Javier Francisco León por sus asesorías, consejos y el tiempo dedicado que me brindaron para hacer de este trabajo.

A mis revisores de tesis, las Dra. Elsa Rueda Ventura y Martha Patricia Silva Payró y el Dr. Gerardo Arceo Moheno por su tiempo y atenciones

Un agradecimiento especial al Registro Público de la Propiedad y del Comercio de Tabasco, por permitir realizar una estancia con ellos y así seguir trabajando sobre este proyecto de investigación.

Dedicatorias

A mis padres, María Ignacia y José Jesús, por ser los pilares que me mantenían en este trayecto y por convertirme en la persona que soy ahora. Además, por aconsejarme en los buenos y malos momentos, por guiarme y motivarme para alcanzar mis metas.

A mis hermanas Dulce Janet, Miriam Elizabeth y Cindy Verónica, que me apoyan y que siempre están a mí lado.

A las hermanas Mendoza de la Cruz por su apoyo y siempre alentarme a que podría lograrlo. En especial a Dolores por ser alguien tan especial para mí.

Resumen

En el presente trabajo se explica la importancia de la seguridad de la información para el Departamento de Informática del Registro Público de la Propiedad y del Comercio de Tabasco, institución pública que tiene por funciones registrales asegurar la legitimación registral, legalidad y publicidad de los actos y hechos jurídicos en materia de la inscripción pública del patrimonio en el Estado. Actualmente se desconoce el estado del Registro Público de la Propiedad y del Comercio en relación con la seguridad de la información. El objetivo de este trabajo es revisar el grado de seguridad del departamento antes mencionado, bajo la norma ISO/IEC 27002:2013 además de dos instrumentos para identificar los activos de información, como sus vulnerabilidades y amenazas basadas en la metodología MAGERIT. Además de uno para evaluar el grado de cumplimiento de la norma, esta mediante el uso de una aplicación móvil Android usando Flutter como herramienta de desarrollo. Así el Registro Público de la propiedad y del comercio de Tabasco contará con mejores prácticas de seguridad para la información basadas en los controles de la norma ISO/IEC 27002:2013 que se proponen en este trabajo de investigación, que permitirá identificar vulnerabilidades y proponer soluciones a la seguridad de la información que puedan existir en el Departamento de Informática del Registro Público de la Propiedad y del Comercio de Tabasco.

Introducción

El presente documento está integrado por cinco capítulos los cuales se describen a continuación:

Capítulo 1. Generalidades. Presentan los antecedentes, el planteamiento del problema, la metodología utilizada y la justificación.

Capítulo 2. Marco teórico – Se introduce al lector la teoría necesaria para la comprensión del tema, en este caso, seguridad de la información, ISO/IEC 27002 y Flutter.

Capítulo 3. Aplicación de la metodología y desarrollo – Describe la forma en que se fue aplicando la metodología para llevar a cabo este trabajo, Este capítulo consiste en tres fases donde la Fase 1 “Análisis del Departamento de Informática”, comprende el análisis de la situación y la recolección de información, así también el análisis de activos y amenazas basados en la metodología MAGERIT. Seguida de la Fase 2 “Diseño y desarrollo de la aplicación” que integra la conceptualización, diseño y el desarrollo de la aplicación móvil. Por último, en la fase 3 “Evaluación de la seguridad”, se utilizó la aplicación móvil desarrollada para evaluar el grado de seguridad de la información bajo la norma ISO/IEC 27002:2013.

Capítulo 4. Resultados - Presenta los resultados obtenidos de la evaluación realizada, que se desprenden de la cuarta fase de la metodología.

Capítulo 5. Conclusiones, recomendaciones y trabajos futuros - El trabajo de investigación se acompaña de las conclusiones obtenidas de la investigación,

recomendaciones para la institución participante y trabajos futuros que se relacionan y enriquecen la presente investigación.

Índice general

Índice de tablas

Índice de figuras

Capítulo 1. Generalidades

1.1 Antecedentes

En la actualidad, las Tecnologías de la Información y las Comunicaciones (TIC's) se han constituido en elementos sustantivos inherentes al desarrollo en todas las esferas de la vida, son de suma importancia ya que es imposible concebir que una organización no se apoye de éstas (Prieto et al., 2011; Saavedra y Tapia, 2013).

De acuerdo con Jesan (2006), la información es uno de los activos de las organizaciones, pero una vez que las redes internas se conectan a internet, se convierte en automáticamente a un objetivo para los ataques cibernéticos.

Los ciberataques son uno de los principales riesgos en las empresas para el futuro a largo plazo. En la figura 1 se observan las siguientes estimaciones en materia de ciberataques, donde se estimaba que para el año 2019 el costo anual de este rubro sobrepasaría los $2 billones de dólares en la economía mundial.

Figura 1
Estadísticas relacionadas al cibercrimen.

Nota: McKinsey & Company (s.f.)

Según la empresa multinacional Willis Towers Watson (2018) estimó que en el 2018 el 83% de las empresas mexicanas fueron víctimas de ciberataques por lo menos una vez al año, lo que posicionó a México dentro de los 10 países con más ataques cibernéticos.

1.1.1 Seguridad de la información

Previo a la globalización de las telecomunicaciones y el internet, el ambiente de los sistemas de información en los años 90’s, se caracterizaba por entornos informáticos que operaban de manera aislada o en redes privadas, donde bastaba para garantizar la seguridad de la información manteniendo el control al acceso físico y el uso de barreras informáticas (Voutssas, 2010) hasta evolucionar a una donde se tienen que concentrar en las políticas, procedimientos y controles basados en las personas (Cárdenas-Solano, Martínez-Ardila y Becerra-Ardila, 2016).

La seguridad de la información tiene por objeto proteger a los sistemas informáticos de las amenazas a los que están expuestos. En la actualidad, la seguridad de la información se ha convertido en un soporte para las empresas y se debe a las constantes amenazas a los que se exponen continuamente los activos de las organizaciones (Tovar y Salguero, 2018).

Según ESET (2019b) en México, las tres principales preocupaciones de las empresas son la infección por código malicioso, el acceso indebido a sistemas y el robo de información.

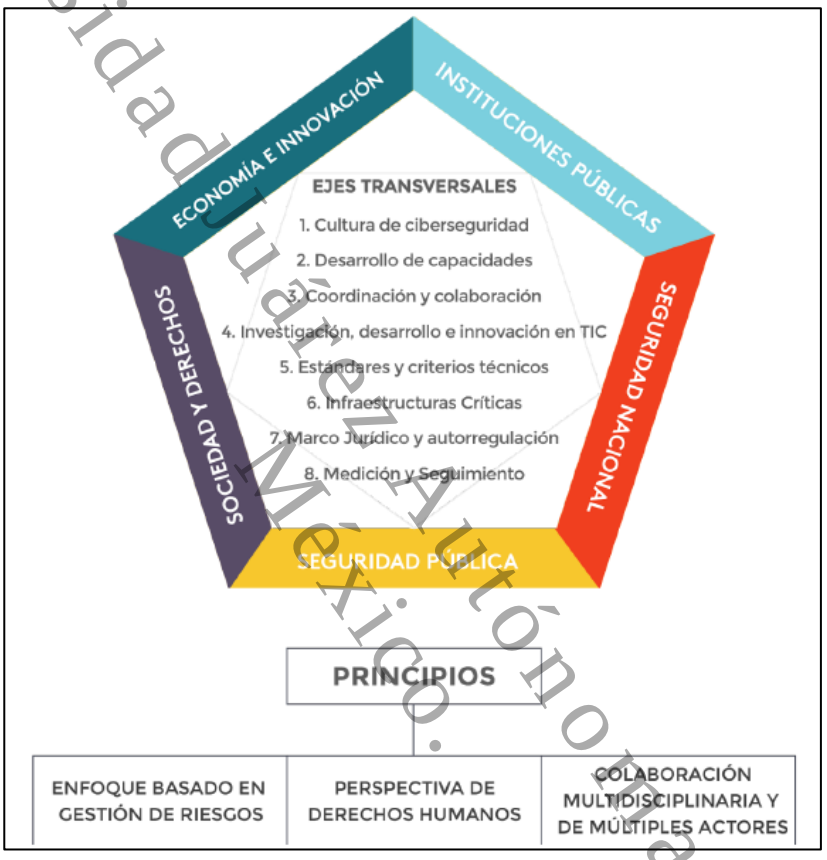
En el año 2017, en México se publicó la Estrategia Nacional de Ciberseguridad que es un documento que plasma la visión de Estado mexicano en la materia en los siguientes rubros (Gobierno de México, 2017):

- La importancia de las Tecnologías de la Información y Comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.
- Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.
- La necesidad de una cultura general de ciberseguridad.

En la figura 2, puede observarse la estructura de la Estrategia Nacional de Ciberseguridad en esta se plantearon cinco objetivos estratégicos, cuyo desarrollo requiere de ochos ejes transversales, los cuales están relacionados, son

interdependientes y contribuyen a alcanzar cada objetivo estratégico. Todas las acciones de cada eje transversal se desarrollan sobre tres principios rectores (ver figura 2).

Figura 2
Objetivos estratégicos.



Nota: Gobierno de México (2017).

En ese documento se señala que no existía una estrategia previa a la realización de Estrategia Nacional de Ciberseguridad, se menciona que entre los objetivos estratégicos se encuentra proteger la información y los sistemas informáticos de las instituciones públicas del país para su correcto funcionamiento y la continuidad en las prestaciones de servicios y trámites a la población.

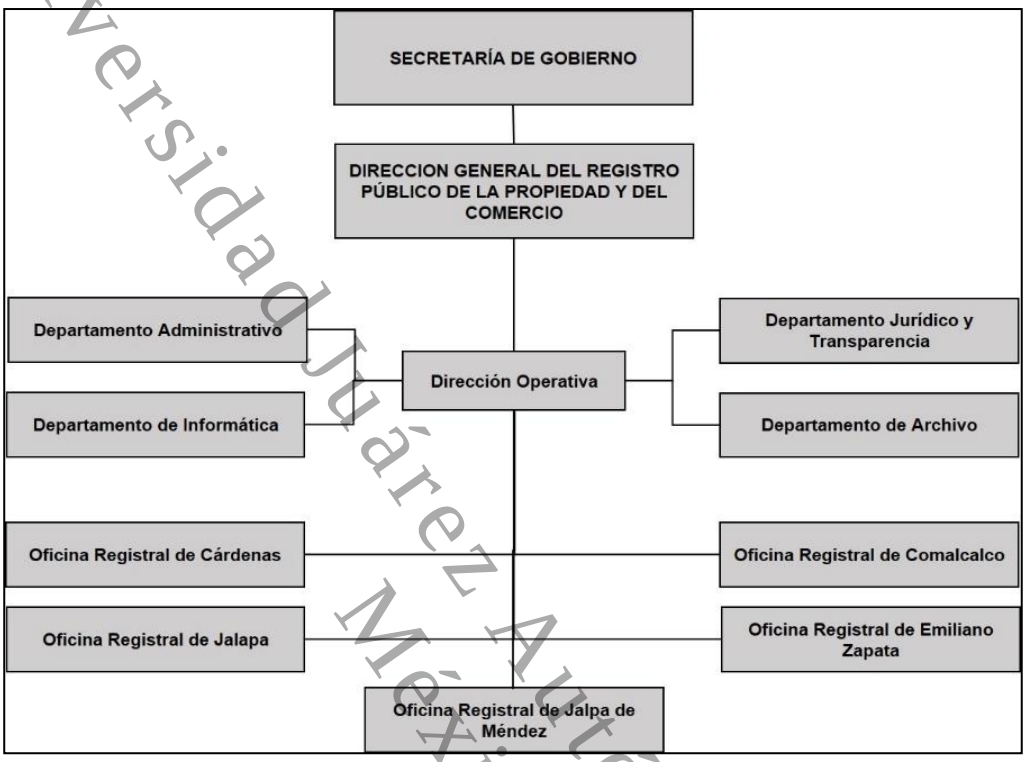
1.1.2 El Registro Público de la Propiedad y del Comercio

Las instituciones públicas necesariamente hacen uso de las Tecnologías de la Información que permiten la eficiencia y eficacia de sus actividades por lo tanto son herramientas indispensables para su correcto funcionamiento, así como para satisfacer las necesidades de los usuarios.

El Registro Público de la Propiedad y del Comercio (RPPyC) de Tabasco es una institución pública estatal que tiene por funciones registrales el asegurar la legitimación registral, legalidad y publicidad de los actos y hechos jurídicos en materia de la inscripción pública del patrimonio del Estado (Gobierno del estado de Tabasco, 2012).

El RPPyC de Tabasco es un organismo actualmente dependiente de la Secretaría de Gobierno (SEGOB) del Estado. En la siguiente figura se puede ver la estructura organizacional actual del RPPyC (ver figura 3).

Figura 3
Estructura organizacional del RPPyC.



Nota: Elaboración propia con información proporcionada por el RPPyC (2020).

De acuerdo con la Secretaría de Desarrollo Agrario Territorial y Urbano (SEDATU), los registros públicos necesariamente hacen uso de las tecnologías de la información para simplificar y hacer más eficientes los procesos registrales (Secretaría de Desarrollo Agrario Territorial y Urbano, s.f.), por lo tanto, son herramientas indispensables para su correcto funcionamiento, así como para satisfacer las necesidades de los usuarios.

Lo anterior, en virtud que la SEDATU en su Modelo Integral del Registro Público de la Propiedad (MIRPP) que la información registral es pública y contempla la necesidad de efectuar transacciones electrónicas públicas, se requiere de altos niveles de seguridad

que garanticen la integridad e inviolabilidad en aras de la certeza jurídica (Secretaría de Desarrollo Agrario Territorial y Urbano, s.f.).

El modelo MIRPP hace mención que la Gestión de calidad es un indicador y debe alinearse a la norma de calidad internacional ISO 9001:2000 para un grado de cumplimiento satisfactorio. Esto hace pensar también el alinear a una norma de la familia ISO el indicador de Tecnologías de Información de este modelo, para garantizar la seguridad de la información registral mínimo e intermedio (Ver tabla 1).

Tabla 1
Componentes del modelo del registro público de la propiedad.

Indicador	Grado de cumplimiento requerido		
	Mínimo	Intermedio	Satisfactorio
Tecnologías de Información	Desarrollar y/o adecuar los sistemas de información registrales, incluyendo la definición de la infraestructura de las tecnologías de información requerida para garantizar el procesamiento y la seguridad de la información registral	Sistemas de información alineados a los procesos, incluyendo la instrumentación de las tecnologías de información requerida para garantizar el procesamiento y la seguridad de la información registral	Adoptar nuevas tecnologías de información como parte del proceso de mejora continua que garanticen la certeza jurídica
Gestión de calidad	Estándares de calidad, definidos conforme al Modelo	Estandarización y documentación de procesos de calidad en la operación	Procesos del RPP certificados bajo la norma ISO 9001:2000

Nota: Elaboración propia basado en Secretaría de Desarrollo Agrario Territorial y Urbano (s.f.).

Un precedente de lo mencionado anteriormente es el Registro Público de la Propiedad y del Comercio de Jalisco (Méndez, 2019). Esta institución se encuentra certificado en la norma de seguridad en la información ISO/IEC 27001:2013 y en la norma de gestión de la calidad ISO 9001:2015.

1.1.3 Flutter SDK

Para Allen (como se citó en Aguado, Martínez y Cañete-Sanz, 2015), las aplicaciones móviles son piezas de software diseñadas para ser instaladas y utilizadas en dispositivos móviles, que se adaptan a las limitaciones de estos dispositivos, pero también permiten aprovechar sus posibilidades tecnológicas.

En la actualidad existen sistemas operativos móviles tales como: iOS y Android, estos dos dominan el mercado con el 90% del mercado, del cual Android es el que ocupa el primer lugar según las estadísticas (Selvaganapathy et al., 2020). Para el desarrollo de las aplicaciones móviles Android se puede hacer uso de herramientas de desarrollo, desde las que son consideradas las herramientas oficiales hasta opciones de desarrollo de terceros; gratuitas o de paga. Una de estas herramientas es Flutter.

En la siguiente figura, se presentan empresas de renombre que utilizan Flutter. Una de las empresas que utiliza esta herramienta es eBay para su aplicación eBay Motors. Esta aplicación tiene la función de la compra y venta de automóviles desde el teléfono (ver figura 4).

Figura 4
¿Quiénes usan Flutter?

Nota: Flutter (2020a).

En el ámbito de la investigación, se consultó información en bases de datos científicas como ScienceDirect y CONRICYT para conocer si existen trabajos donde se haya usado esta herramienta de desarrollo (Ver figura 5), solo se encontraron artículos donde se hace mención del nombre y sus características o comparaciones donde Flutter no era la herramienta principal por usar.

Con base a lo anterior, se concluye que aún no es un SDK que se use en el ámbito académico; tal vez se deba a que sea una herramienta nueva, ya que en mayo de 2017 fue anunciado una versión *alpha* durante la conferencia anual I/O Developers de Google. Mientras que en diciembre de 2018 se lanzó su primera versión 1.0 (Mevada, 2019).

Figura 5
Resultados de Flutter SDK en ScienceDirect.

Nota: Captura de pantalla propia

1.2 Planteamiento del problema

1.2.1 Definición del problema

Hortal (como se citó en Cárdenas, 2017) menciona la importancia que adquiere la existencia de los organismos públicos, ya que son estos los que implementan un cierto orden y equilibrio en las diversas acciones sociales. Así también, las instituciones públicas son inherentes a la vida cotidiana de toda persona.

En este sentido, las instituciones públicas de México forman parte importante de la estructura social del país, sólo basta con pensar en los diferentes servicios que brindan a la ciudadanía y dependiendo de su objetivo; estas tienen en su resguardo información de suma importancia que deben de mantener seguras ya que el posible robo, la alteración de la información, afectaciones a la operación de servicios públicos y el potencial daño a la confianza en las instituciones, son los principales riesgos a lo que se enfrenta el sector público (McKinsey & Company, s.f.).

Las instituciones públicas no han sido exentas de problemas. Un acontecimiento reciente fue el intento de hackeo al Sistema Digital Notarial del Registro Público de la Propiedad y del Comercio de Aguascalientes, donde el secretario de Gestión Urbanística, Ordenamiento Territorial, Registral y Catastral de ese Estado informó que el día 13 de febrero de 2020 se suscitó el incidente y recalcó que al detectarse se implementó el protocolo de seguridad establecido por el área de informática del Gobierno del Estado para prevenir el daño a la información (Ureña, 2020).

En menos de un mes se presentó un segundo caso, esta vez un ataque realizado a la Secretaría de Economía (SE). Donde la SE declaró que el 23 de febrero se detectó

un ataque en algunos de sus servidores y destacaron que la información no se vio comprometida (Redacción, 2020).

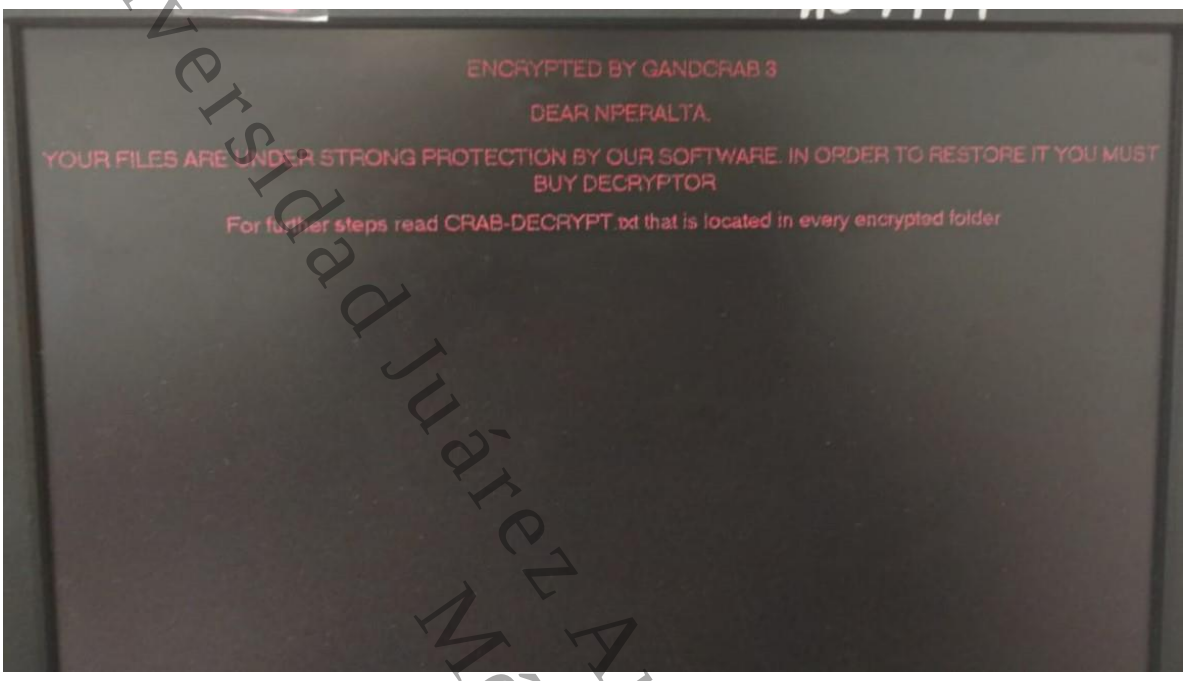
En los casos anteriores, sus servicios fueron suspendidos. Impactando negativamente en la ciudadanía que hace uso de los servicios que brindaba. En el caso de la SE, publicó un acuerdo para establecer que todos los plazos de trámites en curso quedan suspendidos hasta que se emitiera un nuevo acuerdo sobre la reanudación de actividades (Secretaría de Gobernación, 2020).

En relación con lo anterior, Homero Menchaca, director de Nacional de Acero, declaró que la industria del acero sufrió pérdidas derivadas del retraso en la expedición de permisos de exportación por el intento de hackeo a la SE (PolíticoMX, 2020).

La información resguardada en el registro público de todas las propiedades del estado de Tabasco es un elemento clave para el funcionamiento de esta. Así también la infraestructura que permiten el funcionamiento (equipo de cómputo, servidores, SAM, etc.) e incidentes como los mencionados anteriormente causarían que las operaciones se vieran interrumpidas en todo el estado.

El RPPyC de Tabasco no ha estado exenta de incidentes, en la figura 6 se observa un caso en el año 2017, en el auge de los ataques de ransomware (ESET, 2019a) dentro de la institución, dónde la persona encargada declaró que se trató de un caso aislado que no presentó una mayor amenaza más allá de la pérdida total de la información del equipo.

Figura 6
Computadora infectada por un ransomware en el RPPyC.



Nota: Imagen proporcionada por el RPPyC (2020).

Como se mencionó anteriormente, la SEDATU en su modelo del Registro Público de la Propiedad (MRPP) que se debe contemplar la necesidad de efectuar transacciones electrónicas públicas, se requiere de altos niveles de seguridad que garanticen la integridad e inviolabilidad en aras de la certeza jurídica.

Olano (2016) menciona que los estándares de seguridad ayudan a organismos públicos y privados a mantener seguros sus activos y procesos relacionados con la información. Una institución pública de México que cuenta con certificación en seguridad de la información es la siguiente:

La Comisión Nacional de Seguros y Fianzas (CNSF), fue una institución que obtuvo una certificación emitida por primera vez el 10 de noviembre de 2010 y la más

reciente certificación fue refrendada con fecha 17 de diciembre de 2016 y estuvo en vigor hasta el 10 de noviembre de 2019. Esta certificación (ver Figura 7) expedida por la Asociación Española de Normalización y Certificación (AENOR) e IQNet (the International Certification Network) certificó que la CNSF disponía de un sistema de gestión y seguridad de la información (SGSI) conforme a la norma UNE-ISO/IEC 27001:2014.

Figura 7
Certificación de la CNSF.


IQNet
THE INTERNATIONAL CERTIFICATION NETWORK
CERTIFICATE
IQNet and
AENOR
hereby certify that the organization
COMISIÓN NACIONAL DE SEGUROS Y FIANZAS (CNSF)
OFICINAS CENTRALES
AV INSURGENTES SUR No. 1971, TORRE NORTE 2° PISO, COL. GUADALUPE INN, DEL. ÁLVARO OBREGÓN
01020 MEXICO D.F.
México
PARQUE TECNOLOGICO INNOVACION QUERETARO
CARRETERA ESTATAL 431 KM 2.2, EL MARQUES
SANTIAGO DE QUERETARO(QRO.)
México
for the following field of activities
The information systems that support the processes of governance, organization delivery, managements information, locations and resolutions within the General Direction of information technologies that support the supervision activities on the Insurance and Surety National Commission, according to the current Statement of Applicability.
has implemented and maintains a
Information Security Management System
which fulfills the requirements of the following standard
ISO/IEC 27001:2013
First issued on: 2010-11-10 Last issued: 2016-12-17 Validity date: 2019-11-10
Registration Number: ES-SI-0076/2010
IQNet
AENOR
Michael Drechsel
President of IQNet
Avelino BRITO
Chief Executive Officer
IQNet Partners*:
AENOR Spain AFNOR Certification France AIB-Vincotte International Belgium ANCE Mexico APCER Portugal CCC Cyprus CISQ Italy CQC China CQM China CQS Czech Republic Cro Cert Croatia DQS Holding GmbH Germany FCAV Brazil FONDONORMA Venezuela ICONTEC Colombia IMNC Mexico Inspecta Certification Finland IRAM Argentina JQA Japan KFQ Korea MIRTEC Greece MSZT Hungary Nemko AS Norway NSAI Ireland PCBC Poland Quality Austria Austria RR Russia SII Israel SIQ Slovenia SIRIM QAS International Malaysia SQS Switzerland SRAC Romania TEST St Petersburg Russia TSE Turkey YUQS Serbia
IQNet is represented in the USA by: AFNOR Certification, CISQ, DQS Holding GmbH and NSAI Inc.
* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

Nota: Comisión Nacional de Seguros y Fianzas (2017).

1.2.2 Delimitación de la investigación

Alcances

- Formular una propuesta con los controles aplicables para la institución debido la misma norma menciona que no es necesario implementar en su totalidad la norma ISO/IEC 27002:2013 (consta de 14 dominios, 35 objetivos de control y 114 controles), por lo que hay que identificar los controles aplicables ya que los objetivos de estos pueden o no estar presentes en el departamento a analizar.
- Uno de los productos finales es el desarrollo de una aplicación móvil para la aplicación de los controles de la norma en el RPPyC de Tabasco.
- Conocer el grado de cumplimiento de la institución de los controles seleccionados de la norma.

Limitaciones

- Se implementó en el Departamento de Informática de la institución elegida, no se tomaron en cuenta otros departamentos u oficinas foráneas del registro público.
- Se utilizó el *framework* Flutter para el desarrollo de la aplicación móvil.
- Se consideró el uso de un acuerdo de confidencialidad al trabajar con una institución pública, debido por la información que resguarda y al exponer en este trabajo, la seguridad de esta.

1.2.3 Preguntas de investigación

¿Cuál es el nivel de cumplimiento de los mecanismos de seguridad de la información actualmente implementados en el Departamento de Informática del RPPyC respecto a la norma ISO/IEC 27002:2013?

1.2.4 Objetivos

Objetivo general

Evaluar el grado de seguridad del Departamento de Informática del Registro Público de la Propiedad y del Comercio del estado de Tabasco bajo la norma ISO/IEC 27002:2013, mediante el uso de una aplicación móvil Android usando Flutter, para proponer buenas prácticas de seguridad de la información.

Objetivos específicos

- Analizar la seguridad de la información de la institución bajo las recomendaciones de la norma ISO/IEC 27002:2013.
- Formular una propuesta basada en la norma ISO/IEC 27002:2013 con base al análisis de riesgo.
- Diseñar una aplicación móvil con base en la propuesta hecha.
- Desarrollar la aplicación usando el *framework* de desarrollo Flutter SDK.
- Aplicar la norma en la institución haciendo uso de la aplicación desarrollada.

1.3 Justificación

Con los recientes casos de ataques cibernéticos realizados a instituciones públicas (Ureña, 2020; Redacción, 2020), las medidas de seguridad con la que estas contaban

jugaron un papel importante para su pronta detección y evitaron un daño en la información que estas resguardan.

En un registro público de la propiedad se inscriben todos los actos jurídicos y administrativos de los inmuebles, los que acreditan las propiedades, su transferencia, modificación, y cualquier acto que modifique su situación (Instituto de Administración y Avalúos de Bienes Nacionales, 2013).

Entre los años 2010 al 2013, en el rubro de recaudación de registros, se encuentra el RPPyC. En la tabla 2 se observa que tuvo la mayor recaudación los derechos, en comparación a lo que recaudaron (en millones de pesos) en los mismos periodos el Registro civil y los servicios notariales y de archivo; incluso sus recaudaciones juntas no se comparan a lo recaudado por el RPPyC. Se puede inferir que el RPPyC es una institución importante que contribuye en su rubro para la recaudación de ingresos para el estado de Tabasco.

Tabla 2
Recaudación de la hacienda pública estatal de Tabasco, 2010-2013.

Recaudación de registros	**2010**	**2011**	**2012**	**2013**
i.Registro civil	3.32	4.62	6.23	6.25
ii.Registro público de la propiedad y del comercio	69.12	66.88	70.26	67.42
iii.Servicios notariales y de archivo	3.84	3.21	3.14	4.49
Total (i+ii+iii)	76.28	74.72	79.64	78.17

Nota: Adaptado de Dirección de Servicios de Investigación y Análisis (2015)

Para el Ejercicio Fiscal del año 2020, en la ley de Ingresos del estado de Tabasco, la Hacienda Pública del Estado estimaba que percibiría del RPPyC los ingresos estimados de $108,197,650.00 (Secretaría de finanzas, s.f.). Esto hace que esta institución sea importante para la recaudación de ingresos para el estado de Tabasco.

Por lo tanto, la información que el RPPyC de Tabasco resguarda de los actos registrales de todo el Estado, es de vital importancia y posibles amenazas y vulnerabilidades en el Departamento de Informática puede ser crítica para la certeza jurídica de la información y de las actividades diarias, así también para la recaudación de ingresos en el Estado.

En el punto cinco (Estándares y criterios técnicos) de los ejes transversales de la Estrategia Nacional de seguridad (Gobierno de México, 2017) se menciona la identificación y, en su caso, fomento del uso de estándares y mejores prácticas internacionales en materia de ciberseguridad. Gerber y Von-Solms (2008) afirman que la norma ISO 27002 es uno de los estándares internacionales más populares para gestionar la seguridad de la información.

Lo anterior ya que las organizaciones del sector público requieren garantizar niveles aceptables de seguridad de la información, si se tiene en cuenta que en su mayoría es información de la ciudadanía que por lo general es sensible y debe ser adecuadamente protegida en términos de confidencialidad, integridad y disponibilidad (Carvajal, Cardona y Valencia, 2019).

La Secretaría de Desarrollo Agrario Territorial y Urbano (SEDATU) propone un modelo integral para los registros público de la propiedad, en este modelo tiene como objetivo promover que los registros públicos de México sean organismos eficientes en el cumplimiento de su función.

Se desconoce el estado actual del RPPyC en relación con la seguridad de la información. Así que contar con mejores prácticas de seguridad para la información y

basadas en los controles de la norma ISO/IEC 27002:2013 que se propusieron en este trabajo de investigación, permitirá identificar vulnerabilidades y proponer soluciones a la seguridad de la información que puedan existir en el Departamento de Informática del Registro Público de la Propiedad y del Comercio de Tabasco.

Lo anterior puede ayudar a las personas encargadas del Departamento de Informática conocer las buenas prácticas que propone la norma ISO/IEC 27002:2013. Para así mantener los activos que permiten el funcionamiento correcto del registro público.

Se propuso la versión 27002:2013 en vez de la 27001:2013 que esta última es la norma certificable, Fenz & Neubauer (2018) mencionan que para determinar automáticamente el cumplimiento de ISO 27001 se requiere una base de conocimiento de los controles de ISO 27002. Mientras que Días y Reyes (2015), mencionan que las organizaciones que pretendan certificar sus procesos con base en el estándar ISO/IEC 27001, pueden tomar como referencia la implementación de buenas prácticas de seguridad hechas en su trabajo de investigación, que fueron basadas en la norma ISO 27002.

Y dado que se desconoce el estado actual en materia de seguridad de la información del registro, se optó por la norma ISO/IEC 27002:2013 ya que aún es temprano proponer una certificación de sus procesos.

Unos de los trabajos futuros de la tesis “Estudio sobre la seguridad de la información con un enfoque en la norma ISO/IEC 27002:2013, caso: coordinación de desarrollo y soporte de sistemas de la dirección de tecnologías de información e

innovación de la UJAT" se propuso el diseño de una herramienta de software que facilite el proceso de implementación y auditoria de los controles de la norma ISO/IEC 27002 (Zacarias, 2019).

De acuerdo con Sánchez, Collado, Martín y Cano (2018) una aplicación móvil tiene por objetivo facilitar la consecución de una tarea determinada o asistir en gestiones diarias, siendo el modo de interacción entre el usuario y la aplicación el tacto. Por lo anterior se plantea desarrollar una aplicación móvil en Android para agilizar la aplicación del instrumento de recolección basado en la norma en un dispositivo móvil o tableta, y al finalizar la aplicación de esta, obtener un reporte acompañados de gráficos donde se observe el grado de cumplimiento de la norma.

Así también en las búsquedas realizadas por el investigador, en los trabajos de investigación consultadas, no se encontró alguna referencia acerca que para evaluar el grado de cumplimiento de la norma ISO/IEC 27002 se haya hecho uso de una aplicación móvil. Los trabajos consultados la aplicación de la norma antes mencionada la realizaban por medio de una lista de cotejo como instrumento de recolección de datos. Y finalmente se escogió Flutter SDK como la herramienta al no encontrar trabajos de investigación donde se utilizará para el desarrollo de una aplicación.

1.4 Metodología utilizada

La metodología para este estudio estuvo conformada por cuatro fases, las cuales se detallan a continuación:

1.4.1 Fase 1: Análisis del Departamento de Informática

En primera instancia se expuso la finalidad de esta investigación, los alcances y el producto final. Se llevaron a cabo reuniones con el fin de obtener información del Departamento de Informática del RPPyC para conocer el entorno de trabajo, las funciones del área e incidentes relacionados con la seguridad de la información.

Así también en esta fase, se elaboraron los instrumentos para la determinar los activos de información, como la identificación y valoración de las amenazas basados en la metodología MAGERIT para conocer el total de dominios aplicables en este departamento. Lo anterior ya que Gerber y Von-Solms (2008) mencionan que, para garantizar la identificación y la selección de los controles de la norma, es necesario establecer en primer lugar requisitos de seguridad de la información.

MAGERIT se compone de cinco fases, pero como el fin de este trabajo de investigación no es la implementación de un sistema de gestión de seguridad de la información, solo se usaron las primeras dos fases de esta metodología que son para determinar activos relevantes y las amenazas a los que se exponen los activos.

1.4.2 Fase 2: Diseño y desarrollo de la aplicación

Diseñar y desarrollar una aplicación móvil en Flutter para el sistema operativo Android basada en la distribución de la norma ISO/IEC 27002:2013, aplicando el cálculo de evaluación de los controles usado por Tovar y Salguero (2018). Para llevar a cabo el desarrollo de la aplicación usando Flutter SDK, se empleó SCRUM, un modelo de desarrollo interactivo e incremental. Blom (2010) argumenta que Scrum funciona mejor para equipos de cinco a siete personas, pero la mayoría de las técnicas también se

pueden usar para desarrolladores individuales, característica importante, ya que el investigador fue el único desarrollador en el proyecto.

1.4.3 Fase 3: Evaluación de seguridad

En esta fase se empleó la aplicación móvil desarrollada con base en la norma ISO/IEC 27002:2013, para aplicarse en el Departamento de Informática del Registro Público de la Propiedad y del Comercio de Tabasco.

1.4.4 Fase 4: Elaboración del informe

Una vez aplicado los instrumentos, se realizó una evaluación de los resultados y se detalló lo encontrado durante la evaluación de la seguridad de la información del Departamento de Informática. Una vez analizado los resultados, se propusieron buenas prácticas de seguridad de la información para el Departamento de Informática del Registro Público de la Propiedad y del Comercio de Tabasco.

1.5 Enfoque de investigación

El trabajo de investigación se considera de tipo descriptivo con un enfoque cualitativo. Según Orozco (como se citó en Castro, 2010) afirma que la investigación cuanlitativa es un proceso de indagación de un objeto al cual el investigador accede a través de interpretaciones sucesivas, con la ayuda de instrumentos y técnicas, que le permiten involucrarse con el objeto para interpretarlo de la forma más integral posible.

Se consideró este enfoque ya que se requirió analizar e interpretar datos mediante la observación del área donde se realizó la investigación, así también, al efectuar entrevistas con el personal encargado y la valoración hecha con la metodología MAGERIT tuvo de igual manera un enfoque cualitativo. Además de que la aplicación

móvil consistió en un *checklist* para la aplicación de la norma ISO/IEC 27002:2013, que es considerada una herramienta blanda (cualitativa) por Muñoz, Rodríguez y Domínguez (2003).

1.6 Fuentes de investigación

Las fuentes primarias que se emplearon en la investigación fueron: información de los encargados de la institución. Así mismo, las fuentes secundarias fueron libros, artículos de revistas científicas indexadas, entrevistas, tesis y páginas web.

Al tratarse de una investigación en una institución pública, se usaron informes y publicaciones de distintos organismos oficiales, por ejemplo, la Comisión Nacional de Seguros y Fianzas (CNSF), la Dirección General de Servicios de Investigación y Análisis (SEDIA), Secretaría de Finanzas, entre otros. Que fueron usados para los antecedentes y la justificación de este trabajo de investigación.

1.7 Técnicas de recolección de datos

Los instrumentos de recolección de datos fueron entrevistas. La entrevista una técnica de gran utilidad en la investigación cualitativa para recabar datos (Díaz-Bravo, Torruco-García, Martínez-Hernández y Varela-Ruiz, 2013). Su uso se planeó en el primer acercamiento al RPPyC, para conocer en términos generales las funciones del Departamento de Informática; consistió en una entrevista semiestructurada, esto para aclarar términos, identificar ambigüedades y reducir formalismos en el momento.

Así también, para este trabajo de investigación se utilizaron tres diferentes instrumentos de recolección de información, el primero para identificar los activos críticos de información en el Departamento de Informática del RPPyC, el segundo para identificar

las amenazas de los activos de la información del primer instrumento y el tercero fue la aplicación móvil para evaluar el grado de cumplimiento de la norma ISO/IEC 27002:2013.

1.8 Tipos de programación

En este trabajo se utilizaron dos herramientas tecnologías para desarrollar el software planteado. Estas fueron Flutter SDK y MySQL, el primero fue el kit de desarrollo de software para crear la aplicación Android para la aplicación de la norma ISO/IEC 27002:2013. Mientras que el segundo se requirió para almacenar y acceder a los datos que se guardaron por medio de la aplicación móvil desarrollada en Flutter.

Para lograr este vínculo se requirió usar el modelo Cliente-Servidor. El cual es un mecanismo de comunicación que se realiza mediante peticiones y respuestas. Donde los clientes realizan peticiones al servidor, que este las atiende y devuelve la petición solicitada al cliente correspondiente (Sánchez y Montes, 2014).

Lo anterior ya que se requirió que la aplicación móvil (cliente) se conectara a un equipo que realizaba la función de servidor donde se encontraba la base de datos MySQL. Las peticiones que se realizaban fueron para insertar y consultar la información que se originaba de la aplicación móvil. Esas peticiones se realizaban mediante el lenguaje SQL, un lenguaje de programacion que una de sus características es que permite la manipulación de datos (Ramos, 2018). Dentro de la manipulación de los datos que se requirieron fue la inserción, eliminación y consulta de datos.

Capítulo 2. Marco teórico

2.1 Marco referencial

Las organizaciones se enfrentan a distintos tipos de riesgos e inseguridades procedentes de focos diversos (ISOTools, 2019). Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

Lo que ha generado diversos trabajos de investigación en el tema como la seguridad de la información, el análisis y gestión de riesgos o la aplicación de estándares de estándares internacionales sobre la Seguridad de la Información.

Un caso de éxito en la adopción de la familia de estándares ISO/IEC 27000, fue el proyecto realizado por Chierici et al. (2019). Éste consistió en un proyecto de SGSI en el INFN-CNAF para cumplir con la ISO 27001, se describió el proceso realizado y al final se obtuvo la certificación de esta. En las conclusiones, se hace mención de que esa certificación fue sólo el punto de partida de un proceso de mejora continua y ese certificado coloca al centro de datos INFN-CNAF en un buen lugar para futuras colaboraciones que requieran garantía de la seguridad de datos y acato de los estándares de calidad.

En el trabajo de Velasco et al., 2018 se evaluó el bajo nivel de seguridad dentro de los procesos críticos de la industria manufacturera para reducir los riesgos de productividad. Este estudio propuso la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO 27001, aplicando el

Ciclo de Deming (Planificar-Hacer-Verificar-Actuar). En este trabajo se menciona que algunos de los beneficios de la implementación en la organización fueron las siguientes:

- Mitigar vulnerabilidades, amenazas y riesgos en los sistemas de información a niveles aceptables.
- Generar una posición proactiva centrada en la seguridad de la información.
- Determinar roles y responsabilidades centrados en la seguridad de la información.
- Aumentar los niveles de disponibilidad, confidencialidad e integridad en sus procesos.
- Proteger la información vital (clientes internos y externos, procesos).
- Tener planes de continuidad comercial y recuperación ante desastres.
- Desarrollar indicadores de desempeño del SGSI.
- Aumentar la competitividad, la confianza y la garantía en los mercados nacionales e internacionales.

En la investigación de Pacheco (2018), llamada “Políticas de seguridad de la información de aprovechamiento estudiantil en la educación general básica basado en la norma ISO 27002”, se diseñó, elaboró y aplicó un plan de políticas de seguridad de la Información, a través de la metodología MAGERIT y la Norma ISO 27002:2013 para la gestión del riesgo, con el fin de garantizar el cumplimiento de uno de los requerimientos de seguridad de la información, el del servicio de integridad de la información de aprovechamiento del servicio de gestión estudiantil.

En el trabajo anterior se llegó a la conclusión que el plan desarrollado fue una alternativa de solución que no solo buscó proteger y administrar de manera eficiente los

procesos de control de gestión escolar, sino que también buscó proteger, prevenir o disminuir los incidentes provocados por amenazas y riesgos a la información.

Díaz y Reyes (2015) en su trabajo titulado “Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT” buscaron el objetivo principal de describir cómo realizar el aseguramiento de los equipos de cómputo asignados a estaciones de trabajo, con sistema operativo Linux-Debian, pertenecientes a Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), alineados al estándar de buenas prácticas de seguridad de la información ISO/IEC 27002:2013.

De igual manera, el proyecto de tesis presentado en la División Académica de Informática y Sistemas de la universidad Juárez Autónoma de Tabasco el trabajo de tesis de Zacarias (2019) llamado: “Estudio sobre la seguridad de la información con un enfoque en la norma ISO/IEC 27002:2013, caso: Coordinación de Desarrollo y Soporte de Sistemas de la Dirección de Tecnologías de Información e Innovación de la UJAT”. En este trabajo tenía por objetivo identificar las prácticas de seguridad de la información que permitieran mitigar vulnerabilidades y amenazas existentes en la Coordinación.

En la tesis anterior concluyó que la metodología propuesta permitió cumplir exitosamente la finalidad del estudio, que fue proponer prácticas de seguridad de la información para la Coordinación de Desarrollo y Soporte de Sistemas basadas en la norma ISO/IEC 27002:2013 que le permitan mantener y mejorar la confidencialidad, integridad y disponibilidad de la información de la coordinación.

2.2 Marco conceptual

2.2.1 Información

Información es un dato con significado específico, es decir, conocimiento que puede transmitirse en cualquier formato (escritura, audio, visual, electrónica o de otra manera). La información puede ser (Djapić & Lukić, 2007):

- impreso o escrito en papel
- almacenado electrónicamente (memorizado)
- transmitido por correo o electrónicamente
- mostrado en el sitio web de la corporación
- verbal - hablado en una conversación
- conocimiento - habilidades de los empleados

2.2.2 Ciberataque

Intentos de acceder ilegalmente a un sistema electrónico o a una red informática con el fin de extraer información o interrumpir su funcionamiento (McKinsey & Company, s.f.).

2.2.3 Ciberseguridad

Se define como el conjunto de acciones tomadas por organizaciones e individuos para reducir la probabilidad de sufrir un ciberataque (McKinsey & Company, s.f.).

2.2.4 Seguridad de la información

Se define un sistema de seguridad de la información como:

> Un conjunto de lineamientos en los ámbitos de las dimensiones situación actual, seguridad física y seguridad lógica, que consideran estrategias definidas como son los indicadores de estructura organizacional, políticas de seguridad, control de acceso físico, gestión de activos, respaldo de la información, entre otros, los cuales hacen frente a los riesgos de seguridad en una organización, enfocándose en asegurar la continuidad de las operaciones en una empresa, reduciendo las amenazas a los activos y limitando el impacto de violación de seguridad a su mínima expresión, con la finalidad de mantener un ambiente seguro. (Salamanca, 2016, p.121)

La seguridad de la información tiene por objetivo preservar las siguientes propiedades de la información: confidencialidad, integridad y disponibilidad. Estos tres permite mantener y mejorar un SGSI (Bonilla, 2018). La seguridad de la información a menudo se define en el contexto de proporcionar atributos de seguridad de la información (Ver tabla 3).

Tabla 3.
Atributos de seguridad de la información.

Atributo	Características
Confidencialidad	Siempre que el acceso a la información esté restringido sólo para usuarios autorizados
Integridad	Proporcionar que la información se conserve en su forma original, excepto cuando el personal autorizado la actualice o la borre.
Disponibilidad	Siempre que la información esté disponible para personas autorizadas en el momento requerido.

Nota: Adaptado de Szczepaniuk et al. (2019).

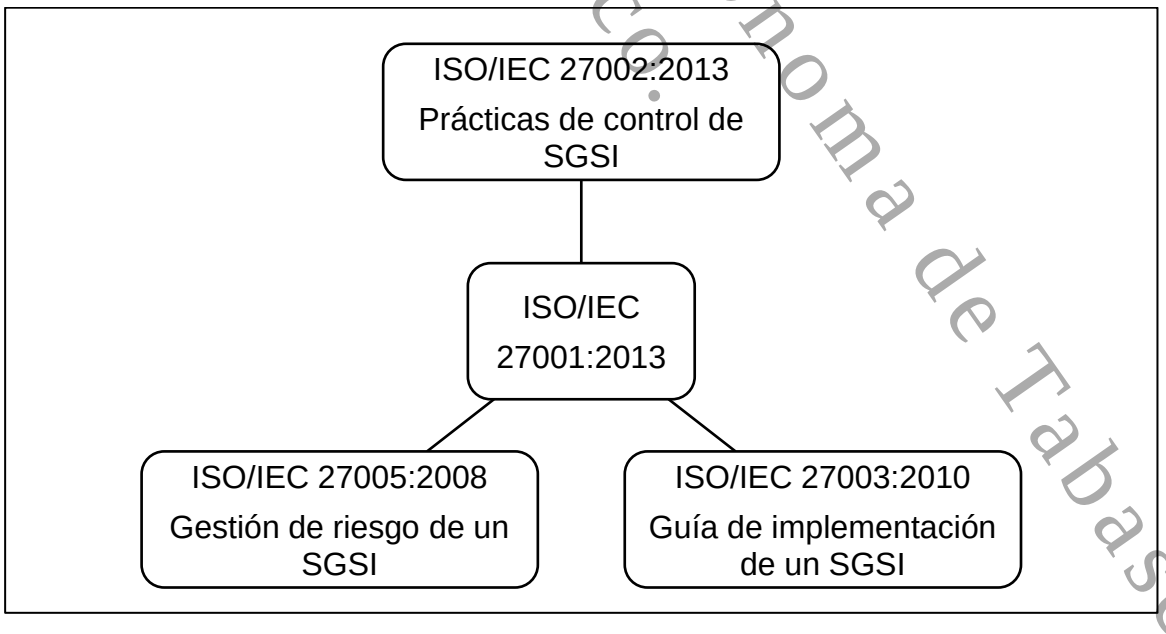
2.2.5 Norma

La Real Academia Española (2020) define una norma como la regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.

2.2.6 Familia ISO/IEC 27000

De acuerdo con Disterer (2013), la Organización Internacional de Normalización (ISO) es una organización fundada en 1946 y apoyada por 159 países; ISO es el principal organismo emisor de normas internacionales. Entre las normas de seguridad de la información se encuentran la serie ISO 27000 que se desarrollaron en cooperación con la Comisión Electrotécnica Internacional (IEC). En la figura 10, se muestran las principales normas de la serie 27000.

Figura 8
Principales normas basadas en los estándares de la ISO/IEC 27000.

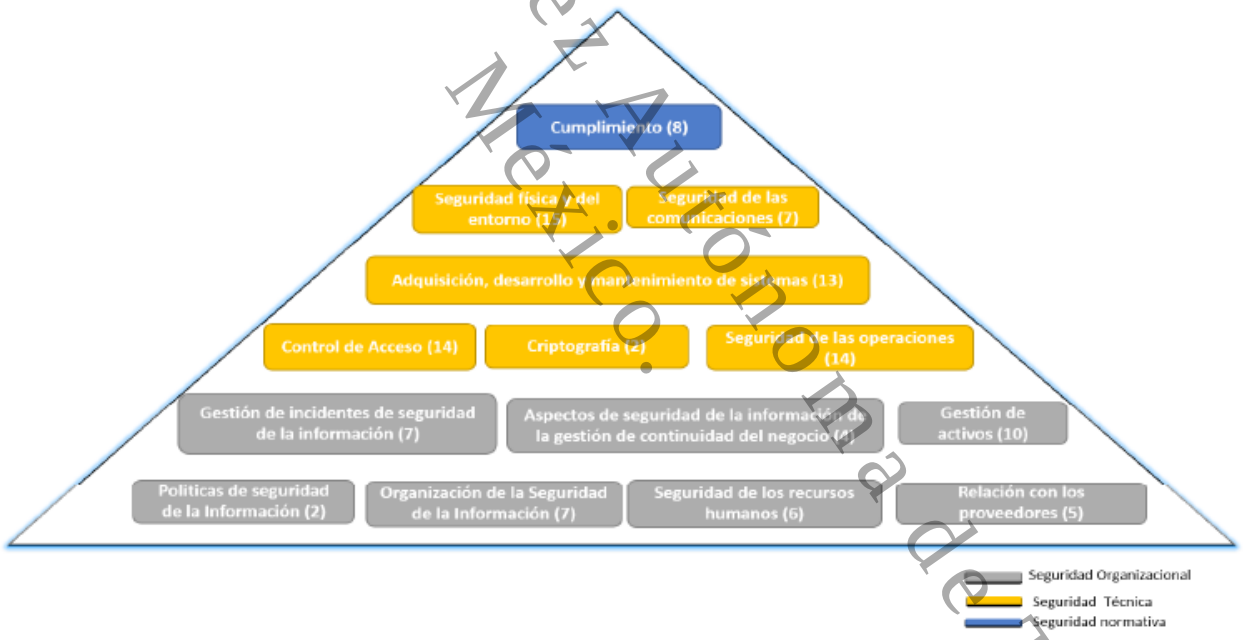


Nota: Valencia-Duque y Orozco-Alzate (2017).

2.2.7 ISO/IEC 27002:2013

Se trata de una guía de buenas prácticas a partir de objetivos de control y controles recomendables a nivel de seguridad de la información. A diferencia de ISO 27001, no es un estándar certificable (Borbón, s.f.). La ISO menciona que esta norma cuenta con 14 dominios (cláusulas de control de seguridad) y 35 objetivos de control (categorías de seguridad) que describen las áreas que hay que considerar para garantizar la seguridad de la información de una organización (Como se citó en Zacarias, 2019) (Ver figura 11).

Figura 9
Estructura de los controles de la norma ISO/IEC 27002:2013



Nota: Valencia-Duque y Orozco-Alzate (2017).

En total, el documento recomienda un total de 114 controles que se pueden considerar para su aplicación (aunque no es obligatorio cumplirlos todos).

De acuerdo con International Organization for Standardization [ISO] (2020) menciona que la ISO/IEC 27002:2013 ha sido diseñada para ser usada en organizaciones que intentan:

- Seleccionar controles dentro de un proceso de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001.
- Implementar controles de seguridad de la información comúnmente aceptados
- Desarrollar sus propias guías de gestión de seguridad de la información.

2.3 Marco tecnológico

2.3.1 Kit de desarrollo de software (SDK): Flutter

Como menciona en la página oficial, Flutter es el kit de herramientas de UI de Google para realizar hermosas aplicaciones, compiladas nativamente, para móvil, web y escritorio desde una única base de código (Flutter, 2020b). Esto mediante Dart, el lenguaje utilizado en este SDK.

Flutter es un proyecto open-source alojado en Github con la contribución de Google y la comunidad. Este framework provee a los desarrolladores con herramientas para crear aplicaciones hermosas y de aspecto profesional, además cuenta con la capacidad de personalizar cualquier aspecto de la aplicación.

2.3.2 Lenguaje de programación: Dart

Un lenguaje de programación es una herramienta que permite desarrollar software o programas para computadora. Los lenguajes de programación son empleados para diseñar e implementar programas encargados de definir y administrar el comportamiento

de los dispositivos físicos y lógicos de una computadora. Lo anterior se logra mediante la creación e implementación de algoritmos de precisión que se utilizan como una forma de comunicación humana con la computadora (Coordinación de Universidad Abierta y Educación a Distancia de la UNAM, s.f.).

Uno de esos lenguajes es Dart. Dart es un lenguaje de programación de propósito general. Es un lenguaje orientado a objetos con sintaxis de estilo C basado en clases, diseñado con facilidad de uso, familiaridad con la gran mayoría de programadores y escalabilidad en mente. Dart está destinado a proporcionar una plataforma específicamente diseñada para satisfacer las necesidades futuras y las plataformas emergentes de software/hardware (Bracha, 2015).

Dart es un lenguaje poderoso e interactivo que se espera que sea ampliamente adoptado por los desarrolladores de la misma manera que se adopta Java en la actualidad. El código Dart se puede reutilizar para teléfonos inteligentes (clientes) o servidores (Hassan, 2020).

2.3.3 Entorno de desarrollo integrado (IDE): Android Studio

Android Studio es el entorno de desarrollo integrado oficial (IDE) para la plataforma Android. La primera versión estable se lanzó en diciembre de 2014. Android Studio está diseñado específicamente para el desarrollo de Android. Ofrece herramientas personalizadas para desarrolladores de Android (AMC College, n.d.).

Android Studio es además un potente editor de códigos y las herramientas para desarrolladores de IntelliJ, Android Studio ofrece funciones que aumentar la productividad

cuando se desarrolla aplicaciones para Android, como las siguientes (Android Developers, 2020):

- Una herramienta flexible de compilación de código basado en Gradle.
- Un emulador rápido y cargado de funciones.
- Un entorno unificado donde puedes desarrollar para todos los dispositivos Android.
- Aplicación de cambios para insertar cambios de códigos y recursos a la aplicación en ejecución sin reiniciar la aplicación.
- Integración con GitHub y plantillas de código para ayudarte a compilar funciones de aplicaciones comunes y también importar código de ejemplo.
- Variedad de marcos de trabajo y herramientas de prueba.
- Herramienta de análisis de código llamada Lint para identificar problemas de rendimiento, usabilidad y compatibilidad de la versión, entre otros.
- Compatibilidad con C++ y NDK.
- Compatibilidad integrada para Google Cloud Platform, que facilita la integración con Google Cloud Messaging y App Engine.

2.3.4 Metodología de análisis y gestión de riesgos

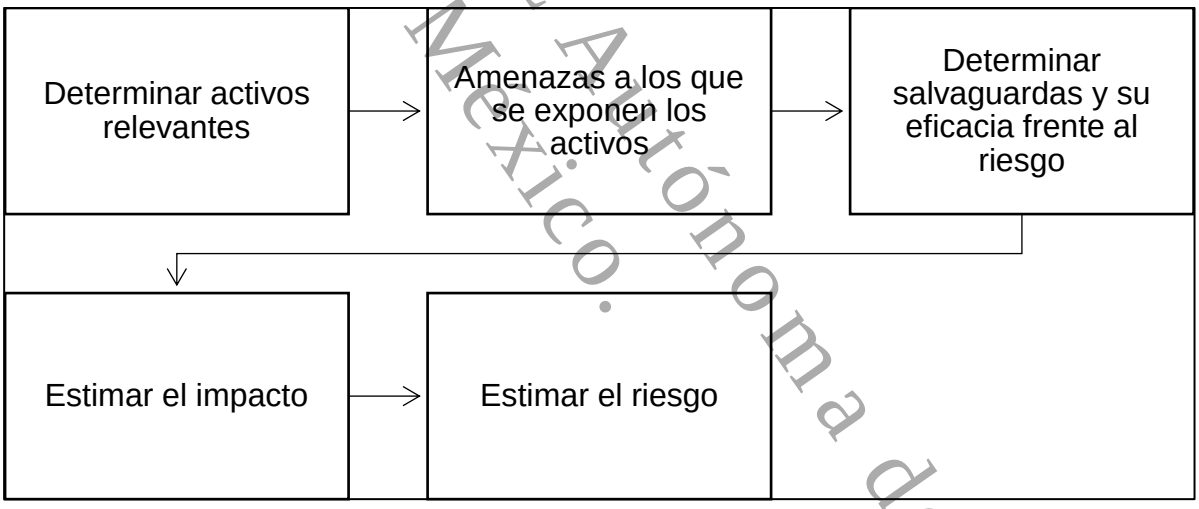
En el caso del análisis y gestión de riesgos se hizo uso de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) en su versión 3. De acuerdo con el Ministerio de Hacienda y Administraciones Públicas de España (2012) MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo

para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

En España, el Consejo Superior de Administración Electrónica estableció la metodología MAGERIT con el objetivo de desplegar un marco común para el análisis y gestión de riesgos en sistemas de información como base de las normas ISO/IEC 27000 (Vicente, Mateos & Jiménez-Martín, 2014).

En la figura 8 se observan los pasos del método de análisis de riesgo de la metodología MAGERIT:

Figura 10
Método de análisis de riesgo



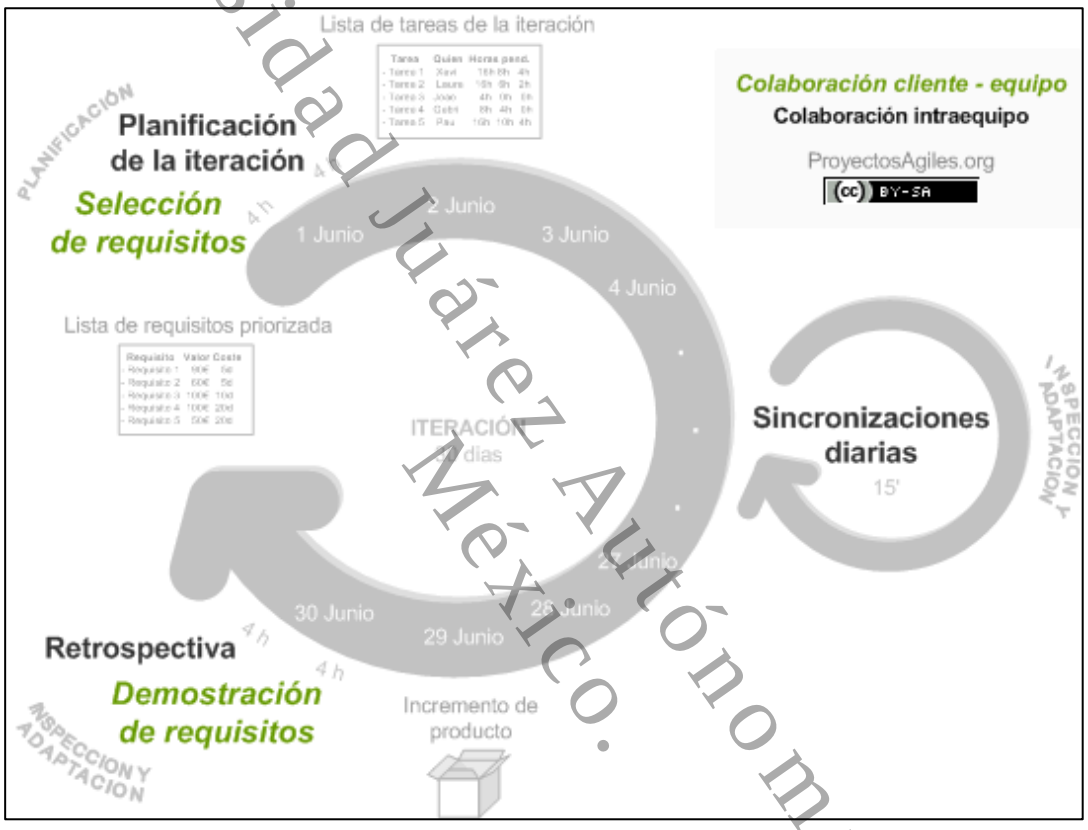
Nota: Elaboración propia basado en Ministerio de Hacienda y Administraciones Públicas de España (2012)

2.3.5 SCRUM

En Scrum, un proyecto se ejecuta en ciclos temporales cortos y de duración fija. Cada iteración tiene que proporcionar un resultado completo, un incremento de producto

final que sea susceptible de ser entregado con el mínimo esfuerzo al cliente cuando lo solicite. En la figura 9 se muestra el marco de trabajo de Scrum.

Figura 11
¿Cómo funciona Scrum?



Nota: Proyectos Agiles (2020).

SCRUM propone las siguientes tres fases (Proyectos Agiles, 2020):

Planificación de la iteración

- Selección de requisitos. Se presenta al equipo la lista de requisitos priorizada del producto o proyecto. El equipo pregunta al cliente las dudas que surgen y selecciona los requisitos más prioritarios que prevé que podrá completar en la iteración, de manera que puedan ser entregados si el cliente lo solicita.

- Planificación de la iteración. El equipo elabora la lista de tareas de la iteración necesarias para desarrollar los requisitos seleccionados. La estimación de esfuerzo se hace de manera conjunta y los miembros del equipo se autoasignan las tareas, se autoorganizan para trabajar incluso en parejas (o grupos mayores) con el fin de compartir conocimiento (creando un equipo más resiliente) o para resolver juntos objetivos especialmente complejos.

Ejecución de la iteración

- Cada día el equipo realiza una reunión de sincronización. El equipo inspecciona el trabajo que el resto está realizando (dependencias entre tareas, progreso hacia el objetivo de la iteración, obstáculos que pueden impedir este objetivo) para poder hacer las adaptaciones necesarias que permitan cumplir con la previsión de objetivos a mostrar al final de la iteración.

Inspección y adaptación

El último día de la iteración se realiza la reunión de revisión de la iteración. Tiene dos partes:

- Revisión (demostración). El equipo presenta los requisitos completados en la iteración, en forma de incremento de producto preparado para ser entregado con el mínimo esfuerzo. En función de los resultados mostrados y de los cambios que haya habido en el contexto del proyecto, se realizan las adaptaciones necesarias de manera objetiva, ya desde la primera iteración, replanificando el proyecto.

- Retrospectiva. El equipo analiza cómo ha sido su manera de trabajar y cuáles son los problemas que podrían impedirle progresar adecuadamente, mejorando de manera continua su productividad.

2.4 Marco legal

Para el desarrollo de la aplicación móvil, no se realizará un marco legal de contratación puesto que las herramientas a utilizar cuentan con las características de uso libre y/o de código abierto.

Las disposiciones legales para la tecnología que se utiliza para el desarrollo de la aplicación de prueba mediante el lenguaje de programación Dart, haciendo uso del SDK Flutter y el IDE Android Studio; autorizados para el uso libre, siempre que se respete las licencias que rigen estas herramientas de software. En el caso de Dart y Flutter, se encuentran bajo la licencia de Creative Commons Attribution 4.0 y Android Studios bajo Apache 2.0. Las licencias de cada una se encuentran detalladas en los Anexos A, B y C.

2.4.1 Creative Commons

Todas las licencias Creative Commons tienen características en común. Cada licencia ayuda a las creadoras (licenciantes) a mantener sus derechos autorales al mismo tiempo que permiten a otras copiar, distribuir, y hacer algunos usos de su obra, por lo menos de forma no comercial. Todas las licencias Creative Commons aseguran también que las licenciantes obtengan el crédito que merecen por sus obras. Las licencias Creative Commons funcionan alrededor del mundo y duran tanto tiempo como sea aplicable el derecho autoral (porque se basan en este). Estas características en común sirven como la base a partir de la cual las licenciantes pueden escoger por otorgar más

permisos cuando decidan cómo quieren que su obra sea usada (Creative Commons, 2020).

2.4.2 Apache 2.0

La versión 2.0 de la licencia Apache, aprobada por la Apache Software Foundation (ASF) en 2004, ayuda a lograr con el objetivo de proporcionar productos de software fiables y de larga duración a través del desarrollo de software colaborativo de código abierto (Apache, 2004).

Como cualquier otra de las licencias de software libre, la Licencia Apache permite al usuario del software la libertad de usarlo para cualquier propósito, distribuirlo, modificarlo, y distribuir versiones modificadas de ese software.

La Licencia Apache no exige que las obras derivadas (versiones modificadas) del software se distribuyan usando la misma licencia, ni siquiera que se tengan que distribuir como software libre/open source. La Licencia Apache sólo exige que se mantenga una noticia que informe a los receptores que en la distribución se ha usado código con la Licencia Apache.

Capítulo 3. Aplicación de la metodología y desarrollo

En este capítulo se describe lo realizado en tres de las cuatro fases que conforman la metodología aplicada. Donde en la primera fase se describe el análisis realizado en el Departamento de Informática del Registro Público de la Propiedad y del Comercio de Tabasco, así también de las dos fases utilizadas de la metodología MAGERIT para el análisis de riesgo. En la fase dos se mencionan los pasos para el desarrollo de la aplicación móvil basado en la norma ISO/IEC 27002:2013 y por último finalizando con la fase tres, de la evaluación de la seguridad del departamento con la herramienta móvil desarrollada.

3.1 Fase 1: Análisis del Departamento de Informática (análisis del área de trabajo)

3.1.1 Entrevista

Debido a las restricciones del acuerdo de confidencialidad, lo recabado en la entrevista se omitieron datos como nombres del personal, nombre del sistema registral, software que utilizan, así como el equipo tecnológico.

Actualmente la institución cuenta con seis oficinas registrales, cada una con sus respectivas jurisdicciones distribuidas en diferentes municipios del estado. Siendo la matriz la oficina ubicada en el municipio de Centro, Tabasco. En esta se encuentran el Departamento de Informática, que se encarga de dar soporte tanto a esta como a las demás oficinas foráneas, mantener el correcto funcionamiento de todas las oficinas, así como del sistema registral.

En la entrevista realizada con el jefe del departamento, se comentó que han sufrido incidencias que han afectado las actividades en las oficinas donde se han presentado como la afectación de software o de hardware en el equipo de cómputo y servidores, fallas en el equipo auxiliar, problemas de energía eléctrica, entre otras. La información recabada, servirá para el siguiente punto a tratar.

3.1.2 Análisis de activos y amenazas

El análisis de riesgo permite identificar los activos de la información con los que cuenta el caso de estudio y así mismo a las amenazas a los cuales están expuestos.

De acuerdo con el libro I – Método, el análisis de los riesgos se lleva a cabo por las siguientes tareas (Ministerio de Hacienda y Administraciones Públicas de España, 2012):

- MAR.1 – Caracterización de los activos
- MAR.2 – Caracterización de las amenazas
- MAR.3 – Caracterización de las salvaguardas
- MAR.4 – Estimaciones de impacto

Pero como se mencionó en la sección 1.4 del presente trabajo, por lo tanto, solo se realizaron las dos primeras tareas de MAGERIT. A continuación, se desarrollarán cada una de éstas.

3.1.3 Caracterización de los activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, especificar por el tipo de activo, identificando las relaciones entre los diferentes activos,

determinando en qué dimensiones de seguridad son importantes y valorar esa importancia.

Esta actividad se divide en tres subtareas, las cuales son las siguientes:

Identificación de los activos

Como resultado de la entrevista, se identificaron 21 activos en el Departamento de Informática, las cuales se muestran en la tabla 4.

Tabla 4
Identificación de activos

Tipo de activo	Nombre
[D] Datos/Información	Código ejecutable
	Copias de respaldo
[K] Claves criptográficas	Claves de autentificación
[SW] Software	Sistema registral 1
	Sistema registral 2
[HW] Hardware	Servidores
	Computadoras
	Switches
	Firewall
	Máquinas Virtuales
[Media] Soportes de información	Almacenamiento de Datos (SAN)
	Discos duros
[AUX] Equipamiento auxiliar	Sistema de alimentación ininterrumpida (UPS)
	Sistema de vigilancia
	Cableado
	Sistema de aire acondicionado
[COM] Redes de comunicaciones	Red local
	Internet
[L] Instalaciones	Edificio
	Departamento de Informática
[P] Personal	Administradores de sistemas

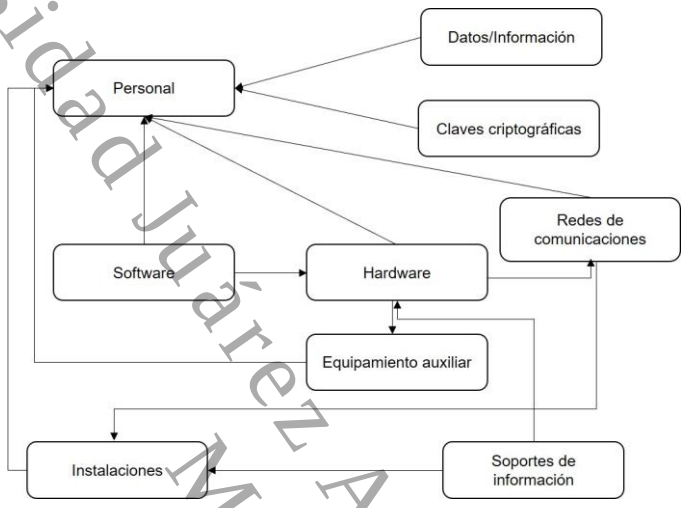
Nota: Elaboración propia.

Dependencias entre activos

En esta sección se identifican mediante un diagrama, las relaciones de dependencia entre los activos identificados en el punto anterior. En la figura 12 se observa

la relación entre cada una de estas y cómo afectaría la falla de alguna entre las que dependan de esta.

Figura 12
Dependencias entre los activos



Nota: Elaboración propia.

Valoración de los activos

Para la valoración de los activos se tomaron en cuenta las siguientes dimensiones según MAGERIT (tabla 5):

Tabla 5
Dimensiones de los activos

		Dimensiones
D	Disponibilidad	Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.
I	Integridad de los datos	Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

C	Confidencialidad	La información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.
A	Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos
T	Trazabilidad	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Nota: Elaboración propia, basado en (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

De acuerdo con la metodología MAGERIT, las dimensiones se valoran de la manera presentada en la tabla 6 conforme al criterio de evaluación presentada por la metodología.

Tabla 6
Dimensiones de valoración

Valor		**Criterio**
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante

Nota: Elaboración propia, basado en (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

En la tabla 7 se observan los resultados de la valoración de los activos.

Tabla 7
Valoración de los activos

Activos	**Dimensiones**				
	D	**I**	**C**	**A**	**T**
Código ejecutable		9			
Copias de respaldo	10	10			
Claves de autentificación				7	
Sistema registral 1		9	8		
Sistema registral 2		9	8		
Servidores	10	10			
Computadoras	7	8			
Switches	6	8			

Firewall	9	
Máquinas Virtuales	9	8
Almacenamiento de Datos (SAN)	9	8
Discos duros	5	7
Sistema de alimentación ininterrumpida (UPS)	8	
Sistema de vigilancia	6	7
Cableado		
Sistema de aire acondicionado	7	
Red local	9	
Internet	8	
Edificio	7	
Departamento de Informática	8	
Administradores de sistemas	8	

Nota: Elaboración propia.

3.1.4 Caracterización de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el activo a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

Identificación de las amenazas

En MAGERIT las amenazas se dividen en 4 rubros. Los cuales son:

- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

Dentro de cada uno de estos, se encuentran categorizados las amenazas que pueden presentarse a los activos. En la tabla 8 se mencionan las amenazas significativas para los activos identificados en el Departamento de Informática.

Tabla 8
Amenazas identificadas

Tipo de activo	Nombre	Amenaza
[D] Datos/Información	Código ejecutable copias de respaldo	Errores del administrador Destrucción de información Modificación deliberada de la información
[K]	Claves de autentificación	Suplantación de la identidad del usuario Acceso no autorizado Errores del administrador
[SW]	Sistema registral 1 Sistema registral 2	Avería de origen físico o lógico Errores de los usuarios Vulnerabilidades de los programas
[HW]	Servidores Computadoras Switches Firewall Máquinas Virtuales	Avería de origen físico o lógico Contaminación mecánica Avería de origen físico o lógico Corte del suministro eléctrico Condiciones inadecuadas de temperatura o humedad Errores de mantenimiento / actualización de equipos (hardware)
[Media]	Almacenamiento de Datos (SAN) Discos duros	Corte del suministro eléctrico Condiciones inadecuadas de temperatura o humedad Avería de origen físico o lógico Errores de mantenimiento / actualización de equipos (hardware) Caída del sistema por agotamiento de recursos
[AUX]	Sistema de alimentación ininterrumpida (UPS) Sistema de vigilancia Cableado Sistema de aire acondicionado	Caída del sistema por agotamiento de recursos Condiciones inadecuadas de temperatura o humedad Avería de origen físico o lógico Errores de mantenimiento / actualización de equipos (hardware)
[COM]	Red local Internet	Fallo de servicios de comunicaciones Errores del administrador
[L]	Edificio	Desastres naturales Ataque destructivo

	Departamento de Informática	Acceso no autorizado
[P]	Administradores de sistemas	Indisponibilidad del personal Ingeniería social (picaresca)

Nota: Elaboración propia.

Valoración de las amenazas

Una vez identificada las amenazas, se debe evaluar sobre la probabilidad de que una amenaza se presente sobre los activos. En la tabla 9 se muestra los niveles que puede alcanzar una amenaza.

Tabla 9
Niveles de las amenazas

Nivel de la amenaza		
VR	10%	Muy raro (very rare)
U	20%	Improbable (unlikely)
P	50%	Posible (possible)
VH	80%	Probable (very high)
AC	100%	Prácticamente segura (almost certain)

Nota: Elaboración propia, basado en (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

Aplicando los criterios mencionados de la tabla 9, se obtuvo la tabla 10 con la valoración de cada uno de los activos del departamento.

Tabla 10
Valoración de las amenazas

Nombre	**Amenaza**	**Nivel de amenaza**
Código ejecutable	Errores del administrador	P
	Destrucción de información	VR
Copias de respaldo	Errores del administrador	P
	Destrucción de información	P
Claves de autentificación	Suplantación de la identidad del usuario	I
	Acceso no autorizado	I
	Errores del administrador	P
Sistema registral 1	Avería de origen físico o lógico	VH

	Errores de los usuarios	VH
	Vulnerabilidades de los programas (Software)	VR
Sistema registral 2	Avería de origen físico o lógico	VH
	Errores de los usuarios	VH
	Vulnerabilidades de los programas (Software)	VR
Servidores	Avería de origen físico o lógico	P
	Contaminación mecánica	VH
	Corte del suministro eléctrico	P
	Condiciones inadecuadas de temperatura o humedad	P
	Errores de mantenimiento / actualización de equipos (hardware)	VR
Computadoras	Avería de origen físico o lógico	VH
	Contaminación mecánica	AC
	Corte del suministro eléctrico	P
	Condiciones inadecuadas de temperatura o humedad	P
	Errores de mantenimiento / actualización de equipos (hardware)	P
Switches	Avería de origen físico o lógico	VR
	Contaminación mecánica	P
	Corte del suministro eléctrico	P
	Condiciones inadecuadas de temperatura o humedad	P
	Errores de mantenimiento / actualización de equipos (hardware)	U
Firewall	Avería de origen físico o lógico	VR
	Contaminación mecánica	P
	Corte del suministro eléctrico	P
	Condiciones inadecuadas de temperatura o humedad	P
	Errores de mantenimiento / actualización de equipos (hardware)	U
Máquinas Virtuales	Errores de mantenimiento / actualización de equipos (hardware)	U
Almacenamiento de Datos (SAN)	Corte del suministro eléctrico	VR
	Condiciones inadecuadas de temperatura o humedad	P
	Avería de origen físico o lógico	P
	Errores de mantenimiento / actualización de equipos (hardware)	VR
	Caída del sistema por agotamiento de recursos	VH
Discos duros	Corte del suministro eléctrico	P
	Condiciones inadecuadas de temperatura o humedad	VR
	Avería de origen físico o lógico	VH

	Errores de mantenimiento / actualización de equipos (hardware)	P
	Caída del sistema por agotamiento de recursos	VH
Sistema de alimentación ininterrumpida (UPS)	Caída del sistema por agotamiento de recursos	P
	Condiciones inadecuadas de temperatura o humedad	P
	Avería de origen físico o lógico	VR
	Errores de mantenimiento / actualización de equipos (hardware)	VR
Sistema de vigilancia	Caída del sistema por agotamiento de recursos	P
	Condiciones inadecuadas de temperatura o humedad	VR
Cableado	Avería de origen físico o lógico	P
	Errores de mantenimiento / actualización de equipos (hardware)	P
Sistema de aire acondicionado	Caída del sistema por agotamiento de recursos	P
	Condiciones inadecuadas de temperatura o humedad	X
	Avería de origen físico o lógico	P
	Errores de mantenimiento / actualización de equipos (hardware)	P
Red local	Fallo de servicios de comunicaciones	P
	Errores del administrador	VR
Internet	Fallo de servicios de comunicaciones	P
	Errores del administrador	VR
Edificio	Desastres naturales	VR
	Ataque destructivo	P
	Acceso no autorizado	P
Departamento de Informática	Desastres naturales	VR
	Ataque destructivo	P
	Acceso no autorizado	P
Administradores de sistemas	Indisponibilidad del personal	P
	Ingeniería social	P

Nota: Elaboración propia.

3.2 Fase 2: Diseño y desarrollo de la aplicación

3.2.1 Conceptualización

Como se mencionó en el marco referencial, la norma costa de 14 dominios, 35 objetivos de control y 114 controles. Para el desarrollo de la aplicación se tomaron en cuenta todos, solo que, al momento de usar la aplicación para evaluar el grado de

cumplimiento de la norma, solo se usarán los dominios que se hayan seleccionado del resultado del análisis de riesgo.

En funcionalidad, esta consiste en una aplicación que se conecta a un servidor para obtener los objetivos y controles de la norma, para así presentarlos en pantalla, así también, los resultados se almacenan en una base de datos para su posterior consulta.

En la tabla 11 se muestra un ejemplo de la distribución de uno de los 14 dominios de la norma.

Tabla 11
Ejemplo de cómo se distribuye la norma

Dominio	Objetivos de control	Controles
Seguridad física y del entorno	Áreas seguras.	Perímetro de seguridad física Controles físicos de entrada Seguridad de oficinas, recintos e instalaciones Protección contra amenazas externas y ambientales Trabajo en áreas seguras Áreas de carga y descarga
	Equipos	Ubicación y protección de los equipos Servicios de suministro Seguridad del cableado Mantenimiento de equipos Retirada de activos Seguridad de equipos y activos fuera de las instalaciones Eliminación segura o reutilización de equipos Equipos de usuario desatendidos Política de escritorio limpio y pantalla limpia

Nota: Elaboración propia.

La aplicación móvil desarrollada se distribuye de igual manera que la tabla anterior. En primer lugar, hay una pantalla donde se muestran los 14 dominios en la pantalla

principal, al entrar en cada una se despliegan los objetivos correspondientes del dominio seleccionado y estas a la vez, los controles que la conforman, en esta sección se evaluarán individualmente cada uno de los controles por medio de un grado de madurez. Al terminar, se permite guardar el resultado obtenido y luego se continúa con el siguiente objetivo de control o comenzar con un nuevo dominio, según sea el caso.

Para establecer el grado de madurez, se maneja una escala de cinco criterios propuesto por Tovar y Salguero (2018), que se describen en la tabla 12, para así evaluar cada uno de los controles de estas y al finalizar, se muestra el resultado del objetivo de control y luego se procede a guardar el resultado del objetivo de control en la base de datos para luego continuar con los siguientes.

Tabla 12
Niveles de madurez

Niveles de madurez		
Criterio	Porcentaje	Descripción
No realizado	0%	No hay controles de seguridad de la información establecidos.
Realizado informalmente	20%	Existen procedimientos para llevar a cabo ciertas acciones en determinado momento. Estas prácticas no se adoptaron formalmente y/o no se les hizo seguimiento y/o no se informaron adecuadamente.
Planificado	40%	Los controles de seguridad de la información establecidos son planificados, implementados y repetibles.
Bien definido	60%	Los controles de seguridad de la información además de planificados son documentados, aprobados e implementados en toda la organización.
Cuantitativamente controlado	80%	Los controles de seguridad de la información están sujetos a verificación para establecer su nivel de efectividad.
Mejora continua	100%	Los controles de seguridad de la información definidos son periódicamente revisados y actualizados. Estos reflejan una mejora al momento de evaluar el impacto.

Nota: (Tovar y Salguero, 2018).

En la tabla 13 se muestran cómo se calcularon los porcentajes de cumplimiento de la norma:

Tabla 13
Cálculos de valores de los controles

Sección	Cálculo de valores
Dominio	= $(OC_1+OC_2+\ldots+OC_X) / X$
Objetivo de control (OC_1)	= C_1
Control	C_1 %
Objetivo de control (OC_x)	= $(C_1+C_2+\ldots+C_n) / n$
Control	C_1 %
Control	C_2 %
Control	C_n %

Nota: Adaptado de (Zacarias, 2019).

En lo que respecta a los objetivos de control, su porcentaje de cumplimiento es calculado mediante el promedio de los valores de los controles que lo conforman, es decir, si un objetivo de control contiene dos o más controles, su valor será el promedio del valor de dichos controles, y en los casos que el objetivo de control solo se conforma con un único control, su valor será el mismo de ese control.

De manera similar, el porcentaje de cumplimiento de cada dominio se calculó mediante el promedio de los valores de los objetivos de control que lo conforman, por lo que, si un dominio contiene dos o más objetivos de control, su valor será el promedio de los objetivos, y con el mismo valor en los casos que solo cuenten solamente con un objetivo de control.

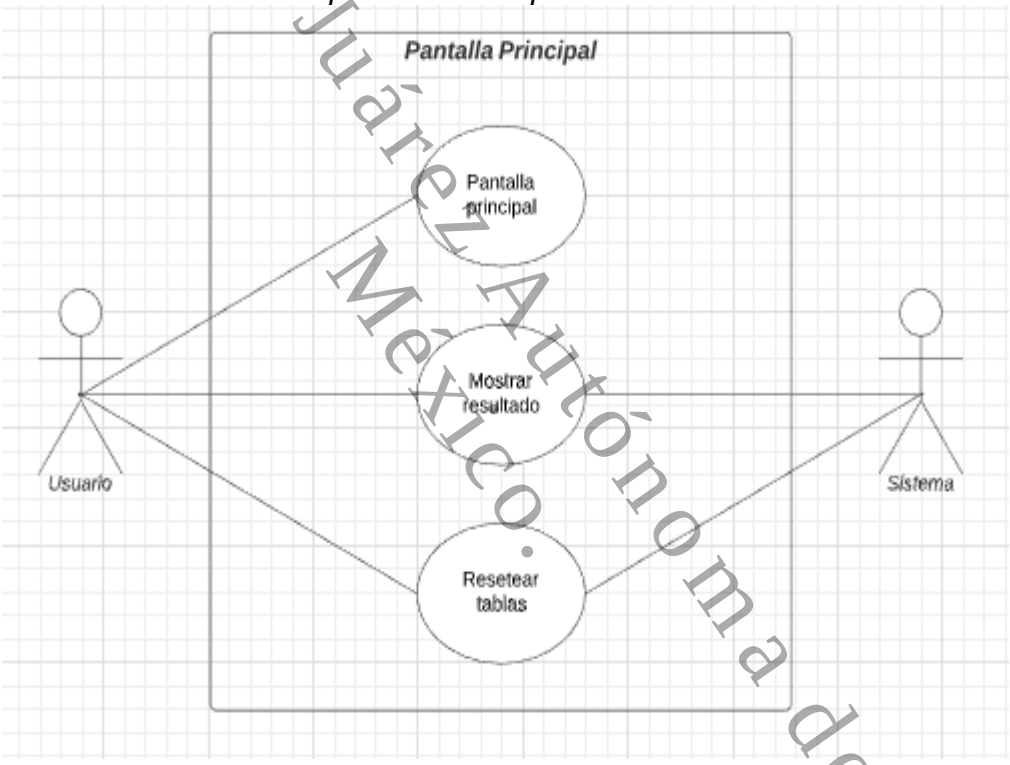
Por último, cabe aclarar que la aplicación no cuenta con un botón de finalizar o que se delimite el momento de ya no permita continuar, queda en consideración del usuario conforme a los dominios seleccionados para la evaluación.

3.2.2 Diseño

En la fase de diseño se realizaron los diagramas UML (Lenguaje Unificado de Modelado), ya que estas permiten tener una perspectiva de como el sistema interactúa con el usuario.

Diagrama de caso de uso

Figura 13
Diagrama de caso de uso de la pantalla Principal



Nota: Elaboración propia.

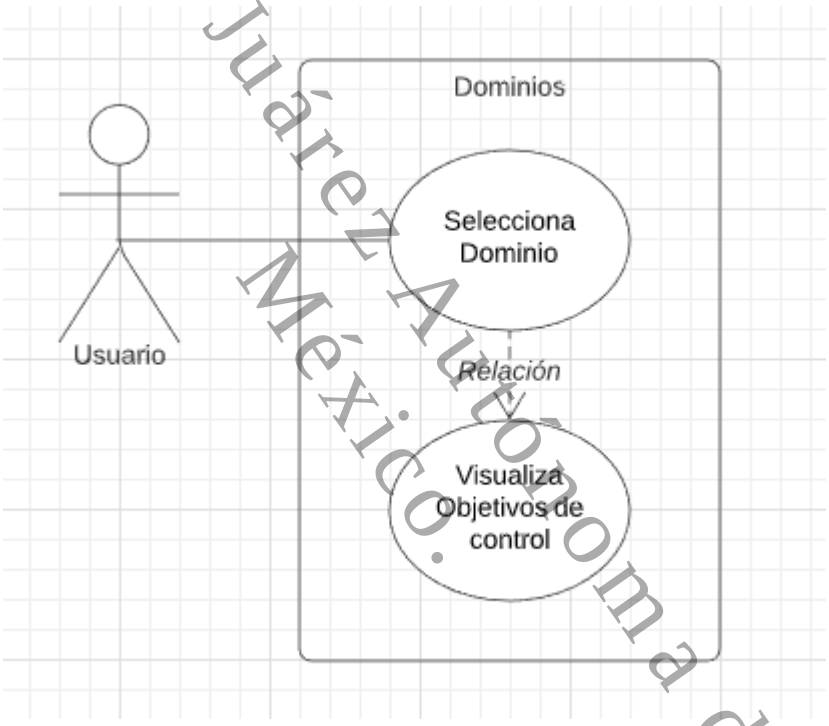
Tabla 14
Caso de uso de la pantalla Principal

Nombre del caso de uso	Pantalla principal
Actor	Usuario
Propósito	Mostrar la pantalla principal
Resumen	Mostrar los 14 dominios, opciones de mostrar resultados, borrar datos, y menú principal

Secuencia Normal	**Paso**	**Acción**
	1	El usuario ingresa a la aplicación
	2	Se muestran los 14 dominios y un menú en la parte inferior con las opciones de mostrar los resultados, una que borra los datos guardados y regresar al menú principal
	3	El usuario selecciona alguna de las opciones
	4	Se ejecuta lo solicitado

Nota: Elaboración propia.

Figura 14
Diagrama de caso de uso de la pantalla Dominios



Nota: Elaboración propia.

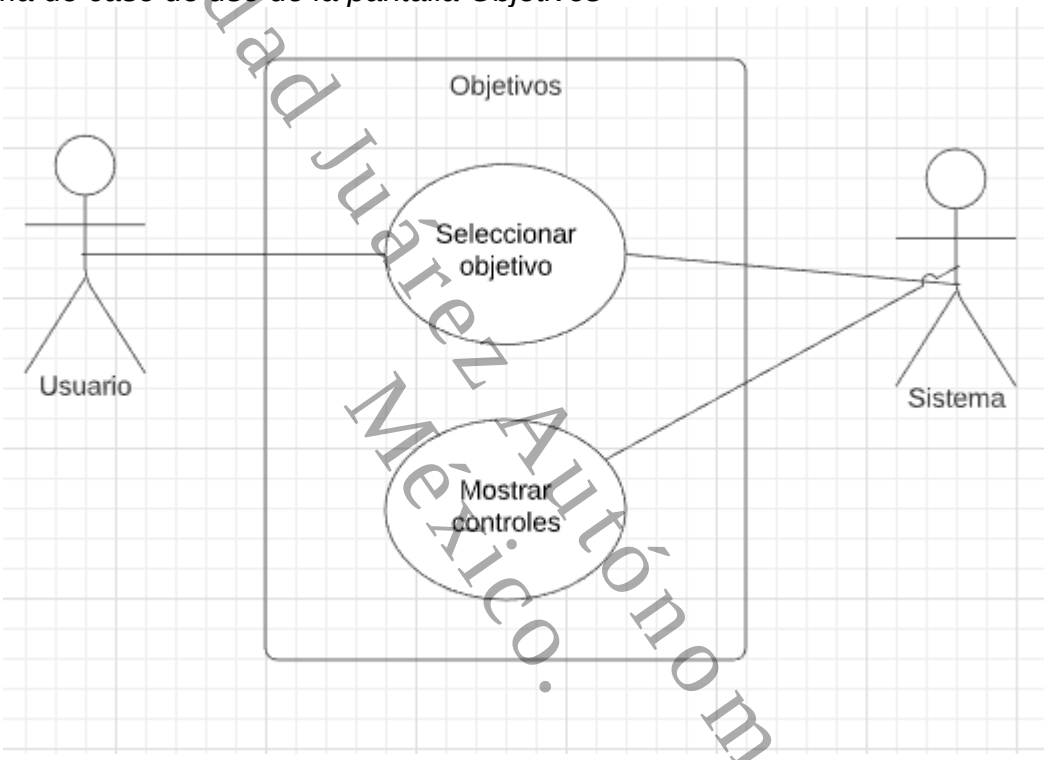
Tabla 15
Caso de uso de la pantalla Dominios

Nombre del caso de uso	Dominios
Actor	Usuario
Propósito	Mostrar los objetivos de control
Resumen	Mostrar los objetivos de control correspondientes del dominio seleccionado
Precondición	El usuario debe tener internet (datos o WiFi)

Secuencia Normal	**Paso**	**Acción**
	1	El usuario selecciona un dominio
	2	Se realiza una consulta SQL y se muestran los objetivos en pantalla.
	3	El usuario selecciona alguno de los objetivos

Nota: Elaboración propia.

Figura 15
Diagrama de caso de uso de la pantalla Objetivos



Nota: Elaboración propia.

Tabla 16
Caso de uso de la pantalla Objetivos

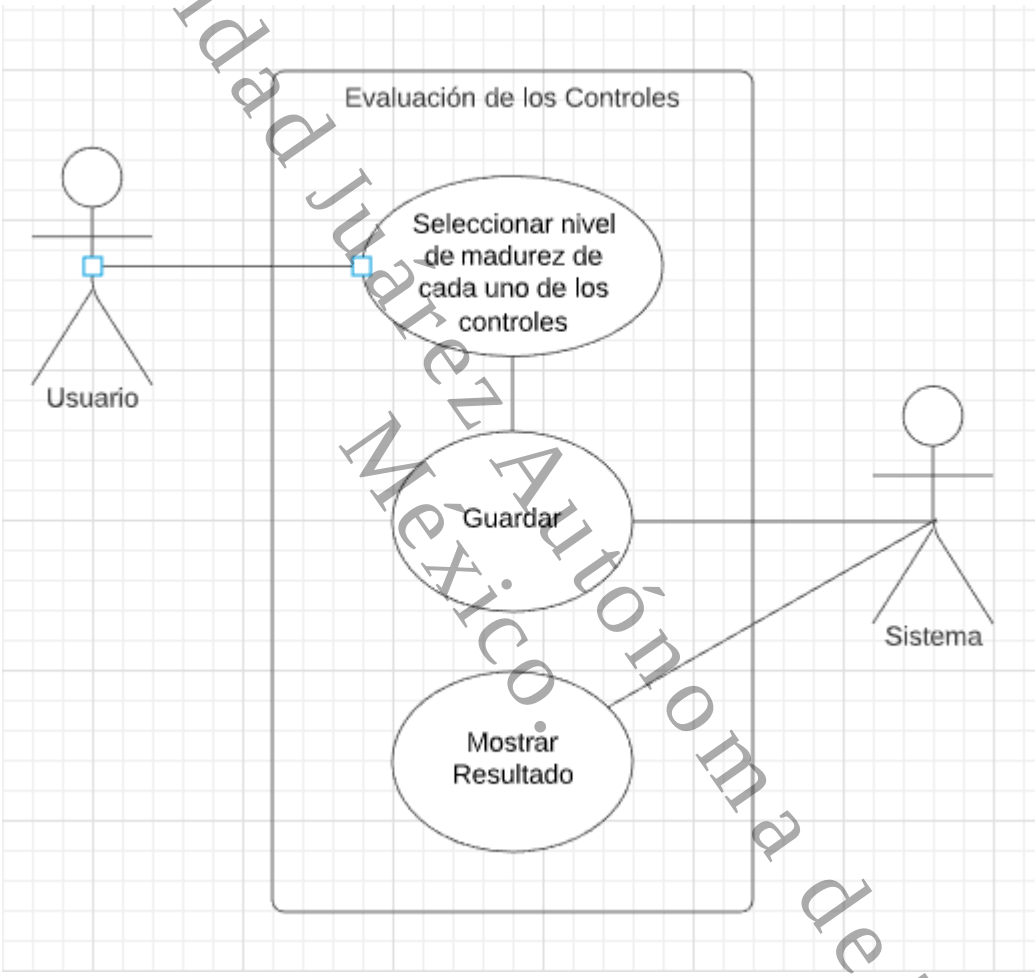
Nombre del caso de uso	Objetivos	
Actor	Usuario	
Propósito	Mostrar los objetivos de control	
Resumen	Mostrar los objetivos de control correspondientes del dominio seleccionado	
Precondición	El usuario debe tener internet (datos o WiFi)	
Secuencia Normal	**Paso**	**Acción**
	1	El usuario selecciona un objetivo de control

	2	Se realiza consulta SQL sobre los controles del objetivo de control seleccionado
	3	Se muestran los controles encontrados

Nota: Elaboración propia.

Figura 16

Diagrama de caso de uso de la pantalla Evaluación de controles



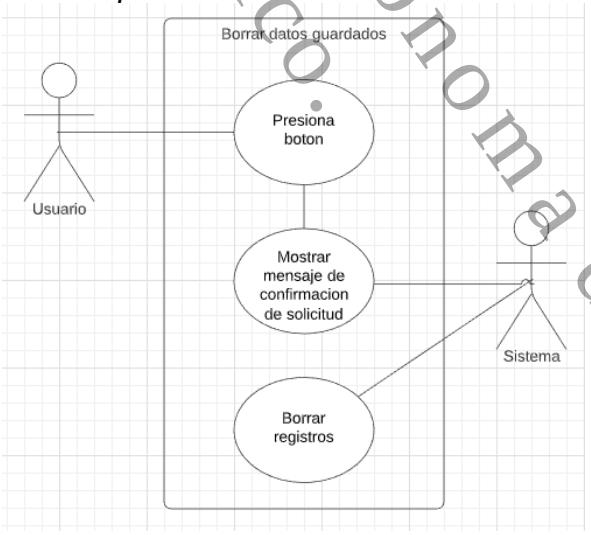
Nota: Elaboración propia.

Tabla 17
Caso de uso de la pantalla Evaluación de los controles

Nombre del caso de uso	Evaluación de los controles	
Actor	Usuario	
Propósito	Realizar la evaluación	
Resumen	Permite evaluar cada control seleccionado de manera individual	
Precondición	El usuario debe tener internet (datos o WiFi)	
Secuencia Normal	**Paso**	**Acción**
	1	El usuario selecciona el nivel de madurez del control
	2	El usuario continua con el siguiente control y repite el punto 1 hasta llegar al último control
	3	El usuario guarda lo realizado
	4	Se ejecuta comando para guardar
	5	Se muestra el resultado de la evaluación del objetivo de control
Excepciones	1	En caso de que el usuario no selecciones un nivel de madurez del control, se le notificará que no puede continuar hasta que seleccione alguno.

Nota: Elaboración propia.

Figura 17
Diagrama de caso de uso de la pantalla Evaluación de controles



Nota: Elaboración propia.

Tabla 18
Diagrama de caso de uso de la pantalla Evaluación de controles

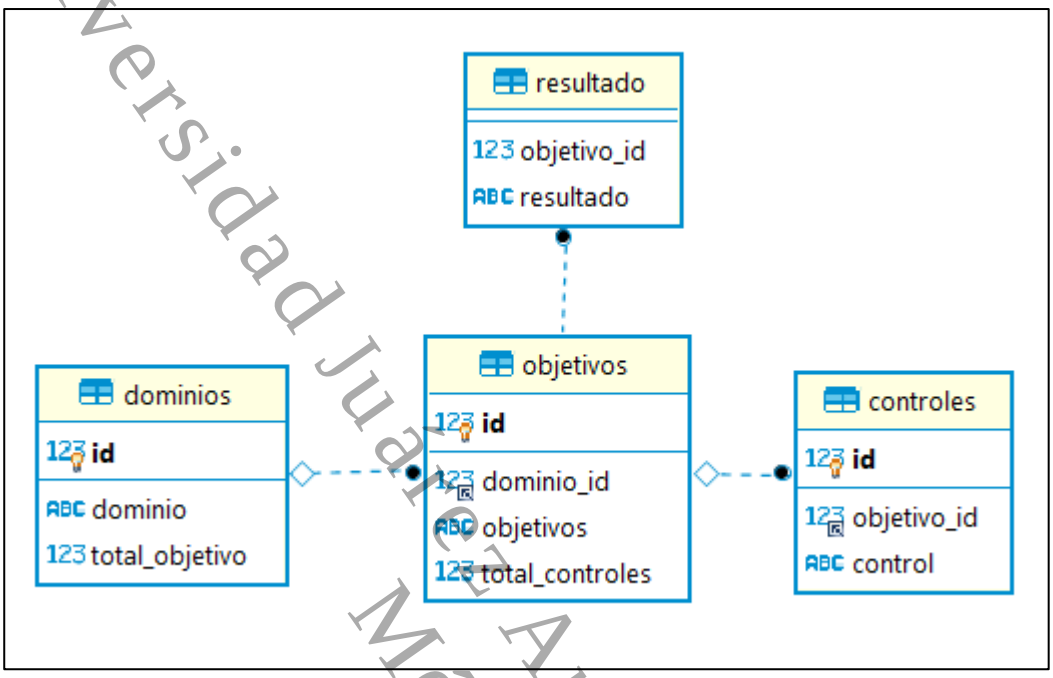
Nombre del caso de uso	Borrar datos guardados	
Actor	Usuario	
Propósito	Borrar los datos almacenados	
Resumen	Borra todos los registros guardados por el usuario para comenzar una nueva evaluación	
Precondición	El usuario debe tener internet (datos o WiFi)	
Secuencia Normal	**Paso**	**Acción**
	1	El usuario pulsa el botón de reiniciar
	2	Se muestra mensaje de advertencia sobre la acción a realizar
	3	El usuario confirma o rechaza la acción
	4	Se ejecuta la acción seleccionada

Nota: Elaboración propia.

Modelado de datos

Se creó una base de datos que consta de 4 tablas para que la aplicación acceda a los dominios, objetivos y controles que componen a la norma, y además de una tabla para almacenar los resultados de los objetivos evaluados. Para comprender esta estructura se efectúo un modelo de datos (ver figura 18), se utilizó el modelo de datos de Entidad-Relación (E-R) este tipo de modelo permite representar el esquema de BD. En donde los objetos son denominados entidades y se establece las relaciones entre ellos.

Figura 18
Modelo entidad-relación

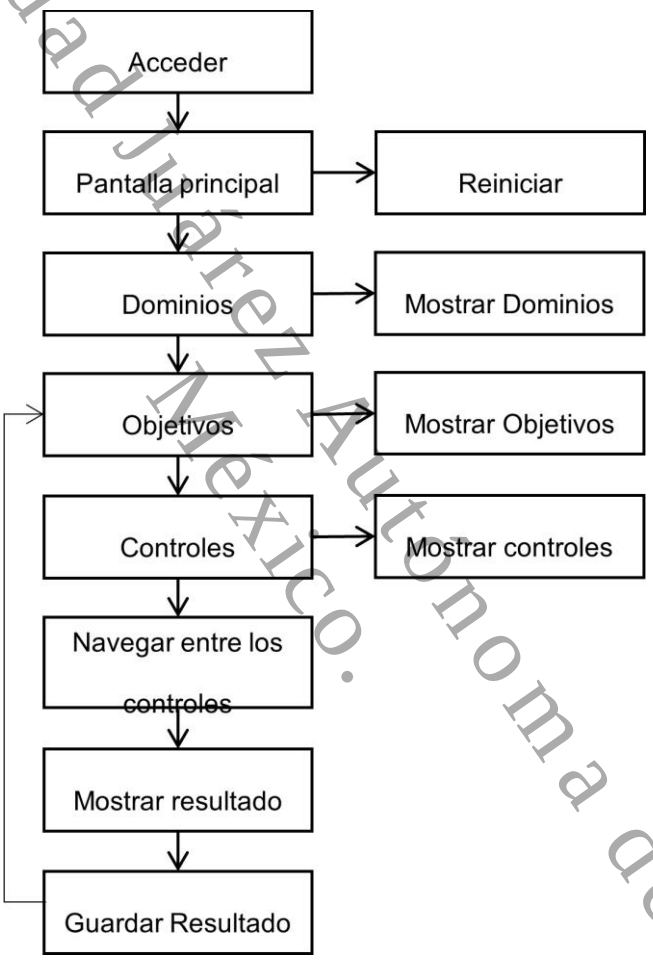


Nota: Elaboración propia.

Diagrama de navegación

En la figura 19 se presenta el diagrama de flujo de la navegación que se planteó para la aplicación móvil.

Figura 19
Diagrama de navegación de la aplicación móvil

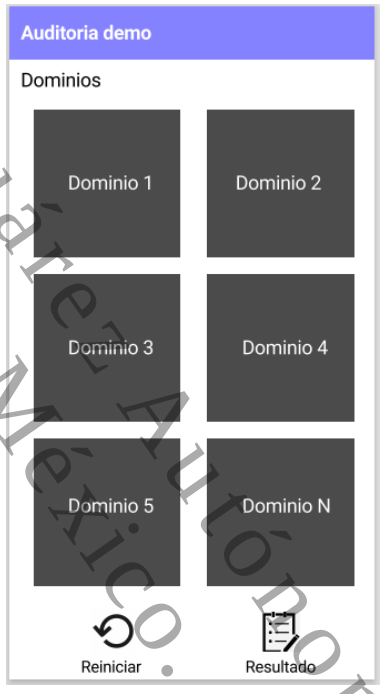


Nota: Elaboración propia.

Interfaz de usuario

A continuación, se presentan los *wireframes* o prototipos correspondientes a cada interfaz de usuario, donde se representa la estructura visual de la aplicación móvil a desarrollar.

Figura 20
Pantalla Principal



Nota: Elaboración propia.

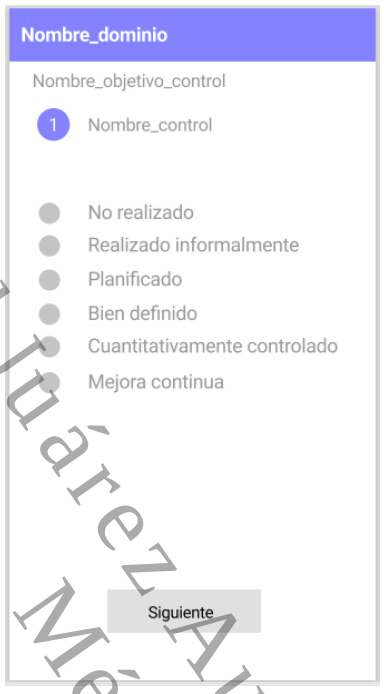
En la figura 20 se representa la pantalla principal donde se muestran los 14 dominios de la norma, así como las opciones de “Reiniciar” y “Resultado”. En “Resultado”, se muestran los resultados guardados en cualquier momento de la evaluación, mientras que, en Reiniciar se eliminan de la base de datos los datos guardados de alguna evaluación previa.

Figura 21
Pantalla Objetivos

Nota: Elaboración propia.

La figura 21 corresponde a la vista de los objetivos de control del dominio seleccionado. Donde el usuario selecciona el objetivo por el cual quiere comenzar para que se desplieguen la siguiente pantalla donde se evalúan los controles correspondientes

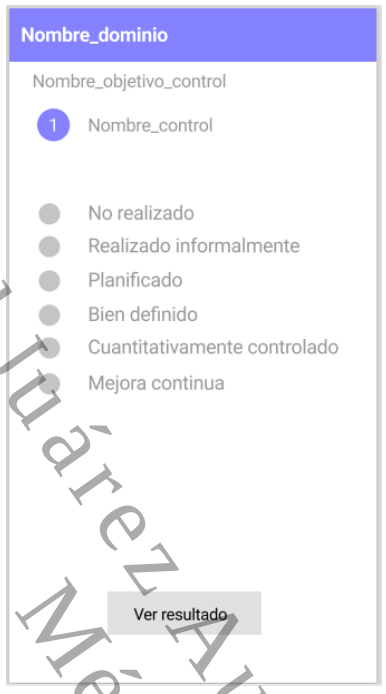
Figura 22
Pantalla Evaluación de controles (1)



Nota: Elaboración propia.

En las figuras 22 y 23 se mostrarán uno por uno los controles del objetivo seleccionado, donde se evalúan individualmente con uno de los seis *checkboxs* disponibles. El desplazamiento entre los controles es mediante el botón inferior.

Figura 23
Pantalla Evaluación de controles (2)



Nota: Elaboración propia.

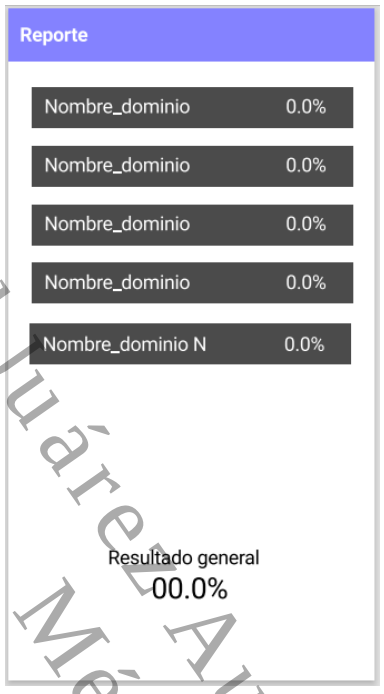
En esta figura anterior se muestra el cambio en la función del botón que anteriormente tenía la función de avanzar al siguiente control, pero al llegar al último control del objetivo correspondiente, se cambia a “Ver resultado”, lo que llevará a la pantalla de la figura 24.

Figura 24
Pantalla de Resultado

Nota: Elaboración propia.

En la figura 25 se muestra los resultados de la evaluación del objetivo de control, donde se aparece el nombre de este, el total de controles que le corresponden y el resultado obtenido. Seguido de un botón de “Guardar el resultado”, lo que permite el guardado en la base de datos para su posterior consulta.

Figura 25
Pantalla de Reporte



Nota: Elaboración propia.

En esta se mostrarán los resultados en general de los dominios que se hayan evaluado.

Figura 26
Pantalla de Reiniciar

Nota: Elaboración propia.

En la figura 26 se muestra el mensaje de advertencia de si el usuario presiona el botón de “Reiniciar”, advirtiendo que tal acción borrará todos los datos de la sección de Reporte, lo que permitiría comenzar desde cero una nueva evaluación.

3.2.3 Desarrollo

En Scrum un proyecto se ejecuta en bloques temporales cortos y fijos. Donde en cada interación (Sprint) se busca incrementar en las funcionalidades agrupadas en los módulos de la aplicación. Al finalizar cada Sprint dio como resultado una nueva versión donde se incrementaban las funcionalidades de la aplicación.

Durante la ejecución de cada interación (Sprint), el desarrollador mostraba al director del presente trabajo los avances y se retroalimentaba con las observaciones hechas para obtener una nueva versión.

Sprints

Como resultado de lo realizado en el diseño, se planificaron cuatro Sprints como puede observarse en las siguientes tablas. En donde se muestra el tiempo que tomó cada Sprint y sus actividades correspondientes (ver tablas 19 a 22).

Tabla 19
Sprint 1

Periodo	02-11-2020 al 13-11-2020	
Ítem	**Descripción**	**Tiempo estimado (horas)**
1	Crear pantalla de Inicio	8
2	Crear pantalla de Objetivos	7
3	Crear pantalla de Controles	16
4	Crear pantalla de Resultados	8
5	Crear pantalla de Reporte	10
6	Vincular pantallas	5

Nota: Elaboración propia.

En este primer Sprint, el objetivo a alcanzar era crear todas las interfaces que conformarían a la aplicación móvil a desarrollar, para que en los posteriores Sprints, se trabajaran sobre estas agregando funcionalidades y tener una nueva versión en las interaciones.

Tabla 20
Sprint 2

Periodo	16-11-2020 al 18-11-2020	
Ítem	**Descripción**	**Tiempo estimado (horas)**
1	Creación de base de datos	14
2	Creación de sentencias SQL necesarias	7

Nota: Elaboración propia.

En el Sprint 2, se trató en crear la base de datos y las tablas que se propusieron en el modelo entidad – relación de la figura 18. Así como las consultas SQL necesarias para el funcionamiento de la aplicación móvil.

Tabla 21
Sprint 3

Periodo	19-11-2020 al 02-12-2020	
Ítem	**Descripción**	**Tiempo estimado (horas)**
1	Desarrollar lógica de negocio de pantalla Inicio	15
2	Desarrollar lógica de negocio de pantalla Objetivos	8
3	Desarrollar lógica de negocio de pantalla Controles	20
4	Desarrollar lógica de negocio de pantalla Resultados	10
5	Desarrollar lógica de negocio de pantalla Reporte	9

Nota: Elaboración propia.

En el Sprint 3 consistió en desarrollar la lógica del negocio de la aplicación, es decir, los programas o clases que representan la funcionalidad de la aplicación al lado del servidor (Vega, 2020). Por lo tanto, se crearon las líneas de código necesarias para que los módulos de la aplicación funciones como se planeó en los modelos de caso de uso.

Tabla 22
Sprint 4

Periodo	03-11-2020 al 10-11-2020	
Ítem	**Descripción**	**Tiempo estimado (horas)**
1	Realizar pruebas	14
2	Corrección de errores de encontrados	29

Nota: Elaboración propia.

En el último Sprint consistió en hacer pruebas sobre lo realizado en los anteriores Sprints, esto es, simular que se realizaba una evaluación y analizar si se ejecutaban correctamente los comandos o si no funcionaba correctamente. Así también se recibió retroalimentación del director del presente trabajo y de un compañero que apoyó en las pruebas del software. Luego de esto se procedía a corregir los errores encontrados para luego volver a realizar pruebas y volver a verificar el correcto funcionamiento.

Capturas de pantalla

En las siguientes ilustraciones se muestran las interfaces de usuario de la aplicación desarrollada en Flutter SDK.

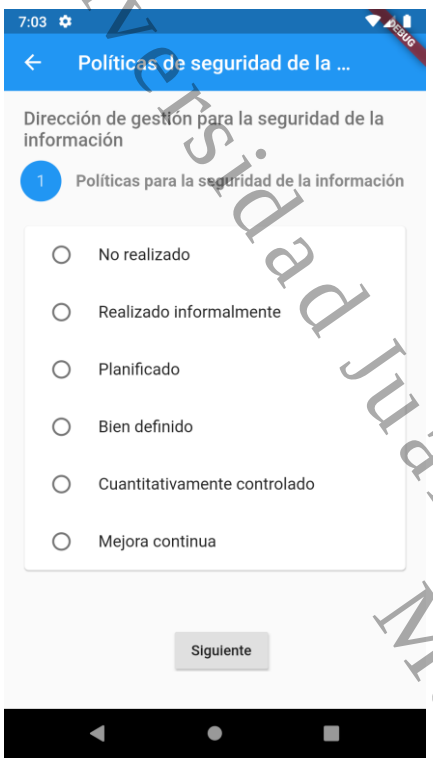
Figura 27
Interfaz: Pantalla de inicio

Nota: Elaboración propia.

Figura 28
Interfaz: Pantalla de Objetivos

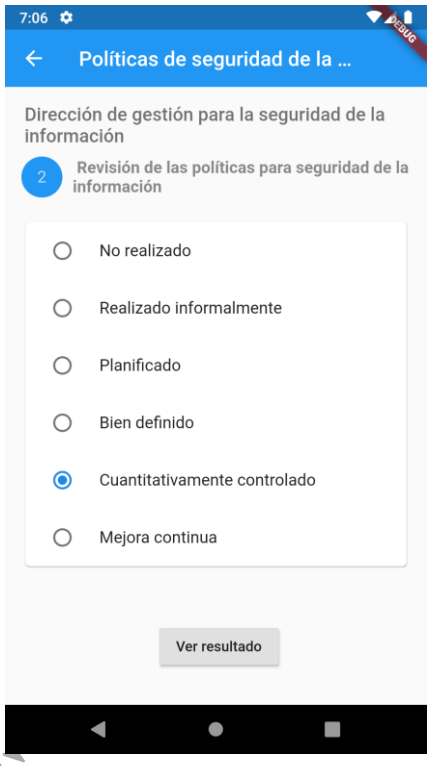
Nota: Elaboración propia.

Figura 29
Interfaz: Pantalla de Controles (1)



Nota: Elaboración propia.

Figura 30
Interfaz: Pantalla de Controles (2)

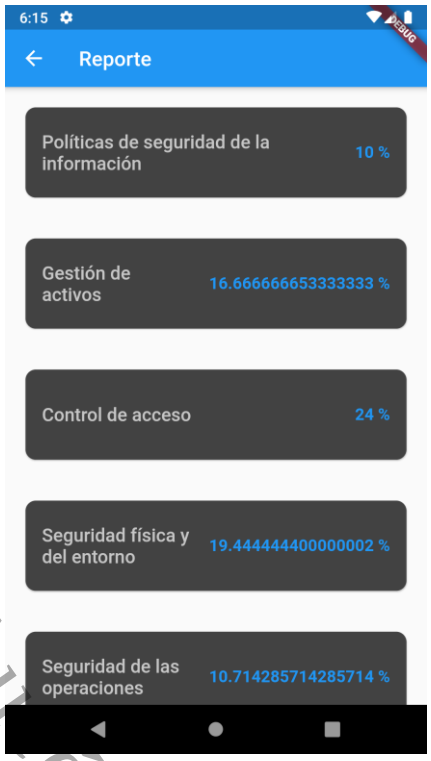


Nota: Elaboración propia.

Figura 31
Interfaz: Pantalla de Resultado

Nota: Elaboración propia.

Figura 32
Interfaz: Pantalla de Reporte



Nota: Elaboración propia.

3.3 Fase 3: Evaluación de la seguridad

3.3.1 Selección de los dominios

La misma norma hace la observación que la selección de los controles depende de las decisiones de la organización basada en criterios de aceptación o tratamiento de riesgo y de los enfoques generales de gestión del riesgo aplicado en la organización (ISO, 2020).

En este trabajo de investigación, para la selección de los controles se tomó con base en lo realizado en la Fase 1 de este trabajo. En la tabla (ver tabla 23) se muestran los dominios que se consideraron aplicables o no para el Registro Público de la Propiedad.

Tabla 23
Dominios seleccionados para el Departamento de Informática del RPPyC

	Dominio	**¿Aplicable?**	
		Si	No
5	Políticas de seguridad de la información	X	
6	Organización de la seguridad de la información		X
7	Seguridad de los recursos humanos		X
8	Gestión de activos	X	
9	Control de acceso	X	
10	Criptografía		X
11	Seguridad física y del entorno	X	
12	Seguridad de las operaciones	X	
13	Seguridad de las comunicaciones	X	
14	Adquisición, desarrollo y mantenimientos de sistemas		X
15	Relación con los proveedores		X
16	Gestión de incidentes de seguridad de la información	X	
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	X	
18	Cumplimiento		X

Nota: Elaboración propia.

Mientras que los dominios no aplicables se muestran en la tabla 24, aquí se exponen las razones por las cuales no se consideraron en este trabajo de investigación.

Tabla 24
Dominios no aplicables para el Departamento de Informática del RPPyC

	Dominio	Objetivo
6	Organización de la seguridad de la información	Este busca establecer un marco de referencia para definir el proceso para la implementación y control de la seguridad de la información dentro de la organización, es decir, es aplicable durante el proceso de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), y no es el caso para este trabajo.
7	Seguridad de los recursos humanos	Este comprende aspectos a tomar en cuenta antes, durante y para el cese o cambio de trabajo. Ya que estas consideraciones son funciones del departamento de recursos humanos del RPPyC, no se consideró aplicable
10	Criptografía	Aplicable si se hace uso de sistemas y/o técnicas criptográficas para la protección de la información así también como la gestión de claves. No se consideró ya que el RPPyC no utiliza ninguna clase de métodos criptográficos actualmente.
14	Adquisición, desarrollo y mantenimientos de sistemas	El objeto de este apartado es la aplicación controles para la seguridad de la información al ciclo de vida completo de los sistemas de información, tanto propios como subcontratados. No se consideró ya que el RPPyC no cuenta con departamento de desarrollo y las adquisiciones las gestiona otro departamento.
15	Relación con los proveedores	Se considera en caso de que empresas o personal externo a la organización tengan acceso a los sistemas de información o a los recursos que manejan activos de información deberemos establecer de modo formal las condiciones para el uso de dichos activos y supervisar el cumplimiento de dichas condiciones. Pero este no es el caso del RPPyC.
18	Cumplimiento	Este está dedicado a las políticas, normas y legislación aplicable enfocándose principalmente en lo que se refiere a seguridad de la información. No se consideró ya que los controles elegidos se limitaron a la seguridad de los activos tecnológicos del RPPyC.

Nota: Elaboración propia.

3.3.2 Aplicación de la norma ISO/IEC 27002:2013

En esta sección se usó la aplicación móvil desarrollada en Flutter, para obtener un resultado inmediato del grado de cumplimento de la norma en el Departamento de Informática del RPPyC. Esta fue aplicada en conjunto con el encargado del departamento, en un principio de explicó rápidamente como está distribuida la norma ISO/IEC 27002 (Dominios, Objetivos y controles) y la escala de valores con la que se evalúa cada control. Una vez concluido, los resultados almacenados en la base de datos se extrajeron para analizarlos.

Capítulo 4. Resultados

En este capítulo se discute y plantea la fase 4 de la metodología propuesta, donde se detallan los resultados de la norma ISO/IEC 27002:2013. Dichos resultados son obtenidos de la aplicación móvil desarrollada con la herramienta de desarrollo Flutter. Así mismo en este capítulo se proponen prácticas de seguridad de la información para el Registro Público de la Propiedad y del Comercio de Tabasco.

4.1 Fase 4: Elaboración del informe

4.1.1 Cumplimiento de la norma

Una vez realizada la evaluación de la norma mediante la aplicación móvil desarrollada, se obtuvieron los siguientes resultados. En el apéndice A se encuentran los resultados de la evaluación de cada uno de los controles seleccionados. En la tabla 25 se muestran los porcentajes de cumplimiento de cada uno de los ocho dominios seleccionados para este trabajo. Como se observa, se obtuvo un promedio de cumplimiento del 15.51% de los dominios seleccionados de la norma.

Tabla 25
Grado de cumplimiento por dominio

Capítulo	Dominio	Porcentaje de cumplimento
5	Políticas de seguridad de la información	0%
8	Gestión de activos	16.6666667%
9	Control de acceso	24%
11	Seguridad física y del entorno	19.4444444%
12	Seguridad de las operaciones	10.7142857%
13	Seguridad de las comunicaciones	13.3333333%
16	Gestión de incidentes de seguridad de la información	20%
17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	20%
	Promedio de cumplimiento general del RPPyC	15.51984127%

Nota: Elaboración propia.

En la tabla 26 se muestran los objetivos de control de los dominios aplicados de la tabla 25. En esta tabla, se muestran los porcentajes de los 21 objetivos de control correspondientes. Se puede observar que se obtuvo un promedio general de 15.75%.

Tabla 26
Grado de cumplimiento por objetivos de control

Capítulo	Objetivos de control	Resultado
5	5.1 Dirección de gestión para la seguridad de la información	0%
8	8.1 Responsabilidad por los activos	30%
	8.2 Clasificación de la información	6.666666667%
	8.3 Manipulación de media	13.33333333%
9	9.1 Requisitos de negocio para el control de acceso	40%
	9.2 Gestión de acceso de usuarios	20%
	9.3 Responsabilidades de los usuarios	20%
	9.4 Control de acceso a sistemas y aplicaciones	165
11	11.1 Áreas seguras	10%
	11.2 Equipos	28.88888889%
12	12.1 Procedimientos operacionales y responsabilidades	5%
	12.2 Protección contra códigos maliciosos	20%
	12.3 Copias de respaldo	40%
	12.4 Registro y monitorización	10%
	12.5 Control de software operacional	0%
	12.6 Gestión de la vulnerabilidad técnica	0%
	12.7 Consideraciones sobre auditorias de sistemas de información	0%
13	13.1 Gestión de seguridad de las redes	26.66666667%
	13.2 Transferencia de información	0%
16	16.1 Gestión de incidentes y mejoras de seguridad de la información	20%
17	17.1 Continuidad de seguridad de la información	0%
	17.2 Redundancias	40%
	Promedio	15.75252525%

Nota: Elaboración propia.

Por último, en la tabla 27 se presentan los 73 controles aplicables, agrupados entre los seis distintos niveles de madurez.

Tabla 27
Total de números de controles por niveles de madurez

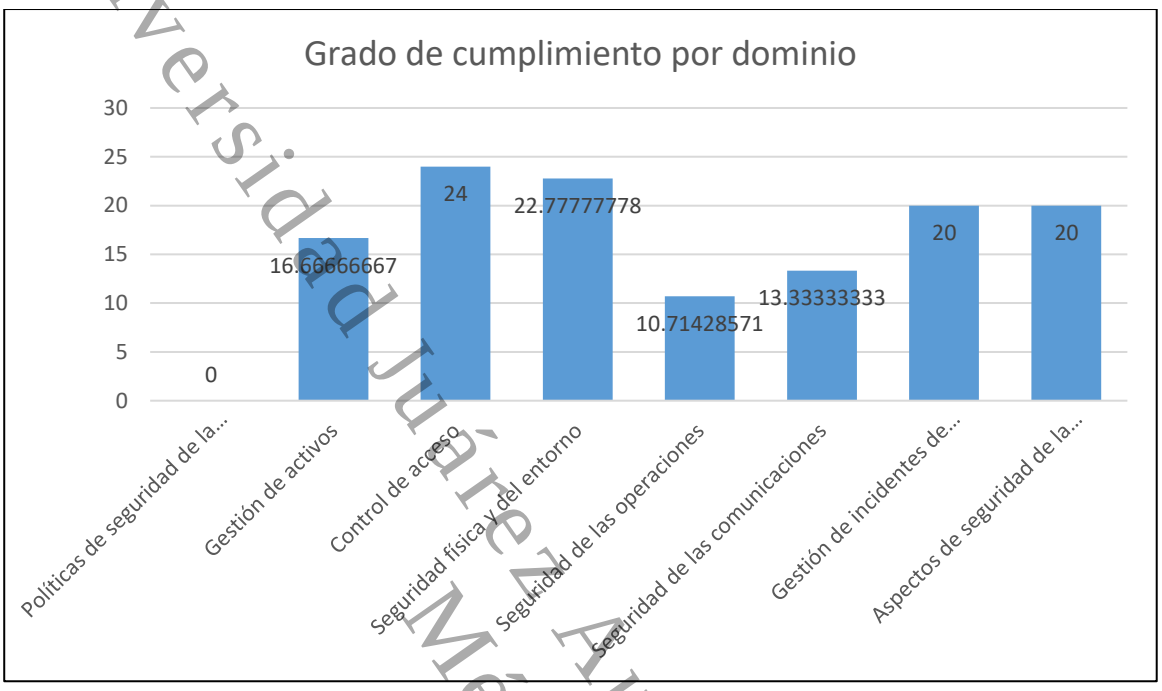
Niveles de madurez		
Criterio	Porcentaje	Totales
No realizado	0%	34
Realizado informalmente	20%	19
Planificado	40%	20
Bien definido	60%	0
Cuantitativamente controlado	80%	0
Mejora continua	100%	0
Total		73

Nota: Elaboración propia con base en (Tovar y Salguero, 2018).

4.1.2 Análisis de los resultados

En la figura 33 se observan los resultados obtenidos de los ocho dominios aplicables de la norma, se identificó que el porcentaje más alto que obtuvo un dominio fue del 24%, mientras que el más bajo fue de 0%. Siendo los dominios llamados “Control de acceso” y “Políticas de seguridad de la información”, respectivamente, los que obtuvieron tales resultados.

Figura 33
Grado de cumplimiento por dominio



Nota: Elaboración propia.

A continuación, se detalla la evaluación de cada uno de los dominios:

- **Políticas de seguridad de la información**: Este proporciona orientación y apoyo según los requisitos del negocio, las leyes y normas pertinentes (ISO27000.es, 2005). Se hace énfasis en lo importante de contar con una política de seguridad apropiada para la organización. El dominio está constituido por un único objetivo de control y se obtuvo un porcentaje de cumplimiento del 0%, esto se debió a que el Departamento de Informática del RPPyC no cuenta actualmente con políticas definidas de seguridad de la información.
- **Gestión de activos**: El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la

administración de riesgos (ISO27000.es, 2005). Está constituido por tres objetivos de control. Este dominio tuvo un porcentaje de cumplimento del 16.66%. Si bien, se cuenta con procedimientos para gestionar el inventario de los activos del departamento, se observó que éste tiene deficiencias por no contar con un software dedicado para el inventario, así también, como la desactualización de esa información ya que se ha observado que se tienen problemas para localizar partes del inventario.

- **Control de acceso**: El objetivo de este dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática (redes y sistemas/plataformas de información) (ISO27000.es, 2005). Está constituido por cuatro objetivos de control y tuvo un porcentaje de cumplimento del 24%, el más alto encontrado en el departamento, ya que se cuenta con controles para el acceso, pero existe un área de oportunidad de mejorar en este dominio.
- **Seguridad física y del entorno**: El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización (ISO27000.es, 2005). El dominio se constituye por dos objetivos de control. Este dominio tuvo un porcentaje de cumplimento del 19.44%, el Departamento de Informática cuenta con rutinas para controlar el acceso de sus activos. Así también se cuentan con medidas para protegerlos como extintores, cámaras de seguridad y el lugar se encuentra bajo llave para evitar el acceso no autorizado.

- **Seguridad de las operaciones**: El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada (ISO27000.es, 2005). Está compuesto por siete objetivos de control. Este dominio tuvo un porcentaje de cumplimento del 10.71% ya que cuentan con medidas mínimas de seguridad para protegerse contra *malware*, registro de eventos, gestión de vulnerabilidades, por mencionar algunas.
- **Seguridad de las comunicaciones**: El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte (ISO27000.es, 2005). Está constituido por dos objetivos de control. Este dominio tuvo un porcentaje de cumplimento del 13.33% ya que solo estuvieron presentes un par de controles para la gestión de seguridad de redes.
- **Gestión de incidentes de seguridad de la información**: El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados para que se apliquen las acciones correctivas en el tiempo oportuno (ISO27000.es, 2005). Está formado por un único objetivo de control. Este dominio tuvo un porcentaje de cumplimento del 20% en el Departamento de Informática ya que se encuentran presentes la mayoría de los controles, aunque están en el nivel de madurez de que se realizan de manera informal (20%).
- **Aspectos de seguridad de la información para la gestión de la continuidad del negocio**: Este objetivo busca preservar la seguridad de la información durante las

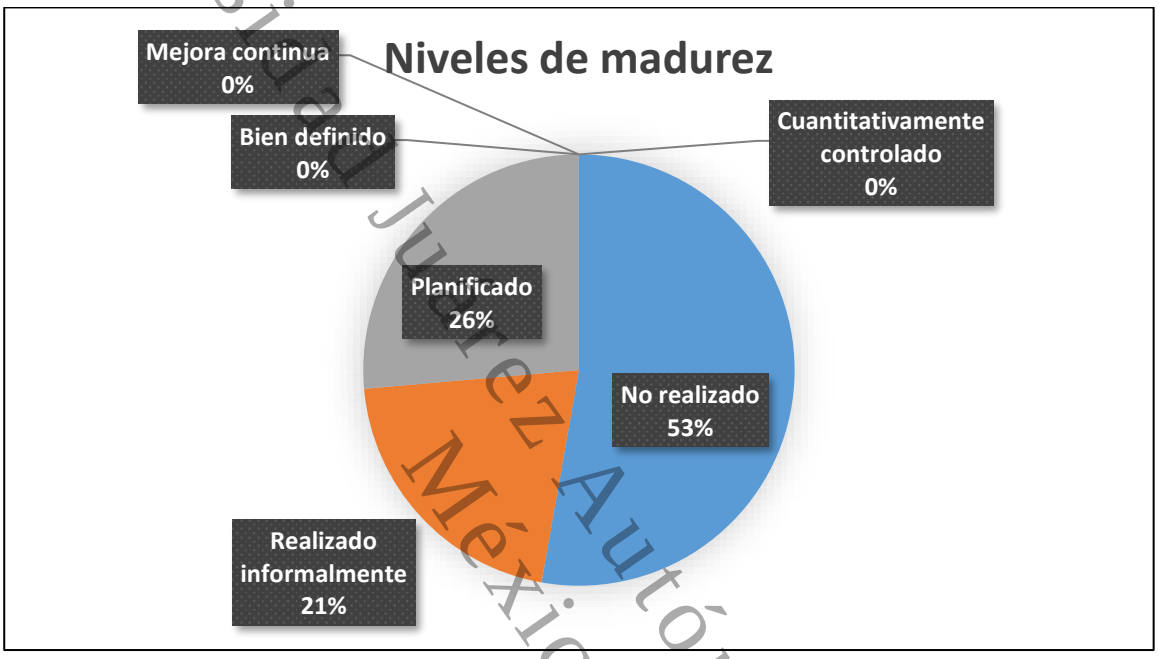
fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad (ISO27000.es, 2005). Está constituido por dos objetivos de control. El dominio tuvo un porcentaje de cumplimento del 20%, en este caso el departamento no cuenta con un plan para garantizar la continuidad de la información, solo se cuentan con medidas informales para garantizar la continuidad de las operaciones, que son la redundancia de la información o de equipos auxiliares como sistemas de alimentación ininterrumpida para evitar el apagado incorrecto de los equipos.

En la figura 34 se aprecian las evaluaciones de los 73 controles que se aplicaron en este trabajo. Estas se encuentran agrupadas por lo niveles de madurez antes mencionados. Observándose que el rango de madurez estuvo en el rango de 0 al 40%. A continuación, se agrupan los resultados:

- Para el 53% (34 controles) no se encontraron controles establecidos de seguridad de la información.
- Para el 21% (19 controles) se encontraron controles que se llevan a cabo de manera informal, son procedimientos que se realizan mecánicamente pero no se encuentran plasmados en un manual o documento que establezca su aplicación.
- Para el 26% (20 controles) Los controles de seguridad de la información que se encuentran establecidos son planificados, implementados y repetibles dentro del Departamento de Informática.

- Para los niveles de madurez restantes, no se encontraron presentes dentro del departamento.

Figura 34
Total de números de controles por niveles de madurez



Nota: Elaboración propia.

En la imagen 34 se observa que poco más del 50% de los controles no se encuentran presentes, mientras que el 21% se realizan de manera informal y el 26% se encuentra planificado dentro del departamento.

4.1.3 Propuestas de seguridad de la información para el RPPyC de Tabasco

Luego del análisis de los resultados de la norma ISO/IEC 27002:2013 para el Departamento de Informática del RPPyC de Tabasco se manifestaron deficiencias en el tema de Seguridad de la Información. No se detectaron controles de seguridad de la información que además de planificados estuvieran documentados, aprobados e

implementados en el caso de estudio de este trabajo. Las siguientes propuestas son las recomendadas por la norma para los controles que tuvieron un grado de madurez de “No realizado” (0%) y realizado informalmente (20%).

Políticas de seguridad de la información

Ya que en este dominio tuvo una ponderación nula, la norma propone que las políticas de seguridad deben estar estructuradas con respecto a las necesidades de la organización. Se propone que el RPPyC tenga políticas de seguridad de la información de los temas de:

- Control de acceso
- Seguridad física y ambiental
- Uso adecuado de los activos
- Planificación de copias de respaldos
- Protección contra software malicioso
- Gestión de vulnerabilidades
- Seguridad de las comunicaciones

Gestión de activos

Se recomienda contar con pautas para identificar y definir las responsabilidades de los activos del Departamento de Informática, como serian el inventario de activos, asignar responsables, uso adecuado y devolución de estos. Así también contar con un esquema de clasificación de información en relación sobre cómo debe tratarse y

protegerse la información por los encargados de administrarla. El esquema debe estar alineado con las políticas del dominio de control de acceso.

Control de acceso

En este domino se proponen la implementación de los siguientes controles:

- Requerir la firma de una carta de compromiso de confidencialidad.
- Implementar técnicas de autentificación alternas a las contraseñas para validar la identidad, por ejemplo, medios criptográficos o medios biométricos.
- Los privilegios de acceso de usuario deberían revisarse periódicamente y tras cualquier cambio, como un ascenso, degradación o finalización del empleo.
- Un sistema de gestión de contraseñas.

Seguridad física y del entorno

Para este dominio se deben de contar con protección física contra los desastres naturales, ataques intencionales y no intencionales por el hombre. Estos últimos mediante métodos de autentificación como credenciales de identificación o acceso por datos biométricos. También que los vigilantes impidan el acceso a cualquier persona que intente acceder o retirar equipo del edificio.

Seguridad de las operaciones

En el caso del Departamento de Informática se debe proporcionar suficiente capacidad mediante el incremento de la misma o reduciendo la demanda. Algunos ejemplos son:

- Borrado de datos obsoletos (liberar espacio en disco).

- Desmantelamiento de aplicaciones, sistemas, bases de datos u otros fuera de uso.
- Optimizar la lógica de la aplicación o las consultas de base de datos.
- Denegar o restringir el ancho de banda para servicios consumidores de muchos recursos, si estos no son críticos para la funcionalidad (por ejemplo, la transmisión de vídeo).

También se deben de contar con controles definidos de registro y supervisión de las actividades de los usuarios como:

- Registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
- Restricciones sobre la instalación de software.

Seguridad de las comunicaciones

Las redes deben ser administradas y controladas para proteger la información en los sistemas y aplicaciones. Deben existir controles para garantizar la seguridad de la información en las redes y la protección de servicios conectados frente a accesos no autorizados o amenazas. Algunas recomendaciones para la seguridad de las comunicaciones pueden ser las siguientes:

- Establecer responsabilidades y procedimientos para la gestión de los equipos de red.
- La responsabilidad operacional de las redes debería estar separada de las operaciones de los sistemas informáticos donde sea apropiado.

- Establecer controles para mantener la confidencialidad e integridad de los datos que pasan a través de la red, además para mantener la disponibilidad de los servicios de red y los servidores conectados.
- Realizar un registro y monitorización que permitan el registro y detección de acciones que podrían afectar la seguridad de la información.
- Los equipos de red deben de contar con claves de seguridad para entrar a su configuración.
- Conexión de los sistemas a la red debería ser restringido.
- Procedimientos para el uso de los servicios de red para restringir el acceso a los mismos o a las aplicaciones, donde sea necesario.

Gestión de incidentes de seguridad de la información

Se deben evaluar cada evento de seguridad de la información recurriendo a una escala de clasificación de eventos e incidentes de seguridad establecida y decidir si el evento puede clasificarse o no, como un incidente de seguridad de información. La clasificación y priorización de incidentes puede ayudar a identificar el impacto y extensión de un incidente. Los resultados de la evaluación y la decisión deberían registrarse a detalle para futuras referencias y verificación.

Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Se deben analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio para desarrollar e implementar planes

de contingencia que aseguren que los procesos del departamento se puedan restaurar en el menor tiempo posible.

De acuerdo con los requisitos de continuidad de seguridad de la información, en la norma se recomienda que la organización debe establecer, documentar, implantar y mantener:

- Controles de seguridad de la información en los procesos, procedimientos y sistemas y herramientas de soporte de continuidad del negocio o de recuperación de desastres.
- Procesos, procedimientos e implantación de cambios para mantener los controles existentes de seguridad de la información durante una situación adversa.
- Controles compensatorios para aquellos controles de seguridad de la información que no puedan mantenerse durante una situación adversa.

4.2 Flutter

En este apartado se expone la experiencia del investigador al desarrollar la aplicación móvil utilizando el *framewok* de desarrollo de Flutter. Se abordará desde cómo fue instalar la herramienta, el software necesario para comenzar a programar y la experiencia de uso.

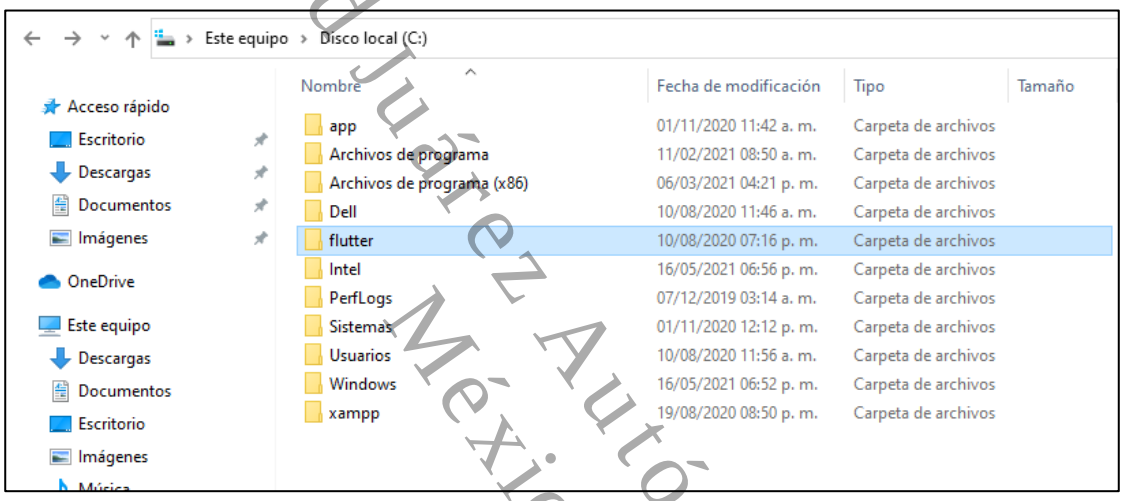
4.2.1 Instalación

En este caso la instalación fue en el sistema operativo Windows 10 Pro. Es importante mencionar ya que los pasos pueden diferir en otros sistemas operativos.

El primer paso fue obtener el SDK de Flutter, el cual se encuentra disponible en la página oficial de Flutter (flutter.dev). Una vez descargado, hay que descomprimir el

archivo zip y colocar la carpeta en la ubicación de instalación que se prefiera. En el caso del investigador, se colocó en la raíz de la unidad C como se observa en la figura 35. Una vez copiado la carpeta en la ubicación seleccionada, hay que localizar el archivo flutter_console.bat y ejecutarlo.

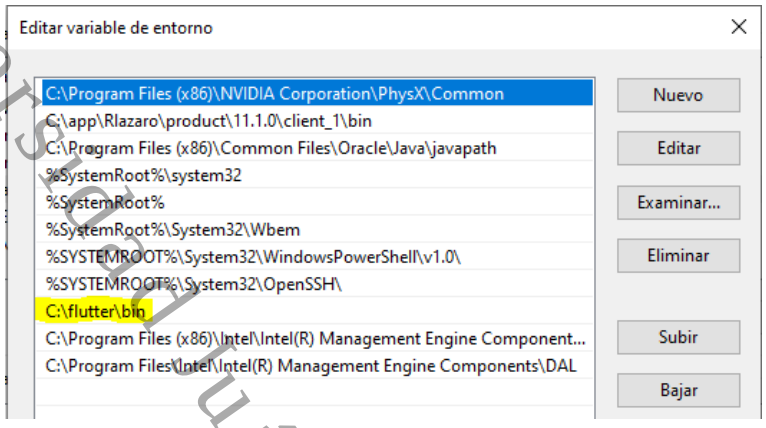
Figura 35
Ubicación de la instalación de Flutter



Nota: Elaboración propia.

El siguiente paso en la configuración es actualizar la variable de entorno *Path*, para esto en Windows 10 hay que abrir la opción de **Editar variables de entorno para tu cuenta**, y en las variables del sistema, editar la entrada llamada *Path* y agregar una nueva variable como se muestra en la figura 36 con la ruta C:\flutter\bin

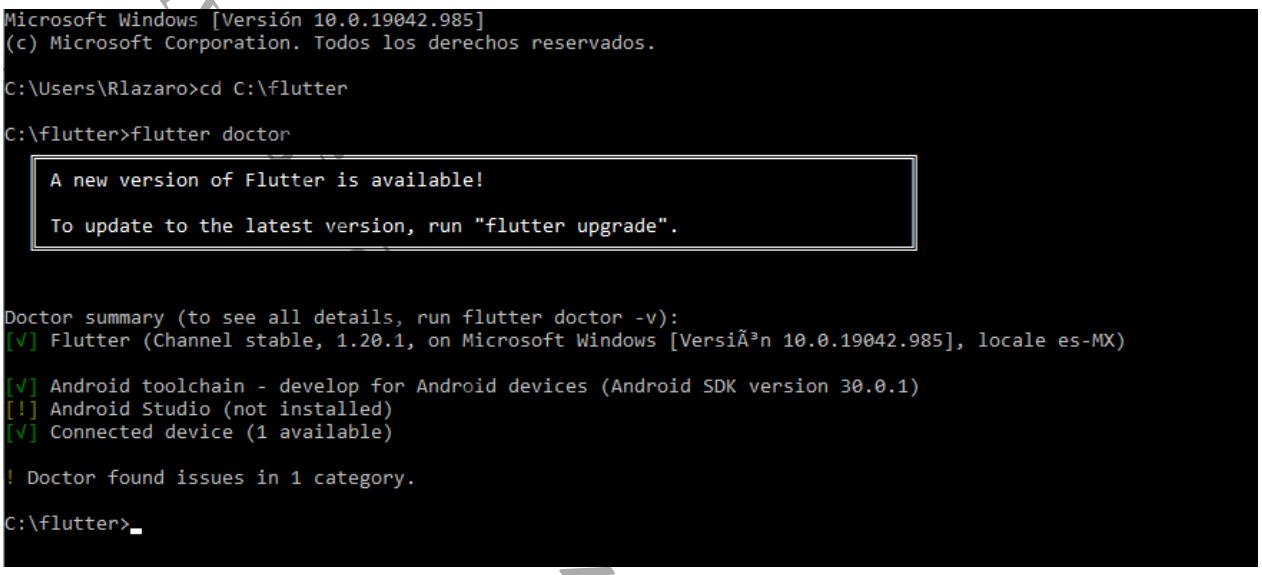
Figura 36
Agregando Flutter en la variable Path



Nota: Elaboración propia.

Por último, solo resta ejecutar la herramienta *flutter doctor*, la cual tiene como función verificar si existe alguna dependencia necesaria para completar la configuración de Flutter. En la figura 37 se presenta como ejecutar *flutter doctor* en la consola de comandos de Windows (CMD). En primer lugar, hay que ubicarse en la carpeta de instalación de Flutter, una vez allí hay que proceder escribir “flutter doctor” y dar en la tecla “Enter”. Lo cual ejecutará un diagnóstico sobre los requerimientos necesarios a tener instalados para la correcta ejecución de Flutter. En la imagen 37 se observa que el entorno de desarrollo de Android Studio no estaba instalado en el momento, aunque es posible utilizar otros entornos como Visual Studio Code o Emacs. Aunque se recomienda usar Android Studio al estar mejor integrado con las herramientas de Flutter.

Figura 37
Agregando Flutter en la variable Path



Nota: Elaboración propia.

Una vez instalado Android Studio, queda instalar los *plugins* de Flutter y el lenguaje Dart. Para esto hay que iniciar Android Studio, luego en **Configuración>Plugins**, escribir en el buscador la palabra “Flutter”, elegir el complemento y dar clic en ***Install*** como se muestra en la figura 38. Luego seguir las indicaciones que aparezcan y restaurar Android Studio.

Figura 38
Instalación del plugin de Flutter en Android Studio.

Nota: Elaboración propia.

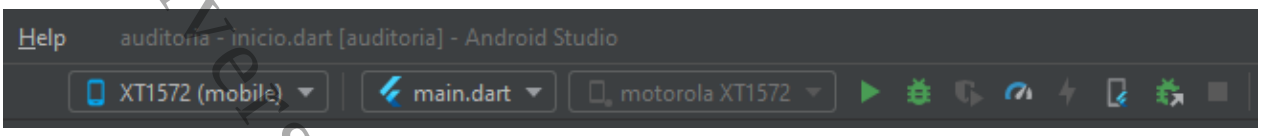
Una vez instalado todo de manera correcta, al iniciar Android Studio, como en la figura 39, aparecerá la opción de crear un nuevo proyecto de Flutter para así comenzar a desarrollar alguna aplicación móvil.

Figura 39
Crear un nuevo proyecto en Flutter.

Nota: Elaboración propia.

El siguiente paso es configurar algún emulador o un dispositivo Android para la ejecución y pruebas de una aplicación de Flutter. En el caso del investigador, usó un teléfono Android. Para esto, hay que tener conectado el teléfono mediante USB a la computadora. Luego habilitar las opciones de desarrollador y depuración por USB. Una vez hecho lo anterior, en el entorno de desarrollo aparecerá el modelo del dispositivo conectado para ejecutar la aplicación como se presenta en la figura 40 que el teléfono utilizado fue un Motorola XT1572.

Figura 40
Crear un nuevo proyecto en Flutter.



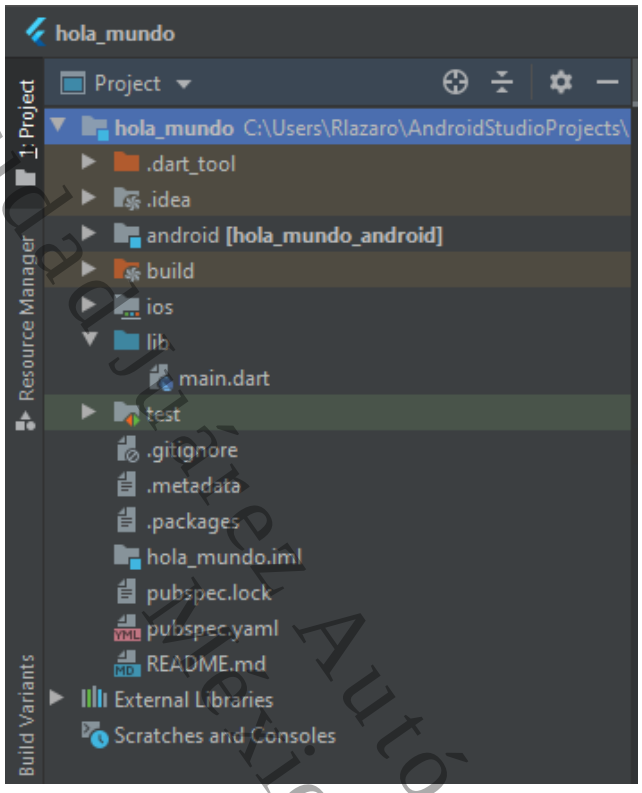
Nota: Elaboración propia.

4.2.2 Estructura de un proyecto

En la imagen 41 se presenta el ejemplo de la estructura de una aplicación en Flutter. Dentro del proyecto se encuentran las siguientes carpetas y archivos importantes:

- android: Contiene la base de la aplicación Android a la que se une la aplicación desarrollada en Flutter.
- ios: Contiene la base de la aplicación iOS a la que se une la aplicación desarrollada en Flutter.
- lib: es la carpeta principal de desarrolla, contiene los archivos del lenguaje Dart de la aplicación.
- pubspec.yaml: En este archivo se manejan las dependencias y los *assets* de una aplicación en Flutter.

Figura 41
Estructura de un proyecto en Flutter.



4.2.3 Experiencia de uso

Para comprender como usar esta herramienta fue necesario documentarse sobre como aprender a usar la herramienta, los recursos fueron desde consultar la información oficial de la página de Flutter, videos de YouTube, tomar cursos básicos y avanzados de Flutter en la plataforma de educación en línea de Platzi. Esto con el fin de comprender mejor la herramienta a utilizar.

De la experiencia de desarrollar la aplicación móvil para la evaluación de la norma de este trabajo se puede mencionar que hubo en un comienzo una curva de aprendizaje

al estar en un entorno desconocido, aunque que el investigador tenía experiencia previa en el desarrollo de aplicaciones utilizando el *framework* de Android SDK.

Flutter utiliza el lenguaje de programación Dart, su sintaxis es similar a otros lenguajes como JavaScript, Java o C++, lo que facilitó ya que el investigador anteriormente había desarrollado en el lenguaje Java. Esto ayudó a simplificar el proceso de aprendizaje al programar en este nuevo lenguaje de programación.

Entre las funciones interesantes se encuentra una característica llamada “Hot Reload”, este consiste en si una vez que se ejecutó la aplicación en el teléfono y si modifica el código del proyecto. Al guardar o hacer clic en el botón de Hot Reload, el cambio realizado se verá reflejado casi instantáneamente. A diferencia de Android SDK donde habría que detener la ejecución, volver a compilar y esperar a que se ejecute para observar si el cambio realizado es satisfactorio o no. La funcionalidad fue de gran ayuda para experimentar, añadir cambio y corregir errores rápidamente.

Una de las características de Flutter es que permite el desarrollo para las plataformas iOS y Android con el mismo código. Solo se pudo probar la aplicación en Android, ya que no se contaba con un equipo Mac y un certificado de desarrollo de aplicaciones iOS. Por lo tanto, no fue posible probar la aplicación en iOS, pero se tiene la certeza de funcionaria al ser una característica esencial de Flutter.

Entre algunas dificultades presentadas en el desarrollo de la aplicación se puede mencionar que existieron problemas al conectar la aplicación con una base de datos MySQL y que al momento de recuperar la información almacenada en la base de datos se desplegara correctamente en el tipo de *widget* seleccionado.

Así también, Flutter no cuenta con una herramienta para diseñar las interfaces de manera visual, esto llevó a conocer bien las propiedades de los distintos tipos de widgets. Era común ejecutar la aplicación y con el Hot Reload verificar la alineación de los distintos componentes, los colores y el tamaño de la fuente.

Una característica del código Dart es que automáticamente se señala mediante comentarios donde comienza y termina los widgets que conformen la interfaz. En la figura 42 se observa por ejemplo en la clase AppBar el entorno de desarrollo delimita que este termina donde se señala con el comentario del mismo nombre de la clase (//AppBar) y así también para las distintas clases. Esto puede causar confusión en primera instancia, pero en un tiempo reducido el programador se logra acostumbrar a esta característica.

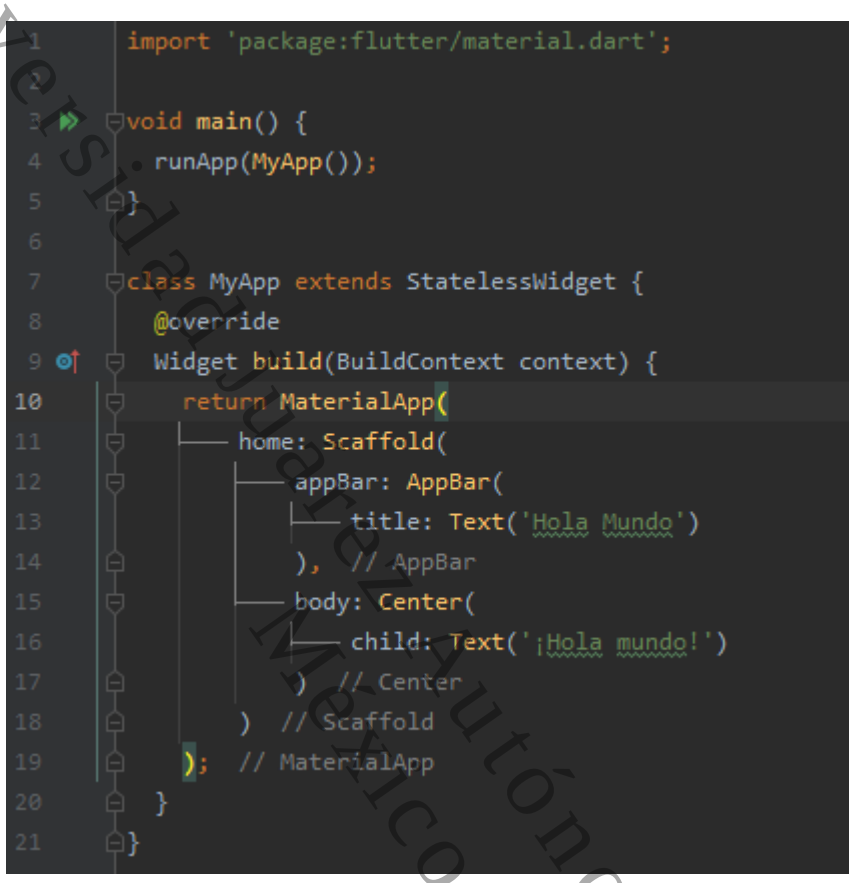
Figura 42
Ejemplo de distribución de los widgets.

Nota: Elaboración propia.

4.2.4 Ejemplo: Hola mundo

A continuación, se muestra una comparativa del código entre Android SDK y Flutter. Se seleccionó Android SDK al ser la herramienta oficial para desarrollar aplicaciones Android. En la imagen 43 presenta el código Dart para una aplicación que presenta en pantalla el mensaje clásico de “¡Hola Mundo!”. En este ejemplo se tiene un código de una extensión de 21 líneas de código contando el *import* de la paquetería necesaria, los saltos de línea y las llaves de cierre que delimitan las sentencias.

Figura 43
Código Dart: Hola Mundo.



```dart
import 'package:flutter/material.dart';

void main() {
  runApp(MyApp());
}

class MyApp extends StatelessWidget {
  @override
  Widget build(BuildContext context) {
    return MaterialApp(
      home: Scaffold(
        appBar: AppBar(
          title: Text('Hola Mundo')
        ),  // AppBar
        body: Center(
          child: Text('¡Hola mundo!')
        )  // Center
      )  // Scaffold
    );  // MaterialApp
  }
}
```

Nota: Elaboración propia.

En la figura 44 se observa el resultado de la ejecución del código de la imagen 42.

Figura 44
Pantalla Hola Mundo (Flutter).

Nota: Elaboración propia.

En el casi de Android SDK, en la figura 45 se visualiza el código Kotlin, este en primera instancia podría parecer menos líneas de código que en Flutter, pero este código hace referencia a un archivo XML llamado activity_main, que define la estructura de la interfaz a desplegar en la aplicación.

Figura 45
Código Kotlin: Hola Mundo.

```kotlin
package com.example.holamundo

import ...

class MainActivity : AppCompatActivity() {
    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)
        setContentView(R.layout.activity_main)
    }
}
```

Nota: Elaboración propia.

El archivo XML contiene todos los elementos para mostrar el texto lo cual puede observarse a continuación en la figura 46.

Figura 46
Código XML: Hola Mundo.

```xml
<?xml version="1.0" encoding="utf-8"?>
<androidx.constraintlayout.widget.ConstraintLayout xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    tools:context=".MainActivity">

    <TextView
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:text="¡Hola Mundo!"
        app:layout_constraintBottom_toBottomOf="parent"
        app:layout_constraintLeft_toLeftOf="parent"
        app:layout_constraintRight_toRightOf="parent"
        app:layout_constraintTop_toTopOf="parent" />

</androidx.constraintlayout.widget.ConstraintLayout>
```

Nota: Elaboración propia.

Ambos elementos presentados en las figuras 44 y 45 dieron como resultado a la aplicación que se aprecia en la figura 47.

Figura 47
Código Dart: Hola Mundo.

Nota: Elaboración propia.

Se puede observar que las aplicaciones presentan un diseño parecido solo difieren en los colores. Además de que en Android SDK se tiene una manera de gestionar el diseño de la interfaz mientras que en Flutter se realiza en su totalidad con el código Dart.

Capítulo 5. Conclusiones, recomendaciones y trabajos futuros

5.1 Conclusiones

En esta tesis se evaluó el grado de seguridad del Departamento de Informática del Registro Público de la Propiedad y del Comercio del estado de Tabasco bajo la norma ISO/IEC 27002:2013, mediante el uso de una aplicación móvil Android desarrollada en Flutter, concluida la evaluación se propusieron buenas prácticas de seguridad de la información.

Lo más importante de la evaluación realizada fue que permitió conocer el estado actual del Departamento de Informática del RPPyC de Tabasco, en relación con las buenas prácticas para la gestión de la seguridad de la información propuestas en la norma ISO/IEC 27002:2013, a través de la aplicación desarrollada en Flutter para realizar la evaluación.

Lo anterior permitió identificar áreas de oportunidad para alcanzar un nivel de seguridad adecuado que garantice la confidencialidad, integridad y la disponibilidad de la información y los activos. Todo esto en conjunto, ayudó a cumplir el objetivo general de este trabajo ya que por medio de esta herramienta tecnológica, la captura de la información se realizó de manera ágil y a la vez se obtuvo la información almacenada rápidamente para su análisis a diferencia de los instrumentos realizados por Tovar y Salguero (2018) y Zacarias (2019), quienes presentaron los instrumentos utilizados para sus investigaciones, los cuales consistían en *checklists* donde a cada dominio se le asignaba un valor. Cabe destacar que en estas investigaciones, no se hace referencia a la forma en la que fueron analizados los datos recabados, ni tampoco especifican si luego

de la recolección, los datos se analizaron manualmente o se vaciaron en una hoja de cálculo u otro tipo de técnica.

Además, con la caracterización de los activos y de las amenazas de los activos de la información del Departamento de Informática, la metodología MAGERIT permitió identificar los activos del Departamento y valorar su importancia dentro de ésta para después continuar con la identificación y valoración de las amenazas a las que se pueden estar expuestas.

Esto no hubiera sido posible sin las facilidades prestadas por parte del Departamento de informática del RPPyC de Tabasco, los cuales estuvieron en la mejor disposición para llevar a cabo este trabajo de investigación.

Referente a la pregunta de investigación planteada a inicios de este proyecto en relación a ¿Cuál es el nivel de cumplimiento de los mecanismos de seguridad de la información actualmente implementados en el Departamento de Informática del RPPyC respecto a la norma ISO/IEC 27002:2013? concluida la investigación se observa que el nivel de cumplimento de los controles evaluados en el Departamento de Informática fue del 15.51% (ver tabla 25).

En la escala de valoración establecida por Tovar y Salguero (2018) este resultado se encuentra en el nivel más bajo de cumplimiento. Aunque como menciona Zacarias (2019), el objetivo de la herramienta no es el de emitir una calificación aprobatoria o reprobatoria, sino identificar el nivel de madurez de la seguridad de la información con respecto a la norma ISO/IEC 27002:2013, y de esta manera, identificar las prácticas de

seguridad de la información que permitan disminuir las probabilidades que vulnerabilidades y amenazas se presenten.

5.2 Recomendaciones

Algunas recomendaciones son que el Departamento de Informática ponga en práctica las propuestas hechas en este trabajo en el capítulo cuatro. Aunado a lo anterior, se sugiere capacitar al personal en temas de seguridad de la información y sobre la importancia de realizar revisiones periódicamente para reducir incidencias que pongan en riesgo la confidencialidad, integridad y disponibilidad de los distintos activos del RPPyC de Tabasco.

Mientras que para el uso de la aplicación móvil desarrollada, se requieren contar con conocimiento sobre la norma ISO/IEC 27002:2013 ya que la aplicación no contiene información detallada sobre qué consisten los dominios, objetivos y controles que la conforman esto debido a que la norma se encuentra protegida por derechos de autor y se prohíbe su reproducción total o parcial.

En el caso de la metodología de gestión de riesgos (MAGERIT) para este trabajo solo se utilizaron los primeros dos pasos de la metodología, pero en general esta metodología presenta un marco de trabajo para que las instituciones tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

5.3 Trabajos futuros

Como trabajos futuros para ampliar esta investigación se proponen los siguientes:

- Realizar una evaluación de la seguridad de la información de todos los departamentos y oficinas registrales del Registro Público de la Propiedad y del Comercio de Tabasco para una perspectiva global de este instituto.
- Continuar en la mejora de funciones de la aplicación móvil desarrollada como podrían ser el despliegue de distintos gráficos para mostrar los resultados, permitir tener activas más de una evaluación, ya que ahora solo permite hacer una a la vez.
- Cambiar el modelo cliente-servidor por un modelo basado en la nube y/o local para el almacenamiento de los datos, esto para dar flexibilidad al usuario cuando disponga o no de una conexión a internet para enviar los datos.
- Tener una versión para iOS, ya que una de las características de Flutter es que con el mismo código fuente se obtiene la versión para este sistema operativo móvil para así tener mayor cobertura al estar presente en los dos principales sistemas operativos móviles del mercado.
- Proponer un Sistema de Gestión de Seguridad de la Información (SGSI) como un comienzo para que el Departamento de Informática del RPPyC de Tabasco se encamine en contar con medidas formales en tema de seguridad. Esto también por si se desea obtener en algún futuro la certificación de la norma ISO/IEC 27001 como los organismos públicos mencionados en el capítulo uno de este trabajo (El RPPyC de Jalisco y el CNSF).

- Realizar el análisis de riesgo cuantitativamente ya que la metodología MAGERIT permite realizar la valoración del análisis de riesgo de manera cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles).

Referencias

Aguado, Juan-Miguel., Martínez, I. y Cañete-Sanz, L. (2015). Tendencias evolutivas del contenido digital en aplicaciones móviles. *El Profesional de la Información, 24*(5) 787-795. Recuperado de http://eprints.rclis.org/30299/

AMC College. (n.d.). *Android Studio: Apps Development*. Sabah, Malasia: Advanced Business System Consultants Sdn. Bhd. Recuperado de https://books.google.com.mx/books?id=BvhGDwAAQBAJ&lpg=PP1&dq=Android%20Studio%3A%20Apps%20Development&pg=PP2#v=onepage&q=Android%20Studio:%20Apps%20Development&f=false

Android Developers. (2020). *Introducción a Android Studio*. Recuperado de https://developer.android.com/studio/intro?hl=es-419

Apache. (2004). *Apache License*. Recuperado de https://www.apache.org/licenses/LICENSE-2.0

Blom, M. (2010). Is scrum and XP suitable for CSE development? *Procedia Computer Science, 1*(1), 1511-1517. Doi: https://doi.org/10.1016/j.procs.2010.04.168

Bonilla, D. (2018). *Diseño de una política de seguridad para el control de la información del área de TICS de la empresa Flower Village Ecuador basada en la norma ISO 27002* (Tesis de Maestría). Universidad Internacional Sek, Quito, Ecuador.

Borbón, J. (s.f.). Buenas prácticas, estándares y normas. *Seguridad*, (11), 14-17. Recuperado de https://revista.seguridad.unam.mx/sites/default/files/revistas/pdf/Seguridad_Num_11_0.pdf

Bracha, G. (2015). *The dart programming language*. Indiana: Addison Wiseley.

Cárdenas, J. (2017). La representación social de instituciones públicas de índole política en la ciudadanía del estado de Colima. *Revista mexicana de opinión pública,* (22), 55-69. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-49112017000100055&lng=es&tlng=es.

Cárdenas-Solano, Leidy-Johanna., Martínez-Ardila, H. y Becerra-Ardila, Luis-Eduardo. (2016). Gestión de seguridad de la información: revisión bibliográfica. *El Profesional de la Información*, *25*(6), 931-948. Doi: https://doi.org/10.3145/epi.2016.nov.10

Carvajal, D., Cardona, A y Valencia, F. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. *Entre Ciencia e Ingeniería 13*(25), 68-76. Doi: https://doi.org/10.31908/19098367.4016

Castro, E. (2010). El estudio de casos como metodología de investigación y su importancia en la dirección y administración de empresas. *Revista Nacional de administración,* *1*(2), 31-54. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3693387

Chierici, A., de Girolamo, D., Guizzunti, G., Longo, S., Maron, G., Martelli, B., Vistoli, G, Zani, S., Castellani, G. & Giampieri, E. (2019). SGSI project at CNAF. *EPJ Web of Conferences*, *214*(), 1-5. Doi: https://doi.org/10.1051/epjconf/201921408017

Comisión Nacional de Seguros y Fianzas [CNSF]. (2017). *Certificado de Sistema de Gestión y Seguridad de la Información SI-0076/2010 de la CNSF*. Recuperado de

https://www.gob.mx/cnsf/documentos/agencias-internacionales-de-certificacion-refrendan-el-certificado-de-sistema-de-gestion-y-seguridad-de-la-informacion-si-0076-2010-de-la-cnsf

Coordinación de Universidad Abierta y Educación a Distancia de la UNAM [CUAED]. (s.f.). *Lenguajes de Programación*. Recuperado de https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/1023/mod_resource/content/1/contenido/index.html

Creative Commons. (2020). *Sobre las licencias*. Recuperado de https://creativecommons.org/licenses/?lang=es

Díaz, P. y Reyes, A. (2015). Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT (Tesis de ingeniería). Universidad Nacional Autónoma de México, D.F.

Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M. y Varela-Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en educación médica*, *2*(7), 162-167. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-50572013000300009&lng=es&tlng=es.

Dirección General de Servicios de Investigación y Análisis [SEDIA]. (2015). *Recaudación de los ingresos públicos estatales y municipales del Estado de Tabasco, 2010-2013*. Recuperado de http://www.diputados.gob.mx/sedia/sia/se/SAE-ISS-17-15/Tabasco.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4(2)*, 92-100. Doi: http://dx.doi.org/10.4236/jis.2013.42011

Djapić, M. & Lukić, L. (11 de mayo de 2007). *ISO/IEC 27000 series standards the best business practice for information security*. (Conferencia). Quality Festival 2007. Kragujevac, Serbia

ESET. (2019a). *ESET Security Report Latinoamérica 2019*. Recuperado de https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

ESET. (2019b). *Estado de la seguridad de las empresas en México en 2019*. Recuperado de https://www.welivesecurity.com/la-es/infographics/estado-seguridad-deempresas-mexico-2019/

Fenz, S. & Neubauer, T. (2018). Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Information & Computer Security, 26*(5), 551-567. Doi: 10.1108/ICS-02-2018-0020

Flutter. (2020a). *Flutter - Beautiful native apps in record time*. Recuperado de https://flutter.dev/

Flutter. (2020b). *Flutter - Crea hermosas aplicaciones nativas en tiempo récord*. Recuperado de https://flutter-es.io/

Gerber, M. & Von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security, 27*(5–6), 124-135, Doi: https://doi.org/10.1016/j.cose.2008.07.009

Gobierno de México. (2017). *Estrategia Nacional de Ciberseguridad*. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno del estado de Tabasco. (2012). *Reglamento de la ley registral del estado de Tabasco*. Recuperado de https://tabasco.gob.mx/leyes/descargar/1/923.pdf

Hassan, A. (2020). JAVA and DART programming languages: conceptual comparison. *Indonesian Journal of Electrical Engineering and Computer Science, 14*(2), 845-849. Doi: 10.11591/ijeecs.v17.i2.pp845-849

Instituto de Administración y Avalúos de Bienes Nacionales [INDAABIN]. (2013). *Registro Público de la Propiedad Federal*. México. Recuperado de https://www.gob.mx/indaabin/articulos/registro-publico-de-la-propiedad-federal?idiom=es

International Organization for Standardization [ISO]. (2020). *ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls*. Recuperado de https://www.iso.org/standard/54533.html

ISO27000.es. (2005). *Iso27002*. Recuperado de http://www.iso27000.es/iso27002.html

ISOTools (s.f.). *¿Cuáles son los riesgos corporativos más importantes para las organizaciones?* Recuperado de https://www.isotools.org/2019/02/04/cuales-son-los-riesgos-corporativos-mas-importantes/

Jesan, J. (2006). Information Security. *Ubiquity*, *2006*(January), 1. Doi: https://doi.org/10.1145/1119621.1117695

McKinsey & Company (s.f.). *Perspectiva de ciberseguridad en México*. Recuperado de https://consejomexicano.org/multimedia/1528987628-817.pdf

Méndez, J. (2019). Dirección General del Registro Público de la Propiedad y del Comercio. Recuperado de https://sgg.jalisco.gob.mx/acerca/areas-de-la-secretaria/direccion-Registro-Publico-Propiedad-Comercio

Mevada, M. (2019). Google Launched Flutter SDK 1.2 and Dart Programming Language 2.2. *SoluteLabs*. Recuperado de https://blog.solutelabs.com/google-launched-flutter-sdk-1-2-and-dart-programming-language-2-2-8ebab5500fb

Ministerio de Hacienda y Administraciones Públicas de España. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método (3a ed.). Recuperado de http://administracionelectronica.gob.es/

Muñoz, P., Rodríguez, E. y Domínguez, A. (2003). Metodología cuantitativa. Métodos y técnicas de evaluación de centros - Una propuesta de clasificación operativo-funcional. *Revista galego-portuguesa de psicoloxía e educación, 7*(9), 69-95. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=1032574

Olano, D. (2016). Aplicabilidad de las normas ISO 27000 en el contexto de la Internet de las Cosas (Universidad Autónoma de Madrid). Recuperado de http://academico.une.org/Documents/TFM1 27000 en internet de las cosas DOA Completo.pdf

Pacheco, L. (2018). *Políticas de seguridad de la información de aprovechamiento estudiantil en la educación general básica basado en la norma ISO 27002* (Tesis de Maestría). Universidad Espíritu Santo, Samborondón, Ecuador

PolíticoMX. (2 de marzo de 2020). Afecta a empresas hackeo a Secretaría de Economía. *Vanguardia.* Recuperado de https://vanguardia.com.mx/articulo/afecta-empresas-hackeo-secretaria-de-economia

Prieto, V., Quiñones, I., Ramírez, G., Fuentes, Z., Labrada, T., Pérez, O. y Montero, M. (2011). Impacto de las tecnologías de la información y las comunicaciones en la educación y nuevos paradigmas del enfoque educativo. *Educación Médica Superior, 25*(1), 95–102. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21412011000100009&nrm=iso

Proyectos Agiles (2020). *Qué es SCRUM*. Recuperado de https://proyectosagiles.org/

Ramos, P. (2018). *Qué es y para qué sirve SQL*. Recuperado de https://styde.net/que-es-y-para-que-sirve-sql/

Real Academia Española. (2020). Información. En *Diccionario de la lengua española* (edición de tricentenario). Recuperado de https://dle.rae.es/norma

Redacción. (24 de febrero 2020). Hackean servidores de la Secretaría de Economía. *El Financiero.* Recuperado de https://www.elfinanciero.com.mx/economia/hackean-servidores-de-la-secretaria-de-economia

Saavedra, M. y Tapia, B. (2013). El uso de las tecnologías de información y comunicación TIC en las micro, pequeñas y medianas empresas (MIPyME) industriales mexicanas. *Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento, 10*(1), 85-104. Recuperado de https://www.redalyc.org/articulo.oa?id=823/82326270007

Sánchez, A. y Montes, J. (2014). *Programación de Servicios y Procesos (GRADO SUPERIOR).* Madrid, España: RA-MA. Recuperado de https://books.google.com.mx/books?id=Uo2fDwAAQBAJ&lpg=PA98&dq=modelo%20Cliente-Servidor&pg=PA3#v=onepage&q=modelo%20Cliente-Servidor&f=false

Salamanca, O. (2016). Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software. *Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento, 13*(3), 114-130. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=5858358

Sánchez, M., Collado, S., Martín, P. y Cano, R. (2018). Apps en neurorrehabilitación. Una revisión sistemática de aplicaciones móviles. *Neurología, 33*(5), 313-326. Doi: https://doi.org/10.1016/j.nrl.2015.10.005

Secretaría de Desarrollo Agrario Territorial y Urbano [SEDATU]. (s.f.). *Modelo del Registro Público de la Propiedad. México*. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/196177/MODELOS_RPP_y_CAT.pdf

Secretaría de Finanzas. (s.f.). *Ley de Ingresos del Estado de Tabasco, para el Ejercicio Fiscal del año 2020*. Recuperado de https://congresotabasco.gob.mx/wp/wp-content/uploads/2020/01/Ley-de-Ingresos-del-Estado-del-ejercicio-fiscal-2020.pdf

Secretaría de Gobernación [SEGOB]. (2020). *Diario Oficial de la Federación*. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5587337&fecha=24/02/2020

Selvaganapathy, S., Sadasivam, G., N, H., N, R., M, D. & Karthik K. (2020). Android Malware Detection. En Kumar L., Jayashree L., Manimegalai R. (Eds). *Proceedings of International Conference on Artificial Intelligence, Smart Grid and Smart City Applications*. (pp. 781-790). Coimbatore, Tamil Nadu, India: Springer

Szczepaniuk, E., Szczepaniuk, H., Rokicki, T. & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security, 90*(), 1-9. Doi: https://doi.org/10.1016/j.cose.2019.101709

Tovar, N. y Salguero, A. (2018). *Auditoría interna a los activos físicos del área de TI en la Universidad Cooperativa de Colombia sede Ibagué, aplicando el estándar ISO/IEC 27002:2013* (Trabajo de seminario de profundización, para optar al título de Ingeniero de Sistemas). Universidad Cooperativa de Colombia, Tolima, Ibagué, Colombia.

Ureña, L. (2020, febrero 20). Intentan hackear Registro Público de la Propiedad de Aguascalientes. *Milenio*. Recuperado de https://www.milenio.com/estados/en-aguascalientes-intentan-hackear-registro-publico-de-la-propiedad

Valencia-Duque, F. y Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI - *Revista Ibérica de Sistemas y Tecnologías de Información*, (22), 73–88. Doi: http://dx.doi.org/10.17013/risti.22.73–88

Vega, A. (2020). Método basado en la programación por capas para generar código automático desde el diagrama de clases. *Revista Peruana De computación Y Sistemas*, 2(2), 25–42. https://doi.org/10.15381/rpcs.v2i2.17015

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P. and Moscoso-Zea, O. (2018). *Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry*. Presentada en 2018 International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador.

Vicente, E., Mateos, A. & Jiménez-Martín, A. (2014). Risk analysis in information systems: A fuzzification of the MAGERIT methodology. *Knowledge-Based Systems, 66*(2014), 1-12. Doi: http://dx.doi.org/10.1016/j.knosys.2014.02.018

Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica, 24*(50), 127-155. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Willis Towers Watson. (2018). *Riesgo Cibernético*. Recuperado de https://www.willistowerswatson.com/-/media/WTW/Insights/2018/12/riesgo-cibernetico-2018-wtw.pdf

Zacarias, N. (2019). *Estudio sobre la seguridad de la información con un enfoque en la norma ISO/IEC 27002:2013, caso: Coordinación de Desarrollo y Soporte de Sistemas de la Dirección de Tecnologías de Información e Innovación de la UJAT* (Tesis de Maestría). Universidad Juárez Autónoma de Tabasco, Cunduacán, Tabasco, México.

Glosario

I

IEC: International Electrotechnical Commission

ISO: Internacional Organization for Standardization

M

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

R

RPPyC: Registro Público de la Propiedad y del Comercio

S

SEDATU: Secretaría de Desarrollo Agrario Territorial y Urbano

SEGOB: Secretaría de Gobernación

SGSI: Sistema de Gestión de Seguridad de la Información

T

TIC: Tecnologías de la Información y las Comunicación

A N E X O S

Anexo A. Licencia de uso de Flutter

Anexo B. Licencia de uso de Dart

[1] http://creativecommons.org/licenses/by/4.0/

Anexo C. Licencia de uso de Android Studio

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of

this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and
You must cause any modified files to carry prominent notices stating that You changed the files; and
You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.
5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the

appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

A P É N D I C E S

Apéndice A. Resultados de la evaluación

Tabla 28
Resultados de la evaluación de la norma

Id	Dominio	Objetivos	Control	Nivel	Resultado	Promedio
5	Políticas de seguridad de la información	Dirección de gestión para la seguridad de la información	Políticas para la seguridad de la información	0	0	0
			Revisión de las políticas para seguridad de la información	0		
8	Gestión de activos	Responsabilidad por los activos	Inventario de activos	40	30	16.66666667
			Propiedad de los activos	40		
			Uso aceptable de los activos	20		
			Devolución de activos	20		
		Clasificación de la información	Clasificación de la información	0	6.666666667	
			Etiquetado de la información	0		
			Manejo de activos	20		
		Manipulación de media	Gestión de medios removibles	20	13.33333333	
			Eliminación de los medios	20		
			Transferencia de medios físicos	0		
9	Control de acceso	Requisitos de negocio para el control de acceso	Política de control de acceso	40	40	24
			Política sobre el uso de los servicios de red	40		
		Gestión de acceso de usuarios	Registro y cancelación del registro de usuarios	20	20	

			Suministro de acceso de usuarios	40		
			Gestión de derechos de acceso privilegiado	40		
			Gestión de información de autenticación secreta de usuarios	0		
			Revisión de los derechos de acceso de usuarios	0		
			Retiro o ajuste de los derechos de acceso	20		
		Responsabilidades de los usuarios	Uso de la información de autenticación secreta	20	20	
		Control de acceso a sistemas y aplicaciones	Restricción de acceso Información	40	16	
			Procedimiento de ingreso seguro	0		
			Sistema de gestión de contraseñas	0		
			Uso de programas utilitarios privilegiados	0		
			Control de acceso a códigos fuente de programas	40		
11	Seguridad física y del entorno	Áreas seguras	Perímetro de seguridad física	20	10	19.444444 44
			Controles físicos de entrada	0		
			Seguridad de oficinas, recintos e instalaciones	0		
			Protección contra amenazas externas y ambientales	40		
			Trabajo en Áreas seguras	0		
			Áreas de carga y descarga	0		

		Equipos	Ubicación y protección de los equipos	40	28.88888889
			Servicios de suministro	40	
			Seguridad del cableado	40	
			Mantenimiento de equipos	40	
			Retirada de activos	40	
			Seguridad de equipos y activos fuera de las instalaciones	20	
			Eliminación segura o reutilización de equipos	20	
			Equipos de usuario desatendidos	20	
			Política de escritorio limpio y pantalla limpia	0	
12	Seguridad de las operaciones	Procedimientos operacionales y responsabilidades	Procedimientos operacionales documentados	20	5	10.71428571
			Gestión de cambios	0	
			Gestión de capacidad	0	
			Separación de los ambientes de desarrollo, pruebas y operación	0	
		Protección contra códigos maliciosos	Controles contra códigos maliciosos	20	20	
		Copias de respaldo	Respaldo de información	40	40	
		Registro y monitorización	Registro de eventos	0	10	
			Protección de la información de registro	40		
			Registros del administrador y del operador	0		

			Sincronización de relojes	0		
		Control de software operacional	Instalación de software en sistemas operativos	0	0	
		Gestión de la vulnerabilidad tÃ©cnica	Gestión de las vulnerabilidades tecnicas	0	0	
			Restricciones sobre la instalación de software	0		
		Consideraciones sobre auditorias de sistemas de información	Información controles de auditoría de sistemas	0	0	
13	Seguridad de las comunicaciones	Gestión de seguridad de las redes	Controles de redes	40	26.66666667	13.33333333
			Seguridad de los servicios de red	40		
			Separación en las redes	0		
		Transferencia de información	Políticas y procedimientos de transferencia de información	0	0	
			Acuerdos sobre transferencia de información	0		
			Mensajería electrónica	0		
			Acuerdos de confidencialidad o de no divulgación	0		
16	Gestión de incidentes de seguridad de la información	Gestión de incidentes y mejoras de seguridad de la información	Responsabilidad y procedimientos	20	20	20
			Reporte de eventos de seguridad de la información	20		

			Reporte de debilidades de seguridad de la información	20		
			Evaluación de eventos de seguridad de la información y decisiones sobre ellos	0		
			Respuesta a incidentes de seguridad de la información	20		
			Aprendizaje obtenido de los incidentes de seguridad de la información	40		
			Recolección de evidencia	20		
17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Continuidad de seguridad de la información	Planificación de la continuidad de la seguridad de la información	0	0	20
			Implementación de la continuidad de la seguridad de la información	0		
			Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0		
		Redundancias	Disponibilidad de instalaciones de procesamiento de información	40	40	

Nota: Elaboración propia.